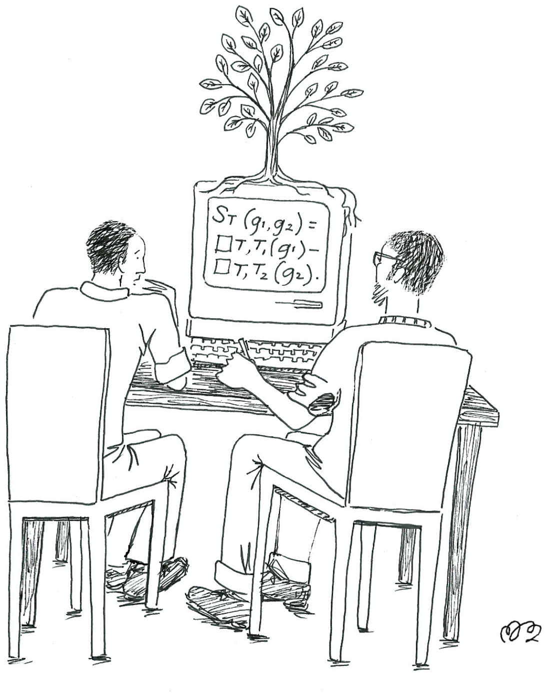
> Murray Bremner and Vladimir Dotsenko, Algebraic Operads: An Algorithmic Companion, research monograph, 2015, xvii+365 pp.


$S_T(g_1,g_2) =$
$\square_{T,T_1}(g_1) -$
$\square_{T,T_2}(g_2).$

Murray Bremner and Vladimir Dotsenko

Algebraic Operads: An Algorithmic Companion version 0.999

Now that we have learned to be abstract we can afford again to be concrete.

Gian-Carlo Rota

Owl explained about the Necessary Dorsal Muscles. He had explained this to Pooh and Christopher Robin once before and had been waiting for a chance to do it again, because it is a thing you can easily explain twice before anybody knows what you are talking about.

Alan Alexander Milne

Contents

Preface

This book is intended as an introduction to concrete methods for working with associative structures of all sorts, most notably commutative associative algebras, noncommutative associative algebras, and operads. The first two are very well known; the third is an algebraic device that captures properties exhibited by substitutions of operations with several arguments into one another (and of course these compositions of operations are associative). In each of these cases, an object is often presented by generators and relations: commutative associative algebras are quotients of algebras of commutative polynomials, noncommutative associative algebras are quotients of tensor algebras, where elements are linear combinations of noncommutative monomials, or words, and operads are quotients of free operads, where elements are combinations of monomials shaped in the form of a tree.

Both testing hypotheses and proving theorems about polynomial expressions of all those types often involves highly complex symbolic computations which can never be completed in a reasonable time unless one approaches them in an extremely structured way. The least one can do to that end is to come up with a reasonable way to represent elements of the given quotient algebra, that is to determine unique "normal forms" of such elements. A general strategy for accomplishing that comes from a very powerful theoretical result known as the diamond lemma of Newman [204]. Our goal in this book is to present the solution to the problem of determining normal forms in a way that all the individual building blocks of that solution are clearly identified; this makes desired generalizations of the theory straightforward. We give complete proofs of key facts, many detailed examples, a large array of exercises, mostly coming from actual research questions, and references to further reading.

This book is a result of a collaboration of two people coming from two very different backgrounds. The first author did his graduate studies in Lie theory, and then developed a focus on computational methods for the study of nonassociative structures, using methods involving linear algebra over large integer matrices and the representation theory of the symmetric group. He strongly prefers to explain even the most abstract concepts in the most concrete and algorithmic way, which, he believes, is the main way to truly understand them. The second author encountered during his formative years many instances where a high level of abstraction with minimum examples was a commonplace and learned to find that style enjoyable and stimulating, so he generally prefers to use computational methods mainly at the stage of forming conjectures and making educated guesses, and then replace them by abstract reasoning at all other stages whenever possible. Together, the authors represent a team which is not afraid of either a computational challenge or abstract reasoning; this combination is often useful when attacking a research problem. Merging these approaches resulted in this book, which aims to demonstrate both the theoretical value of the subject and the power of actual computations involved. Whether the authors have succeeded at it is for the reader to decide.

Both authors have an extensive experience of teaching courses and doing research on topics that are related, both directly and indirectly, to normal forms, diamond lemmas, and their applications. The first author has taught graduate courses in quantum groups, Lie algebras, computer algebra, and lattice basis reduction, and a short course on algorithms for free associative algebras. At present he is especially interested in applications of CoCoA (computational commutative algebra) to the classification of operads. The second author has taught courses on Gröbner bases on various occasions in all possible flavors: an undergraduate course, a masters course, and mini-courses at research schools. He has been working on various questions of operads theory for several years. The authors' combined experience provided them with an insight into how to convey the topics presented in the book in a way that would be useful to researchers in both nonassociative algebra and the operad theory; to those who prefer a theoretical approach, and to those whose main interest is computation.

While writing this book, we had three particular books in mind as our inspiration. The first book is the monograph *Ideals, Varieties and Algorithms* by Cox, Little, and O'Shea [64], which convinced us that a large and very complex subject could be made basically comprehensible at the undergraduate level with enough focus on letting the readers "get their hands dirty" applying general methods to particular examples. The second one is the survey *Combinatorial and Asymptotic Methods in Algebra* by Victor Ufnarovski [252], a book that fundamentally shaped our view of the subject. The last inspiration was the extraordinary monograph *Algebraic Operads* by Jean-Louis Loday and Bruno Vallette [180], which became the standard and encyclopedic treatment of the topic from the moment it appeared. It is fairly accurate to say that the aim of this book is to create an accessible companion book to [180] which would, in the spirit of [64], contain enough hands-on methods for working with specific operads: making experiments, formulating conjectures, and, hopefully, proving theorems, as well as, in the spirit of [252], include enough interesting examples to stimulate the reader toward those experiments, conjectures, and theorems.

The first author would like to thank first and foremost his wonderful parents, who instilled in him from an early age a love for knowledge and a capacity for hard work. Although they have both passed away, they remain a great inspiration. A number of primary and high school teachers let him proceed at his own pace and thus permitted him to develop his own taste in mathematics at a very early age. His most important mentor as an undergraduate and beyond was Robert V. Moody, co-discoverer of Kac–Moody algebras and co-winner of the Wigner Medal. The further contributions of his teachers and supervisors in graduate school, and his early career mentors, have also been of inestimable value. He has also been very fortunate to have had very talented graduate students and postdoctoral fellows: Jiaxiong Hu, Stavros Stavrou, Hader Elgendy, Marina Tvalavadze, Juana Sánchez Ortega, and Sara Madariaga.

The second author wishes to thank first and foremost his mother, who has always encouraged him to be curious about anything and everything, and to not give up no matter what. He also is eternally grateful to his teachers from his undergraduate years in Moscow: Boris Feigin and Michael Finkelberg, who first introduced him to the captivating world of homotopical algebra and Koszul duality, and Natalia Iyudu, Victor N. Latyshev, and Dmitri Piontkovski, who taught him about the power of the diamond lemma and Gröbner bases. During early stages of his development as an independent researcher he also benefited a lot from the mentorship of Jean-Louis Loday whose untimely death in 2012 marked the end of an era in operad theory. He also learned important things related to the topics of this book from his collaborators James Griffin, Eric Hoffbeck, Anton Khoroshkin, and Bruno Vallette. Finally, he would like to thank Ewan Dalby and Joshua Tobin who wrote their B. Sc. theses under his supervision on subjects related to the topic of this book and ended up teaching him something new about the subject, and Stephen Lavelle who read some parts of the final draft of the book and made a few very valuable comments.

Both authors thank the staff at CRC Press for their assistance: Robert Ross, Kathryn Everett, Olivia Anderson, and Shashi Kumar.

The epigraph by Gian-Carlo Rota is from his dialogue with David Sharp entitled “Mathematics, Philosophy, and Artificial Intelligence”, published in *Los Alamos Science*, spring/summer 1985, pages 92–104. The epigraph by Alan Alexander Milne is from “The House at Pooh Corner”, first published by Methuen & Co. Ltd. (London) in 1928.

The artwork on the front cover of the book is original work of Matilda Moreton (`http://www.matildamoreton.com`).

No doubt there remain some errors in the book, either typographical or otherwise, for which the authors accept full responsibility. The authors would be very happy to receive comments, suggestions, and corrections from readers, by email at the addresses below.

Murray R. Bremner (`bremner@math.usask.ca`)
Vladimir Dotsenko (`vdots@maths.tcd.ie`)

Authors

Murray R. Bremner is a professor at the University of Saskatchewan in Canada. He attended that university as an undergraduate, and received an M. Comp. Sc. degree at Concordia University in Montréal under the supervision of John McKay in 1984. His thesis work resulted in the book by Bremner, Moody, and Patera entitled *Tables of Dominant Weight Multiplicities for Representations of Simple Lie Algebras*, published by Marcel Dekker in 1985. He obtained a doctorate in mathematics at Yale University in 1989, under the supervision of George Seligman, with a thesis entitled *On Tensor Products of Modules over the Virasoro Algebra.* Prior to returning to Saskatchewan, he held shorter positions at MSRI in Berkeley and at the University of Toronto. He authored the book *Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications*, published by CRC Press in 2012, and is a co-translator with M. V. Kotchetov of *Selected Works of A. I. Shirshov in English Translation*, published by Birkhäuser in 2009. His primary research interests are algebraic operads, nonassociative algebra, representation theory, and computer algebra.

Vladimir Dotsenko is an assistant professor in pure mathematics at Trinity College Dublin. He studied at the Mathematical High School 57 in Moscow, Independent University of Moscow, and Moscow State University, where he worked under the supervision of Boris Feigin and Mikhail Zaicev (M. Sc. thesis *Catalan Numbers and Vertex Operators*, 2003, Ph. D. thesis *Analogues of Orlik–Solomon Algebras and Related Operads*, 2007). He also held shorter positions at Dublin Institute for Advanced Studies and the University of Luxembourg. His collaboration with Murray started in February 2013 in CIMAT (Guanajuato, Mexico), where they both lectured in the research school "Associative and Nonassociative Algebras and Dialgebras: Theory and Algorithms". His primary research interests are algebraic operads, homotopical algebra, combinatorics, and representation theory.

Introduction

Normal forms: a historical overview

One of the most common things to do in mathematics is solving equations. Since the introduction of the coordinate method for geometric problems by Descartes, everyone knows that combining algebra and geometry leads to mutual benefits: geometric problems may be approached in a uniform way through solving algebraic equations, and algebraic equations may become easier to deal with if one tries to think in terms of geometric properties of solutions to those equations. On the other hand, in the 20th century it became common to view geometric objects via algebras of functions on those objects. Once this viewpoint is taken, it becomes absolutely crucial to be able to work with algebras in an effective way. That does not necessarily have to mean using computer algebra systems; a computation using pen and paper, or blackboard and chalk, also needs to represent elements of algebras in a concrete way in order to write them down, decide whether two elements are equal to each other, etc. This naturally leads to hunting for "normal forms", some canonical ways to represent elements. In this book, we mainly use that philosophy to study algebraic objects that are somewhat more abstract than polynomial equations that Descartes would have used: noncommutative algebras, twisted associative algebras, and operads.

Since determining normal forms within some algebraic structure is such a natural question to consider, one cannot really make decisive conclusions on priority. Many mathematicians for over a century considered eliminating leading terms of the ideal generated by given polynomials as a way to determine normal forms, and most of them remained blissfully unaware of each other's work until much later. For that reason, it is mere curiosity that made us conduct our own little historical investigation and mention some of these mathematicians here; we are not implying any completeness of our brief survey. (We also refer the reader to the surveys in [34, 36, 46, 85] which highlight a range of different historical aspects.)

Commutative Gröbner bases

The term “Gröbner bases” was coined by Buchberger [48, 49], whose supervisor Gröbner posed to him in 1964 a question of finding a basis in the quotient of the polynomial algebra by an ideal. At that stage, Gröbner himself had been making computations for particular cases of this problem for many years, since at least 1939 [123], his inspiration coming from the 1927 paper by Macaulay [181]. However, similar ideas for determining normal forms can be traced back to a 1900 paper by Gordan [116]. It is also worth mentioning papers by Gjunter from the 1910s [107, 108] published in *Proceedings of the Institute of Railway Engineers*, which for that reason had remained unnoticed for a long time until they were accidentally discovered in the list of references of [109], see [216, 217]. For power series rings, these ideas are prominent in works of Hironaka [134] and Grauert [120]. It is true, however, that only Buchberger’s approach made the algorithmic side of the story receive due attention.

Noncommutative Gröbner bases

At the same time, more general term rewriting aiming to compute normal forms has been of interest to mathematicians for many decades as well. The earliest general result that certainly belongs to the core of this research area is a result of Newman [204] that he used to prove the Church–Rosser theorem [59]; this result is conventionally known as the diamond lemma. Similar ideas emerged in other research areas of mathematics and theoretical computer science, for instance in the works of Evans [91], Prawitz [209], and Robinson [220]; this culminated in the Knuth–Bendix completion procedure [150]. In the early 1960s, a version of the diamond lemma for Lie algebras was proved by Shirshov [232] (see also [233]), who used the term “composition”; independently, Cohn emphasized the importance of the diamond lemma for studying normal forms in algebras in his famous book [63, Th. III.9.3]. A version of Shirshov’s Composition lemma for associative algebras was proved by Bokut’ [24], while the diamond lemma of Newman (and, importantly, Cohn’s view of it) inspired the diamond lemma in the paper of Bergman [21]. It is also worth mentioning the work of Priddy [210] who used normal forms in the noncommutative case for some striking homological applications a few years before [21, 24]; in the language that did not exist when Priddy published his result, he in particular proved that an associative algebra with a quadratic Gröbner basis is Koszul. Nowadays, noncommutative Gröbner bases are frequently used by mathematicians doing research in many different areas of algebra.

Operads, their normal forms, and Gröbner bases

Operads give a language to discuss algebraic properties of operations with several arguments. They were originally invented for purposes of topology, and remained a relatively isolated area of algebraic topology until the period of “renaissance of operads” (in the words of Jean-Louis Loday [174]) in the 1990s, marked by a wide range of influential works in algebraic geometry and mathematical physics demonstrating the relevance of operad theory for those subjects [101, 102, 105, 154, 155, 156, 157, 158]. Since then, as more and more research in operad theory was done, many ingenious methods tailored specifically for dealing with individual operads emerged, but only few general approaches have been made available. On the algebraic side, many researchers studied operads under the name varieties of algebras, using the language of identities and T-ideals going back to Specht [240]; we refer the reader to recent monographs [103, 143] and references therein for some insight into the very impressive results obtained using that language. For about a decade, the only monograph in operad theory systematically reflecting the development of that theory since the renaissance period has been [187], however, many aspects of the theory have been clarified and extended during that decade, and at this stage, we believe, the state-of-art exposition of the theory of algebraic operads is given in [180]. As it is apparent from the title of our book, one of the aims of our work is to augment the book [180], making some aspects of the operad theory more concrete and amenable to experiments.

Elements of operads are conventionally represented by linear combinations of trees, “tree polynomials”. In the past decade, a few papers discussing tree polynomials appeared [80, 99, 212]; however, these papers deal with Gröbner bases in nonassociative algebras, not allowing any kind of substitutions of operations, and as such remain infinitely far from operadic applications. Until 2007, the only paper that briefly discussed normal forms in operads was [127]; that paper highlights some similarities and differences between operads and associative algebras, but does not go as far as to develop a functioning theory of normal forms. In 2007, the situation changed dramatically when Hoffbeck released a preprint [135] proving an operadic version of Priddy’s theorem mentioned above. He introduced a monomial basis of the free operad, and a partial ordering of that basis which was enough to prove what instantly became the most general criterion in operadic Koszul duality. Once the second author of this book saw the paper [135], he recalled the Gröbner basis reformulation of Priddy’s theorem, and became convinced that there must be a theory of Gröbner bases for operads of which Hoffbeck’s criterion is a shadow. After some preliminary work, he teamed up with his former classmate Khoroshkin, which resulted in releasing on the Christmas eve of 2008 the preprint [74] introducing the notion of a shuffle operad and using that notion to establish a theory of Gröbner bases for operads and prove the corresponding diamond lemma. (To be historically fair, partitional composition [94, 141] of combinatorial species admits an analogue for “ordered species” [20, Sec. 5.1], and it is merely coincidental that no one previously considered the corresponding monoids, which effectively are shuffle operads.) Later, methods of [74] were used in [78] to work with algebras over arbitrary nonsymmetric operads. Generalizations of these methods to algebraic structures where monomials are graphs that possibly have loops and are possibly disconnected, e.g., properads, PROPs, wheeled operads, etc., are still unknown, and it is not quite clear if it is at all possible to extend Gröbner-flavored methods to those structures.

Outline of the book

This book, roughly speaking, consists of two parts. In the first part, we explain the general theory of Gröbner bases for operads, building it from scratch in several accessible steps, from noncommutative associative algebras to nonsymmetric operads to twisted associative algebras to general algebraic operads. We believe that it is generally sensible from the pedagogical point of view to highlight the core factors that make these theories work, and illustrate those individual factors on examples that are much simpler than the simplest examples for the most general version of the theory; a similar strategy is used in [180]. Quite fortunately for the reader, in the case of operadic Gröbner bases it is entirely possible: for each particular aspect of the theory, there is a way to illustrate that very aspect without diving at the deep end straight away. In particular, the way to deal with symmetries of operations that is crucial for the operad theory is first illustrated on the example of twisted associative algebras; those algebras have become more prominent recently, following recent breakthroughs in representation stability [161, 225, 223, 224]. In the second part, we show how more familiar Gröbner bases for commutative algebras can be utilized for classification of operads. For that, we focus on the two simplest instances going beyond classification questions where no theory is required. All the way through, we discuss a wide range of examples and connections to various topics in algebra; some of those examples may be the terminal stop for a fraction of the readers who are mainly interested in noncommutative associative algebras, or combinatorics of patterns in permutations and trees, or computations in nonsymmetric operads. Because of this, we felt inclined to include a detailed outline of the book, hoping that it would help the reader who is interested in particular aspects of the topic with choosing chapters to focus on, and to allow ourselves to be occasionally repetitive, both highlighting similarities between different theories and helping the readers who are only interested in certain aspects of the book to localize their reading.

In Chapter 1, we use examples of linear reductions in subspaces of vector spaces and long division for polynomials in one variable to give some important intuition for normal forms. This chapter is used in most of the subsequent chapters, and we strongly recommend to the reader to browse through it, since it in particular fixes some terminology used throughout the book.

In Chapter 2, we develop the theory of normal forms and Gröbner bases for noncommutative associative algebras, and discuss its various applications. This chapter may be viewed as an elaborate version of some of the sections of [252], told from the perspective that is easily generalizable to the setup of algebraic operads later on. We want to emphasize that the theory for noncommutative associative algebras bears many important similarities with the more general theory for operads, while the possibly most famous instance of a theory of Gröbner bases, that for commutative associative algebras, has many features which are "too good to be true" in the general case. For that reason, we do not discuss commutative Gröbner bases in the beginning, hoping to avoid developing unnecessary false intuition.

In Chapter 3, we discuss normal forms and Gröbner bases for nonsymmetric operads. In many ways, this is the next logical step in generalizing the theory: technical issues arising from extra symmetries do not arise yet, while the combinatorics of monomials changes (words are replaced by trees). We use a definition of trees which we have not encountered in the literature in that exact form; we believe that this definition is quite useful in the operadic context, and that using it in the setup of nonsymmetric operads is optimal for the reader to get used to it. We also explain how the theory developed in this chapter leads to normal forms in algebras over nonsymmetric operads; this was first established in the paper [78] focusing on higher Koszul duality for associative algebras, and for that reason may have remained partly unnoticed.

In Chapter 4, we explain how the theory must be adapted to deal with twisted associative algebras, that is graded algebras whose components are equipped with symmetric group actions, and whose product is reasonably equivariant with respect to those actions. This is the most elementary instance where the idea of applying the forgetful functor between two monoidal categories proves to be very useful. We define a "less symmetric" notion of a shuffle algebra, explain how to develop a theory of Gröbner bases for shuffle algebras, and how to associate to a twisted associative algebra $\mathcal{A}$ a shuffle algebra $\mathcal{A}^f$ which encodes basis elements of $\mathcal{A}$ in a faithful way but is much easier to study. This chapter would be of particular interest to readers interested in applications of Gröbner methods in combinatorics and representation theory.

In Chapter 5, we consolidate the methods of previous chapters to work with algebraic operads in full generality. We explain how to adapt combinatorics of trees to encode operations with symmetries, define a "less symmetric" notion of a shuffle operad, develop a theory of Gröbner bases and normal forms for shuffle operads, and associate to an algebraic operad $\mathcal{O}$ a shuffle operad $\mathcal{O}^f$ which encodes basis elements of $\mathcal{O}$ in a faithful way but is much easier to study. This chapter would be of particular interest to readers who need hands-on methods to work with symmetric operads, and is, in some sense, the main focus of this book.

In Chapter 6, we explain how various aspects of the theory must be adapted for the purposes of homological algebra, incorporating the "Koszul sign rule" in all computations, and illustrate applications of Gröbner bases in a wide range of applications. This chapter would be especially useful to those who would like to use operadic Gröbner bases for homotopical algebra, in particular for the Koszul duality theory.

In Chapter 7, we recall some necessary background on Gröbner bases for commutative algebras, which is then applied to the study of operads in the last two chapters of the book. Since this theory has already been explained extremely well from different points of view in many different textbooks, we focus on presenting the results that we need, and on some results that are usually not covered at length in the standard presentations. In particular, we include a proof of Robbiano's classification theorem on monomial orders, and a historical survey of results on the complexity of computing Gröbner bases (which to the surprise of many turned out to be EXPSPACE-complete). We also include (in Appendix A) detailed `Maple` code for implementing Buchberger's algorithm, which is built from the ground up, in the sense that it does not rely on any of the standard `Maple` commands from the `Groebner` package.

Chapter 8 discusses an important topic related to commutative Gröbner bases which hides in the background in many applications but is not often brought into the foreground: we mean using Gröbner basis to study linear algebra over matrices whose entries belong to polynomial rings. As soon as the number of variables becomes greater than one, the coefficient ring is no longer a PID and this introduces a number of difficulties that can be used to motivate many of the theoretical and computational developments in commutative algebra in the last 100 years.

Chapters 9 and 10 apply the results of the previous two chapters in an initial attempt to classify nonsymmetric operads in two cases: one binary operation satisfying cubic relations, and one ternary operation satisfying quadratic relations. The basic idea here is to consider parameterized families of operads defined by relations of a given arity, and then construct the consequences of these relations in the next arity. The coefficients of the consequences are polynomials in the original parameters, and this allows us to combine computational commutative algebra with Gröbner bases for nonsymmetric operads to obtain information about the original families of operads. Thus, this chapter blends several different methods discussed in this book for the purposes of operad theory. An example of a similar blend applied to a problem involving symmetric operads is our recent preprint [42].

Terminological and notational remarks

Our decision on terminology is a result of some tough choices. It is quite common nowadays to refer to machinery that provides normal forms in quotient algebras (for some algebraic structures, often nonassociative), as "Gröbner–Shirshov bases", and refer to the key result that makes those methods constructive as the "Composition–Diamond lemma". After a careful deliberation, we chose to use the terms "Gröbner bases" and "diamond lemma" throughout this book. This, of course, should not by any means suggest that Shirshov's influence on the subject area should be neglected. (In recent years, exploring applicability of Shirshov's ideas to various nonassociative structures led to interesting discoveries in an impressive range of cases; see, e.g., a very incomplete list [23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 56] and references therein.) In our humble opinion, the remarkable ideas of [232] are particularly notable because their generality allows one to adapt them to nonassociative structures; moreover, it appears that these ideas were coined specifically for the purpose of advancing research of nonassociative algebras, while our exposition can only accomplish the level of uniformity that we aim for by considering normal forms for monoids in various monoidal categories. Besides our genuine belief that using the words "diamond lemma" is a good way to emphasize the pioneering work of Newman, our preference is prompted by the fact that the word "composition" in the context of monoids is unnecessarily ambiguous, since it is used to refer to product is many natural examples of monoids, including operads.

Finally, let us mention one rather unconventional notational decision. In the last few chapters of the book we occasionally had to display large sparse matrices, and using the standard symbol 0 for zero often makes it difficult to recognize the pattern of the nonzero entries. In these cases we found it convenient to follow the eastern Arabic custom of writing dot instead of zero (that is, $\cdot$ instead of 0); we hope that a little experience will lead the reader to appreciate the advantage of this convention.

Computer algebra systems

Over the years, commutative Gröbner bases have been implemented in many different computer algebra systems, and it is hardly possible to give a comprehensive survey of those within a short paragraph, so we just mention some examples that we find interesting. Notable instances of free software that can handle commutative Gröbner bases are Axiom (`http://www.axiom-developer.org`), CoCoA (`http://cocoa.dima.unige.it`), Macaulay (`http://www.math.uiuc.edu/Macaulay2`), and Singular (`http://www.singular.uni-kl.de`). Needless to say, most respectable proprietary software systems, e.g., Maple, Mathematica, and Magma, have implementations of commutative Gröbner bases inside them; those implementations are used to solve systems of polynomial equations and as such are used by scientists around the world in a most extensive way. Our particular choice of Maple for commutative Gröbner basis computations is a historical accident based on the fact that one of the authors is Canadian.

The most powerful free computer algebra software for computing noncommutative Gröbner bases that we are aware of is bergman (http://servus.math.su.se/bergman/). Many proprietary software systems also have some packages for computing noncommutative Gröbner bases. Notably, the experience of the second author suggests that the web interface http://magma.maths.usyd.edu.au/calc/ for Magma which permits one (for free) to perform calculations that do not require more than two minutes, turned out to be more efficient than any other system, free or proprietary.

The Haskell package for computing operadic Gröbner bases created by M. Vejdemo Johansson [67, 68], who was mentored by the second author, is particularly notable as a proof of concept: there was no focus on optimization, and most Gröbner bases which that package can compute, the second author can compute by hand in a comparable time. Currently, a new package for computing operadic Gröbner bases, also written in Haskell, is being finished by W. Heijltjes, also under the mentorship of the second author; once finished, this package will be made available on the second author's webpage http://www.maths.tcd.ie/~vdots.

Chapter 1

Normal Forms for Vectors and Univariate Polynomials

In this chapter, we recall two very classical approaches to normal forms in quotients, one relying on the celebrated Gaussian elimination method for solving systems of linear equations, and the other based on the Euclidean algorithm for computing the greatest common divisor of univariate polynomials. We present them in a way that emphasizes some general ideas we are going to use extensively in the rest of the book, and lay out some terminology and notation which is used in many subsequent chapters. For both key results on normal forms that we present in this chapter, we give two proofs, a theoretical one which proves existence of something without a specific computational recipe, and a constructive one which gives an algorithm one can use to achieve the goal. Throughout the book, we aim to keep a certain balance between the two approaches: theoretical applications are always our goal, but actual computations sometimes end up being the key to them, and as such cannot be dismissed. Knowing that something exists is always useful, but knowing how to construct it may be even more useful.

1.1 Standard forms

In order to work with any kind of monomials and polynomials in practice, some sort of convention on standard forms is needed: we regard polynomials as vectors in a vector space that has a basis of monomials, and strictly speaking we can only write down those vectors when some order of basis monomials is imposed. Let us recall some basic terminology related to orders of sets.

1.1.1 Orders of sets

Definition 1.1.1.1 (Order on a set)**.** A (*partial*) *order* on a set M is a binary relation $\Xi \subset M \times M$ which is:

- *irreflexive*: $(m, m) \notin \Xi$ for all $m \in M$;
- *asymmetric*: for any $m_1, m_2 \in M$, if $(m_1, m_2) \in \Xi$ then $(m_2, m_1) \notin \Xi$;

- *transitive*: for any $m_1, m_2, m_3 \in M$, if $(m_1, m_2) \in \Xi$ and $(m_2, m_3) \in \Xi$, then $(m_1, m_3) \in \Xi$.

Instead of writing $(m_1, m_2) \in \Xi$, we shall write $m_1 \prec_\Xi m_2$, or even $m_1 \prec m_2$, if Ξ is clear from the context. We shall also write $m_1 \succ m_2$ iff $m_2 \prec m_1$. We shall describe the relation $m_1 \prec m_2$ by saying that m_1 is *less than* m_2 or *precedes* m_2, and that m_2 is *greater than* m_1 or *succeeds* m_1.

Definition 1.1.1.2 (Total order)**.** An order Ξ is said to be a *total order* if for all $m_1 \neq m_2 \in M$, we have either $m_1 \prec_\Xi m_2$ or $m_1 \succ_\Xi m_2$.

The most important type of total orders which we shall use throughout the book is given by well-orders.

Definition 1.1.1.3 (Well-order)**.** A total order on a set M is said to be a *well-order*, or a *Noetherian order*, or a *well-founded order*, if each (nonempty) subset S of M has a (unique) minimal element with respect to that order.

1.1.2 Monomials and polynomials

In the following chapters, we shall be working with various kinds of algebras, operads, etc. In the first place, each such object is a vector space with a basis of monomials, or sequence of vector spaces with distinguished bases. We now fix some general terminology for monomials and polynomials of any sort which we shall be using throughout the book.

Unless otherwise specified, $\mathbb{F}$ denotes an arbitrary field. Vector spaces we work with are usually finite-dimensional or at least are direct sums of finite-dimensional components, although the well-order assumption for the basis removes the need for finite-dimensionality for theoretical results we establish. (Of course, in the case of infinite-dimensional spaces, it is not realistic to talk about the algorithmic side.)

Definition 1.1.2.1 (Terminology for monomials and polynomials)**.** Suppose that V is a vector space over $\mathbb{F}$ with a well-ordered basis $\{e_i\}_{i\in\mathsf{I}}$.

While we do not assume V to possess any specific algebraic structure, in practice we shall be only dealing with the cases where some algebraic structure is present, and for that reason we introduce the following terminology:

- each basis element $e_i \in V$ is called a *monomial*, and each vector $v \in V$ is called a *polynomial*;
- for each polynomial
$$f = \sum_{i\in\mathsf{I}} c_i e_i \in V,$$
we call the set $\{e_i \colon c_i \neq 0\}$ the *support* of the polynomial f, and denote it by $\mathrm{supp}(f)$;

- for each nonzero polynomial f,
  - we call the maximal element of $\operatorname{supp}(f)$ the *leading monomial* of f, and denote it by $\textsc{lm}(f)$,
  - we call the coefficient of $\textsc{lm}(f)$ in f the *leading coefficient* of f, and denote it by $\textsc{lc}(f)$,
  - we call the corresponding term $\textsc{lc}(f)\,\textsc{lm}(f)$ of f the *leading term* of f, and denote it by $\textsc{lt}(f)$;
- we call a polynomial $f \in V$ with $\textsc{lc}(f) = 1$ *monic*.

Using the notion of the leading monomial and the leading coefficient, we can normalize polynomials that we encounter in computations.

Definition 1.1.2.2 (Standard form)**.** The *standard form* of a nonzero polynomial $f \in V$ consists of f divided by $\textsc{lc}(f)$ with the monomials in decreasing order.

1.2 Normal forms

1.2.1 Normal forms of vectors

One of our main goals throughout this book is to develop (at least somewhat) constructive methods to work with the quotients of various types of free algebras modulo their ideals. That goal will be achieved in several steps. What we will discuss now is a first step toward that goal; it approaches this problem within just basic linear algebra. For that, we shall mimic the row reduction operations, not utilizing any algebra structure.

Definition 1.2.1.1 (Space of leading terms)**.** Let S be a subset of V. We shall consider the vector space

$$\textsc{lt}(S) := \operatorname{span}(\textsc{lm}(f) \colon f \neq 0 \in S),$$

which we call the *space of leading terms of S*.

Note that the elements of $\textsc{lt}(S)$ are all possible linear combinations of leading terms, and not just leading terms alone.

We introduce the notion of linearly reduced elements and self-reduced sets, which are abstract counterparts of row canonical forms (reduced row echelon forms) of matrices.

Definition 1.2.1.2 (Linearly reduced elements)**.** Let S be a subset of V. A monomial e_i is said to be *linearly reduced with respect to* S if $e_i \notin \textsc{lm}(S)$; in other words, if e_i is not a leading monomial of an element of S. More generally, an element $f \in V$ is said to be *linearly reduced with respect to* S, if its support consists of basis monomials that are linearly reduced with respect to S.

A subset $S \subset V$ is said to be *linearly self-reduced* if each element $s \in S$ is monic and linearly reduced with respect to $S \setminus \{s\}$.

Lemma 1.2.1.3. *Let S be a subspace of V. Cosets of the monomials that are linearly reduced with respect to S form a basis of the quotient V/S.*

Proof. Let us first prove the spanning property. For that, it is enough to show that the coset $f + S$ of every element $f \in V$ contains an element that is linearly reduced with respect to S. Assume that is not true, and let us pick a counterexample f with the smallest possible leading monomial. There are two possibilities.

First, it is possible that $e_i = \textsc{lm}(f) \in \textsc{lm}(S)$, in which case we take some $s \in S$ for which $e_i = \textsc{lm}(s)$, and replace f by

$$f' = f - \frac{\textsc{lc}(f)}{\textsc{lc}(s)} s.$$

Note that $f' + S = f + S$, and $f' = 0$ or $\textsc{lm}(f') \prec \textsc{lm}(f)$; in either of these cases, by our assumption, $f' + S$ contains a linearly reduced element, a contradiction.

Second, it is possible that $m = \textsc{lm}(f) \notin \textsc{lm}(S)$, in which case we consider the element $f' = f - \textsc{lt}(f)$. By our assumption, $f' + S$ contains a linearly reduced element g, so

$$f + S = \textsc{lt}(f) + f' + S$$

contains a linearly reduced element $\textsc{lt}(f) + g$, a contradiction.

It remains to prove linear independence. For that, note that if $f \neq 0 \in S$, then $\textsc{lm}(f) \in \textsc{lm}(S)$, so f is not linearly reduced with respect to S. Therefore, the zero coset S does not contain nonzero linearly reduced elements. □

In the language of undergraduate linear algebra, our viewpoint basically translates to a well known result stating that once an ordered basis is chosen for a vector space V, each subspace S corresponds to a unique matrix in row canonical form (RCF), the columns of that RCF containing the pivots correspond to the basis in the space of leading terms of S, and hence the other columns correspond to the basis of the quotient V/S; see, for example, [136] for a detailed discussion from this angle.

The result of Lemma 1.2.1.3 justifies the following definition.

Definition 1.2.1.4 (Normal forms)**.** Let S be a subspace of V. We call monomials that are linearly reduced with respect to S *normal modulo* S, and linear combinations of normal monomials *normal forms*. For each f in V, we call the unique element in the coset $f + S$ that is reduced with respect to S the *normal form of f modulo S*.

If we know a self-reduced basis B of a subspace S, the normal forms are precisely elements that are linearly reduced with respect to B, and that is the smallest set of conditions one has to check. Moreover, from the proof of Lemma 1.2.1.3 it is possible to infer an algorithm for computing the normal form of a given element f, which we will now describe. For these reasons, self-reduced bases are invaluable for working with normal forms.

Algorithm 1.2.1.5 (Normal form computation)**.**

> **Input**: A linearly self-reduced basis B of a subspace S of V, and an element $f \in V$.
>
> **Output**: The normal form of f modulo S.

- If $f = 0$, return f.
- If there exists $b \in B$ for which $\text{LM}(b) = \text{LM}(f)$, return the normal form of $f - \text{LC}(f)b$.
- Otherwise, $\text{LM}(f)$ is linearly reduced with respect to S, so let $\tilde{f}$ be the normal form of $f - \text{LT}(f)$; return $\text{LT}(f) + \tilde{f}$.

Proposition 1.2.1.6. *Every subspace $S \subset V$ has a linearly self-reduced basis B.*

Proof 1 (*theoretical*)*.* In fact, we shall prove more: not only does such a basis exist but it is unique.

Let us first prove uniqueness. If B is a linearly self-reduced basis of S, then $\text{LM}(S) = \text{LM}(B)$. Moreover, because B is linearly self-reduced, for each $e_i \in \text{LM}(S)$ there exists exactly one element $b \in B$ with $\text{LM}(b) = e_i$; for such b we have $b = e_i - h$, where h is linearly reduced with respect to S. Finally, this element h must be equal to the unique linearly reduced element in the coset $e_i + S$.

Let us now prove existence. As we just saw, the only feasible candidate for B is the set of all elements $e_i - h$, where $e_i \in \text{LM}(S)$, and h is the unique linearly reduced element in the coset $e_i + S$. This set B is linearly self-reduced by construction, and hence is linearly independent. Suppose that $S \neq \text{span}(B)$; take an element $s \in S \setminus \text{span}(B)$ with the smallest possible leading monomial. Since $s \in S$, we have $\text{LM}(s) - h \in B$ for some h with $\text{LM}(h) \prec \text{LM}(s)$, so the element $s - \text{LC}(s)(\text{LM}(s) - h)$, which belongs to the same coset but has a smaller leading monomial, is in $\text{span}(B)$. In that case we have $s \in \text{span}(B)$, which is a contradiction. □

Proof 2 (*constructive*)*.* From a constructive point of view, it only makes sense to talk about a subspace if it is actually defined in an effective way; an effective way to define a subspace is via a basis $s_1, \ldots, s_m$.

Recall that the *row canonical form* of a matrix A, is a matrix R obtained from A by elementary row operations for which the first nonzero entry of each nonzero row of R is equal to 1 (this entry is called the *pivot* of that row), the positions of the pivots increase with the increase in the row number, and all entries in each column containing a pivot are equal to zero.

The following algorithm for computing canonical forms of matrices is well-known. (This algorithm is recursive in the number of rows of the matrix.)

```
Algorithm 1.2.1.7 (Row canonical form computation).

    Input: A $m \times n$-matrix $A = [a_{ik}]_{1 \leq i \leq m, 1 \leq k \leq n}$.

    Output: The row canonical form of $A$.

  • Find the smallest $k$ for which $a_{ik} \neq 0$ for at least one $i$, that is, the
    $k^{\text{th}}$ column of the matrix $A$ has a nonzero entry. Pick one such $i$, and
    swap the first row of $A$ with the $i^{\text{th}}$ one.
  • Divide row 1 by $a_{1k}$.
  • If $m = 1$, return $A$.
  • Else, if $m > 1$
      – For each $j = 2, \ldots, m$, subtract from row $j$ the first row multiplied by $a_{jk}$.
      – Compute the row canonical form of the matrix consisting of the last $m - 1$ rows.
      – For each $j = 2, \ldots, m$, if $s$ is the smallest number for which
        $a_{js} \neq 0$ (in which case $a_{js} = 1$ is a pivot), subtract from row 1
        row $j$ multiplied by $a_{1s}$.
```

To compute a linearly self-reduced basis of S, one should put the coordinates of s_1, …, s_m in rows of a matrix, and compute the row canonical form of that matrix. For the set B, one may take the set of polynomials whose coordinates are the nonzero rows of the row canonical form. (They are linearly independent, which is clear from looking at pivotal coordinates, and they span the same subspace as $s_1, \ldots, s_m$, since all the operations we performed are invertible.) □

Methods that we recalled in this section lead to normal forms in quotients of an arbitrary vector space with a well-ordered basis. For instance, our results lead to a strategy for working with the quotients $T(X)/I$ of free associative algebras: one should just regard I as a subspace, find its space of leading terms, and apply basic linear algebra to determine normal forms. However, that strategy has serious deficiencies: on the one hand, we have to work with the whole ideal I, a very large (most certainly infinite-dimensional) space; on the other hand, it makes no use of the multiplicative structure of an ideal at all. In the next section, we demonstrate, on the toy model of polynomials in one variable, how one can use the algebra structure to simplify this approach. This will be greatly generalized in the following chapters, where for the general case we shall consider a special class of total orders, and a better notion of reducibility.

1.2.2 Normal forms of univariate polynomials

A very important feature of the ring $\mathbb{F}[x]$ of univariate polynomials with coefficients in a field is that it is a Euclidean domain: for every two polynomials $f(x)$ and $g(x) \neq 0$, we can divide $f(x)$ by $g(x)$ with remainder, that is there exist polynomials $q(x)$, the *quotient*, and $r(x)$, the *remainder*, for which

$$f(x) = q(x)g(x) + r(x),$$

and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. This property is behind most nice properties of $\mathbb{F}[x]$.

The following result about ideals in $\mathbb{F}[x]$ is well known; we shall present here two different proofs that resonate well with the two recurring approaches from the subsequent chapters.

Theorem 1.2.2.1. *Every ideal $I \subset \mathbb{F}[x]$ is a principal ideal, that is the ideal of multiples of some polynomial $d(x)$.*

Proof 1 (*theoretical*). The ring of polynomials is an $\mathbb{F}$-vector space with a basis $\{x^n\}_{n\geq 0}$; this basis is assumed to have the standard well-order

$$1 \prec x \prec x^2 \prec \ldots \prec x^n \prec \ldots$$

Let us apply our methods of the previous section, and consider $\textsc{lt}(I)$, the space of leading terms of I.

First, we note that if x^n is the leading monomial of some $f \in I$, then x^{n+k} is the leading monomial of $x^k f \in I$, so the space of leading terms is spanned by x^n for $n \geq p$ for some (uniquely determined) integer p.

Next, it is clear that there is a unique monic polynomial $d(x) \in I$ of degree p, for otherwise, if there were two different ones, $d_1(x)$ and $d_2(x)$, we would have $d_1(x) - d_2(x) \in I$ of smaller degree, which is a contradiction with the definition of p as the lowest degree of a monomial from $\textsc{lt}(I)$.

Finally, every element $f(x) \in I$ must be divisible by $d(x)$: otherwise the remainder $r(x)$ from division of $f(x)$ by $d(x)$ would be a nonzero polynomial of degree smaller than $d(x)$ which belongs to I (since $r(x) = f(x) - q(x)d(x)$). □

Proof 2 (*constructive*). From a constructive point of view, it only makes sense to talk about an ideal if it is actually defined in an effective way; an effective way to define an ideal I is to give its generators $f_1(x), \ldots, f_m(x)$ so that every element of I is equal to a combination $c_1(x)f_1(x) + \cdots + c_m(x)f_m(x)$.

Recall the following algorithm for computing greatest common divisors.

Algorithm 1.2.2.2 (Euclidean algorithm)**.**

Input: Two monic polynomials $f_1(x), f_2(x) \in \mathbb{F}[x]$.

Output: A monic polynomial $h(x) \in \mathbb{F}[x]$ which is the greatest common divisor of $f_1(x)$ and $f_2(x)$.

- If $f_1(x)$ is divisible by $f_2(x)$, $f_1(x) = f_2(x)q(x)$ for some polynomial $q(x)$, return $h(x) = f_2(x)$.
- If $f_1(x)$ is not divisible by $f_2(x)$, write $f_1(x) = f_2(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(f_2(x))$.
- Set $f_1(x) \leftarrow f_2(x)$ and $f_2(x) \leftarrow \frac{1}{\mathrm{LC}(r(x))}r(x)$, and perform the Euclidean algorithm on these $f_1(x)$ and $f_2(x)$.

To prove our result, we just need to go through the following loop, computing as a result the greatest common divisor of $f_1, \ldots, f_m$:
For j from m down to 2 do:

- Perform the Euclidean algorithm on $f_{j-1}(x)$ and $f_j(x)$; let $d_j(x)$ be the result.
- Set $f_{j-1}(x) \leftarrow d_j(x)$.

Once it is completed, the resulting value of $f_1(x)$ generates the ideal I. To see that, let us note that the Euclidean algorithm can be modified to include a proof that $h(x)$ belongs to the ideal generated by $f_1(x)$ and $f_2(x)$ by computing a representation

$$h(x) = a_1(x)f_1(x) + a_2(x)f_2(x)$$

for some polynomials $a_1(x), a_2(x)$. It is enough to ensure that we compute such representations for the polynomials $f_1(x)$ and $f_2(x)$ that we deal with at each step of the algorithm. That can be easily accomplished by setting $a_{11}(x) \leftarrow 1$, $a_{12}(x) \leftarrow 0$, $a_{21}(x) \leftarrow 0$, $a_{22}(x) \leftarrow 1$, and putting in the end of each iteration

$$\begin{aligned}
a_{11}(x) &\leftarrow a_{21}(x),\\
a_{12}(x) &\leftarrow a_{22}(x),\\
a_{21}(x) &\leftarrow \frac{1}{\mathrm{LC}(r(x))}(a_{11}(x) - q(x)a_{21}(x)),\\
a_{22}(x) &\leftarrow \frac{1}{\mathrm{LC}(r(x))}(a_{12}(x) - q(x)a_{22}(x)).
\end{aligned}$$

Therefore, the result of completion of the loop above, the greatest common divisor of the polynomials $f_1(x), \ldots, f_m(x)$, belongs to the ideal I, and hence generates it. This completes the proof. □.

Chapter 2

Noncommutative Associative Algebras

The theory of commutative Gröbner bases is well known and properly documented in many textbooks, however it exhibits too many lucky coincidences to be fully generalizable to more complex algebraic structures. The goal of this chapter is to present the similar theory of noncommutative Gröbner bases in a way that is amenable to adaptations for other algebraic structures discussed in this book; as the reader will see later, in many ways, noncommutative Gröbner bases **are** closer to Gröbner bases for operads than to Gröbner bases for commutative associative algebras.

2.1 Introduction

In the classical case of commutative algebras which we review in Chapter 7, Gröbner bases solve a very important practical problem: they provide an algorithm for solving systems of polynomial equations, which makes them a technical tool of utmost importance in various research areas, both in pure and applied mathematics.

However, as we hinted in the previous chapter, there is another viewpoint one can take which makes Gröbner bases particularly useful for a mathematician, and also amenable to meaningful generalizations. This viewpoint is that knowing a Gröbner basis G for an ideal I of a polynomial algebra R allows one to work with elements of R/I in an efficient and algorithmic way: the cosets of the monomials that are reduced with respect to G form a basis of R/I, and computing, for all pairs of two reduced monomials g_1 and g_2, the reduced form of the product g_1g_2 modulo G provides the multiplication table for this basis. In this chapter, this approach is implemented for noncommutative polynomials. Of course, when developing such theory, one must have in mind some goal one wants to achieve beyond merely generalizing the existing theory for commutative algebras. In this introductory part, we outline some reasons that we find convincing.

2.1.1 Noncommutative polynomial equations

If one wishes to keep the viewpoint of solving polynomial equations, then, as the polynomials are now noncommutative, a natural thing to do is to attempt to solve them in matrices of some size (rather than numbers). Classification of solutions in this sense is the main focus of representation theory of associative algebras. There are many natural examples of associative algebras presented by generators and relations, of which we mention a few below. In fact, it is fair to say that most natural known examples of noncommutative algebras are algebras presented by generators and relations. Therefore, it is most beneficial to develop methods for studying such algebras in a way that at least would allow us to find a basis and the multiplication table of such an algebra.

Definition 2.1.1.1 (Lie algebra)**.** A *Lie algebra* is a vector space L with a bilinear operation $a_1, a_2 \mapsto [a_1, a_2]$ that is anticommutative and satisfies the Jacobi identity, so that for all $a_1, a_2, a_3 \in L$, we have

$$[a_1, a_2] = -[a_2, a_1],$$
$$[[a_1, a_2], a_3] + [[a_2, a_3], a_1] + [[a_3, a_1], a_2] = 0.$$

This identity is satisfied in many meaningful examples, e.g., the operation $[a, b] = ab - ba$ in every associative algebra or the bracket $[\xi, \eta]$ of two vector fields on a manifold. The original motivation of Lie himself was that Lie algebras arise as infinitesimal symmetries of differential equations, and so they can be used to develop an analogue of Galois theory that would control solvability of differential equations by one or more integrations ("solvability in quadratures"), similarly as Galois theory for symmetries of algebraic equations controls solvability in radicals. Classifying representations of Lie algebras corresponds to classifying different types of symmetries that an action of that Lie algebra may exhibit. It turns out that for each Lie algebra L, there exists an associative algebra with the same representations.

Definition 2.1.1.2 (Universal enveloping algebra)**.** Let L be a Lie algebra. The *universal enveloping algebra* of L is the associative algebra $U(L)$ presented by generators and relations (that is, as a quotient of the tensor algebra $T(L)$ by a certain ideal) as follows:

$$U(L) = T(L)/(xy - yx - [x, y] \colon x, y \in L).$$

The Lie algebra $U(L)^-$ is the vector space $U(L)$ equipped with the operation $[a, b] = ab - ba$. (This operation makes every associative algebra into a Lie algebra.) The *canonical map* $\alpha \colon L \to U(L)$ is the composition of the embedding $L \hookrightarrow T(L)$ and the canonical projection $T(L) \twoheadrightarrow U(L)$.

Another natural example of algebras presented by generators and relations are various "quantum" algebras; informally, those are algebras over the field $\mathbb{F}(q)$ which, after setting $q = 1$, specialize to various familiar algebras, for example, algebras of functions on various algebraic varieties. Let us give two simple instances of quantum algebras to clarify what we mean.

Example 2.1.1.3. The quantum plane, or, more precisely, the algebra of functions on the quantum plane, is the $\mathbb{F}(q)$-algebra with two generators x_1, x_2, and one defining relation $x_2x_1 = qx_1x_2$. Note that setting $q = 1$ does indeed make this relation into $x_2x_1 = x_1x_2$, and the algebra into the algebra of polynomials, that is the algebra of (polynomial) functions on the two-dimensional plane.

Example 2.1.1.4. The quantized algebra of functions on 2×2-matrices is the $\mathbb{F}(q)$-algebra with four generators $x_{11}, x_{12}, x_{21}, x_{22}$, and defining relations

$$\begin{gathered} x_{12}x_{11} = qx_{11}x_{12}, \quad x_{22}x_{12} = qx_{12}x_{22}, \\ x_{21}x_{11} = qx_{11}x_{21}, \quad x_{22}x_{21} = qx_{21}x_{22}, \\ x_{11}x_{22} - x_{22}x_{11} = (q^{-1} - q)x_{12}x_{21}, \quad x_{12}x_{21} = x_{21}x_{12}. \end{gathered}$$

Note that setting $q = 1$ does make these relations into the usual relations saying that all these variables commute with each other. This algebra contains an important element $x_{22}x_{11} - qx_{12}x_{21}$ called the quantum determinant. Imposing an extra relation $x_{22}x_{11} - qx_{12}x_{21} - 1$ defines the quantized algebra of functions on the group SL_2; see [55] for more details.

Further examples of naturally arising algebras presented by generators and relations include quantum enveloping algebras [90], rational Cherednik algebras, symplectic reflection algebras and double affine Hecke algebras [57, 117, 118], Calabi–Yau algebras [104], etc.

2.1.2 Noncommutative algebras and Koszul duality

There are several instances when viewing a commutative algebra as a particular case of a noncommutative algebra is very beneficial. A celebrated example of applying this viewpoint is viewing the algebra of polynomials in several variables in the larger universe of noncommutative algebras allows one to relate it to the Grassmann algebra by means of the so-called Koszul duality.

Definition 2.1.2.1 (Koszul duality)**.** Let $A = T(V)/(R)$ be an associative algebra for which the space of relations R is a subspace of $V \otimes V$, in other words, a *quadratic algebra*. The *Koszul dual* algebra $A^!$ is the quotient $T(V^*)/(R^\perp)$, where $R^\perp$ is the annihilator of R under the natural pairing between $V^* \otimes V^*$ and $V \otimes V$. The algebras A and $A^!$ are graded,

$$A = \bigoplus_{n \geq 0} A_n, \qquad A^! = \bigoplus_{n \geq 0} A^!_n$$

The *Koszul complex* of A is the graded vector space $K_\bullet(A)$ with components

$$K_n(A) = (A^!_n)^* \otimes A.$$

This space is equipped with the boundary map d, which is the composite of the inclusion $\imath_n\colon (A^!_n)^* \hookrightarrow V^{\otimes n}$ with the map

$$\kappa\colon V^{\otimes n} \otimes A \to V^{\otimes (n-1)} \otimes A$$

defined by the formula $\kappa(v_1 \otimes \cdots \otimes v_n \otimes a) = v_1 \otimes \cdots \otimes v_{n-1} \otimes (v_n a)$, where in the product $v_n a$ we regard v_n as an element of A under the map

$$V \to T(V) \twoheadrightarrow T(V)/(R) = A.$$

The map d makes $K_\bullet(A)$ a chain complex. The algebra A is said to be a *Koszul algebra* if the inclusion $\mathbb{F} \to K_\bullet(A)$, which sends $1 \in \mathbb{F}$ to $1^\vee \otimes 1 \in (A^!_0)^* \otimes A$, induces an isomorphism on the homology.

Example 2.1.2.2. Suppose that $A = S(V)$, the quotient of $T(V)$ by the ideal generated by the elements $v_1 \otimes v_2 - v_2 \otimes v_1$ (the symmetric algebra of V). Then $A^!$ is the quotient of $T(V^*)$ by the ideal generated by the elements $\xi_1 \otimes \xi_2 + \xi_2 \otimes \xi_1$, also known as $\Lambda(V^*)$, the Grassmann algebra of V^*. The Koszul complex in this case is the linear dual of the polynomial de Rham complex of V, and the homological condition of Definition 2.1.2.1 is satisfied (Exercise 2.1), so the symmetric algebra is Koszul.

The previous example is at the core of the following theorem which is a perfect illustration of how some property of commutative algebras may be better understood in the noncommutative world.

Theorem 2.1.2.3 ([15, 22])**.**

(i) *There is an equivalence of triangulated categories between the bounded derived categories of complexes of graded finitely generated $S(V)$-modules* (*that is, coherent sheaves on $\mathbb{P}^n$*) *and the same for $\Lambda(V^*)$.*

(ii) *More generally, if A is Koszul, there is an equivalence of triangulated categories between the bounded derived categories of complexes of graded finitely generated modules for A and $A^!$.*

2.2 Free associative algebras

2.2.1 Monomials and polynomials

Definition 2.2.1.1 (Noncommutative monomials)**.** Let $X = \{x_1, \ldots, x_n\}$ be a set of indeterminates, or an *alphabet*. A *noncommutative monomial*, or a *word*, in $x_1, \ldots, x_n$ is an expression $x_{i_1} x_{i_2} \cdots x_{i_k}$ for all possible choices of $k \geq 0$ and $1 \leq i_p \leq n$. (If $k = 0$ then we have the *empty word* $w = 1$.) The *weight* of a word $w = x_{i_1} \cdots x_{i_k}$, denoted $\mathrm{wt}(w)$, is equal to its length k. The *product* of words u and v is the word uv obtained by *concatenation*. The *free monoid* generated by the set X is the set X^* of all words in the alphabet X, equipped with the concatenation product. The *unit element* of this monoid is the empty word.

Remark 2.2.1.2. In the case of commutative algebras, it is conventional to refer to weight as *degree*. We choose to avoid this in order not to clash with [180]: associative algebras are particular cases of operads, where each letter in a word is viewed as a unary operation, and the standard way to work with operads forces the convention for associative algebras that we adopt.

Example 2.2.1.3. If $X = \{a\}$ then $X^* = \{\, a^k \mid k \geq 0 \,\}$ consists of the nonnegative powers of a; we have $a^i a^j = a^{i+j}$ so X^* is commutative. If $|X| \geq 2$ then X^* is noncommutative. If $X = \{a, b\}$ then X^* has 2^k distinct words of degree k for $k \geq 0$.

Definition 2.2.1.4 (Noncommutative polynomials)**.** Let $X = \{x_1, \ldots, x_n\}$ be an alphabet. A *noncommutative polynomial* in $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}$ is a linear combination of noncommutative monomials. The *support* of a noncommutative polynomial f, denoted $\mathrm{supp}(f)$, is the set of all noncommutative monomials that appear in f with nonzero coefficients. The vector space $\mathbb{F}X^*$ of all noncommutative polynomials has a binary operation $f, g \mapsto fg$, the *product*, that extends the concatenation product of words by *bilinearity*, so for any polynomials f, g, h and for any scalar $a \in \mathbb{F}$ we have

$$f(g+h) = fg + fh, \quad (f+g)h = fh + gh, \quad (af)g = a(fg) = f(ag). \tag{2.1}$$

The vector space $\mathbb{F}X^*$ equipped with the product operation is the *free associative algebra generated by* X. It is often denoted by $\mathbb{F}\langle x_1, \ldots, x_n \rangle$, or by $\mathbb{F}\langle X \rangle$. We will mainly use the notation $T(X)$, or $T(V)$, where $V = \mathrm{span}(x_1, \ldots, x_n)$, viewing each word $x_{i_1} \cdots x_{i_n}$ as shorthand notation for $x_{i_1} \otimes \cdots \otimes x_{i_n} \in T^n(V)$, called a *decomposable tensor* (or *tensor of rank 1* or *simple tensor*).

In this chapter, we consider noncommutative monomials and polynomials, so we will often drop the word "noncommutative", hoping that it does not lead to confusion.

2.2.2 Presentation by generators and relations

Let us formalize the intuitive notion of a presentation of an algebra by generators and relations that we used throughout Section 2.1. Suppose that an algebra A is generated by finitely many elements $a_1, \ldots, a_n$. In that case, there is a surjective homomorphism from $T(x_1, \ldots, x_n)$ onto A sending x_i to a_i which is uniquely defined by the universal property of the tensor algebra. By First Homomorphism Theorem, that homomorphism is the canonical map onto the quotient of $T(x_1, \ldots, x_n)$ by some ideal I. Therefore, working with finitely generated algebras is essentially equivalent to working with ideals in free associative algebras.

Let A be an associative algebra, and suppose that $S \subset A$. Recall that the ideal of A generated by S, conventionally denoted by (S), is the smallest (by inclusion) ideal of A that contains S as a subset. Explicitly, the ideal (S) is the linear span of all elements $r_1 s r_2$ for all $r_1, r_2 \in A$, $s \in S$.

Definition 2.2.2.1 (Presentation by generators and relations)**.** Suppose that the algebra A is a quotient of the free algebra $T(X)$ by some ideal I, and that the ideal I is generated by the set S. In this case, we will say that the algebra A is *presented by generators X and relations S.*

This way, working with finitely generated algebras can be approached through their presentations by generators and relations. Our goal in the next few sections is to explain how to convert a given presentation into another one which is easy to use for computing normal forms.

2.3 Normal forms

2.3.1 Monomial orders

If we aim to involve the multiplicative structure in computing normal forms, a very natural step to begin with is to consider well-orders that are compatible with that multiplicative structure.

Definition 2.3.1.1 (Monomial order)**.** A total order Ξ of X^* is said to be a *monomial order* if the following two conditions are satisfied:

- Ξ is a well-order;
- the product of monomials is a strictly increasing function in each of its arguments; that is,

$$m_1 m_2 \prec m_1' m_2 \text{ if } m_1 \prec m_1', \qquad m_1 m_2 \prec m_1 m_2' \text{ if } m_2 \prec m_2'.$$

Unless otherwise specified, all definitions and theoretical results presented throughout this chapter are valid for an arbitrary monomial order Ξ.

The main property of leading monomials is given by the following result.

Proposition 2.3.1.2. *For any two nonzero elements $f_1, f_2 \in T(X)$, we have*

$$\mathrm{LM}(f_1 f_2) = \mathrm{LM}(f_1)\,\mathrm{LM}(f_2).$$

Proof. Since the product on $T(X)$ is multilinear, the element $f_1 f_2$ is equal to a linear combination of elements $m_1 m_2$, where $m_p \in \mathrm{supp}(f_p)$. It remains to notice that for each $m_p \neq \mathrm{LM}(f_p)$ we have $m_p \prec \mathrm{LM}(f_p)$, so the defining property of monomial orders implies that $m_1 m_2 \prec \mathrm{LM}(f_1)\,\mathrm{LM}(f_2)$, unless $m_1 = \mathrm{LM}(f_1)$, $m_2 = \mathrm{LM}(f_2)$. □

Let us give an example of a monomial order which is similar to the `glex` order on commutative monomials.

Definition 2.3.1.3 (Graded lexicographic order)**.** Let us fix a total order Ξ of the alphabet X. It induces an order on X^*, called the *graded lexicographic order*, or `glex`, as follows. If $m, m' \in X^*$ then $m \prec m'$ if and only if

(i) either $\mathrm{wt}(m) < \mathrm{wt}(m')$,

(ii) or $\mathrm{wt}(m) = \mathrm{wt}(m')$, and $m = \bar{m}x_i m_1$ and $m' = \bar{m}x_j m_1'$ for some $\bar{m}, m_1, m_1' \in X^*$ and $x_i, x_j \in X$ with $x_i \prec x_j$.

Condition (ii) says that if two monomials have the same weight, in order to compare them we compare the first (leftmost) letters where they differ.

Remark 2.3.1.4. There are two important warnings that we would like to make at this stage. First, though the same notation `glex` is commonly used for the order we just described, it is important to emphasize that in the commutative case, `lex` in `glex` stands for the lexicographic order of the exponent sequences of the letters, and in the noncommutative case it stands for the (more logical) lexicographic order of words. Second, the pure lexicographic order of words is not a monomial order at all: the sequence of words

$$ab \succ aab \succ aaab \succ \dots$$

shows that the dictionary order is not a well-order, and moreover, the very first pair of words in this sequence shows that the product is not an increasing function, as $a \prec aa$, but $ab \succ aab$.

(Both authors have to confess that on some occasions they have made the mistake of believing that the concatenation product is an increasing function for the lexicographic order, and so they believe that it is their professional duty to prevent others from committing the same error.)

Example 2.3.1.5. For $X = \{a, b\}$ with $a \prec b$, the nonempty words in X^* of weight ≤ 3 are:

$$a \prec b \prec a^2 \prec ab \prec ba \prec b^2 \prec a^3 \prec a^2b \prec aba \prec ab^2 \prec ba^2 \prec bab \prec b^2a \prec b^3.$$

Proposition 2.3.1.6. *The order* `glex` *is a monomial order.*

Proof. Exercise 2.2. □

The available literature on noncommutative monomial orders mainly deals with questions of what ordinal types can appear rather than classifying the orders, and seems to have more precise statements for two generators only [61, 189, 190, 191, 206, 228]. We used these references in further examples that we give below. An interesting discussion of the multitude of orders for three generators arises naturally when exploring possible reduced Gröbner bases for the commutator ideal $(ab - ba, bc - cb, ca - ac) \subset T(a, b, c)$; see, e.g, [131, 132]. It is not unexpected for the commutator ideal to play a key role: after all, in the commutative case all orders can be classified, as we will see in Chapter 7, and the commutator ideal measures the discrepancy between the commutative and the noncommutative case.

Example 2.3.1.7. The order `glex` can be modified in a way that different variable haves different weights. Let us give an example of how this can be done for $T(a,b)$. Let $\lambda \in \mathbb{R}_{>0}$, and denote by $\mathrm{wt}_a(m)$ and $\mathrm{wt}_b(m)$ the number of occurrences of a and b, respectively, in the monomial m. For any $m, m' \in \{a,b\}^*$ we define $m \prec_\lambda m'$ if

- $\mathrm{wt}_a(m) + \lambda\,\mathrm{wt}_b(m) < \mathrm{wt}_a(m') + \lambda\,\mathrm{wt}_b(m')$, or
- $\mathrm{wt}_a(m) + \lambda\,\mathrm{wt}_b(m) = \mathrm{wt}_a(m') + \lambda\,\mathrm{wt}_b(m')$, and $m' = mm''$ for some m'', or
- $\mathrm{wt}_a(m) + \lambda\,\mathrm{wt}_b(m) = \mathrm{wt}_a(m') + \lambda\,\mathrm{wt}_b(m')$, and for the first position where m and m' differ, there is the letter a in the monomial m.

For example, one can easily check that

$$ba^2 \prec_2 a^2ba \prec_2 a^4b \prec_2 a^3ba.$$

Example 2.3.1.8. There is a class of monomial orders for $T(a,b)$ called *matrix orders*, defined as follows. Let $m \in \{a,b\}^*$ with $\mathrm{wt}_b(m) = k$. Then m can be written as $m = a^{n_0}ba^{n_1}\cdots ba^{n_k}$, with nonnegative exponents n_i, in which case we put $\rho(m) = (n_0, n_1, \ldots, n_k) \in \mathbb{Z}_{\geq 0}^{k+1}$. For each $\lambda \in \mathbb{R}_{>0}$, we define the matrix

$$\Omega_k = \begin{bmatrix} 1 & \lambda & \lambda^2 & \ldots & \lambda^{k-1} & \lambda^k \\ 0 & 1 & \lambda & \ldots & \lambda^{k-2} & \lambda^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & \lambda \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{bmatrix}.$$

Let $m, m' \in \{a,b\}^*$. We define $m \prec^\lambda m'$ if

- $\mathrm{wt}_b(m) < \mathrm{wt}_b(m')$, or
- $\mathrm{wt}_b(m) = \mathrm{wt}_b(m') = k$, and the first nonzero entry of $\Omega_k(\rho(m')-\rho(m))^T$ is positive.

For instance, we have

$$\rho(a^3ba) = (3,1), \quad \rho(ba^2) = (0,2), \quad \rho(a^2ba) = (2,1), \quad \rho(a^4b) = (4,0),$$

and a small computation demonstrates that for $\lambda = 2$ we have

$$a^4b \prec^2 a^2ba \prec^2 ba^2 \prec^2 a^3ba.$$

Example 2.3.1.9. The following example of a monomial order on $T(a, b)$ is a modification of an order frequently used for term rewriting [191]. For all $m, m' \in \{a, b\}^*$, we define $m \prec_L m'$ if

- $\mathrm{wt}_b(m) < \mathrm{wt}_b(m')$, or
- $\mathrm{wt}_b(m) = \mathrm{wt}_b(m')$ and $m' = mm''$ for some $m'' \neq 1$, or
- $\mathrm{wt}_b(m) = \mathrm{wt}_b(m')$ and for the first (leftmost) position where m and m' differ, the letter in the monomial m is b.

For example, one can easily check that

$$ba^2 \prec_L a^2ba \prec_L a^3ba \prec_L a^4b.$$

2.3.2 Long division

We are now ready to approach normal forms using a direct generalization of long division. That approach is more economic than merely viewing the given ideal I as a subspace of $T(X)$. To improve the notion of reduced elements, we will utilize divisibility of monomials by one another in the free algebra. An important factor that helps the algorithmic/computational side is that the algebraic notion of divisibility of monomials which uses the existing algebra structure is described in a very straightforward way combinatorially. As we will see, this approach does not necessarily result in unique normal forms; that last deficiency will be resolved in the next section using the notion of a Gröbner basis.

Definition 2.3.2.1 (Divisibility of monomials)**.** We say that the monomial m is *divisible by a monomial* m' if m contains m' as a subword: precisely, $m = x_{i_1} \cdots x_{i_r}$ and $m' = x_{i_p} \cdots x_{i_q}$ for $1 \leq p \leq q \leq r$ (note that we exclude the empty subword as a divisor).

We would like to emphasize that in what happens next it is important that we consider not just a divisor, but the place where it occurs. For example, if we consider the monomials $m = aaaa$ and $m' = aa$ in $T(a)$, then m' is a divisor of m, but moreover, it is a divisor of m "in three different ways": there are three subwords of m equal to m', underlined in

$$\underline{aa}aa, \qquad a\underline{aa}a, \qquad aa\underline{aa}.$$

Definition 2.3.2.2 (Reduced monomials and polynomials)**.** Let $S \subset T(X)$. A monomial m is said to be *reduced with respect to* S if $m \notin (\textsc{lm}(S))$; in other words, if m is not divisible by any of the leading monomials of elements of S.

In general, a noncommutative polynomial $f \in T(X)$ is said to be *reduced with respect to* S, if it is equal to a linear combination of monomials which are reduced with respect to S. A subset $S \subset T(X)$ is said to be *self-reduced* if each element $s \in S$ is monic and reduced with respect to $S \setminus \{s\}$.

The linear reductions that mimic row operations on vectors are now replaced by reductions that take into account divisibility of monomials.

Definition 2.3.2.3 (Reduction operator)**.** Let $f, g \in T(X)$ be two nonzero elements. We say that f is *reducible with respect to g* if $\textsc{lm}(f)$ is not reduced with respect to $\{g\}$, or, in plain words, if the leading monomial of f is divisible by the leading monomial of g, $\textsc{lm}(f) = m_1 \textsc{lm}(g) m_2$ for some $m_1, m_2 \in X^*$. In that case, the *reduction of f with respect to g*, denoted by $r_g(f)$, is defined by the formula

$$r_g(f) = f - \frac{\textsc{lc}(f)}{\textsc{lc}(g)} m_1 g m_2.$$

Remark 2.3.2.4. Our notation is not completely precise, since there may be several divisors of $\textsc{lm}(f)$ equal to $\textsc{lm}(g)$, and hence several different reductions. We implicitly incorporate a choice of one particular divisor (which will always be clear from the context) in the definition of a reduction.

Lemma 2.3.2.5. *For all elements $f, g \in T(X)$ such that $r_g(f)$ is defined, we have*

$$r_g(f) = 0 \quad \text{or} \quad \textsc{lm}(r_g(f)) \prec \textsc{lm}(f).$$

Proof. Indeed, by construction we have $\textsc{lt}(f) = \textsc{lt}\left(\frac{\textsc{lc}(f)}{\textsc{lc}(g)} m_1 g m_2\right)$. □

One can view a reduction as one step of a version of the long division algorithm. We make it more precise as follows.

Algorithm 2.3.2.6 (Long division for noncommutative algebras)**.**

Input: An element $f \in T(X)$, and a finite subset $S \subset T(X)$.

Output: An element $\tilde{f}$, reduced with respect to S, for which $\textsc{lt}(\tilde{f}) \preceq \textsc{lt}(f)$ such that $f + (S) = \tilde{f} + (S)$.

- If $f = 0$, return f.
- Replace S by its linear self-reduction.
- If $D := \{s \in S \colon \textsc{lm}(f) \text{ is divisible by } \textsc{lm}(s)\} \neq \varnothing$, take $s_0 \in D$ with the least leading monomial (s_0 is unique since S is linearly self-reduced), and return the result of long division of $f' := r_s(f)$ by S.
- Otherwise, $\textsc{lm}(f)$ is reduced with respect to S, so let $\tilde{f}$ be the result of long division of $f' := f - \textsc{lt}(f)$ by S; return $\textsc{lt}(f) + \tilde{f}$.

Note that this algorithm is deterministic only because we made the decision of choosing $s_0 \in D$ with the least leading monomial. The following example demonstrates that for other choices of s_0, the result of long division could be different.

Example 2.3.2.7. Let $X = \{a, b\}$, and let $s_1 = a^2 - 1$, $s_2 = ab - a$, and $f = a^2b$. Then $r_{s_1}(f) = b$, and $r_{s_2}(f) = a^2$. Therefore, if we order $S = \{s_1, s_2\}$ in a way that $s_1 < s_2$, then the long division terminates after just one reduction, and returns b. If we order $S = \{s_1, s_2\}$ in a way that $s_1 > s_2$, then the long division takes two reductions, and returns 1.

Lemma 2.3.2.8. *For every $f \in T(X)$, the long division algorithm terminates in a finite number of steps. Its output is an element $\tilde{f}$ reduced with respect to S, for which $\text{LT}(\tilde{f}) \preceq \text{LT}(f)$ and $f + (S) = \tilde{f} + (S)$.*

Proof. By Lemma 2.3.2.5, the leading monomial of the dividend (the element that the algorithm is applied to) decreases at each step, so termination follows from the fact that Ξ is a well-order. This also proves the second claim about the output. Suppose that for some f the output is not reduced. Let us pick among such f an element with the smallest leading monomial (again using the well-order Ξ). If $\text{LM}(f)$ is not reduced with respect to S, then the first step applies the same algorithm to $f' = r_s(f)$, and by Lemma 2.3.2.5 we have $f' = 0$ or $\text{LM}(f') \prec \text{LM}(f)$, so the output of the long division is reduced. If $\text{LM}(f)$ is reduced, then the second step of the algorithm applies the same algorithm to $f' = f - \text{LT}(f)$, so $f' = 0$ or $\text{LM}(f') \prec \text{LM}(f)$, and the output of the long division is reduced, a contradiction. Finally, note that each reduction subtracts an element in (S), which justifies the claim about the coset, and completes the proof. □

Remark 2.3.2.9. We see that in fact there is nothing particularly problematic if S is an infinite self-reduced set: it is clear from the proof of Lemma 2.3.2.8 that for the given $f \in T(X)$ the elements $s \in S$ which we use at various steps of our computation have decreasing leading monomials, and so there can be only finitely many reductions performed; that is, for each f we never use more than a finite subset of S. While for purposes of implementation this is not particularly important, it will be beneficial for theoretical results where S may be infinite.

We will now establish that the set of elements that are reduced with respect to I is a suitable candidate for the set of normal forms for the elements of the quotient $T(X)/I$. This is an improvement of Lemma 1.2.1.3 which takes into account the extra structures we have on the underlying vector spaces.

Lemma 2.3.2.10. *Suppose that I is an ideal of $T(X)$. Monomials that are reduced with respect to I form a basis of the quotient $T(X)/I$.*

Proof. Let us first prove the spanning property. For that, it is enough to show that the coset $f + I$ of every element $f \in T(X)$ contains an element that is reduced with respect to I. This is true, since we can take $\tilde{f}$ to be the result of long division of f with respect to I, in which case $\tilde{f}$ is reduced, and $\tilde{f} + I = f + I$.

It remains to prove linear independence. For that, note that if $f \neq 0 \in I$, then $\textsc{lm}(f) \in \textsc{lm}(I)$, so f is not even linearly reduced with respect to I, so I does not contain nonzero reduced elements. □

Similarities between the results that we proved using the long division algorithm and those obtained using the constructive proof of Proposition 1.2.1.6 make one think that it is possible to use long division to compute, for each set S, a self-reduced set S' generating the same ideal so that the elements that are reduced with respect to S' are precisely normal forms modulo (S). Alas, that is not true, as the following example demonstrates.

Example 2.3.2.11. Consider the self-reduced set $S = \{a^2 - 1, ab - a\}$ from Example 2.3.2.7. Two different series of reductions with respect to S that we computed in that example demonstrate that the ideal (S) contains the element $b - 1$ which is reduced with respect to S.

Nevertheless, it is possible to use long division to find, for each finite set, a finite self-reduced set that generates the same ideal.

Algorithm 2.3.2.12 (Self-reduction for noncommutative algebras)**.**

Input: A finite subset $S \subset T(X)$.

Output: A finite self-reduced subset $S' \subset T(X)$ with $(S) = (S')$.

- Replace S by its linear self-reduction.
- If S is self-reduced, return S.
- Let s be the element of S with the maximal leading monomial, and compute the self-reduction S' of $S \setminus \{s\}$.
- Compute $\tilde{s}$, the result of long division of s by S'.
- Compute the self-reduction of $S' \cup \{\tilde{s}\}$.

We leave it as an exercise (Exercise 2.3) for the reader to check that for each finite S this algorithm terminates after finitely many steps (in which case it of course outputs a finite self-reduced set).

2.3.3 Gröbner bases

As we saw in Example 2.3.2.7, in general, there are several different reduced forms one may obtain when doing reductions with respect to a set S; however, there is a *canonical* form with respect to the ideal (S), namely the corresponding normal form. In this section, we will explain how to fix this discrepancy.

Proposition 2.3.3.1. *Let I be an ideal of $T(X)$. The space of leading terms $\textsc{lt}(I)$ is an ideal of $T(X)$.*

Proof. By definition, $\mathrm{LT}(I)$ is a subspace, so we just have to show that the product of two elements belongs to $\mathrm{LT}(I)$ whenever at least one of the elements belongs to $\mathrm{LT}(I)$. Since the product is multilinear, it is enough to consider the case that both elements are monomials m_1 and m_2, and one of them, say m_1, is the leading monomial of some element f_1 of I. By Proposition 2.3.1.2, in this case we have $\mathrm{LM}(f_1 m_2) = m_1 m_2$, and therefore $m_1 m_2 \in \mathrm{LT}(I)$. □

We are now ready to define a Gröbner basis of an ideal.

Definition 2.3.3.2 (Gröbner basis)**.** Let I be an ideal of $T(X)$. We say that a subset $G \subset I$ is a *Gröbner basis* of I with respect to a given monomial order Ξ if the set of leading monomials $\mathrm{LM}(G) := \{\mathrm{LM}(g) \colon g \in G\}$ generates the leading term ideal of the ideal I:

$$\mathrm{LT}(I) = (\mathrm{LM}(G)).$$

A Gröbner basis which is a self-reduced subset of $T(X)$ is said to be *reduced*.

Remark 2.3.3.3. A Gröbner basis is not a basis for I as a vector space, but rather a *set of generators* for I as a (two-sided) ideal in $T(X)$.

Lemma 2.3.3.4. *A Gröbner basis of an ideal $I \subset T(X)$ generates I.*

Proof. Suppose that G is a Gröbner basis of I, and that (G) is a proper subset of I. (Clearly, $(G) \subset I$ since (G) is the smallest ideal containing G.) Let us take $f \in I \setminus (G)$ with the least possible leading monomial. Since $\mathrm{LM}(f) \in \mathrm{LT}(I)$, there exists $g \in G$ for which $\mathrm{LM}(f)$ is divisible by $\mathrm{LM}(g)$. Then $r_g(f)$ is defined and belongs to I, and by Lemma 2.3.2.5, we have $\mathrm{LM}(r_g(f)) \prec \mathrm{LM}(f)$, so $r_g(f) \in (G)$ by minimality of f. But this implies $f \in (G)$, since $r_g(f)$ is obtained by subtracting an element of (G) from f, which is a contradiction. □

Proposition 2.3.3.5. *Let I be an ideal of $T(X)$. A subset $G \subset I$ is a Gröbner basis if and only if the cosets of monomials that are reduced with respect to G form a basis of the quotient $T(X)/I$.*

Proof. Let us note that the cosets of monomials that are reduced with respect to G form a basis of the quotient $T(X)/I$ if and only if every coset modulo I contains a unique element that is reduced with respect to G.

First of all, we remark that if $f \in T(X)$, then $\tilde{f}$, the result of the long division of f by G, is reduced, and $\tilde{f} + (G) = f + (G) \subset f + I$, so every coset contains at least one reduced element whether G is a Gröbner basis or not.

Suppose now that G is a Gröbner basis of I. Suppose that the cosets of reduced monomials are linearly dependent, or, in other words, that the zero coset I contains a nonzero reduced element f. In that case, $\mathrm{LM}(f) \in \mathrm{LT}(I)$ is reduced with respect to G, which is a contradiction.

Suppose that G is not a Gröbner basis. This implies that there exists an element $f \in I$ for which $\mathrm{LM}(f)$ is reduced with respect to G. Let $\tilde{f}$ be the result of the long division of f by G. Clearly, $\tilde{f}$ is a nontrivial linear combination of reduced monomials, so the cosets of reduced monomials are in this case linearly dependent. □

Corollary 2.3.3.6. *Suppose that G is a Gröbner basis of the ideal $I \subset T(X)$. Then the result of long division of $f \in T(X)$ by G does not depend on either the choices or the order of the reductions performed.*

Proof. Suppose that two different choices of order of reductions yield two different results. In this case, the coset $f + I$ contains two different elements that are reduced with respect to G, hence reduced monomials are linearly dependent, a contradiction. □

We summarize Proposition 2.3.3.5 and its corollary as follows.

Theorem 2.3.3.7.

(*i*) *Let I be an ideal of $T(X)$. A subset $G \subset I$ is a Gröbner basis if and only if the normal forms modulo I are precisely the elements that are reduced with respect to G.*

(*ii*) *Suppose that G is a Gröbner basis of the ideal $I \subset T(X)$. Given an element $f \in I$, its normal form modulo I can be computed using long division by G. In fact, in this long division the reductions and their order can be chosen arbitrarily.*

Previously, we proved Proposition 1.2.1.6 which showed that the linear span of a set S contains a unique linearly self-reduced basis S'. For ideals, it is not enough to deal with self-reduced systems of generators: for example, $(a^2 - 1, ab - a) = (a^2 - 1, b - 1)$, see Examples 2.3.2.7, 2.3.2.11. The following result shows that the right way to state that proposition to adapt it from linear reductions to polynomial reductions is to use Gröbner bases.

Proposition 2.3.3.8. *Each ideal $I \subset T(X)$ has a unique reduced Gröbner basis.*

Proof. Let us first prove uniqueness. If G is a Gröbner basis, then $\textsc{lt}(I) = (\textsc{lm}(G))$; if G, in addition, is reduced, then $\textsc{lm}(G) \subset \textsc{lm}(I)$ must coincide with the set M of all elements $m \in \textsc{lm}(I)$ that are not divisible by other elements of $\textsc{lm}(I)$. (In other words, M is the set of minimal elements of $\textsc{lm}(I)$ with respect to the partial order of divisibility.) Indeed, each $m \in M \subset \textsc{lm}(I)$ must be divisible by a leading term of an element $g \in G$, and by definition of M, this can only happen if $\textsc{lm}(g) = m$, so $M \subset \textsc{lm}(G)$. Also, if $g \in \textsc{lm}(G) \setminus M$, then $\textsc{lm}(g)$ is divisible by m' for some $m' \in \textsc{lt}(I)$ by definition of M, and m' is divisible by $\textsc{lt}(g')$ for some $g' \in G$ by definition of a Gröbner basis, so since G is reduced, we have $g = g'$, and $\textsc{lm}(g) = m$, a contradiction. Moreover, since G is reduced, then for each $m \in M = \textsc{lm}(G)$ there exists a unique element $g \in G$ with $\textsc{lm}(g) = m$; for such g we have

$g = m - h$, where h is reduced with respect to I. Finally, this element h must be equal to the unique element in the coset $m + I$ that is reduced with respect to I.

Now we will prove existence. As we have just seen, the only feasible candidate for G is the set of all elements of the form $m - h$, where $m \in M$, and h is the unique element in the coset $m + I$ that is reduced with respect to I. This set G is self-reduced by construction. Note that every element of $\textsc{lm}(I)$ is divisible by some element $m \in M$; indeed, the smallest element which is not divisible by any element of M is either not divisible by any other element of $\textsc{lm}(I)$, and hence must be in M, or is divisible by some (smaller) element, and hence has a divisor from M; either way we get a contradiction. Therefore, $\textsc{lt}(I) = (M) = (\textsc{lm}(G))$, which shows that G is a Gröbner basis. □

2.4 Computing Gröbner bases

In this section, we will explain how to compute Gröbner bases for ideals of $T(X)$. Unlike the commutative case, this does not necessarily lead to an algorithm in the proper sense, since some ideals have infinite Gröbner bases. However, we will be able to make the solution as algorithmic as possible.

2.4.1 Diamond lemma

If the generating set S of the ideal I in $T(X)$ is not a Gröbner basis, then we saw in the proof of Proposition 2.3.3.5 that the cosets of reduced monomials are linearly dependent. Those linear dependencies, see Example 2.3.2.7, may arise as results of an "ambiguity", where two different reductions may be applied to an element f. This can be pictorially represented by the diagram

$$\begin{tikzcd}
& f \arrow[dl] \arrow[dr] & \\
r_{g_1}(f) & & r_{g_2}(f)
\end{tikzcd}$$

In the case of a Gröbner basis, subsequent reductions of those two distinct elements lead to the same reduced element $\mathrm{NF}(f)$, the normal form of f:

$$\begin{tikzcd}
& f \arrow[dl] \arrow[dr] & \\
r_{g_1}(f) \arrow[dr, dashed] & & r_{g_2}(f) \arrow[dl, dashed] \\
& \mathrm{NF}(f) &
\end{tikzcd}$$

This is a diamond-shaped diagram that gave the name to the corresponding formalism. Informally, in order to extend S to a Gröbner basis, one must look for ambiguities and, in case two different reductions lead to two different reduced expressions of the same element, we adjoin the difference of those reduced expressions to S ("resolve the ambiguity"), making the new set a more plausible candidate for a Gröbner basis. In other words, "to compute a Gröbner basis, one must ensure that all rewriting diagrams close up into diamonds".

Definition 2.4.1.1 (S-polynomial)**.** Let $g_1, g_2 \in T(X)$ be two monic polynomials. Assume that for some monomials u_1, u_2, v which are all different from 1, we have $\text{LM}(g_1) = u_1 v$ and $\text{LM}(g_2) = v u_2$. (This means that $\text{LM}(g_1)$ and $\text{LM}(g_2)$ are not proper divisors of each other, and that a terminal segment of the former is equal to an initial segment of the latter.) In this case we say that $\text{LM}(g_1)$ and $\text{LM}(g_2)$ have an *overlap* v; we call the element $\text{LM}(g_1)u_2 = u_1 v u_2 = u_1 \text{LM}(g_2)$ a *small common multiple* of $\text{LM}(g_1)$ and $\text{LM}(g_2)$. We call the element

$$S_v(g_1, g_2) := g_1 u_2 - u_1 g_2,$$

an *S-polynomial* of g_1 and g_2; the common leading term cancels, since both g_1 and g_2 are monic. Note that S-polynomials depend not only on g_1 and g_2, but on v as well, since in some cases there are several different small common multiples; we chose the notation to reflect that.

Remark 2.4.1.2. The word "small" in "small common multiple" is a way to emphasize that we only consider small common multiples where the occurrences of $\text{LM}(g_1)$ and $\text{LM}(g_2)$ do overlap. (Of course, there are other common multiples, for instance, the product of those two monomials.)

Sometimes S-polynomials are called "compositions" in the literature, however, we believe that this term has too many unnecessary connotations to be used here. Intuitively, an S-polynomial should be thought of as a "discrepancy between two different ways to reduce a small common multiple". Moreover, S-polynomials represent linear dependences of relations, often called "syzygies", which is one way to motivate the choice of letter.

Example 2.4.1.3. Consider $w_1 = a^2bcba$ and $w_2 = bacba^2$ in X^* where $X = \{a, b, c\}$:

- w_1 has a self-overlap: $w_1 = u_1 v = v u_2$ for $u_1 = a^2bcb$, $v = a$, $u_2 = abcba$.
- w_1 and w_2 overlap: $w_1 = u_1 v$, $w_2 = v u_2$ for $u_1 = a^2bc$, $v = ba$, $u_2 = cba^2$.
- w_2 and w_1 have overlaps of length 1 and length 2:
  - $w_2 = u_2 v$, $w_1 = v u_1$ for $u_2 = bacba$, $v = a$, $u_1 = abcba$.
  - $w_2 = u_2 v$, $w_1 = v u_1$ for $u_2 = bacb$, $v = a^2$, $u_1 = bcba$.

We will now prove the result which is at the core of most feasible ways to check that some subset of an ideal is a Gröbner basis. To state it, we need a definition.

Definition 2.4.1.4 (Parameter of a representation of an element)**.** Let $I = (G)$ be an ideal of $T(X)$. Consider the representation of an element $f \in I$ as a two-sided linear combination of elements $g_1, \ldots, g_N \in G$:

$$f = \sum_{i=1}^{N} a_i g_i b_i. \tag{2.2}$$

We will call $\max(\textsc{lm}(a_i g_i b_i))$ the *parameter* of such a linear combination.

If $f = S_v(g_1, g_2)$ is the S-polynomial of $g_1, g_2 \in G$ (with all the notation as above in Definition 2.4.1.1), then it has an obvious representation

$$f = g_1 u_2 - u_1 g_2,$$

with parameter $\textsc{lm}(g_1)u_2 = u_1 \textsc{lm}(g_2)$. We call a representation of that S-polynomial *nontrivial* if its parameter is smaller than $\textsc{lm}(g_1)u_2 = u_1 \textsc{lm}(g_2)$.

Theorem 2.4.1.5. *Let G be a self-reduced set of elements of $T(X)$, and let $I = (G)$. The following statements are equivalent:*

(i) *G is a Gröbner basis of I.*

(ii) *Every S-polynomial $S_v(g_1, g_2)$ has reduced form 0 with respect to G.*

(iii) *Every S-polynomial $S_v(g_1, g_2)$ admits a nontrivial representation as a two-sided linear combination of elements of G.*

(iv) *Every element $f \in I$ admits a representation as a two-sided linear combination of elements of G with parameter $\textsc{lm}(f)$.*

Remark 2.4.1.6. Conventionally, the equivalence (i) ⇔ (ii) is referred to as the diamond lemma. The implication (ii) ⇒ (i) is not at all easy to prove directly, so the proof introduces two auxiliary statements (iii) and (iv) for expository purposes.

Proof. We will prove the chain of implications (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (i).

(i) implies (ii): Note that each S-polynomial belongs to I, and each element of I has reduced form 0 with respect to G for a Gröbner basis.

(ii) implies (iii): If each S-polynomial has reduced form 0 with respect to G, we record all the steps of long division of $S_v(g_1, g_2)$ by G, and obtain a representation of the desired form.

(iii) implies (iv): This is the hardest part of the proof. Suppose the statement (iv) is not true for some $f \in T(X)$. If we drop the assumption on the parameter of the representation, then the statement is obvious, since $I = (G)$. Using bilinearity of products, we may expand the terms and only consider the combinations

$$f = \sum_{i=1}^{N} c_i m_i g_i m_i', \qquad c_i \in \mathbb{F}, \qquad m_i, m_i' \in X^*.$$

In general, $\text{LM}(f)$ may be less than $\max\limits_i(m_i \text{LM}(g_i)m_i')$ for such a combination because some leading terms may cancel. Suppose that for each representation of f of that form we have $\text{LM}(f) \prec \max\limits_i(m_i \text{LM}(g_i)m_i')$. Let us consider the "most economic counterexample"; in other words, we assume:

- that f does not have a representation of the form (2.2) with $\text{LM}(f) = \max\limits_i(m_i \text{LM}(g_i)m_i')$,
- that among the representations $f = \sum_{i=1}^N c_i m_i g_i m_i'$ for some N, some $m_i, m_i' \in X^*$, and some $g_i \in G$, we choose the one where the parameter $m = \max\limits_i(\text{LM}(m_i g_i m_i'))$ is the least possible;
- that among the representations with the chosen parameter m, the number of i for which $\text{LM}(m_i g_i m_i')$ is equal to m is the least possible.

Without the loss of generality, we have $\text{LM}(m_i g_i m_i') = m$ for $i = 1, \ldots, k$, and $\text{LM}(m_i g_i m_i') \prec m$ for $i > k$. Clearly, $k \geq 2$, in order for the leading monomials of this combination to cancel each other so that the resulting leading monomial is equal to $\text{LM}(f)$. We have

$$m_{k-1} \text{LM}(g_{k-1})m_{k-1}' = \text{LM}(m_{k-1}g_{k-1}m_{k-1}') = \\ \text{LM}(m_k g_k m_k') = m_k \text{LM}(g_k)m_k',$$

so both $\text{LM}(g_{k-1})$ and $\text{LM}(g_k)$ are divisors of m. Let us examine the relative position of those divisors. In general, given two different divisors of the same monomial, one may be a subword of the other, they may overlap, or they may be disjoint.

The first of these possibilities is especially easy to handle: since G is assumed self-reduced, this can only happen if $g_{k-1} = g_k$, and the subwords $\text{LM}(g_{k-1})$ and $\text{LM}(g_k)$ coincide. In this case, we also must have $m_{k-1} = m_k$ and $m_{k-1}' = m_k'$, and so the two terms $c_{k-1}m_{k-1}g_{k-1}m_{k-1}' + c_k m_k g_k m_k'$ can be merged into a single term $(c_{k-1} + c_k)m_{k-1}g_{k-1}m_{k-1}'$, resulting in a representation for f where either the parameter is smaller (that happens if $k = 2$ and $c_{k-1} + c_k = 0$) or the parameter is the same, but k is smaller, which is a contradiction.

Suppose that $\text{LM}(g_{k-1})$ and $\text{LM}(g_k)$ have an overlap inside m. Without loss of generality, we have $\text{LM}(g_{k-1}) = u_1 v$ and $\text{LM}(g_k) = v u_2$ for some monomials u_1, u_2, v with $v \neq 1$, so that

$$m_{k-1}u_1 v m_{k-1}' = m_{k-1} \text{LM}(g_{k-1})m_{k-1}' = m = m_k \text{LM}(g_k)m_k' = m_k v u_2 m_k'.$$

This implies that $m_k = m_{k-1}u_1$, and $m_{k-1}' = u_2 m_k'$. Recall the definition of the corresponding S-polynomial $S_v(g_{k-1}, g_k) = g_{k-1}u_2 - u_1 g_k$, which we will use in the form

$$u_1 g_k = g_{k-1}u_2 - S_v(g_{k-1}, g_k).$$

Let us examine the sum $c_{k-1}m_{k-1}g_{k-1}m'_{k-1} + c_k m_k g_k m'_k$:

$$\begin{aligned} &c_{k-1}m_{k-1}g_{k-1}u_2m'_k + c_k m_{k-1}u_1 g_k m'_k = \\ &\quad c_{k-1}m_{k-1}g_{k-1}u_2m'_k + c_k m_{k-1}(g_{k-1}u_2 - S_v(g_{k-1}, g_k))m'_k = \\ &\qquad (c_{k-1} + c_k)m_{k-1}g_{k-1}u_2m'_k - c_k m_{k-1}S_v(g_{k-1}, g_k)m'_k. \end{aligned} \tag{2.3}$$

We assumed that every S-polynomial has a nontrivial representation

$$S_v(g_{k-1}, g_k) = \sum_{i=1}^{N'} c'_i r_i g_i r'_i,$$

for some N', some $r_i, r'_i \in X^*$, and some $g_i \in G$, with

$$\max_i(\mathrm{LM}(r_i g_i r'_i)) \prec \mathrm{LM}(g_{k-1})u_2 = u_1\,\mathrm{LM}(g_k).$$

Substituting this into (2.3), we obtain

$$\begin{aligned} &c_{k-1}m_{k-1}g_{k-1}u_2m'_k + c_k m_{k-1}u_1 g_k m'_k = \\ &\qquad (c_{k-1} + c_k)m_{k-1}g_{k-1}u_2m'_k - c_k m_{k-1}\sum_{i=1}^{N'} c'_i r_i g_i r'_i m'_k. \end{aligned} \tag{2.4}$$

Replacing the terms $c_{k-1}m_{k-1}g_{k-1}u_2m'_k + c_k m_{k-1}u_1 g_k m'_k$ in the minimal counterexample by the right-hand side of (2.4), we obtain a representation for f where either the parameter is smaller (that happens if $k = 2$ and $c_{k-1} + c_k = 0$) or the parameter is the same, but k is smaller, which is a contradiction.

Suppose that $\mathrm{LM}(g_{k-1})$ and $\mathrm{LM}(g_k)$ are disjoint inside m. Without loss of generality, we have $m = u_1\,\mathrm{LM}(g_{k-1})v\,\mathrm{LM}(g_k)u_2$ for some monomials u_1, u_2, v, so that $m_{k-1} = u_1$, $m'_{k-1} = v\,\mathrm{LM}(g_k)u_2$, $m_k = u_1\,\mathrm{LM}(g_{k-1})v$, and $m'_k = u_2$. Let us transform the sum $c_{k-1}m_{k-1}g_{k-1}m'_{k-1}+c_k m_k g_k m'_k$, using the notation $g_{k-1} = \mathrm{LM}(g_{k-1}) + g'_{k-1}$ and $g_k = \mathrm{LM}(g_k) + g'_k$:

$$\begin{aligned} &c_{k-1}m_{k-1}g_{k-1}m'_{k-1} + c_k m_k g_k m'_k = c_{k-1}u_1 g_{k-1}v\,\mathrm{LM}(g_k)u_2 + \\ &c_k u_1\,\mathrm{LM}(g_{k-1})v g_k u_2 = c_{k-1}u_1 g_{k-1}v\,\mathrm{LM}(g_k)u_2 + c_k u_1(g_{k-1} - g'_{k-1})v g_k u_2 = \\ &\quad c_{k-1}u_1 g_{k-1}v\,\mathrm{LM}(g_k)u_2 + c_k u_1 g_{k-1}v(\mathrm{LM}(g_k) + g'_k)u_2 - c_k u_1 g'_{k-1}v g_k u_2 = \\ &\qquad (c_{k-1} + c_k)u_1 g_{k-1}v\,\mathrm{LM}(g_k)u_2 + c_k(u_1 g_{k-1}v g'_k u_2 - u_1 g'_{k-1}v g_k u_2), \end{aligned}$$

where the terms $c_k(u_1 g_{k-1}v g'_k u_2 - u_1 g'_{k-1}v g_k u_2)$ can be expanded as a linear combination of elements $m_i g_i m'_i$ with the leading monomial smaller than m. Therefore, as in the case of an overlap, we can merge two contributions to the leading monomial m at the cost of increasing the number of terms $m_i g_i m'_i$ with the smaller leading monomial, so we obtain a representation for f where either the parameter is smaller (that happens if $k = 2$ and $c_{k-1} + c_k = 0$) or the parameter is the same, but k is smaller. This contradiction completes the proof of the present implication.

(iv) implies (i): For such a representation of an element f, we have

$$\textsc{lm}(f) = \textsc{lm}(m_i g_i m_i') = m_i \, \textsc{lm}(g_i) m_i',$$

for some i, so $\textsc{lm}(f)$ is divisible by $\textsc{lm}(g_i)$. Since this is assumed true for every $f \in I$, it follows that G is a Gröbner basis. □

2.4.2 The Buchberger algorithm

Theorem 3.5.1.6 leads naturally to a recipe for computing reduced Gröbner bases: given a set of generators of an ideal, one has to compute all pairwise S-polynomials, adjoin all reduced forms of those to the set of generators, and repeat the same. It is rather a "recipe" than an algorithm since we are not guaranteed termination, but it is nevertheless very useful.

Algorithm 2.4.2.1 (Buchberger algorithm for noncommutative algebras)**.**

Input: A finite subset $G \subset T(X)$ generating an ideal $I \subset T(X)$.

Output: If terminates, the output is the reduced Gröbner basis of I.

```
• Set newSpolynomials ← true.
• While newSpolynomials do:
    – Convert the elements of $G$ to standard form.
    – Sort $G$ by glex order of leading monomials: $G = \{g_1, \dots, g_n\}$.
    – Compute the self-reduction of $G$.
    – Set Spolynomials ← $\varnothing$.
    – Set newSpolynomials ← false.
    – For $g \in G$ do for $h \in G$ do:
        ∗ If $\textsc{lm}(g)$ and $\textsc{lm}(h)$ have an overlap $w$ then:
            1. Define $u, v$ by $\textsc{lm}(g) = vw$ and $\textsc{lm}(h) = wu$.
            2. Set $s \leftarrow gu - vh$.
            3. Compute $t$, the result of long division of $s$ by $G$.
            4. If $t \neq 0$ and $t \notin$ Spolynomials then
                ∗ Set newSpolynomials ← true.
                ∗ Set Spolynomials ← Spolynomials $\cup \{t\}$.
    – Set $G \leftarrow G \cup$ Spolynomials.
• Return $G$.
```

Proposition 2.4.2.2. *If Algorithm 2.4.2.1 terminates then its output is the reduced Gröbner basis of I.*

Proof. Immediate corollary to Theorem 2.4.1.5. □

In many computations, instead of explicitly finding the standard form at each step, we will merely underline the leading monomial (which is being reduced).

Example 2.4.2.3. For the quantum plane from Example 2.1.1.3, the noncommutative Buchberger algorithm terminates instantly, since the only leading monomial (for `glex` order with $x_1 \prec x_2$) is x_2x_1 which has no self-overlaps.

Example 2.4.2.4. We consider the ideal $(y^2 + x^2)$ of the tensor algebra $T(x, y)$, and impose the `glex` order with $x \prec y$. The leading monomial y^2 has just one self-overlap: $y^2 \cdot y = y \cdot y^2$. The corresponding S-polynomial is

$$(y^2 + x^2)y - y(y^2 + x^2) = x^2y - yx^2.$$

It is already reduced with respect to $g_1 = y^2 + x^2$, and self-reduction just multiplies it by -1 to make it monic. The leading monomial yx^2 has no self-overlaps, and one overlap with y^2, namely $y^2 \cdot x^2 = y \cdot yx^2$. The corresponding S-polynomial is

$$(y^2 + x^2)x^2 - y(yx^2 - x^2y) = x^4 + yx^2y.$$

Reducing this with respect to $\{ g_1 = y^2 + x^2,\ g_2 = yx^2 - x^2y \}$ goes as follows:

$$x^4 + \underline{yx^2y} \xrightarrow{g_2} x^4 + \underline{x^2y^2} \xrightarrow{g_1} 0\,.$$

The symbol above each arrow is the element with respect to which we reduce, and the leading monomial is underlined. This means that there are no new elements to adjoin, and the algorithm terminates. Therefore, the reduced Gröbner basis for $(y^2 + x^2)$ consists of the elements $y^2 + x^2$ and $yx^2 - x^2y$.

Example 2.4.2.5. Let us consider the algebra $\mathbb{F}[x_1, x_2, x_3]$ of polynomials in three variables, viewed as the quotient of $T(x_1, x_2, x_3)$ by the commutator ideal

$$(\ x_2x_1 - x_1x_2,\ x_3x_1 - x_1x_3,\ x_3x_2 - x_2x_3\ ).$$

The leading monomials (for `glex` order with $x_1 \prec x_2 \prec x_3$) of these elements are x_2x_1, x_3x_1, and x_3x_2, with the only overlap corresponding to the common multiple $x_3x_2x_1$ of the first and last monomials. The corresponding S-polynomial is

$$(x_3x_2 - x_2x_3)x_1 - x_3(x_2x_1 - x_1x_2) = x_3x_1x_2 - x_2x_3x_1.$$

We compute the reduced form of this element, underlining the leading monomials:

$$\underline{x_3x_1x_2} - x_2x_3x_1 \longrightarrow x_1x_3x_2 - \underline{x_2x_3x_1} \longrightarrow x_1x_3x_2 - \underline{x_2x_1x_3} \longrightarrow \\ \underline{x_1x_3x_2} - x_1x_2x_3 \longrightarrow 0.$$

Therefore, our set of relations forms a Gröbner basis. We will see a very sophisticated generalization of this example in Theorem 2.5.3.1 below.

2.4.3 Triangle lemma

Definition 2.4.3.1 (Essential overlap)**.** Let G be a self-reduced subset of $T(X)$, and let $g_1, g_2 \in G$ be two elements for which $\textsc{lm}(g_1) = u_1v$ and $\textsc{lm}(g_2) = vu_2$ have an overlap $v \neq 1$. We call this overlap *essential* if u_1v and vu_2 are the only two subwords of u_1vu_2 which belong to $\textsc{lm}(G)$.

The term "essential" that we use is somewhat justified by the following result.

Proposition 2.4.3.2 (Triangle lemma, [252])**.** *Let G be a self-reduced subset of $T(X)$, and let $g_1, g_2 \in G$ be two elements for which $\textsc{lm}(g_1) = u_1v$ and $\textsc{lm}(g_2) = vu_2$ have an overlap $v \neq 1$. Suppose that this overlap is not essential, so that there exists $g_3 \in G$ for which $\textsc{lm}(g_3)$ is a divisor of u_1vu_2 different from u_1v and vu_2. Then:*

- *The divisors u_1v and $\textsc{lm}(g_3)$ have an overlap $v' \neq 1$, and the divisors $\textsc{lm}(g_3)$ and vu_2 have an overlap $v'' \neq 1$.*
- *If the S-polynomials $S_{v'}(g_1, g_3)$ and $S_{v''}(g_3, g_2)$ admit nontrivial representations as two-sided linear combinations of elements of G, then the S-polynomial $S_v(g_1, g_2)$ also admits a nontrivial representation.*

Proof. Note that since G is assumed self-reduced, $\textsc{lm}(g_3)$ cannot be a subword of either $\textsc{lm}(g_1)$ or $\textsc{lm}(g_2)$. Therefore, it has an overlap with both $\textsc{lm}(g_1)$ and $\textsc{lm}(g_2)$. This means that u_1vu_2 can be factorized as $u_1vu_2 = u_1'u_1''vu_2'u_2''$, where

$$u_1'u_1''v = \textsc{lm}(g_1), \quad u_1''vu_2' = \textsc{lm}(g_3), \quad vu_2'u_2'' = \textsc{lm}(g_2),$$

$u_1'' \neq 1$, $u_2' \neq 1$, the small common multiple of $\textsc{lm}(g_1)$ and $\textsc{lm}(g_3)$ is $v' = u_1''v$, and the small common multiple of $\textsc{lm}(g_3)$ and $\textsc{lm}(g_2)$ is $v'' = vu_2'$. Therefore,

$$S_v(g_1, g_2) = g_1u_2 - u_1g_2 = g_1u_2'u_2'' - u_1'u_1''g_2 = \\ g_1u_2'u_2'' - u_1'g_3u_2'' + u_1'g_3u_2'' - u_1'u_1''g_2 = S_{v'}(g_1, g_3)u_2'' + u_1'S_{v''}(g_3, g_2).$$

Note that multiplying a nontrivial representation for the S-polynomial $S_{v'}(g_1, g_3)$ by u_2'' on the right, we get a two-sided linear combination with parameter less than $u_1'u_1''vu_2'u_2''$, and the same is true if we multiply a nontrivial representation for the S-polynomial $S_{v''}(g_3, g_2)$ by u_1' on the left. This completes the proof. □

This proposition has an immediate corollary which prevents unnecessary computations when testing or computing the reduced Gröbner basis.

Corollary 2.4.3.3. *Let G be a self-reduced set of elements of $T(X)$.*

(i) If each S-polynomial of two elements of G corresponding to an essential overlap has reduced form 0 *with respect to G, then G is the reduced Gröbner basis of (G).*

(ii) While computing the reduced Gröbner basis using Algorithm 2.4.2.1, we may ignore all non-essential overlaps.

The Triangle Lemma seems to be better known to specialists in commutative Gröbner bases, where it is called "Buchberger's second criterion" [153, 44]. Lecture notes [167], that in principle discuss the noncommutative case, only mention this result for commutative Gröbner bases. The only source we are aware of where this result is mentioned in the noncommutative case is the survey [252]. We believe that this result deserves to be known much better in the noncommutative case, since it provides an important shortcut for otherwise tedious computations.

2.5 Examples of Gröbner bases and their applications

2.5.1 Dimensions and Hilbert series of algebras

One of the first natural questions about a vector space is to determine its dimension. For a finite-dimensional vector space, the dimension is a good measure of the "size" of a space; if a vector space is infinite-dimensional, it is still beneficial to look for some way to know "how big" it is. In the case of algebras presented by generators and relations, there is a standard way to introduce some measures.

Definition 2.5.1.1 (Hilbert series)**.** Let $A = T(X)/I$ be an algebra presented by generators and relations. The number of normal monomials modulo I of the given weight k is denoted by $n_k(A)$. The *Hilbert series* of A, denoted $h_A(t)$, is the generating function defined by the following equation:

$$h_A(t) := \sum_{k\geq 0} n_k(A)t^k.$$

Remark 2.5.1.2. An important class of algebras are algebras with homogeneous relations, that is, relations $f = 0$, where all monomials of $\mathrm{supp}(f)$ are of the same weight. For an algebra with homogeneous relations, the weight of each element is well defined, and $n_k(A)$ is the dimension of A_k, the weight k homogeneous component of A. If relations are not homogeneous, the numbers $n_k(A)$ may depend on the monomial order Ξ, but still may be useful to study the algebra A.

One of the most important results that allows us to deal with Hilbert series is based on an elegant combinatorial construction of Ufnarovski which we will now outline. The next definition and the two statements that follow first appeared in [249], see also [251].

Definition 2.5.1.3 (Graph of normal forms)**.** Let $A = T(X)/I$ be an algebra presented by generators and relations, and suppose that I has a finite Gröbner basis $G = \{g_1, \dots, g_m\}$. Let $\ell = \max_i \mathrm{wt}(\textsc{lm}(g_i))$; we denote by V the set of all monomials of weight $\ell - 1$ that are reduced with respect to G. Let us define a directed graph Γ, called the *graph of normal forms*. The vertex set of Γ is V; two vertices $v', v'' \in V$ are connected by a directed edge $v' \to v''$ if and only if there exist $x', x'' \in X$ for which $v'x' = x''v''$ is reduced with respect to G. Thus, edges of Γ correspond to monomials of weight ℓ that are reduced with respect to G.

Proposition 2.5.1.4. *There exists a bijection between the monomials of weight $w \geq \ell - 1$ that are reduced with respect to G and directed paths of length $w - \ell + 1$ in the graph Γ.*

Proof. Each monomial $x_{i_1} \cdots x_{i_w}$ of weight $w \geq \ell - 1$ that is reduced with respect to G corresponds to the directed path

$$u_1 \to u_2 \to \cdots \to u_{w-\ell+1},$$

where $u_p = x_{i_p} \cdots x_{i_{\ell-1+p}}$. □

Theorem 2.5.1.5. *Let $A = T(X)/I$ be an algebra presented by generators and relations, and suppose that I has a finite Gröbner basis. Then the Hilbert series $h_A(t)$ is a rational function.*

Proof. By Proposition 2.5.1.4, if we denote by $f_\Gamma(t)$ the generating function for the numbers of directed paths in Γ enumerated by length, we have

$$h_A(t) = n_0(A) + n_1(A)t + \cdots + n_{\ell-2}(A)t^{\ell-2} + t^{\ell-1} f_\Gamma(t),$$

so it is enough to prove that $f_\Gamma(t)$ is a rational function. That latter statement is true for any finite directed graph Γ, and is established as follows. We define a square matrix M_Γ of size $|V| \times |V|$, whose entry m_{ij} is equal to the number of arrows from v_i to v_j. Then for each w the entry in the row i and column j of the matrix M_Γ^w is the number of directed paths of length w from v_i to v_j, and the total number of paths is equal to the sum of all matrix elements, that is, $eM_\Gamma^w e^T$, where $e = [1, 1, \dots, 1]$. Note that by Cayley–Hamilton theorem, we have, for $k = |V|$,

$$M_\Gamma^k = \sum_{i=0}^{k-1} c_i M_\Gamma^i$$

with some scalars c_i, which implies a recurrence relation for powers

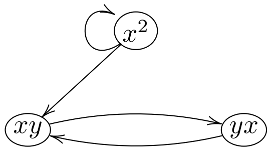
$$M_\Gamma^{k+N} = \sum_{i=0}^{k-1} c_i M_\Gamma^{i+N},$$

and the same recurrence relation for the numbers of directed paths. It follows that the corresponding generating function is rational, which completes the proof. □

Example 2.5.1.6. Consider the ideal $(y^2 + x^2) \subset T(x, y)$, and use the `glex` order with $x \prec y$. The reduced Gröbner basis is

$$G = \{y^2 + x^2, yx^2 - x^2y\},$$

as we saw in Example 2.4.2.4. The leading monomials of G are y^2 and yx^2. Therefore, $\ell = 3$, and $V = \{x^2, xy, yx\}$. The graph Γ is as follows:



From this, we can immediately read the matrix M_Γ:

$$M_\Gamma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

with the characteristic polynomial $t^3 - t^2 - t + 1$, so

$$M_\Gamma^3 = M_\Gamma^2 + M_\Gamma - I_3.$$

Since the sequence for numbers of directed paths satisfies the recurrence relation whose coefficients are the coefficients of the characteristic polynomial, and starts with 3 (the number of vertices), 4 (the number of edges), 5 (the number of paths of length 2), it continues with $6 = 5 + 4 - 3$, $7 = 6 + 5 - 4$, etc. Thus, the Hilbert series of the algebra $T(x, y)/(y^2 + x^2)$ is

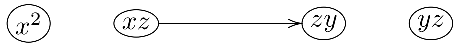
$$1 + 2t + 3t^2 + 4t^3 + \cdots = \frac{1}{(1-t)^2}.$$

Interestingly, it is the same as the Hilbert series of the algebra of commutative polynomials, that is the quotient by the ideal $(xy - yx)$, even though the normal monomials for the two algebras have completely different combinatorics (for any monomial ordering).

Example 2.5.1.7. Let us consider the ideal $I = (xy - z, yz - x, zx - y)$ in $T(x, y, z)$. A computation of the reduced Gröbner basis of I for the `glex` order with $x \prec y \prec z$ gives the following set of 10 elements:

$$xy - z, \quad yz - x, \quad zx - y, \quad y^2 - x^2, \quad z^2 - x^2,$$
$$x^3 - zy, \quad x^2z - yx, \quad yx^2 - xz, \quad yxz - xzy, \quad zyx - xzy.$$

The maximal weight of a leading monomial ℓ is 3, so $V = \{x^2, xz, zy, yz\}$, and the graph of normal forms is



We conclude that the set of reduced monomials is finite, and consists of 9 elements $1, x, y, z, x^2, xz, zy, yx, xzy$. An interesting remark made in [252] is that if we forget about the normal word 1, and view the equations $xy = z$, $yz = x$, $zx = y$ as defining relations of a semigroup (rather than monoid), we can easily conclude that the given relations give a presentation of Q_8 as a semigroup by generators and relations. (There is a natural surjective map from this semigroup to the quaternion group Q_8 sending x, y, z to i, j, k respectively.)

2.5.2 The group algebra of the symmetric group

In this subsection we discuss how noncommutative Gröbner bases can be used to construct matrix representations of finite semigroups. The most important example is of course the symmetric group S_n of all permutations of $\{1, \ldots, n\}$. The $n-1$ standard generating transpositions will be denoted $x_i = (i, i+1)$ for $i = 1, \ldots, n-1$. They satisfy these standard relations:

$$\begin{cases} x_i^2 = 1 \qquad (1 \leq i \leq n-1) \\ x_i x_j = x_j x_i \qquad (1 \leq i < i+1 \leq j-1 < j \leq n-1) \\ x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \qquad (1 \leq i \leq n-2) \end{cases} \tag{2.5}$$

We write these relations as $f - g = 0$ instead of $f = g$. The first three nontrivial cases are as follows, avoiding subscripts:

2	$a^2 - 1 = 0$		
3	$a^2 - 1 = 0$ $b^2 - 1 = 0$	$aba - bab = 0$	
4	$a^2 - 1 = 0$ $b^2 - 1 = 0$ $c^2 - 1 = 0$	$aba - bab = 0$ $bcb - cbc = 0$	$ac - ca = 0$

We fix a field $\mathbb{F}$, arbitrary for the moment, and consider the tensor algebra $P_n = T(x_1, \ldots, x_{n-1})$. For each $n \geq 2$ we consider the two-sided ideal $I_n \subset P_n$ generated by the standard relations (2.5). We write G_n for the `glex` Gröbner basis of I_n; see Figure 2.1. In general the size of this Gröbner basis is $n^2 - 3n + 3$; see [37].

For all n, there are only finitely many normal words with respect to the Gröbner basis G_n, and so the quotient ring P_n/I_n is finite dimensional; in fact $\dim(P_n/I_n) = n!$. Moreover, $P_n/I_n \cong \mathbb{F}S_n$ as associative algebras: the quotient ring is isomorphic to the group algebra. To work out the multiplication table, we compute the normal forms of the products of the normal words.

$n = 2$	$n = 3$	$n = 4$
$a^2 - 1$	$a^2 - 1$	$a^2 - 1$
	$b^2 - 1$	$b^2 - 1$
	$bab - aba$	$ca - ac$
		$c^2 - 1$
		$bab - aba$
		$cbc - bcb$
		$cbac - bcba$

FIGURE 2.1: The `glex` Gröbner bases for standard relations of S_n ($n = 2, 3, 4$).

We then use algorithms for the Wedderburn decomposition [40] to determine the structure of the group algebra, and from this we can obtain the character table and the representation matrices.

We will determine explicitly the structure for $n = 3$, and leave the case $n = 4$ to the reader (Exercise 2.8). For $n = 3$, the normal words are $1, a, b, ab, ba, aba$ and the multiplication table is as follows, using the Gröbner basis $a^2 = 1$, $b^2 = 1$, $bab = aba$ from Figure 2.1:

	1	a	b	ab	ba	aba
1	1	a	b	ab	ba	aba
a	a	1	ab	b	aba	ba
b	b	ba	1	aba	a	ab
ab	ab	aba	a	ba	1	b
ba	ba	b	aba	1	ab	a
aba	aba	ab	ba	a	b	1

(2.6)

This is just the multiplication table for S_3, written in terms of the transpositions $a = (12)$ and $b = (23)$, and regarded as a monomial basis of $\mathbb{F}S_3$. At this point we apply the computational structure theory of finite dimensional associative algebras:

1. Compute the integral $n! \times n!$ Dickson matrix Δ, which is invertible if and only if the group algebra is semisimple. The radical of the group algebra is the nullspace of Δ, and the primes p dividing $\det(\Delta)$ are exactly those for which the group algebra is not semisimple in characteristic p.

2. Factoring out the radical (if necessary), we are left with a semisimple algebra, and we can easily determine its center using linear algebra.

3. The center is a commutative semisimple algebra, and we can decompose it into a direct product of fields using a splitting algorithm based on the Chinese Remainder Theorem. This gives a basis for the center consisting of orthogonal primitive idempotents.

4. We lift these central basis elements back to the full algebra and determine the corresponding simple two-sided ideals.

5. Each simple two-sided ideal is isomorphic to a full matrix algebra; it is in theory extremely difficult in general, but in practice usually quite easy, to construct an explicit isomorphism, which gives us the matrix units.

6. From this we recover the representation matrices for all the permutations in S_n and all partitions of n (which are in bijection with the simple ideals).

We summarize the details of this procedure in the case $n = 3$.

Part (1). To recover the Dickson matrix from the multiplication table (2.6), we replace the elements by their index numbers, writing μ_{ij} for the i, j entry:

$$
\begin{array}{c|cccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
1 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 2 & 1 & 4 & 3 & 6 & 5 \\
3 & 3 & 5 & 1 & 6 & 2 & 4 \\
4 & 4 & 6 & 2 & 5 & 1 & 3 \\
5 & 5 & 3 & 6 & 1 & 4 & 2 \\
6 & 6 & 4 & 5 & 2 & 3 & 1
\end{array}
\tag{2.7}
$$

The entries of the Dickson matrix Δ are defined by this general equation which applies to all semigroups:

$$\Delta_{ij} = |\{\, k \mid \mu(\mu(j,i),k)) = k \}| \, .$$

In the case of groups, Δ_{ij} equals the number of g_k for which $(g_j g_i) g_k = g_k$, and cancellation gives $g_j g_i = 1$; thus for S_n we have $\Delta_{ij} = n!$ if $g_i g_j = 1$ and 0 otherwise. For $n = 3$, we obtain

$$
\Delta = \begin{bmatrix}
6 & 0 & 0 & 0 & 0 & 0 \\
0 & 6 & 0 & 0 & 0 & 0 \\
0 & 0 & 6 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 6 & 0 \\
0 & 0 & 0 & 6 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 6
\end{bmatrix}
\qquad\qquad \det(\Delta) = -2^6 3^6
$$

If we avoid characteristics 2 and 3, the group algebra $\mathbb{F}S_3$ will be semisimple, and we make this assumption from now on.

Part (2). To find the center Z of $\mathbb{F}S_3$, we apply some linear algebra to (2.7). Consider an element $X \in \mathbb{F}S_3$; then X is central if and only if $Xg - gX = 0$ for all $g \in S_3$, and this gives a homogeneous system of linear equations in $n!$ variables. Solving these equations produces the following basis elements for $Z(\mathbb{F}S_3)$, which are the sums over the conjugacy classes (identity, transpositions, 3-cycles):

$$f_1 = 1, \qquad\qquad f_2 = a + b + aba, \qquad\qquad f_3 = ab + ba.$$

We now have to find a new basis of the center consisting of orthogonal primitive idempotents. It will be useful to have the multiplication table for the center:

$$f_2^2 = 1 + ab + ba + ba + 1 + ab + ab + ba + 1 = 3f_1 + 3f_3,$$

$$f_2f_3 = b + aba + aba + a + a + b = 2f_2, \qquad f_3^2 = ba + 1 + 1 + ab = 2f_1 + f_3$$

The multiplication table is therefore

$$\begin{array}{c|ccc} & f_1 & f_2 & f_3 \\ \hline f_1 & f_1 & f_2 & f_3 \\ f_2 & f_2 & 3f_1 + 3f_3 & 2f_2 \\ f_3 & f_3 & 2f_2 & 2f_1 + f_3 \end{array} \tag{2.8}$$

Part (3). Choose a non-identity central basis element, say f_2, and compute its minimal polynomial. Using (2.8) we obtain

$$f_2^3 = 9f_2 \implies f_2^3 - 9f_2 = 0 \implies f_2(f_2 - 3f_1)(f_2 + 3f_1) = 0.$$

which splits over $\mathbb{Q}$ as expected. We have $f_2^2 - 9f_1 = -3(2f_1 - f_3)$. Since the ideals $I_1 = (2f_1 - f_3)$ and $I_2 = (f_2)$ and have coprime generators, we have $I_1 \cap I_2 = \{0\}$ and $I_1I_2 = \{0\}$, so there is an orthogonal direct sum $Z = I_1 \oplus I_2$. It is easy to check that I_1 is 1-dimensional:

$$(2f_1 - f_3)^2 = 4f_1 - 4f_3 + f_3^2 = 4f_1 - 4f_3 + 2f_1 + f_3 = 3(2f_1 - f_3).$$

This gives the primitive idempotent

$$g_1 = \tfrac{1}{3}(2f_1 - f_3).$$

It remains to split I_2. Since I_2 is the orthogonal complement of I_1, we find a basis by solving this equation:

$$0 = (2f_1 - f_3)(af_1 + bf_2 + cf_3) = (a - c)(2f_1 - f_3).$$

Thus the elements of I_2 have the form $af_1 + bf_2 + af_3$ and we can take $\{\, f_1 + f_3,\ f_2 \,\}$ as a basis. (In this particular case, the same could be observed by inspection of the second column of (2.8)). To continue, we need to find the identity element e in this ideal; solving the equations $e(f_1 + f_3) = f_1 + f_3$, $ef_2 = f_2$, and $e^2 = e$, we obtain $e = \frac{1}{3}(f_1 + f_3)$. From (2.8), we see that $f_2^2 = 9e$, so the two remaining primitive idempotents are

$$g_2 = \tfrac{1}{2}(e + \tfrac{1}{3}f_2) = \tfrac{1}{6}(f_1 + f_2 + f_3), \qquad g_3 = \tfrac{1}{2}(e - \tfrac{1}{3}f_2) = \tfrac{1}{6}(f_1 - f_2 + f_3).$$

We renumber these idempotents for reasons which will soon be clear:

$$h_1 = \tfrac{1}{6}(f_1 + f_2 + f_3), \qquad h_2 = \tfrac{1}{3}(2f_1 - f_3), \qquad h_3 = \tfrac{1}{6}(f_1 - f_2 + f_3)$$

Part (4). We first rewrite these central idempotents using the original basis of coset representatives:

$$\begin{aligned} h_1 &= \tfrac{1}{6}(1 + a + b + ab + ba + aba), \\ h_2 &= \tfrac{1}{3}(2 - ab - ba), \\ h_3 &= \tfrac{1}{6}(1 - a - b + ab + ba - aba). \end{aligned}$$

The meaning of these equations becomes immediately obvious if we remember that $a = (12)$ and $b = (23)$ and write permutations using cycle notation:

$$\begin{aligned} h_1 &= \tfrac{1}{6}(() + (12) + (23) + (123) + (132) + (13)), \\ h_2 &= \tfrac{1}{3}\Big(2() - (123) - (132)\Big), \\ h_3 &= \tfrac{1}{6}(() - (12) - (23) + (123) + (132) - (13)). \end{aligned}$$

The permutations naturally appear in `lex` order: 123, 132, 213, 231, 321, 321. It is now straightforward to verify that h_1 and h_3 generate 1-dimensional simple two-sided ideals in $\mathbb{F}S_3$, whereas h_2 generates a 4-dimensional simple two-sided ideal.

Part (5). In this example, the only remaining nontrivial step is to find an explicit isomorphism $(h_2) \cong M_2(\mathbb{F})$, and this is left as an exercise for the reader. This can usually be accomplished by trial and error. But in theory, we have the following problem.

Problem 2.5.2.1. Let A be an associative algebra over $\mathbb{F}$ of dimension n^2 given by a basis $a_1, \dots, a_{n^2}$ and structure constants

$$a_i a_j = \sum_{k=1}^{n^2} c_k^{(i,j)} a_k \qquad (1 \le i, j, k \le n^2).$$

Assume that $A \cong M_n(\mathbb{F})$, the algebra of $n \times n$ matrices over $\mathbb{F}$. Determine explicitly a basis of A consisting of elements e_{ij} $(1 \le i, j \le n)$ corresponding to matrix units:

$$e_{ij} e_{k\ell} = \delta_{jk} e_{i\ell} \qquad (1 \le i, j, k, \ell \le n).$$

That is, the linear isomorphism $A \cong M_n(\mathbb{F})$ induced by the correspondence $e_{ij} \mapsto E_{ij}$ must be an isomorphism of algebras.

Solving this problem is equivalent to finding a minimal left ideal in A: a subspace of “column vectors” on which A can act by (left) “matrix-vector” multiplication. However, finding minimal left ideals can be surprisingly difficult. In fact, the best-known algorithms for this problem, when $\mathbb{F}$ is an algebraic number field, achieve polynomial time only because they are allowed to call oracles for factoring integers and factoring univariate polynomials over finite fields [139].

2.5.3 Universal enveloping algebras of Lie algebras

Theorem 2.5.3.1 (Poincaré–Birkhoff–Witt (PBW) theorem)**.** *If L is a finite dimensional Lie algebra over a field F with a totally ordered basis $X = \{x_1, \dots, x_n\}$, then a basis of its universal associative enveloping algebra $U(L)$ consists of the monomials $x_1^{e_1} \cdots x_n^{e_n}$ with $e_1, \dots, e_n \geq 0$. Therefore:*

(i) $U(L)$ is infinite dimensional.

(ii) The canonical map $\alpha\colon L \to U(L)$ is injective.

(iii) L is isomorphic to a subalgebra of the Lie algebra $U(L)^-$.

Proof. By Definition 2.1.1.2, the algebra $U(L)$ is a quotient of $T(L) \cong T(X)$. We equip $T(X)$ with the `glex` order with $x_1 \prec \cdots \prec x_n$. Since both the Lie bracket and the product in $T(L) \cong T(X)$ are bilinear, it is sufficient to take x, y in Definition 2.1.1.2 to be basis elements, so the universal associative envelope $U(L)$ is the quotient of the free associative algebra $T(X)$ by the ideal I generated by the elements

$$g_{ij} = x_i x_j - x_j x_i - [x_i, x_j] = x_i x_j - x_j x_i - \sum_{k=1}^{n} c_{ij}^k x_k,$$

where the last equation defines the set of scalars c_{ij}^k, the structure constants of L. Note that due to anticommutativity of the Lie bracket we have $g_{ii} = 0$, and for $i \neq j$ we may assume $i > j$, and hence $x_i x_j$ is the leading monomial of g_{ij}.

We will show that the set $G = \{\, g_{ij} \mid 1 \leq j < i \leq n \,\}$ is the reduced Gröbner basis for I. Consider two leading monomials, $\textsc{lm}(g_{ij}) = x_i x_j$ $(i > j)$ and $\textsc{lm}(g_{\ell k}) = x_\ell x_k$ $(\ell > k)$. The only possible overlaps of these monomials occur when either $j = \ell$ or $k = i$. Without loss of generality, $j = \ell$, so we consider g_{ij} and g_{jk} where $i > j > k$. We have $\textsc{lm}(g_{ij})\, x_k = x_i x_j x_k = x_i \, \textsc{lm}(g_{jk})$, which produces the S-polynomial

$$\begin{aligned} g_{ij} x_k - x_i g_{jk} &= \big(x_i x_j - x_j x_i - [x_i, x_j]\big) x_k - x_i \big(x_j x_k - x_k x_j - [x_j, x_k]\big) \\ &= x_i x_j x_k - x_j x_i x_k - [x_i, x_j] x_k - x_i x_j x_k + x_i x_k x_j + x_i [x_j, x_k] \\ &= -x_j x_i x_k - [x_i, x_j] x_k + x_i x_k x_j + x_i [x_j, x_k] \\ &= x_i x_k x_j - x_j x_i x_k - [x_i, x_j] x_k + x_i [x_j, x_k]. \end{aligned}$$

(It is convenient to avoid explicit structure constants in this calculation; recall that $[x_i, x_j]$ is a homogeneous polynomial of weight 1.) This element is not reduced; both its leading monomial $x_i x_k x_j$ and the non-leading monomial $x_j x_i x_k$ are divisible by $x_i x_k = \textsc{lm}(g_{ik})$. To reduce those, we subtract $g_{ik} x_j$ and add $x_j g_{ik}$:

$$\begin{aligned} &x_i x_k x_j - x_j x_i x_k - [x_i, x_j] x_k + x_i [x_j, x_k] \\ &\quad - \big(x_i x_k - x_k x_i - [x_i, x_k]\big) x_j + x_j \big(x_i x_k - x_k x_i - [x_i, x_k]\big) \end{aligned}$$

$$\begin{aligned}
&= x_i x_k x_j - x_j x_i x_k - [x_i, x_j] x_k + x_i [x_j, x_k] \\
&\quad - x_i x_k x_j + x_k x_i x_j + [x_i, x_k] x_j + x_j x_i x_k - x_j x_k x_i - x_j [x_i, x_k] \\
&= -[x_i, x_j] x_k + x_i [x_j, x_k] + x_k x_i x_j + [x_i, x_k] x_j - x_j x_k x_i - x_j [x_i, x_k] \\
&= -x_j x_k x_i + x_k x_i x_j - [x_i, x_j] x_k + x_i [x_j, x_k] + [x_i, x_k] x_j - x_j [x_i, x_k].
\end{aligned}$$

We see that the leading monomial $x_j x_k x_i$ is divisible by $x_j x_k = \textsc{lm}(g_{jk})$, and that the other monomial of weight 3 is divisible by $x_i x_j = \textsc{lm}(g_{ij})$. To reduce those, we add $g_{jk} x_i$ and subtract $x_k g_{ij}$:

$$\begin{aligned}
&- x_j x_k x_i + x_k x_i x_j - [x_i, x_j] x_k + x_i [x_j, x_k] + [x_i, x_k] x_j - x_j [x_i, x_k] \\
&\quad + \big(x_j x_k - x_k x_j - [x_j, x_k]\big) x_i - x_k \big(x_i x_j - x_j x_i - [x_i, x_j]\big) \\
&= -x_j x_k x_i + x_k x_i x_j - [x_i, x_j] x_k + x_i [x_j, x_k] + [x_i, x_k] x_j - x_j [x_i, x_k] \\
&\quad + x_j x_k x_i - x_k x_j x_i - [x_j, x_k] x_i - x_k x_i x_j + x_k x_j x_i + x_k [x_i, x_j] \\
&= -[x_i, x_j] x_k + x_i [x_j, x_k] + [x_i, x_k] x_j - x_j [x_i, x_k] - [x_j, x_k] x_i + x_k [x_i, x_j] \\
&= x_i [x_j, x_k] - [x_j, x_k] x_i + x_j [x_k, x_i] - [x_k, x_i] x_j + x_k [x_i, x_j] - [x_i, x_j] x_k.
\end{aligned}$$

The last expression, once the brackets are expanded in structure constants, and all the quadratic leading monomials are reduced, has the reduced form $[x_i, [x_j, x_k]] + [x_j, [x_k, x_i]] + [x_k, [x_i, x_j]]$, which is zero by the Jacobi identity. Thus every S-polynomial has reduced form zero, proving that we have a Gröbner basis. The leading monomials of this Gröbner basis are $x_i x_j$ where $i > j$. A basis for $U(L)$ consists of all monomials w which are not divisible by any of these. That is, if w contains a subword $x_i x_j$ then $i \leq j$. It follows that the monomials in the statement of the theorem form a basis for $U(L)$. In particular, the monomials $x_1, \ldots, x_n$ of degree 1 are linearly independent in $U(L)$, and hence the canonical map from L to $U(L)$ is injective. □

Corollary 2.5.3.2. *Every polynomial identity satisfied by the Lie bracket in every associative algebra is a consequence of anticommutativity and the Jacobi identity.*

Proof. If $p(a_1, \ldots, a_n) \equiv 0$ is a polynomial identity which is not a consequence of anticommutativity and the Jacobi identity, then $p(a_1, \ldots, a_n)$ is a nonzero element of the free Lie algebra L generated by $\{a_1, \ldots, a_n\}$. If A is any associative algebra, and $\epsilon\colon L \to A^-$ is any morphism of Lie algebras, then by definition of polynomial identity, $\epsilon(p) = 0$. If we take $A = U(L)$ and let ϵ be the injective map $L \to U(L)^-$ from the PBW theorem, then $p \neq 0$ implies $\epsilon(p) \neq 0$, a contradiction. □

The proof of the Poincaré–Birkhoff–Witt theorem that we presented here is due to [21, 24]. It is deemed by many people to be one of the most remarkable early theoretical applications of Gröbner bases in ring theory. It is important to emphasize that our proof only works for Lie algebras over a field (the assumption that we made that the Lie algebra is finite-dimensional is not essential). For Lie algebras over commutative rings our approach would not work, but the PBW theorem does not hold in general over every commutative unital ring anyway; there are counterexamples in the papers [51, 62, 170, 231], see also Exercise 2.9. A Gröbner bases-driven approach to Lie algebras over rings can come from developing a theory of Gröbner bases for ideals in the algebra $\mathbb{F}[x_1, \dots, x_n] \otimes T(y_1, \dots, y_m)$, see [198], or from developing a theory of Gröbner–Shirshov bases for Lie algebras over rings, see [27]. The reader interested in the history of the PBW theorem is referred to [39, 122, 125, 248].

Two-dimensional solvable Lie algebra. The PBW theorem shows that for every Lie algebra L, the ideal generators obtained from the structure constants form a Gröbner basis. These generators can be interpreted as rewriting rules in $U(L)$ as follows:

$$x_i x_j - x_j x_i - \sum_{k=1}^{n} c_{ij}^k x_k \in I \qquad \Longleftrightarrow \qquad x_i x_j = x_j x_i + \sum_{k=1}^{n} c_{ij}^k x_k \in U(L).$$

Repeated application of these rules allows us to work out multiplication formulas for monomials in $U(L)$. Let us demonstrate how this is done on an example of the 2-dimensional solvable Lie algebra, that is the Lie algebra L with a basis $\{a, b\}$ for which $[a, b] = b$.

The basis of its universal enveloping algebra $U(L)$ from the PBW theorem consists of the monomials $a^r b^s$ for $r, s \geq 0$. The ideal I is generated by $ab - ba - b$, and so for the ordering $a \prec b$ the element ba is the leading monomial; it has no self-overlaps, so it forms the reduced Gröbner basis.

In $U(L)$ we have $ba = ab - b = (a-1)b$, which tells us how to move one b to the right past one a. Using this, and induction on the exponents, we can work out a formula for the product $(a^r b^s)(a^t b^u)$ as a linear combination of basis monomials. In fact, it suffices to prove a formula which expresses $b^s a^t$ as a linear combination of basis monomials, for then

$$\big(a^r b^s\big)\big(a^t b^u\big) = a^r \big(b^s a^t\big) b^u = a^r \left(\sum_{p,q} x_{pq} a^p b^q \right) b^u = \sum_{p,q} x_{pq} a^{p+r} b^{q+u}. \quad (2.9)$$

Computing the reduced forms for $b^s a^t$ for small s and t directly using the Gröbner bases, one starts noticing some patterns. For example, multiplying the defining relation $ba = ab - b$ by b on the left and computing the reduced form, we get

$$b^2 a = bab - b^2 = (ba - b)b = (ab - 2b)b = (a-2)b^2.$$

Iterating this, we can figure out how to move any power of b to the right past a.

Lemma 2.5.3.3. *We have $b^s a = (a - s) b^s$ for all $s \geq 0$.*

Proof. Induction on s; the basis is the defining relation $ba = (a-1)b$. If the claim holds for some particular $s \geq 1$, we have

$$b^{s+1} a = b(b^s a) = b(a-s)b^s = \big(ab - (s+1)b\big)b^s = \big(a - (s+1)\big)b^{s+1},$$

and this completes the proof. □

In general, we wish to be able to move any power of b to the right past any power of a; then by Equation (2.9) this will give us the formula we seek. Iterating Lemma 2.5.3.3, we get the following result.

Proposition 2.5.3.4. *We have $b^s a^t = (a-s)^t b^s$ for all $s, t \geq 0$.*

Proof. Induction on t; the basis is Lemma 2.5.3.3. □

Combining Equation (2.9) and Proposition 2.5.3.4 gives the final result.

Theorem 2.5.3.5. *Multiplication in the universal associative envelope of the 2-dimensional solvable Lie algebra is given by the following formula:*

$$(a^r b^s)(a^t b^u) = a^r (a-s)^t b^{u+s}.$$

Jordan algebras and finite-dimensional enveloping algebras. Let us discuss an example of a nonassociative structure whose universal associative envelope is finite dimensional. (See also Exercises 2.12–2.14.) The underlying vector space consists of the 2×2 matrices $M_2(\mathbb{F})$ over $\mathbb{F}$ with basis:

$$a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad c = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \qquad d = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

We make $M_2(\mathbb{F})$ into a special Jordan algebra J using the product $x \circ y = xy + yx$. The universal associative envelope $U(J)$ is $T(a,b,c,d)/I$, where the ideal I is generated by the following 10 elements, obtained from the structure constants of J:

$$\begin{aligned} &g_1 = a^2 - a, \quad g_2 = ba + ab - b, \quad g_3 = b^2, \quad g_4 = ca + ac - c, \\ &g_5 = cb + bc - d - a, \quad g_6 = c^2, \quad g_7 = da + ad, \\ &g_8 = db + bd - b, \quad g_9 = dc + cd - c, \quad g_{10} = d^2 - d. \end{aligned} \tag{2.10}$$

We obtain three distinct S-polynomials from the ordered pairs (g_5, g_2), (g_5, g_3) and (g_6, g_5); reducing them with respect to (2.10) we obtain their standard forms:

$$s_1 = ad, \quad s_2 = bd - ab, \quad s_3 = cd - ac. \tag{2.11}$$

Combining (2.10) and (2.11) we obtain a new set of 13 generators:

$$\begin{aligned} &a^2 - a, \quad ad, \quad ba + ab - b, \quad b^2, \quad bd - ab, \quad ca + ac - c, \\ &cb + bc - d - a, \quad c^2, \quad cd - ac, \quad da + ad, \quad db + bd - b, \\ &dc + cd - c, \quad d^2 - d. \end{aligned} \tag{2.12}$$

The set of polynomials (2.12) is not self-reduced; making it self-reduced, we obtain the following set in which every S-polynomial has reduced form 0:

$$a^2 - a, \quad ad, \quad ba + ab - b, \quad b^2, \quad bd - ab, \quad ca + ac - c,$$

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	2	6	7	·	6	7	9	9
3	3	3−6	·	8	6	·	8−9	·	·
4	4	4−7	2+5−8	·	7	5−8+9	·	4	4−7
5	5	·	3−6	4−7	5	·	·	8−9	·
6	6	·	·	9	6	·	·	·	·
7	7	·	2−9	·	7	·	·	7	·
8	8	9	3	·	8−9	6	·	8	9
9	9	9	6	·	·	6	·	9	9

FIGURE 2.2: Structure constants for the universal associative envelope $U(J)$ of the special Jordan algebra $J = M_2(\mathbb{F})^+$.

$$\begin{aligned} &cb + bc - d - a, \quad c^2, \quad cd - ac, \quad da, \quad db + ab - b, \\ &dc + ac - c, \quad d^2 - d. \end{aligned} \tag{2.13}$$

There are only 9 monomials in $T(a, b, c, d)$ which are not divisible by any of the leading monomials of the Gröbner basis elements (2.13):

$$1, \quad a, \quad b, \quad c, \quad d, \quad ab, \quad ac, \quad bc, \quad abc,$$

which we denote by $u_1, \dots, u_9$. The cosets of these monomials modulo I form a basis for $U(J)$.

Figure 2.2 contains the multiplication table for $U(J)$, where u_i is denoted i and dot, as we mentioned in Introduction, indicates 0. The entry in position (i, j) is the normal form of the product $u_i u_j$; in this case, computing the normal form of $u_i u_j$ for all i, j is rather trivial. For example,

$$\begin{aligned} u_7 u_3 = acb = a(-bc + d + a) = -abc + ad + a^2 = \\ - abc + 0 + a = a - abc = u_2 - u_9. \end{aligned}$$

The algorithms described in the survey paper [40] applied to the structure constants in Figure 2.2 lead to the conclusion that $U(J)$ is a semisimple associative algebra with the following Wedderburn decomposition:

$$U(J) \approx \mathbb{F} \oplus M_2(\mathbb{F}) \oplus M_2(\mathbb{F}).$$

2.5.4 PBW bases, Gröbner bases, and Koszul duality

The PBW theorem, besides its applications in representation theory of Lie algebras and theory of polynomial identities, inspired Priddy [210] to introduce a class of quadratic algebras for which the Koszul property is easy to establish.

We will recall his original definition, and explain how to view it in the language of Gröbner bases.

Definition 2.5.4.1 (PBW basis)**.** Let $A = T(x_1, \dots, x_n)/(R)$ be a quadratic algebra. Suppose that for each $i \geq 0$, cosets of monomials belonging to the set $\mathsf{B} := B_i \subset X^i$ is a basis for the homogeneous component A_i. This means, as usual, that the structure constants of A with respect to B are defined:

$$(b_1 + I)(b_2 + I) = \sum_{b \in B} c^b_{b_1,b_2}(b + I). \tag{2.14}$$

Equip $T(x_1, \dots, x_n)$ with the `glex` order. The basis B is called a *Poincaré–Birkhoff–Witt (PBW) basis* of A if the following two conditions hold:

1. for each two basis elements $b_1, b_2 \in \mathsf{B}$, we either have $b_1 b_2 \in B$, or the structure constants $c^b_{b_1,b_2}$ vanish for $b \prec b_1 b_2$ in X^*,
2. an element $m \in X^*$ belongs to B if and only if each two-letter subword of m belongs to B.

Proposition 2.5.4.2. *An algebra $A = T(V)/(R)$ has a PBW basis if and only if the ideal (R) has a quadratic Gröbner basis for the* `glex` *order with $x_n \prec x_{n-1} \prec \cdots \prec x_1$.*

Proof. Suppose that A has a PBW basis. Note that for the order we specified, the left hand side of Equation 2.14 is the leading monomial of the relation

$$b_1 b_2 - \sum_{b \in B} c^b_{b_1,b_2} b = 0.$$

The PBW condition states that the reduced monomials with respect to this set of elements form a basis of A, hence these elements form a Gröbner basis (for the leading monomial of any other element that we could possibly need to adjoin would make one of the reduced monomials nonreduced). Similarly, if the ideal (R) has a quadratic Gröbner basis G, cosets of all monomials that are reduced with respect to G form a PBW basis of A. □

Remark 2.5.4.3. It is common to state Proposition 2.5.4.2 somewhat informally, saying that "PBW bases are dual to Gröbner bases" (meaning that a Gröbner basis generates the ideal, while a PBW basis is a basis for the quotient). We hope that it is apparent to the reader that the notion of a Gröbner basis is much more general than that of a PBW basis (which, to be precise, is dual to the notion of a *quadratic Gröbner basis*).

Theorem 2.5.4.4. *A quadratic algebra equipped with a PBW basis is Koszul.*

Proof. See [210], or alternatively, use Proposition 2.5.4.2 together with a much more general Theorem 6.3.3.2. □

This result, in the view of Proposition 2.5.4.2, is extremely useful for Koszul duality, since it allows, in many cases, to prove Koszulness by a short direct computation. Note that the PBW condition is something that is hard to check directly: without Gröbner bases, we don't really have good intuition for constructing monomial bases.

We conclude this section with an example of a Koszul algebra that does not admit a quadratic Gröbner basis. For another example, see Exercise 2.16.

Example 2.5.4.5. Assume that the ground field $\mathbb{F}$ has characteristic 0. In [18], Berger considers a family of algebras with three generators a, b, c and three quadratic relations depending on the point $(\alpha : \beta : \gamma) \in \mathbb{P}^2$ as follows:

$$\alpha ab + \beta ba = \gamma c^2, \qquad \alpha bc + \beta cb = \gamma a^2, \qquad \alpha ca + \beta ac = \gamma b^2.$$

These algebras are "type A algebras" of Artin and Schelter [5], also commonly known as "three-dimensional Sklyanin algebras", since many of their properties resemble those of "four-dimensional Sklyanin algebras", certain algebras with four generators and six relations introduced earlier by Sklyanin [234, 235]; see [237] for more details on connections between those algebras. It is known [4] that these algebras are Koszul for all generic values of parameters, e.g., for parameters that are algebraically independent over $\mathbb{Q}$. It is also known that for such values of parameters the Hilbert series of this algebra is equal to $(1-t)^{-3}$; that is, it coincides with the Hilbert series of the algebra of polynomials in three variables (it is a particular case of these relations for $\alpha = 1$, $\beta = -1$, $\gamma = 0$).

Berger established the lack of a quadratic Gröbner basis combining the observation that one of the squares a^2, b^2, c^2 is the leading term of the corresponding relation with the following pretty combinatorial result [18, Lemma 5.2]:

> Let M be the set of all noncommutative monomials of degree two in a, b, c. For each subset N of M of cardinality 6, we denote by $c(N)$ the number of monomials uvw of degree three whose submonomials uv, vw of degree two belong to N. If N does not contain c^2, then $d(N) > 10$.

(The set M has $3^2 = 9$ elements, so there are 84 choices for N.) For a more general statement, see Exercise 2.18.

For the particular values of parameters $(\alpha : \beta : \gamma) = (1 : -1 : 1)$ we obtain the following beautiful relations,

$$ab - ba = c^2, \qquad bc - cb = a^2, \qquad ca - ac = b^2, \tag{2.15}$$

in which the commutator of any two generators is the square of the third. This algebra is also known to be Koszul. Let us outline the first few elements in its reduced Gröbner basis, using the `glex` order with $a \prec b \prec c$. With this order, the original relations take this ordered form:

$$ca - b^2 - ac, \qquad cb - bc + a^2, \qquad c^2 + ba - ab.$$

There are two nontrivial S-polynomials whose reduced forms are as follows:

$$b^2a - bab + ab^2 + a^2c, \qquad b^2c - aba.$$

The set containing the last five polynomials is already self-reduced. The second iteration produces another two S-polynomials:

$$bab^2 + ba^2c - abac, \qquad b^4 + babc - aba^2 - a^3b.$$

The set containing the last seven polynomials is already self-reduced, and the third iteration produces 12 new S-polynomials. The combined set of 19 relations is not self-reduced; after self-reduction we obtain the 15 relations

$$\begin{gathered}
ca - b^2 - ac, \quad cb - bc + a^2, \quad c^2 + ba - ab, \quad b^2a - bab + ab^2 + a^2c, \\
b^2c - aba, \quad bab^2 + ba^2c - abac, \quad b^4 + babc - aba^2 - a^3b, \quad babab - a^2bac, \\
ba^3b + ababa - aba^2b, \; ba^2b^3 + ba^2bac - ba^5 - ababac + aba^4 + a^3ba^2 - a^4ba, \\
ba^2bc - ba^4 - ababc + aba^3 + a^3ba, \quad baba^2c - ba^2bac + a^2babc - a^2ba^3, \\
ba^4ba + a^2baba^2 - a^2ba^2ba - a^3baba + a^3ba^2b, \quad baba^2ba - a^2ba^2b^2, \\
baba^2b^2 + baba^3c - ba^2ba^2c - ba^4bc + a^3babc.
\end{gathered}$$

Iteration 4 produces 82 new S-polynomials, the combined set of 97 relations self-reduces to 34, and at this point further computation becomes impractical.

While preparing the final draft of the book, we became aware of a preprint [140], where Gröbner methods are utilized to study homological properties of Sklyanin algebras. It is possible that ideas in that preprint admit further extension to other notable examples of quadratic algebras.

2.5.5 Viewing commutative algebras as noncommutative ones

As we mentioned in the beginning of this chapter, it sometimes is beneficial to consider commutative algebras as particular cases of noncommutative ones. Formally, if $A = \mathbb{F}[x_1, \dots, x_n]/I$, then we can consider the preimage $\widehat{I} = \pi^{-1}(I)$ of the ideal I under the canonical projection $\pi\colon T(x_1, \dots, x_n) \to \mathbb{F}[x_1, \dots, x_n]$; in that case, of course, $\widehat{A} := T(x_1, \dots, x_n)/\widehat{I} \cong A$.

Since each ideal I of $\mathbb{F}[x_1, \dots, x_n]$ is finitely generated, we can at least be sure that the corresponding ideal $\widehat{I}$ is finitely generated; if $I = (g_1, \dots, g_m)$, then the ideal $\widehat{I}$ is generated by the set $\{x_ix_j - x_jx_i\colon 1 \leq i < j \leq n\} \cup \{\hat{g}_1, \dots, \hat{g}_m\}$, where the elements $\hat{g}_1$, …, $\hat{g}_m$ are arbitrary lifts of $g_1, \dots, g_m$ to $T(x_1, \dots, x_n)$. One however must be very careful about lifting Gröbner bases.

Example 2.5.5.1 ([86])**.** Consider the ideal $(x_1x_2x_3) \subset \mathbb{F}[x_1, x_2, x_3]$. Let us show that $\widehat{I}$ does not admit a finite Gröbner basis, regardless of the choice of a monomial order. Without loss of generality, $x_1 \prec x_2 \prec x_3$.

In that case, the only element of $\widehat{I}$ of degree 3 which is reduced with respect to $\{x_1x_2 - x_2x_1, x_1x_3 - x_3x_1, x_2x_3 - x_3x_2\}$ is $x_1x_2x_3$. We must adjoin this element in order to get a Gröbner basis; after that $x_1x_2^2x_3$ is the only element of $\widehat{I}$ of degree 3 which is reduced with respect to $\{x_1x_2 - x_2x_1, x_1x_3 - x_3x_1, x_2x_3 - x_3x_2, x_1x_2x_3\}$ etc. Altogether, the reduced Gröbner basis of this ideal is

$$\{x_1x_2 - x_2x_1, x_1x_3 - x_3x_1, x_2x_3 - x_3x_2\} \cup \{x_1x_2^kx_3 \colon k \geq 1\}.$$

We refer the reader to [86] for general results on lifting Gröbner bases. In particular, an interesting unexpected phenomenon is that when $\mathbb{F}$ is infinite, it is possible to perform a linear change of variables after which the lifted ideal $\widehat{I}$ admits a finite Gröbner basis, but this may fail over a finite field.

One instance where it would be particularly beneficial to lift Gröbner bases is the case of algebras with quadratic relations because of Theorem 2.5.4.4 as the easiest possible criterion for algebra to be Koszul. Unfortunately, there are examples of algebras which have a quadratic Gröbner basis as commutative algebras, but not as noncommutative algebras, as we will now see.

Example 2.5.5.2 ([207])**.** Consider the ideal

$$I = (x_1^2, x_2^2, \ldots, x_7^2, x_1x_4, x_2x_5, x_3x_6, x_2x_7, x_4x_7, x_6x_7)$$

of $\mathbb{F}[x_1, \ldots, x_7]$. For the algebra $A = \mathbb{F}[x_1, \ldots, x_7]/I$, its Hilbert series is $1+7z+15z^2+11z^3+z^4$. Suppose that the ideal $\widehat{I}$ admits a quadratic Gröbner basis G (for some monomial order). Consider the corresponding graph of normal words, as in Definition 2.5.1.3. Since the relations are assumed quadratic, the vertices are $x_1, \ldots, x_7$, and the edges correspond to quadratic elements outside $\textsc{lm}(G)$. Since A is finite-dimensional, this graph cannot have loops or directed cycles, and there is just one directed path of length 3. Let it be $v_1 \to v_2 \to v_3 \to v_4$ for some vertices $v_1, \ldots, v_4$, and denote by w_1, w_2, w_3 the three remaining vertices. To avoid cycles, the subgraph with the vertices $v_1, \ldots, v_4$ cannot have more than 6 edges, and the subgraph with the vertices w_1, w_2, w_3 cannot have more than 3 edges. Absence of cycles together with the uniqueness of a path of length 3 implies that each of the vertices w_1, w_2, w_3 can be joined with the set $\{v_1, \ldots, v_4\}$ by at most 2 edges. Altogether, we may have at most 15 edges, which is the dimension of A_2, so all these estimates must be attained. Examining these conditions, we find just one graph with 7 vertices, 15 edges, and exactly one path of length 3. However, it can be checked directly (Exercise 2.20) that it has 10 paths of length 2, a contradiction.

2.5.6 Computation of noncommutative Gröbner bases

In this section, we will give some examples that show that unlike the commutative case, computation of a noncommutative Gröbner basis may never terminate, even for the case when the ideal I is finitely generated (of course, for infinitely generated ideals, like $I = (ab^k a \colon k \geq 1) \subset T(a,b)$, it would be too naïve to hope for a finite Gröbner basis). The lack of termination here could mean, for example, any of the following three increasingly strong assertions:

- The algorithm does not terminate for a particular monomial order.
- The algorithm does not terminate for any monomial order.
- The algorithm does not terminate for any monomial order, allowing for arbitrary invertible linear changes of variables. That is, we are allowed not only to change the monomial order but also to replace the original variables $[X] = [x_1, \ldots, x_n]$ by new variables

$$[X'] = [X]A = [x'_1, \ldots, x'_n], \qquad A \in GL_n(\mathbb{F}).$$

We learned some of the examples of this section from the paper [121] which exhibits several interesting instances of "monsters" in the theory of noncommutative Gröbner bases.

The first kind of non-termination is extremely easy to encounter: this kind of behavior is exhibited in many cases. However, sometimes one may be lucky enough to be able to change the order to obtain a finite Gröbner basis.

Example 2.5.6.1 ([121])**.** Consider two indeterminates $X = \{a, b\}$, and the principal ideal $I = (g_0) \subset T(a,b)$ generated by the relation $g_0 = a^2 - ab$. Suppose that we take some monomial order with $b \prec a$. In that case, the leading monomial a^2 has an overlap with itself, and the reduction of the corresponding S-polynomial $g_0 a - a g_0 = a^2 b - aba$ is $ab^2 - aba$, with the leading monomial aba; this leading monomial has an overlap with itself and with the leading monomial of g_0. A few more iterations suggest that all elements $g_i = ab^i a - ab^{i+1}$ must belong to the reduced Gröbner basis of I; in fact, it is true that the set

$$R = \{\, g_i \mid i \geq 0 \,\}$$

is the reduced Gröbner basis (Exercise 2.21). However, if we consider a monomial order with $a \prec b$, then the leading monomial ab has no self-overlaps, and so g_0 is a Gröbner basis.

Unfortunately, for some cases, it is impossible to achieve termination by changing the monomial order. One source of such examples comes from 2.5.1.5; there are examples of algebras with an irrational Hilbert series, and this of course contradicts the possibility of having a finite Gröbner basis.

Example 2.5.6.2. Let us again take $X = \{a, b\}$. We consider, for the element $g_1 := aba - ba$ the principal ideal $I = (g_1) \subseteq T(a,b)$. Note that since for any monomial order Ξ we have $1 \prec a$, so $ba \prec aba$, and $\textsc{lm}(g_1) = aba$. The first iteration of the algorithm produces one S-polynomial:

$$g_1 ba - ab g_1 = (aba - ba)ba - ab(aba - ba) = -baba + ab^2 a \longrightarrow baba - ab^2 a = g'_2.$$

Computing the reduced form of g_2' with respect to $\{ g_1 \}$, we obtain:

$$(baba - ab^2a) - b(aba - ba) = -ab^2a + b^2a \longrightarrow ab^2a - b^2a = g_2.$$

We obtain a new bigger self-reduced set:

$$R_1 = \{ \ g_1 = aba - ba, \ g_2 = ab^2a - b^2a \ \}.$$

Again, we see that $\textsc{lm}(g_2) = ab^2a$ for any monomial order. The second iteration produces three S-polynomials:

$$\begin{aligned}
&g_1b^2a - abg_2 = (aba - ba)b^2a - ab(ab^2a - b^2a) \longrightarrow bab^2a - ab^3a = g_3',\\
&g_2ba - ab^2g_1 = (ab^2a - b^2a)ba - ab^2(aba - ba) \longrightarrow b^2aba - ab^3a = g_4',\\
&g_2b^2a - ab^2g_2 = (ab^2a - b^2a)b^2a - ab^2(ab^2a - b^2a) \longrightarrow b^2ab^2a - ab^4a = g_5'.
\end{aligned}$$

Computing the normal forms of g_3', g_4', g_5' with respect to $\{ g_1, g_2 \}$ gives:

$$\begin{aligned}
&(bab^2a - ab^3a) - b(ab^2a - b^2a) = -ab^3a + b^3a \longrightarrow ab^3a - b^3a = g_3,\\
&(b^2aba - ab^3a) - b^2(aba - ba) = -ab^3a + b^3a \longrightarrow ab^3a - b^3a = g_3 \text{ (again)},\\
&(b^2ab^2a - ab^4a) - b^2(ab^2a - b^2a) = -ab^4a + b^4a \longrightarrow ab^4a - b^4a = g_4.
\end{aligned}$$

We obtain the new self-reduced set:

$$R_2 = \{ \ g_1 = aba - ba, \ g_2 = ab^2a - b^2a, \ g_3 = ab^3a - b^3a, \ g_4 = ab^4a - b^4a \ \}.$$

At this point it becomes fairly clear what is happening: the size of the set doubles after each iteration, and the highest degrees also increase exponentially.

Proposition 2.5.6.3. *We have*

$$R_n = \{ \, (a-1)b^ia \mid 1 \leq i \leq 2^n \, \}.$$

For the `glex` *order $a \prec b$, the algorithm never terminates. Moreover, the set*

$$R_\infty = \{ \, (a-1)b^ia \mid i \geq 1 \, \},$$

is the reduced Gröbner basis for the principal ideal $(aba - ba)$ for any monomial order.

Proof. Exercise 2.22. □

The former example used an inhomogeneous relation. Let us give one example with homogeneous relations.

Example 2.5.6.4 ([10, 121, 250])**.** Let $X = \{a, b, c\}$, and consider the homogeneous ideal $I = (\, a^2, \ ca + ab \,) \subset T(a, b, c)$ generated by two quadratic relations. It turns out that the reduced Gröbner basis of this ideal is infinite for any monomial order. Let us outline an argument establishing that. Without loss of generality, $ab \prec ca$ (the case $ca \prec ab$ is completely analogous), in which case $\text{LM}(ca + ab) = ca$. After n iterations of the noncommutative Buchberger algorithm, the set of relations is as follows (Exercise 2.23):

$$n = 0\colon\ \{\, a^2,\ ca + ab \,\} \qquad\qquad n \geq 1\colon\ \{\, a^2,\ ca + ab,\ aba,\ \dots,\ ab^n a \,\}.$$

In fact, it is true that in this case the computation does not terminate for any monomial order even after allowing for arbitrary invertible linear changes of variables. To the best of our knowledge, it is not known if there exists a homogeneous *principal* ideal with the same properties (infinite Gröbner basis for all monomial orders and changes of basis).

Example 2.5.6.5 ([121])**.** Given a principal ideal generated by a *nonhomogeneous* polynomial f, a fundamental question is to determine whether $(f) = (1)$; this is particularly difficult over a field of positive characteristic, where leading terms may be harder to control. The simplest (interesting) example is $f = aba^2 - a^2ba + 1$ with $a \prec b$. Over $\mathbb{F} = \mathbb{Q}$, after the third iteration of the noncommutative Buchberger algorithm, the set of relations obtained from the original innocent polynomial is as follows:

$$\begin{gathered} ba^2 - 2aba + a^2b, \qquad a^2ba - a^3b + 1, \qquad baba - \tfrac{1}{2}ab^2a - 2abab + \tfrac{3}{2}a^2b^2, \\ a^3b^2a - a^4b^2 - 2ba + 4ab, \qquad a^3b^3a - a^4b^3 - 5b^2a + 4bab + 4ab^2, \\ a^4b^4a - a^5b^4 - 5bab^2a - 4ab^3a + 2ab^2ab + 16abab^2 - 5a^2b^3, \end{gathered}$$

and it rapidly gets worse after that. Over $\mathbb{F} = \mathbb{F}_p$, the behavior is less predictable, and is not fully understood; see Exercises 2.24–2.26.

2.6 Rewriting systems and Gröbner bases

In this section, we briefly touch the universe of rewriting systems and compare them with Gröbner bases. For more details, we refer the reader to [8].

2.6.1 Abstract rewriting systems

Definition 2.6.1.1 (Abstract rewriting system)**.** An *abstract rewriting system* (ARS) is a pair $(A, \to)$, where A is a set and $\to$ is a binary relation, usually called a *rewriting rule*, or a *reduction relation*.

Throughout this section, we denote by $(A, \to)$ an arbitrary ARS.

Let us fix some general notation for binary relations. We denote by $\overset{*}{\to}$ the reflexive transitive closure of the relation $\to$; we write $g \overset{*}{\to} g'$, if and only if there is a sequence of $s \geq 0$ rewritings beginning with g and ending with g':

$$g = g_0 \longrightarrow g_1 \longrightarrow g_2 \longrightarrow \cdots \longrightarrow g_{s-1} \longrightarrow g_s = g'. \tag{2.16}$$

It will be convenient also to define the inverse relation $g' \leftarrow g$, which means the same as $g \rightarrow g'$, and its reflexive transitive closure $g' \overset{*}{\leftarrow} g$.

Definition 2.6.1.2 (Joinability for an ARS)**.** Two elements $f, g \in A$ are said to be *joinable*, or have a *common successor*, if there exists $h \in A$ such that

$$f \overset{*}{\rightarrow} h \overset{*}{\leftarrow} g.$$

We use the simpler notation $f \downarrow g$ for the joinability relation, so that

$$f \downarrow g \quad \Longleftrightarrow \quad \exists\, h \in \mathcal{P},\ f \overset{*}{\rightarrow} h \overset{*}{\leftarrow} g.$$

Definition 2.6.1.3 (Normal forms for an ARS)**.** An element $f \in A$ is said to be *reducible* if there exists $g \in A$ such that $f \rightarrow g$; otherwise it is said to be *irreducible*, or a *normal form*. If $f \overset{*}{\rightarrow} g$, and g is irreducible, g is said to be a *normal form of* f. An ARS is said to be *normalizing*, if every $f \in A$ has at least one normal form.

An important class of ARS for which the normalizing property holds consists of all terminating ones.

Definition 2.6.1.4 (Termination)**.** An ARS is said to be *terminating*, if there is no infinite chain $f_0 \rightarrow f_1 \rightarrow f_2 \rightarrow \ldots$.

The following property, called confluence, formalizes the intuitive principle "if f and g have a common predecessor, they also have a common successor".

Definition 2.6.1.5 (Confluence)**.** An ARS is said to be *confluent* if for all $f, g, h \in A$, $f \overset{*}{\leftarrow} h \overset{*}{\rightarrow} g$ implies $f \downarrow g$. This is best viewed through the following diagram:

$$\begin{tikzcd}
& h \arrow[dl, "*"'] \arrow[dr, "*"] & \\
f \arrow[dr, "*"'] & & g \arrow[dl, "*"] \\
& r &
\end{tikzcd} \tag{2.17}$$

An ARS is said to be *locally confluent*, or *weakly confluent*, if for all $f, g, h \in A$, $f \leftarrow h \rightarrow g$ implies $f \downarrow g$.

Theorem 2.6.1.6 (Diamond Lemma, [138, 204])**.** *A terminating ARS is confluent if and only if it is locally confluent.*

Definition 2.6.1.7 (Convergence)**.** An ARS is said to be *convergent* if it is confluent and terminating.

For a convergent system, normal forms exist and are unique (Exercise 2.28), so convergent systems are analogous to Gröbner bases in the context of ARS. According to Theorem 2.6.1.6, to check convergence, it is sufficient to check termination and local confluence; this shows that in the theory of rewriting systems, the Knuth–Bendix algorithm [150] plays the role of Buchberger's algorithm.

2.6.2 Ordered rewriting systems

Let us now explain how noncommutative polynomials give rise to particular types of rewriting systems. Let us, as usual, fix a monomial order Ξ on $T(X)$.

Definition 2.6.2.1 (Ordered rewriting system)**.** Let $S \subset T(X)$. Suppose that f is a polynomial which is not reduced with respect to S. Consider one reduction step in the long division of a polynomial $f \neq 0$ by S, which replaces f by $\tilde{f} = f - cm_1gm_2$, where $g \in S$ is a polynomial for which $\textsc{lm}(g)$ divides some monomial $m \in \operatorname{supp}(f)$. The *ordered rewriting system associated to S* is $(T(X), \rightarrow_S)$, where $f \rightarrow_S g$ if and only if $g = \tilde{f}$ as above.

It is easy to see that ordered rewriting systems are always terminating (Exercise 2.29). Local confluence for such a rewriting system is the requirement that every S-polynomial can be reduced to zero, which connects to the content of Theorem 2.4.1.5.

In general, we could mimic Definition 2.6.2.1 without any monomial order. Instead, we could pick, for each $g \in S$, an arbitrary monomial $m \in \operatorname{supp}(g)$, call that monomial $\textsc{lm}(g)$, and use it throughout. Of course, if we do that, we do not have termination for free, but this can be useful otherwise, as the following example shows.

Example 2.6.2.2. Let $X = \{x, y, z\}$, and let

$$S = \{xyz - x^3 - y^3 - z^3\} \in T(x, y, z).$$

We somewhat arbitrarily define $\textsc{lm}(xyz - x^3 - y^3 - z^3) := xyz$. It is clear that there does not exist a monomial order Ξ for which xyz is the leading monomial of $xyz - x^3 - y^3 - z^3$: indeed, whichever of x, y, z is the largest one would have its cube bigger than xyz.

Note that while the "honest" leading monomials x^3, y^3, and z^3 have overlaps with themselves, the term xyz has no overlaps with itself, so "there are no diamonds to close", and this rewriting rule is locally confluent.

Let us establish termination. Suppose that a monomial m is divisible by xyz, so that our rewriting rule can be applied. Note that the result of rewriting m is a combination of three monomials: m_1 (where xyz is replaced by x^3), m_2 (where xyz is replaced by y^3), and m_3 (where xyz is replaced by z^3). The number of occurrences of xyz in m is not smaller than that in m_1 and m_3 and is bigger than that in m_2, and the number of occurrences of y in m is bigger than that in m_1 and m_3 and is bigger by two than that in m_2. Thus, the quantity

$$J(m) = 3\#\{\text{occurrences of } xyz \text{ in } m\} + \#\{\text{occurrences of } y \text{ in } m\}$$

can only decrease for $m \in \operatorname{supp}(f)$ when we apply our rewriting rule, and termination follows. Thus, our rewriting system is convergent, and even though xyz cannot be made the leading monomial for any monomial order, monomials not divisible by xyz form a basis in $T(x, y, z)/(xyz - x^3 - y^3 - z^3)$.

The last example is due to the second author, who mentioned it to the authors of [124], where it first appeared. That paper is a very stimulating article illustrating further applications of rewriting systems to homological algebra. We encourage a motivated reader to generalize results of that article to the case of operads, thus improving various results of Chapter 6 in this book.

2.7 Exercises

Exercise 2.1. Prove the claim made in Example 2.1.2.2.

Exercise 2.2. Prove Proposition 2.3.1.6.

Exercise 2.3. Prove that Algorithm 2.3.2.12 terminates after finitely many steps.

Exercise 2.4.

(i) Pick a monomial order of $T(a, b)$, and compute the reduced Gröbner basis for the algebra $A = T(a, b)/(a^2, ab^2 + bab + b^2a)$.

(ii) Using the reduced Gröbner basis G you computed, compute the Hilbert series $h_A(t)$.

Exercise 2.5. Pick some monomial order of $T(a, b, c)$, and use computer algebra software to obtain experimental data which would allow you to guess Gröbner bases for algebras

(i) $P := T(a, b, c)/(ac - ca, aba - bc, b^2a)$;

(ii) $Q := T(a, b, c)/(ac - ca, aba - bc, b^2)$.

According to Shearer [230], if we assign unconventional weights $\mathrm{wt}'(a) = 1$, $\mathrm{wt}'(b) = 1$, $\mathrm{wt}'(c) = 2$ (so that these relations become homogeneous), the Hilbert series $h_P(t)$ and $h_Q(t)$ are irrational, so it is certain that the Gröbner bases that you guess would be infinite.

Exercise 2.6. This exercise is motivated by the following problem that was mentioned by Kevin Buzzard in a discussion of linear algebra questions on `MathOverflow` as an instance of a really hard problem in linear algebra (`http://mathoverflow.net/questions/15050/linear-algebra-problems#comment27043_15050`):

> Let $X, Y \in M_n(\mathbb{R})$. Suppose that $X^2 + Y^2 = XY$ and $XY - YX$ is invertible. Prove that n is divisible by 3.

(i) Using the `glex` order on $T(x, y)$ for, say, $x \prec y$, compute the reduced Gröbner basis for the principal ideal $(x^2 - xy + y^2)$.

(ii) Compute the center of the algebra $A = T(x, y)/(x^2 - xy + y^2)$, and find the structure of A as a module over its center.

(iii) Classify finite-dimensional complex irreducible A-modules, and solve the problem stated above.

Exercise 2.7. Pick a monomial order of $T(x_{11}, x_{12}, x_{21}, x_{22})$, and compute the reduced Gröbner basis for

(i) the algebra of quantum 2×2-matrices,

(ii) the quantum group SL_2

(see Example 2.1.1.4 for definitions). Verify that the dimensions of homogeneous components of these algebras over $\mathbb{F}(q)$ are the same as the dimensions over $\mathbb{F}$ for the algebras obtained by setting $q = 1$ in the defining relations.

Exercise 2.8. Generalize the approach of Section 2.5.2 to the symmetric group on 4 letters, using a computer algebra system if necessary.

Exercise 2.9. The easiest counterexample to the PBW theorem is constructed as follows. Consider the ring $A = \mathbb{F}_2[a, b, c]/(a^2, b^2, c^2)$, and define a Lie algebra L which is the quotient of the free Lie algebra over A generated by x_1, x_2, x_3 modulo the relation $ax_1 + bx_2 + cx_3 = 0$. Show that the natural map $L \to U(L)$ is not an isomorphism.

Exercise 2.10. Consider the group of upper triangular matrices with 1s on the diagonal:

$$\mathfrak{H} = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; a, b, c \in \mathbb{F} \right\}$$

This group is called the *Heisenberg group*; it is nilpotent and its real version arises in the description of 3-dimensional quantum mechanical systems. (The celebrated Stone–von Neumann Theorem [244, 256], on the uniqueness of the canonical commutation relations between position and momentum operators, shows that there is a unique, up to isomorphism, irreducible unitary representation in which the center of $\mathfrak{H}$ acts by a given nontrivial character.)

(i) Find the center of $\mathfrak{H}$ and its nontrivial characters.

(ii) Let $\mathfrak{h}$ be the Lie algebra of $\mathfrak{H}$, called the Heisenberg (Lie) algebra. This is the 3-dimensional nilpotent Lie algebra with basis $\{a, b, c\}$ and commutation relations

$$[a, b] = c, \quad [a, c] = 0, \quad [b, c] = 0.$$

Consider the polynomial ring $\mathbb{F}[x]$ and these linear operators on it:

$$A(f) = \frac{d}{dx} f, \quad B(f) = xf, \quad C(f) = f, \quad f \in \mathbb{F}[x].$$

We easily calculate

$$A(B(f)) = \frac{d}{dx}(xf) = f + xf', \quad B(A(f)) = xf', \quad [A, B](f) = C(f).$$

This is the irreducible representation of $\mathfrak{h}$ in which the center C acts as the identity map. The PBW basis of $U(\mathfrak{h})$ is $\{\, a^i b^j c^k \mid i, j, k \geq 0 \,\}$. In $U(L)$ we have

$$ba = ab - c, \quad ac = ca, \quad bc = cb.$$

Determine a formula for $(a^p b^q c^r)(a^s b^t c^u)$ as a linear combination of basis monomials.

Exercise 2.11. Assume that $\mathbb{F}$ has characteristic 0. Consider the simple Lie algebra $\mathfrak{sl}_2$ with basis $\{e, f, h\}$ where

$$[h, e] = 2e, \qquad [h, f] = -2f, \qquad [e, f] = h.$$

The PBW basis of $U(\mathfrak{sl}_2)$ consists of $f^p h^q e^r$ for $p, q, r \geq 0$, where the generators satisfy these relations:

$$eh = he - 2e, \qquad hf = fh - 2f, \qquad ef = fe + h.$$

Using these relations we can express $(f^p h^q e^r)(f^s h^t e^u)$ as a linear combination of basis monomials, but this is a little more difficult than it looks.

(i) Prove the following formulas, where $[x, y] = xy - yx$ in $U(sl_2)$:

$$[h, f^s] = -2sf^s, \qquad [h, e^u] = 2ue^u.$$

Derive formulas for moving h to the right past f, and for moving h to the left past e.

(ii) State and prove formulas for $[e, f^s]$ and $[f, e^u]$.

(iii) State and prove the formula for $[e^r, f^s]$. (This formula is extremely useful for classifying finite-dimensional simple $\mathfrak{sl}_2$-modules.)

(iv) State and prove the general formula for $(f^p h^q e^r)(f^s h^t e^u)$ in $U(\mathfrak{sl}_2)$.

Exercise 2.12. Verify all of the structure constants in the table from Figure 2.2.

Exercise 2.13. Suppose that $\text{char}(\mathbb{F}) \neq 2$. Let $J = M_3(\mathbb{F})^+$ be the special Jordan algebra of all 3×3 matrices over $\mathbb{F}$; its structure operation is $a \circ b = ab + ba$. Let $I \subset T(x_1, \ldots, x_9)$ be the ideal defining the universal enveloping algebra: $U(J) = T(x_1, \ldots, x_9)/I$, where $I = (x_i x_j + x_j x_i + x_i \circ x_j)$. Find a Gröbner basis for I, a monomial basis for $U(I)$, and calculate the structure constants of $U(I)$.

Exercise 2.14.

(i) Prove that if J is an n-dimensional Jordan algebra with zero product, then $U(J)$ is the exterior algebra of an n-dimensional vector space.

(ii) Prove that if J is a finite dimensional Jordan algebra then its universal enveloping algebra is also finite dimensional.

Exercise 2.15. Let $X = \{a, b\}$ with $a \prec b$, and

$$g_1 = aba - a^2b - a, \qquad g_2 = bab - ab^2 - b.$$

Note that $g_2 = \rho(\sigma(g_1))$ where $\sigma\colon T(a,b) \to T(a,b)$ is the endomorphism interchanging a and b, and $\rho\colon T(a,b) \to T(a,b)$ is the anti-endomorphism which reverses each monomial. The problem of computing the reduced Gröbner basis of (g_1, g_2) arose during the computation of the universal enveloping algebra of a two-dimensional nonassociative triple system based on the trilinear operation $abc - bca$; see Elgendy [87].

(i) Compute the first iteration of noncommutative Buchberger algorithm, both with and without the optimization suggested by Corollary 2.4.3.3.

(ii) Use computer algebra software to compute the first few elements of the reduced Gröbner basis, guess the general formula for the (infinite) reduced Gröbner basis, and prove it.

Exercise 2.16 ([207])**.** Fix an element $a \in \mathbb{F}$, and consider the ideal $I = (x^2 + yz, x^2 + azy)$ of $T(x, y, z)$.

(i) Show that for $a \neq 0$ there is no monomial order for $T(x, y, z)$ for which I admits a quadratic Gröbner basis.

(ii) Show that for $a \neq 0, 1$ there is no linear change of variables x', y', z' and a monomial order for $T(x', y', z')$ for which I admits a quadratic Gröbner basis.

Exercise 2.17. Let M_n be the set of all 3^n noncommutative monomials $w_1 \cdots w_n$ of degree n in the generators a, b, c. For each subset $N \subset M_2$ with $|N| = 6$, write $c(N)$ for the number of monomials $uvw \in M_3$ whose two subwords $uv, vw \in M_2$ belong to N. Prove (using a computer or otherwise) that if $c(N) \leq 10$ then $a^2, b^2, c^2 \in N$.

Exercise 2.18 ([18, Theorem 6.1])**.** The setting is similar to Exercise 2.17 except that now we have r generators. Let M_n be the set of all r^n noncommutative monomials $w_1 \cdots w_n$ of degree n in the generators $x_1, \cdots, x_r$. For each subset $N \subset M_2$ with $|N| = \binom{r+1}{2}$, write $c(N)$ for the number of monomials $uvw \in M_3$ whose two subwords $uv, vw \in M_2$ belong to N. For any permutation $\sigma \in S_r$ acting on the indices $1, \dots, r$ we write

$$\sigma(N) = \{\, x_{\sigma(i)} x_{\sigma(j)} \mid x_i x_j \in N \,\} \subset M_2.$$

(i) Prove that $c(\sigma(N)) = c(N)$ for all N and all σ.

(ii) Prove that for $N_0 = \{\, x_i x_j \mid 1 \le i \le j \le r \,\}$ we have $c(N_0) = \binom{r+2}{3}$.

(iii) Prove that $c(N) = \binom{r+2}{3}$ if and only if $N = \sigma(N_0)$ for some $\sigma \in S_r$.

(iv) Prove that for all N we have $c(N) \ge \binom{r+2}{3}$.

Exercise 2.19 ([247])**.**

(i) Show that for the choice of parameters $(1, 1, \gamma)$ in Example 2.5.4.5, that is for the algebra $A(\gamma)$ with three generators a, b, c and the defining relations

$$\begin{cases} ab + ba = \gamma c^2, \\ bc + cb = \gamma a^2, \\ ca + ac = \gamma b^2, \end{cases}$$

the reduced Gröbner basis for the `glex` order with $a \prec b \prec c$ is finite (for each $\gamma \in \mathbb{F}$).

(ii) Find how the dimension of the weight n component of the algebra $A(\gamma)$ depends on γ.

(iii) Assume that $\gamma \ne 0, 1$. Show that the elements a^2, b^2, and c^2 belong to the center of the algebra $A(\gamma)$, and are algebraically independent.

(iv) Assume that $\gamma \ne 0, 1$. Describe the center of the algebra $A(\gamma)$.

(v) Use your results to determine whether Conjecture 10.37ii of [5] is true.

Exercise 2.20. Fill in the details for the argument of Example 2.5.5.2.

Exercise 2.21. Prove that the set R from Example 2.5.6.1 is the reduced Gröbner basis of I with respect to any monomial order satisfying $b \prec a$.

Exercise 2.22. Prove Proposition 2.5.6.3.

Exercise 2.23. Verify the claim on the results of iterations of the noncommutative Buchberger algorithm from Example 2.5.6.4.

Exercise 2.24.

(i) Suppose that the ground field $\mathbb{F}$ is algebraically closed. Consider an inhomogeneous polynomial $f \in T(a, b)$ for which all monomials in $\operatorname{supp}(f)$ are of weight at most 2. Show that there exists a linear change of variables for which f becomes the reduced Gröbner basis of the ideal it generates.

(ii) Use the result you obtained to derive a yet another computation of the Hilbert series in Example 2.5.1.6.

Exercise 2.25. Suppose that the ground field $\mathbb{F}$ is algebraically closed. Consider an inhomogeneous polynomial $f \in T(a, b)$ for which all monomials in $\operatorname{supp}(f)$ are of weight at most 3. Is it true that there always exists a linear change of variables for which f becomes the reduced Gröbner basis of the ideal it generates? Naïvely, one can argue that there are four among the eight weight 3 monomials that have self-overlaps and thus are undesirable as leading monomials, and nontrivial changes of variables form a three-dimensional group $PGL_2(\mathbb{F})$, so it is likely that we fail in some cases. Is it possible to repair that argument?

Exercise 2.26.

(i) Prove that for $\mathbb{F} = \mathbb{Q}$ the ideal (f) of Example 2.5.6.5 is different from (1).

(ii) Answer the same question for $\mathbb{F} = \mathbb{F}_p$, where $p = 2, 3, 5, 7, 11, 13, 17, 19$.

Exercise 2.27. Show that each terminating ARS is normalizing. Is the converse true?

Exercise 2.28. Prove that for a convergent ARS normal forms exist and are unique.

Exercise 2.29. Show that ordered rewriting systems are always terminating.

Exercise 2.30.

(i) Fill in the details to justify claims made in Example 2.6.2.2.

(ii) Apply noncommutative Gröbner bases to obtain different normal forms in Example 2.6.2.2. Compare the normal forms thus obtained.

(iii) What about the rewriting rule $xy \to x^2 + y^2$? Is it confluent? Terminating?

Chapter 3

Nonsymmetric Operads

One of the main reasons to study associative algebras is the notion of a module over an associative algebra, that is a vector space where an algebra acts by endomorphisms. Similarly, when talking about some class of algebras, e.g., associative algebras, Lie algebras, Jordan algebras, etc., it is useful to consider the collection of all operations with several arguments made of structure operations on this algebra, and study algebraic structures of that collection. This leads naturally to various notions of an operad. Sergei Merkulov [196] came up with a beautiful analogy for that: similar to how the Cheshire Cat from *Alice's Adventures in Wonderland* tends to disappear almost completely so that the only thing left is the cat's grin, an operad is a "grin of an algebra", that is what remains when we take an algebra, that is a vector space with structure operations, and remove the vector space.

3.1 Introduction

In this chapter, we will discuss nonsymmetric operads. This type of operads controls algebraic properties of operations that can be expressed in terms of substitutions of multilinear maps into one another, completely avoiding permutations of arguments. For example, the associativity axiom

$$(a_1a_2)a_3 = a_1(a_2a_3)$$

belongs to that universe because the arguments on the left and on the right appear in the same order; erasing those arguments we do not lose any information whatsoever. Meanwhile, the Jacobi identity for Lie algebras

$$[[a_1, a_2], a_3] + [[a_2, a_3], a_1] + [[a_3, a_1], a_2] = 0$$

is not of that kind. Using the skew-symmetry of the Lie bracket, we can rewrite the second term as $-[a_1, [a_2, a_3]]$, restoring the status quo, but for the last term we cannot bring the arguments in the standard order $1, 2, 3$, however much we try. Moreover, it turns out that there are no linear dependencies between those Lie monomials of any given arity for which all arguments appear in the standard order; see, e.g., [221]. In this chapter, we will focus on operations without special symmetries; further chapters will gradually bring us a way to handle symmetries.

3.1.1 Nonsymmetric collections

As we said, a model example of an associative algebra is the set of endomorphisms of a vector space V where the associative product is given by composition. The structure of a left module over an associative algebra A on a vector space V is equivalent to an algebra homomorphism from A to $\mathrm{End}(V)$. Various notions of an operad arise in a similar way when one does not restrict oneself to linear transformations, but considers multilinear maps with any number of arguments.

Instead of vector spaces, we will use the so-called nonsymmetric collections. Superficially, a nonsymmetric collection is the same as a nonnegatively graded vector space. However, an important conceptual leap that we need already at this stage is that instead of looking at graded spaces as direct sums, it is often really helpful to think of them as sequences of their components, and never add elements of different degrees.

Definition 3.1.1.1 (Nonsymmetric collection)**.** A *nonsymmetric collection* is a sequence $\mathcal{V} = \{\mathcal{V}(n)\}_{n\geq 0}$ of vector spaces. A *morphism* between two nonsymmetric collections $\mathcal{V}$ and $\mathcal{W}$ is a collection of linear maps $\phi_n\colon \mathcal{V}(n) \to \mathcal{W}(n)$, $n \geq 0$. If each ϕ_n is an embedding of a subspace, we call the collection of their images a *subcollection* of $\mathcal{W}$, and write $\mathcal{V} \subset \mathcal{W}$.

Let us define two frequently used somewhat trivial nonsymmetric collections. In the context of operations, the first one is used to incorporate a single operation without any arguments, like the unit element in an algebra, and the second one is used to incorporate a single operation with one argument, like the identity endomorphism of a vector space.

Definition 3.1.1.2 (Collections $\underline{\mathbb{F}}$ and $\mathbb{1}$)**.** The nonsymmetric collection $\underline{\mathbb{F}}$ is defined as follows:

$$\underline{\mathbb{F}}(k) = \begin{cases} \mathbb{F}, & k = 0, \\ 0, & k > 0. \end{cases}$$

The nonsymmetric collection $\mathbb{1}$ is defined as follows:

$$\mathbb{1}(k) = \begin{cases} \mathbb{F}, & k = 1, \\ 0, & k \neq 1. \end{cases}$$

3.1.2 Nonsymmetric endomorphism operad

For the purpose of dealing with operads, the most important example of a nonsymmetric collection is the endomorphism operad of a vector space.

Example 3.1.2.1. The *endomorphism operad* of a vector space V is the nonsymmetric collection End_V with $\mathrm{End}_V(n) := \mathrm{Hom}(V^{\otimes n}, V)$, $n \geq 0$. In particular, $\mathrm{End}_V(0) = \mathrm{Hom}(\mathbb{F}, V) \cong V$, and $\mathrm{End}_V(1) = \mathrm{Hom}(V, V) = \mathrm{End}(V)$.

Similar to how the set of all endomorphisms of a vector space has a binary product, there are natural operations on End_V defined as follows.

Definition 3.1.2.2 (Nonsymmetric composition of multilinear maps)**.** Suppose that $f \in \mathrm{End}_V(r)$, $g_1 \in \mathrm{End}_V(n_1)$, $\ldots$, $g_n \in \mathrm{End}_V(n_r)$. The *nonsymmetric composition* $\gamma(f; g_1, \ldots, g_r)$, or $f \circ (g_1, \ldots, g_r)$ is an element of $\mathrm{End}_V(n_1 + \cdots + n_r)$ defined by the formula

$$f \circ (g_1, \ldots, g_r) \colon x_1, \ldots, x_{n_1+\cdots+n_r} \mapsto$$
$$f(g_1(x_{k_1+1}, \ldots, x_{k_1+n_1}), g_2(x_{k_2+1}, \ldots, x_{k_2+n_2}) \ldots, g_r(x_{k_r+1}, \ldots, x_{k_r+n_r})),$$

where $k_i = n_1 + \cdots + n_{i-1}$ (in particular, $k_1 = 0$).

There are several different ways to summarize algebraic properties of nonsymmetric compositions; two of them are outlined in the next section.

3.2 Nonsymmetric operads

3.2.1 Classical definition of a nonsymmetric operad

The approach that is probably most straightforward is to write down the associativity conditions of two-level compositions, that is, compositions where each substituted operation is itself a composition $g_i \circ (h_1, \ldots, h_{p_i})$: of course, such a composition can be computed in two different ways, either computing each $g_i \circ (h_1^{(i)}, \ldots, h_{p_i}^{(i)})$ individually or first computing $f \circ (g_1, \ldots, g_r)$, and then computing the composition of that with all the elements $h_j^{(i)}$. This leads to the most classical approach to operads, a nonsymmetric version of the definition of May [192].

Definition 3.2.1.1 (Classical definition of a nonsymmetric operad)**.** A *nonsymmetric operad* is a nonsymmetric collection of vector spaces $\mathcal{P} = \{\mathcal{P}(n)\}_{n \geq 0}$ equipped with an element $\mathrm{id} \in \mathcal{P}(1)$ and maps

$$\gamma^{(r)}_{n_1,\ldots,n_r} \colon \mathcal{P}(r) \otimes \mathcal{P}(n_1) \otimes \cdots \otimes \mathcal{P}(n_r) \to \mathcal{P}(n_1 + \cdots + n_r)$$

(for which the shorthand notation

$$f \circ (g_1, \ldots, g_r) := \gamma^{(r)}_{n_1,\ldots,n_r}(f \otimes g_1 \otimes \cdots \otimes g_r)$$

is commonly used), which satisfy the following properties:

- *associativity*:

$$f \circ (g_1 \circ (h_1^{(1)}, \dots, h_{q_1}^{(1)}), \dots, g_r \circ (h_1^{(r)}, \dots, h_{q_r}^{(r)})) = \\ (f \circ (g_1, \dots, g_r)) \circ (h_1^{(1)}, \dots, h_{q_1}^{(1)}, \dots, h_1^{(r)}, \dots, h_{q_r}^{(r)}).$$

- *unit axiom*:

$$\gamma_n^{(1)}(\mathrm{id}; \alpha) = \alpha, \quad \gamma_{1,1,\dots,1}^{(r)}(\alpha; \mathrm{id}, \dots, \mathrm{id}) = \alpha. \tag{3.1}$$

Similar to the case of associative algebras, we can define ideals in nonsymmetric operads.

Definition 3.2.1.2. Suppose that $\mathcal{P}$ is a nonsymmetric operad. An *ideal* $\mathcal{I}$ of $\mathcal{P}$ is a subcollection $\mathcal{I} \subset \mathcal{P}$ for which the element $f \circ (g_1, \dots, g_n)$ belongs to $\mathcal{I}$ if at least one of the elements $f, g_1, \dots, g_n$ belongs to $\mathcal{I}$.

3.2.2 Definition via partial compositions

An elegant economic way of dealing with nonsymmetric compositions comes from using the identity map $\mathrm{id} \in \mathrm{End}_V(1)$; it is done as follows.

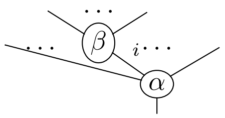
Definition 3.2.2.1 (Partial composition)**.** Let $f \in \mathrm{End}_V(n)$, $g \in \mathrm{End}_V(m)$, and $1 \le i \le n$. The *partial composition of f and g at the i-th slot*, or *infinitesimal composition of f and g at the i-th slot* is the operation

$$f \circ_i g := f \circ (\mathrm{id}, \dots, \mathrm{id}, g, \mathrm{id}, \dots, \mathrm{id}),$$

where g is at the i-th argument of f.

Remark 3.2.2.2. Both the term "partial" and the term "infinitesimal" highlight a very important feature of operads which makes them more complicated than associative algebras: the composition $\circ$ in the classical definition needs one element on the left, but several elements on the right. The word "partial" indicates, literally, that instead of performing all substitutions simultaneously, one can perform them step by step, accomplishing the goal partially at each step. The word "infinitesimal" indicates that those compositions may be viewed as directional derivatives of the full composition map.

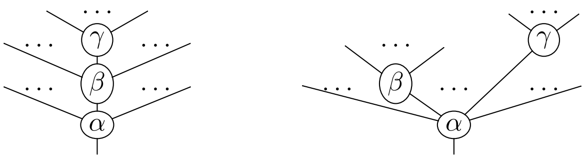
When dealing with multilinear operations it is extremely useful to depict elements by rooted trees. For example, the partial composition $\alpha \circ_i \beta$ is represented by the tree



.

whose internal vertices are labelled by α and β.

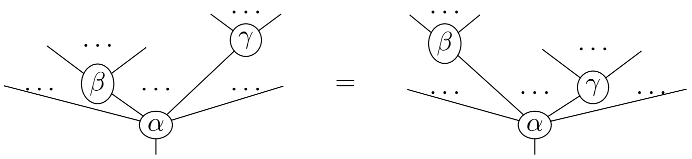
Suppose that we use partial compositions to create a single element out of three elements $\alpha \in \mathrm{End}_V(n)$, $\beta \in \mathrm{End}_V(m)$, $\gamma \in \mathrm{End}_V(r)$. This can be done in two essentially different ways represented by the following three-vertex trees:



For the first of those trees, we compose the three operations in a sequence, and this kind of composition satisfies a property that generalizes the associativity of composition of linear transformations. Basically, the corresponding composition can be computed in two different ways, and those ways must give the same result. On the level of formulas, this gives

$$(\alpha \circ_i \beta) \circ_j \gamma = \alpha \circ_i (\beta \circ_{j-i+1} \gamma) \quad \text{for } i \le j \le i+m-1.$$

For the second of those trees, we compose two operations in parallel, and this kind of composition satisfies a property that is somewhat closer to commutativity; that property is not visible on the level of associative algebras. More precisely, here two operations are composed in parallel, and there are two different ways to compute that composition depending on a choice of levels of vertices in trees. These ways must produce the same result:



(3.2)

On the level of formulas, this gives

$$(\alpha \circ_i \beta) \circ_j \gamma = \begin{cases} (\alpha \circ_{j-m+1} \gamma) \circ_i \beta, & i+m \le j \le n+m-1, \\ (\alpha \circ_j \gamma) \circ_{i+r-1} \beta, & 1 \le j \le i-1 \end{cases}$$

(there are two formulas, the first one corresponds to the picture above, and the second one corresponds to its mirror reflection).

Abstracting from the concrete endomorphism collection, we arrive at the following definition. In this definition, we slightly abuse the notation by using the notation id for an element which, strictly speaking, is not the identity endomorphism of any vector space. However, this notation is so helpful for forming the right intuition that it would be a pedagogical mistake to not use it.

Definition 3.2.2.3 ("Partial" definition of a nonsymmetric operad).

A *nonsymmetric operad* is a nonsymmetric collection of vector spaces $\mathcal{P} = \{\mathcal{P}(n)\}_{n\geq 0}$ equipped with an element $\mathrm{id} \in \mathcal{P}(1)$ and maps

$$\circ_i \colon \mathcal{P}(n) \otimes \mathcal{P}(m) \to \mathcal{P}(n+m-1), \quad \alpha \otimes \beta \mapsto \alpha \circ_i \beta$$

which satisfy the following properties for all $\alpha \in \mathcal{P}(n)$, $\beta \in \mathcal{P}(m)$, $\gamma \in \mathcal{P}(r)$:

- *sequential axiom*:

$$(\alpha \circ_i \beta) \circ_j \gamma = \alpha \circ_i (\beta \circ_{j-i+1} \gamma) \quad \text{for } i \leq j \leq i+m-1; \tag{3.3}$$

- *parallel axiom*:

$$(\alpha \circ_i \beta) \circ_j \gamma = \begin{cases} (\alpha \circ_{j-m+1} \gamma) \circ_i \beta, & i+m \leq j \leq n+m-1, \\ (\alpha \circ_j \gamma) \circ_{i+r-1} \beta, & 1 \leq j \leq i-1; \end{cases} \tag{3.4}$$

- *unit axiom*:

$$\mathrm{id} \circ_1 \alpha = \alpha, \quad \alpha \circ_i \mathrm{id} = \alpha \quad \text{for } 1 \leq i \leq n. \tag{3.5}$$

The following result is well known; it is featured in every textbook on operads. Throughout this book, we will furnish some proofs having in mind the classical definition of a nonsymmetric operad, and some others with the partial definition; the reader is advised to not be wary of that.

Proposition 3.2.2.4. *The classical and the partial definition of a nonsymmetric operad are equivalent to each other.*

3.3 Free nonsymmetric operads

Similar to the case of associative algebras, a nonsymmetric operad can be presented via generators and relations, that is, as a quotient of the free nonsymmetric operad $\mathcal{T}(\mathcal{M})$. To define that object, we will first develop a language for working with trees, and then use that language to define appropriate monomials that represent composite operations with many arguments in the same way as words represent compositions of endomorphisms.

3.3.1 Trees

The following abstract definition is one possible way to formalize the naïve notion of a rooted tree.

Definition 3.3.1.1 (Rooted tree)**.** A *rooted tree* τ consists of:

- a finite set of *vertices* $\mathrm{Vert}(\tau)$ represented as a disjoint union
$$\mathrm{Vert}(\tau) = \mathrm{Int}(\tau) \sqcup \mathrm{Leaves}(\tau) \sqcup \{r\},$$
where elements of the (possibly empty) set $\mathrm{Int}(\tau)$ are called *internal vertices*, elements of the (possibly empty) set $\mathrm{Leaves}(\tau)$ are called *leaves*, and the element r is called the *root* of τ, and denoted $\mathrm{Root}(\tau)$, and

- a *parent function*
$$\mathrm{Parent}_\tau \colon \mathrm{Vert}(\tau) \setminus \{r\} \to \mathrm{Vert}(\tau),$$
for which
$$|\,\mathrm{Parent}_\tau^{-1}(r)| = 1,$$
$$\mathrm{Parent}_\tau^{-1}(l) = \varnothing \text{ for each } l \in \mathrm{Leaves}(\tau).$$
The only requirement imposed on this function is *connectivity*: for each vertex $v \in \mathrm{Vert}(\tau)\setminus\{r\}$ there is a (unique) positive integer l and vertices $v_0 = v$, v_1, …, $v_l = r$, such that $v_i = \mathrm{Parent}_\tau(v_{i-1})$ for all $i = 1, \dots, l$. This number l is called the *depth* of the vertex v, and the sequence v_l, v_{l-1}, …, v_0 is referred to as the *path from root to v*.

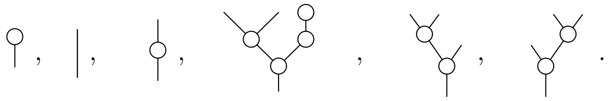
An *endpoint* of a tree τ is a vertex $v \in \mathrm{Vert}(\tau)$ for which $\mathrm{Parent}_\tau^{-1}(v) = \varnothing$; from the above conditions we see that each leaf of τ is an endpoint, but there may be endpoints that are not leaves.

The only tree τ for which $\mathrm{Int}(\tau)$ is empty is called the *trivial tree*.

Two rooted trees are said to be *isomorphic* if there is a map between their sets of vertices that respects all the data described above.

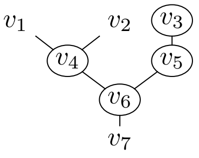
Rooted trees are conventionally depicted by diagrams made of points, little circles, and edges, that is, straight lines connecting points and circles. Each point represents a leaf or the root, each little circle represents an internal vertex, and each edge between v and v' directed downward from v to v' represents the relation $v' = \mathrm{Parent}_\tau(v)$. In particular, the root is always at the bottom of the diagram.

Example 3.3.1.2. The following diagrams represent rooted trees:



The second tree is the trivial tree. The last two trees are isomorphic.

The fourth diagram which we now represent with labels that give names to all the vertices



represents a rooted tree τ for which

$$\begin{gathered} r = v_7, \\ \mathrm{Leaves}(\tau) = \{v_1, v_2\}, \\ \mathrm{Int}(\tau) = \{v_3, v_4, v_5, v_6\}, \\ \mathrm{Parent}(v_1) = \mathrm{Parent}(v_2) = v_4, \\ \mathrm{Parent}(v_3) = v_5, \\ \mathrm{Parent}(v_4) = \mathrm{Parent}(v_5) = v_6, \\ \mathrm{Parent}(v_6) = v_7. \end{gathered}$$

To represent operations with many arguments in this book, we will mostly be using planar rooted trees, defined as follows.

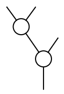
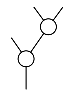
Definition 3.3.1.3 (Planar rooted tree)**.** A *planar rooted tree* τ is a rooted tree together with a *planar structure*, i.e., a total order on the preimage $\mathrm{Parent}_\tau^{-1}(v)$ for each $v \in \mathrm{Vert}(\tau)$.

Two rooted trees are said to be *isomorphic* if there is a map between their sets of vertices that respects all the rooted tree data and their respective planar structures.

A planar structure of a tree τ induces a total order on the set of its endpoints as follows. Let e and e' be two different endpoints of τ, and consider the paths from the root to e and e'. Suppose that the first k vertices of those paths coincide, and the $k+1$-st vertices, say v_{k+1} and v'_{k+1}, are different. Under this assumption, $\mathrm{Parent}_\tau(v_{k+1}) = \mathrm{Parent}_\tau(v'_{k+1})$, and hence the planar structure allows to compare v_{k+1} and v'_{k+1}. We say that $e \prec e'$ if $v_{k+1} \prec v'_{k+1}$.

Throughout this book, we will be drawing planar rooted trees in the plane in a way that the planar order on $\mathrm{Parent}_\tau^{-1}(v)$ is determined by ordering the corresponding edges left-to-right.

Example 3.3.1.4. The trees

 , and  ,

viewed as planar rooted trees with the left-to-right planar structures are no longer isomorphic.

3.3.2 Tree monomials and tree polynomials

Let us describe an explicit construction of the free nonsymmetric operad with a given set of generators; for a formal categorical construction see [180]. Similarly to how free associative algebras are spanned by words, which can also be viewed as decomposable tensors, free nonsymmetric operads are spanned by decorated trees, which are often viewed as “tree-shaped tensors”. Similarly how individual letters of a word representing a monomial in the free associative algebra can be thought of as representing some linear transformations, individual internal vertices of a tree represent multilinear operations; they should be decorated accordingly.

Definition 3.3.2.1 (Operation alphabet)**.** An *operation alphabet* is a collection $\mathcal{X} = \{\mathcal{X}(n)\}_{n\geq 0}$ of finite sets $\mathcal{X}(n)$ indexed by nonnegative integers n. The number n is referred to as *arity* of an element $x \in \mathcal{X}(n)$.

Throughout this chapter, unless otherwise specified, $\mathcal{X}$ denotes an arbitrary operation alphabet.

Definition 3.3.2.2 (Nonsymmetric tree monomial)**.** A *nonsymmetric tree monomial* in $\mathcal{X}$ is a pair $T = (\tau, \mathsf{x})$, where τ is a planar rooted tree and x is a labelling of all internal vertices of τ by elements of $\mathcal{X}$; each vertex v must have a label $\mathsf{x}_v \in \mathcal{X}(|\operatorname{Parent}^{-1}(v)|)$.

The tree monomial for which the underlying tree τ is the trivial tree is called the *trivial tree monomial*, or the *empty tree monomial.*

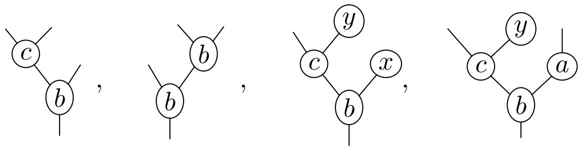
The *arity* of a tree monomial T, denoted $\operatorname{ar}(T)$, is the number of leaves of τ, and its *weight*, denoted $\operatorname{wt}(T)$, is the number of internal vertices of τ.

The set of all tree monomials in $\mathcal{X}$ of arity n is denoted $\operatorname{Tree}_{\mathcal{X}}(n)$. The collection of all these sets for all $n \geq 0$ is denoted $\operatorname{Tree}_{\mathcal{X}}$.

Example 3.3.2.3. Suppose that

$$\mathcal{X}(0) = \{x, y\}, \quad \mathcal{X}(1) = \{a\}, \quad \mathcal{X}(2) = \{b, c\}.$$

The following are examples of tree monomials in $\operatorname{Tree}_{\mathcal{X}}$:



The first two of them have arity 3 and weight 2, the third one has arity 1 and weight 4, and the last one has arity 2 and weight 4.

Definition 3.3.2.4. (Nonsymmetric tree polynomial) A *nonsymmetric tree polynomial* in $\mathcal{X}$ with coefficients in $\mathbb{F}$ is a linear combination of nonsymmetric tree monomials of the same arity. The *support* of a nonsymmetric tree polynomial f, denoted $\operatorname{supp}(f)$, is the set of all nonsymmetric tree monomials that appear in f with nonzero coefficients.

We denote the vector space of all nonsymmetric tree polynomials of arity n by $\mathcal{T}(\mathcal{X})(n)$; of course we have $\mathcal{T}(\mathcal{X})(n) = \mathbb{F}\operatorname{Tree}_{\mathcal{X}}(n)$.

3.3.3 Grafting trees and the free nonsymmetric operad

In the case of associative algebras, we use the intuitive notion of concatenation of words to define products. For operations, the notion that serves a similar purpose is that of grafting of trees. We will discuss two different types of graftings, full and partial; these correspond to compositions from the classical definition of a nonsymmetric operad and partial compositions, respectively.

Full grafting of planar trees $\tau_1, \ldots, \tau_r$ to a planar tree τ_0 corresponds, in terms of our graphical representation, to joining the open edges corresponding to the roots of $\tau_1, \ldots, \tau_r$ with the open edges corresponding to leaves of τ_0, in the total planar order.

Definition 3.3.3.1 (Full grafting of planar rooted trees)**.** Let $\tau_0, \tau_1, \ldots, \tau_r$ be planar rooted trees, and suppose that τ_0 has r leaves. We define a planar rooted tree $\tau_0 \circ (\tau_1, \ldots, \tau_r)$, called the result of *full grafting* of $\tau_1, \ldots, \tau_r$ to τ_0, to be the planar rooted tree τ for which:

$$\begin{aligned} \mathrm{Root}(\tau) &= \mathrm{Root}(\tau_0), \\ \mathrm{Int}(\tau) &= \bigsqcup_{i=0}^{r} \mathrm{Int}(\tau_i), \\ \mathrm{Leaves}(\tau) &= \bigsqcup_{i=1}^{r} \mathrm{Leaves}(\tau_i). \end{aligned}$$

The parent function and the planar structure on the thus defined set of vertices are induced by the respective parent functions and planar structures of τ_i, $0 \leq i \leq r$, with the following exceptions. For each $j = 1, \ldots, r$, for the only vertex v_j in $\mathrm{Parent}_{\tau_j}^{-1}(\mathrm{Root}(\tau_j))$, we define

$$\mathrm{Parent}_{\tau}(v_j) := \mathrm{Parent}_{\tau_0}(\ell_j),$$

where ℓ_j is the j-th leaf of τ_0 in the total planar order on leaves induced from the total planar order of endpoints of τ_0. This means that

$$\mathrm{Parent}_{\tau}^{-1}(\mathrm{Parent}_{\tau_0}(\ell_j)) = \{v_j\} \sqcup \mathrm{Parent}_{\tau_0}^{-1}(\mathrm{Parent}_{\tau_0}(\ell_j)) \setminus \{\ell_j\};$$

the total order needed by the planar structure puts v_j in the place of ℓ_j.

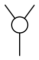
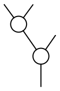
If all the grafted trees τ_i except for one are trivial, we end up with the definition of partial grafting.

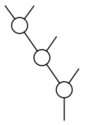
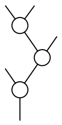
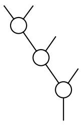
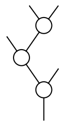
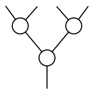
Definition 3.3.3.2 (Partial grafting of planar rooted trees)**.** Suppose that τ_1 and τ_2 are two rooted planar trees. Let $\ell \in \mathrm{Leaves}(\tau_1)$. We define a planar rooted tree $\tau_1 \circ_\ell \tau_2$, called the result of *partial grafting* of τ_2 to τ_1 at ℓ, as follows. We put

$$\mathrm{Root}(\tau_1 \circ_\ell \tau_2) = \mathrm{Root}(\tau_1),$$

$$\mathrm{Int}(\tau_1 \circ_\ell \tau_2) = \mathrm{Int}(\tau_1) \sqcup \mathrm{Int}(\tau_2),$$
$$\mathrm{Leaves}(\tau_1 \circ_\ell \tau_2) = \mathrm{Leaves}(\tau_1) \sqcup \mathrm{Leaves}(\tau_2) \setminus \{\ell\}.$$

The parent function and the planar structure on the thus defined set of vertices are induced by the respective parent functions and planar structures of τ_1 and τ_2 with two small exceptions. For the only vertex v in $\mathrm{Parent}_{\tau_2}^{-1}(\mathrm{Root}(\tau_2))$, we define $\mathrm{Parent}_{\tau_1 \circ_\ell \tau_2}(v) = \mathrm{Parent}_{\tau_1}(\ell)$. This means that $\mathrm{Parent}_{\tau_1 \circ_\ell \tau_2}^{-1}(\mathrm{Parent}_{\tau_1}(\ell)) = \{v\} \sqcup \mathrm{Parent}_{\tau_1}^{-1}(\mathrm{Parent}_{\tau_1}(\ell)) \setminus \{\ell\}$; the total order needed by the planar structure puts v in the place of ℓ.

Example 3.3.3.3. Let $\tau_1 =$  and $\tau_2 =$  . Various partial compositions of these trees are summarized in the following table:

$\tau_1 \circ_1 \tau_2$	$\tau_1 \circ_2 \tau_2$	$\tau_2 \circ_1 \tau_1$	$\tau_2 \circ_2 \tau_1$	$\tau_2 \circ_3 \tau_1$
				

Grafting of trees allows us to give an explicit construction of free nonsymmetric operads.

Definition 3.3.3.4 (Free nonsymmetric operad)**.** Suppose that we are given nonsymmetric tree monomials $T_0 = (\tau_0, \mathsf{x}_0) \in \mathrm{Tree}_{\mathcal{X}}(r)$, $T_1 = (\tau_1, \mathsf{x}_1) \in \mathrm{Tree}_{\mathcal{X}}(n_1)$, $\ldots$, $T_r = (\tau_r, \mathsf{x}_r) \in \mathrm{Tree}_{\mathcal{X}}(n_r)$. We define the *nonsymmetric composition*

$$T_0 \circ (T_1, \ldots, T_r)$$

to be the nonsymmetric tree monomial (τ, x), where

$$\tau = \tau_0 \circ (\tau_1, \ldots, \tau_r),$$

and the labelling x of $\mathrm{Int}(\tau) = \bigsqcup_{i=0}^{r} \mathrm{Int}(\tau_i)$ is given by the disjoint union of labellings x_j, $1 \le j \le r$.

These nonsymmetric compositions may be extended by multilinearity to the collection $\mathcal{T}(\mathcal{X}) = \{\mathcal{T}(\mathcal{X})(n)\}_{n \ge 0}$ of all nonsymmetric tree polynomials of all arities, giving operations

$$\gamma^{(r)}_{n_1,\ldots,n_r} \colon \mathcal{T}(\mathcal{X})(r) \otimes \mathcal{T}(\mathcal{X})(n_1) \otimes \cdots \otimes \mathcal{T}(n_r) \to \mathcal{T}(\mathcal{X})(n_1 + \cdots + n_r).$$

Equipped with these operations, $\mathcal{T}(\mathcal{X})$ is the *free nonsymmetric operad generated by* $\mathcal{X}$. In addition to the notation $\mathcal{T}(\mathcal{X})$, we will use the notation $\mathcal{T}(\mathcal{M})$, where $\mathcal{M} = \{\mathcal{M}(n)\}_{n \ge 0}$ is a collection of vector spaces for which $\mathcal{M}(n) = \mathrm{span}(\mathcal{X}(n))$ for all $n \ge 0$.

Throughout this chapter, we only consider nonsymmetric tree monomials and polynomials, so we will occasionally drop the word "nonsymmetric", hoping that it does not lead to confusion.

3.3.4 Presentation by generators and relations

The analogue of First Homomorphism Theorem holds for nonsymmetric operads, and we may utilize it to define presentations of operads. Suppose that a nonsymmetric operad $\mathcal{P}$ is generated by a collection of operations $\alpha_i \in \mathcal{P}(n_i)$. In that case, we can consider the collection $\mathcal{X}$ of operations $\kappa_i \in \mathcal{X}(n_i)$, one operation for each generator of $\mathcal{P}$. There is a surjective homomorphism from the free nonsymmetric operad $\mathcal{T}(\mathcal{X})$ onto $\mathcal{P}$ sending κ_i to α_i which is uniquely defined by the universal property of the free operad. By the First Homomorphism Theorem, that homomorphism is the canonical map onto the quotient of $\mathcal{T}(\mathcal{X})$ by some ideal $\mathcal{I}$.

Definition 3.3.4.1 (Ideal generated by a subset)**.** Let $\mathcal{P}$ be a nonsymmetric operad, and suppose that $\mathcal{S} \subset \mathcal{P}$ is a subcollection. The *ideal of $\mathcal{P}$ generated by $\mathcal{S}$*, denoted by $(\mathcal{S})$, is the smallest (by inclusion) ideal of $\mathcal{P}$ containing $\mathcal{S}$.

We are now ready to define a presentation of a nonsymmetric operad.

Definition 3.3.4.2 (Presentation of a nonsymmetric operad)**.** Suppose that the nonsymmetric operad $\mathcal{P}$ is a quotient of the free operad $\mathcal{T}(\mathcal{X})$ by some ideal $\mathcal{I}$, and that the ideal $\mathcal{I}$ is generated by the collection $\mathcal{S}$. In this case, we will say that the operad $\mathcal{P}$ is *presented by generators $\mathcal{X}$ and relations $\mathcal{S}$*.

3.4 Normal forms

This section is a detailed account of [78, Sec. 2], which, in turn, adapts methods of [74, 135] to nonsymmetric operads, including operads with arity zero generators.

3.4.1 Monomial orders

Let us generalize the definition of a monomial order to the case of nonsymmetric tree monomials.

Definition 3.4.1.1 (Monomial order)**.** A collection of total orders Ξ_n of $\mathrm{Tree}_{\mathcal{X}}(n)$, $n \geq 0$, is said to be a *monomial order* if the following two conditions are satisfied:

- each Ξ_n is a well-order;
- each nonsymmetric composition is a strictly increasing function in each of its arguments; that is if $T_0, T_0' \in \mathrm{Tree}_{\mathcal{X}}(r)$, $T_1, T_1' \in \mathrm{Tree}_{\mathcal{X}}(n_1)$, $\dots$, $T_r, T_r' \in \mathrm{Tree}_{\mathcal{X}}(n_r)$, then

$$T_0 \circ (T_1, \dots, T_r) \prec T_0' \circ (T_1, \dots, T_r) \text{ if } T_0 \prec T_0',$$
$$T_0 \circ (T_1, \dots, T_i, \dots, T_r) \prec T_0 \circ (T_1, \dots, T_i, \dots, T_r) \text{ if } T_i \prec T_i'.$$

Unless otherwise specified, throughout this chapter, we will give definitions as well as state and prove all theoretical results for an arbitrary monomial order Ξ.

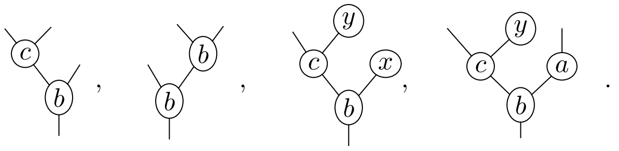
We continue with an important construction of monomial orders. We denote $X := \bigsqcup_{n\geq 0} \mathcal{X}(n)$. We will first explain how to replace every tree monomial by a sequence of words in the alphabet X that transform in a controllable way under composition.

Definition 3.4.1.2 (Path sequence of a nonsymmetric tree monomial)**.** Let $T = (\tau, \mathsf{x})$ be a tree monomial. For each endpoint e of τ in the total order induced by the planar structure, we record the labels of internal vertices of the path from the root of τ to e, forming a word in the alphabet X. The sequence of these words, denoted $\mathrm{Path}(T)$, is called the *path sequence* of the tree monomial T.

Example 3.4.1.3. Suppose that

$$\mathcal{X}(0) = \{x, y\}, \quad \mathcal{X}(1) = \{a\}, \quad \mathcal{X}(2) = \{b, c\}.$$

Let us consider the tree monomials from Example 3.3.2.3



The corresponding path sequences are, respectively,

$$(bc, bc, b), \quad (b, bb, bb), \quad (bc, bcy, bx), \quad (bc, bcy, ba).$$

Note that the two path sequences (bc, bcy, bx) and (bc, bcy, ba) from the example we just considered look deceptively similar, but if we recall that the letter x corresponds to an operation of arity zero (that is, constants), while the letter a corresponds to a unary operation, we instantly see that the path sequences correspond to tree monomials whose underlying trees are combinatorially different. This observation is the key to the following result.

Lemma 3.4.1.4. *A tree monomial* $T = (\tau, \mathsf{x})$ *is uniquely determined by the sequence* $\mathrm{Path}(T)$*: if* $\mathrm{Path}(T_1) = \mathrm{Path}(T_2) = p$*, then* $T_1 = T_2$*.*

Proof. We will prove this statement by induction on the sum of weights of all words of the path sequence p in question. If that sum is equal to zero, the path sequence is empty, and it corresponds to the trivial monomial. Assume that the statement is proved for all path sequences for which the sum of weights of words is at most k, and consider some path sequence with the sum of weights $k+1$. Let w be the maximal weight of words in p, and let p_i be the first word of weight w, so that $\mathrm{wt}(p_j) < w$ for $j < i$. If the word p_i ends with an element $x \in \mathcal{X}(0)$, then the i-th endpoint of both T_1 and T_2 is an internal vertex labelled by x, so we can chop that letter off the i-th word of p, obtaining a sequence p', reconstruct $T_1' = T_2'$, and proceed by induction. Therefore, we may assume that the last letter x of p_i belongs to $\mathcal{X}(k)$ for some $k > 0$. This means that in both T_1 and T_2 the parent of the leaf i (in the total planar order) is a vertex v with $|\operatorname{Parent}^{-1}(i)| = k$; moreover, the condition that i is the first position where the weight w occurs implies that the leaf i is the minimal element of $\operatorname{Parent}^{-1}(i)$ in the planar structure, and the maximality of w also implies that other elements of $\operatorname{Parent}^{-1}(i)$ are leaves as well. Therefore, we can replace the words $p_i = \cdots = p_{i+k-1}$ by a single word obtained by chopping the last letter off p_i, thus obtaining a sequence p', reconstruct $T_1' = T_2'$, and proceed by induction. □

Definition 3.4.1.5 (Path extension)**.** Suppose that Ξ is a monomial order on X^*. The *path extension of* Ξ is the degree-lexicographic order on path sequences that is derived from Ξ. In other words:

- if for two tree monomials $T_1 = (\tau_1, \mathsf{x}_1)$ and $T_2 = (\tau_2, \mathsf{x}_2)$ the number of endpoints of τ_1 is less than the number of endpoints of τ_2, we put $T_1 \prec T_2$;

- if τ_1 and τ_2 have the same numbers of endpoints, we compare the sequences $\operatorname{Path}(T_1)$ and $\operatorname{Path}(T_2)$ word by word, comparing words using the order Ξ.

Proposition 3.4.1.6. *The path extension of any monomial order Ξ, viewed as an order of tree monomials, is a monomial order.*

Proof. From Lemma 3.4.1.4 it follows immediately that the path extension is a total order of tree monomials. The fact that it is a well-order is clear from the same assumption on the order Ξ. Finally, let us prove that each nonsymmetric composition is strictly increasing in each of its arguments. Let us note that the endpoints of a tree τ are its leaves and its internal vertices v with $\operatorname{Parent}^{-1}(v) = \varnothing$. On the level of sequences, it is easy to distinguish between the two: words that correspond to non-leaf vertices end with elements of $\mathcal{X}(0)$. With that in mind, let us observe that for tree monomials

$$T_0 = (\tau_0, \mathsf{x}_0), \quad T_1 = (\tau_1, \mathsf{x}_1) \quad , \dots, \quad T_r = (\tau_r, \mathsf{x}_r),$$

we obtain the sequence $\operatorname{Path}(T_0 \circ (T_1, \dots, T_r))$ as follows:

- first record the words corresponding to endpoints of T_0 before its first leaf,

- then the words obtained by concatenating the word corresponding to the first leaf of T_0 with each of the words of $\operatorname{Path}(T_1)$,

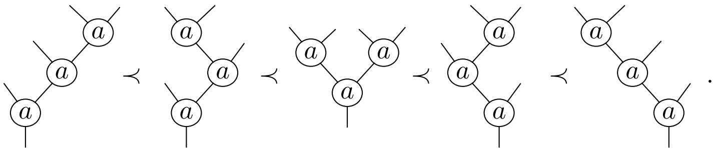
- then the words corresponding to endpoints of T_0 before its second leaf,

- then the words obtained by concatenating the word corresponding to the second leaf of T_0 with each of the words of $\mathrm{Path}(T_2)$,
- ...
- then the words corresponding to endpoints of T_0 before its r-th leaf,
- then the words obtained by concatenating the word corresponding to the r-th leaf of T_0 with each of the words of $\mathrm{Path}(T_r)$,
- and finally the words corresponding to endpoints of T_0 after its r-th leaf.

Since the order Ξ is assumed increasing in each argument for the concatenation product, the statement follows. $\square$

Definition 3.4.1.7 (Graded path lexicographic order)**.** Let us fix some order Ξ of $X := \bigsqcup_{n\geq 0} \mathcal{X}(n)$. The *graded path lexicographic order* of tree monomials, denoted `gpathlex`, is the path extension of the `glex` order induced by Ξ.

Example 3.4.1.8. Let $\mathcal{X}_2 = \{a\}$. For the `gpathlex` order, we have



This follows from comparing the corresponding path sequences

$$(a, a^2, a^3, a^3) \prec (a, a^3, a^3, a^2) \prec (a^2, a^2, a^2, a^2) \prec \\ \prec (a^2, a^3, a^3, a) \prec (a^3, a^3, a^2, a).$$

Remark 3.4.1.9. Suppose that $\mathcal{X}(0) = \mathcal{X}(1) = \varnothing$, and that for each n the set $\mathcal{X}(n)$ is finite. Under this assumption, if a total order Ξ of words in the alphabet X is such that the concatenation product is increasing in each argument, then the path extension of Ξ is a monomial order even if Ξ is not a well-order. The reason for that is that under our assumption there are only finitely many tree monomials with the given number of endpoints, and so the well-order property of the path extension is obtained for free.

3.4.2 Long division

In the case of associative algebras, it was crucial to have two views of divisibility of words; one can define divisibility in terms of structure operations of an algebra, as well as combinatorially, as inclusion of a subword. Both definitions are immensely useful: the first one is meaningful, while the second one allows one to work with divisibility algorithmically. We will now explain how the same is done for nonsymmetric operads. First of all, the notion of a subword of a word becomes, in the case of operations, the notion of a subtree of a given tree.

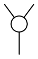
Definition 3.4.2.1 (Subtree of a planar rooted tree)**.** Let τ be a rooted tree. Suppose that $V' \subset \mathrm{Int}(\tau)$ is a nonempty subset satisfying the following properties:

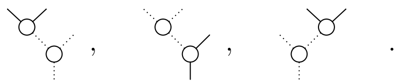
- there exists just one vertex $v' \in V'$ for which $\mathrm{Parent}_\tau(v')$ is not in V',
- for each vertex $v'' \in V'$ there is a (unique) nonnegative integer l and vertices $v_0 = v'$, v_1, …, $v_l = v''$, such that $v_i = \mathrm{Parent}_\tau(v_{i-1})$ for all $i = 1, \dots, l$,
- for each vertex v'' in V' the preimage $\mathrm{Parent}_\tau^{-1}(v')$ is either contained in V' or is disjoint from V'.

Each such subset V' defines a planar rooted tree τ' called a *subtree* of τ. We put

$$\begin{aligned} \mathrm{Root}(\tau') &= \mathrm{Parent}_\tau(v'), \\ \mathrm{Int}(\tau') &= V', \\ \mathrm{Leaves}(\tau') &= \left(\bigcup_{v' \in V'} \mathrm{Parent}_\tau^{-1}(V') \right) \setminus V', \end{aligned}$$

and use the induced parent function and the induced planar structure on the thus defined set of vertices. If $\mathrm{Parent}_\tau(v') = r$, we say that the subtree τ' and the ambient tree τ *share the root.* If $\mathrm{Int}(\tau')$ is a proper subset of $\mathrm{Int}(\tau)$, we say that τ' is a *proper subtree* of τ.

Example 3.4.2.2. In each of the following trees, the vertices connected by dotted lines form a subtree isomorphic to  :

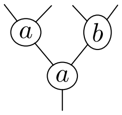


Definition 3.4.2.3 (Maximal subtree)**.** Let τ be a planar rooted tree, and let $v \in \mathrm{Int}(\tau)$. Consider the set of all vertices v' of τ for which the path from v' to the root contains $r' := \mathrm{Parent}(v)$. This set of vertices satisfies the conditions of Definition 3.4.2.1, and therefore defines a subtree τ' of τ. We call this subtree the *maximal subtree of* τ *rooted at* r'.

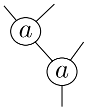
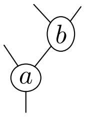
The following definition of divisibility is a combinatorial definition generalizing occurrence of a subword.

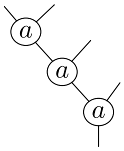
Definition 3.4.2.4 (Divisibility of tree monomials)**.** A tree monomial $T_1 = (\tau_1, \mathsf{x}_1)$ is *divisible* by a (nontrivial) tree monomial $T_2 = (\tau_2, \mathsf{x}_2)$ if the tree τ_1 contains a subtree τ_1' isomorphic to the tree τ_2, and the labels of internal vertices of that subtree in the monomial T_1 match the labels of τ_2 in the monomial T_2.

Example 3.4.2.5. Let $\mathcal{X} = \{a, b\}$. The monomial

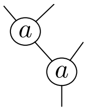


$\in \mathcal{T}(\mathcal{X})(4)$

has two different divisors of weight 2: the "left divisor"  and the "right divisor" . In comparison, the tree monomial



$\in \mathcal{T}(\mathcal{X})(4)$

has two divisors which are both occurrences of the monomial .

Let us prove that the notion of divisibility we just introduced matches the notion of divisibility coming from the existing algebraic structure on $\mathcal{T}(\mathcal{X})$.

Proposition 3.4.2.6. *Let $T_1 = (\tau_1, \mathsf{x}_1)$ and $T_2 = (\tau_2, \mathsf{x}_2)$ be two tree monomials. Then T_1 is divisible by T_2 if and only if it can be obtained from T_2 by iterated nonsymmetric compositions with elements of $\mathcal{T}(\mathcal{X})$.*

Proof. If T_1 can be obtained from T_2 by iterated nonsymmetric compositions, the set of all internal vertices of T_1 which come from T_1 define an appropriate subtree with matching labels. Suppose that τ_1 contains a subtree τ_1' rooted at some vertex r' which is isomorphic to τ_2, and that labels of that subtree match x_2.

If $T_1 = T_2$, then there is nothing to prove. Let us first demonstrate that it is enough to consider the case where τ_1' and τ_1 share a root. Otherwise, let us consider τ_1'', the maximal subtree of τ_1 rooted at r', and the tree monomial $T = (\tau, \mathsf{x})$ obtained from T_1 by collapsing τ_1'':

$$\begin{aligned}\mathrm{Root}(\tau) &= \mathrm{Root}(\tau_1),\\ \mathrm{Int}(\tau) &= \mathrm{Int}(\tau_1) \setminus \mathrm{Int}(\tau_1''),\\ \mathrm{Leaves}(\tau) &= \{\mathrm{Parent}_{\tau_1}^{-1}(r')\} \sqcup \mathrm{Leaves}(\tau_1) \setminus \mathrm{Leaves}(\tau_1'')\mathsf{x} = \mathsf{x}_1|_{\mathrm{Int}(\tau)}.\end{aligned}$$

It is clear that $T_1 = T \circ_\ell T'$, where $\ell = \mathrm{Parent}_{\tau_1}^{-1}(r')$, and $T' = (\tau_1'', \mathsf{x}_1|_{\mathrm{Int}(\tau'')})$, and T_2 is a divisor of T' that shares the root with T'. Now consider the set leaves of τ_1' which we now view as a subtree of τ_1''. For each of these leaves which is not a leaf of τ_1'', we can collapse the subtree of τ_1'' rooted at the parent of that leaf, as above. This represents T' as a nonsymmetric composition of T_2 with the tree monomials whose underlying trees were collapsed during this process. □

Definition 3.4.2.7 (Insertion into a tree monomial)**.** Suppose that T_1 and T_2 are tree monomials, and T_1 is divisible by T_2. In this case, there is an *insertion* operation

$$\square_{T_1,T_2} \colon \mathcal{T}(\mathcal{X})(\mathrm{ar}(T_2)) \to \mathcal{T}(\mathcal{X})(\mathrm{ar}(T_1)).$$

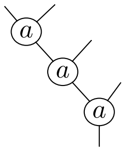
If $T = (\tau, \mathsf{x})$ is a tree monomial of the same arity as T_2, the insertion operation replaces the subtree τ_1' by τ (ensuring that each subtree of τ_1 that was grafted at a certain leaf of τ_1' gets grafted at the respective leaf of τ), and changing labels of internal vertices accordingly. Then, this operation is extended by linearity to all tree polynomials of the same arity.

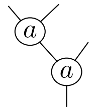
Remark 3.4.2.8.

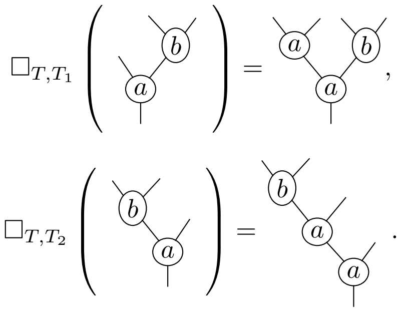
- Our notation is not completely precise, since there may be several different divisors T_2 inside T_1. We always assume that the operation $\square_{T_1,T_2}$ inserts everything at a particular occurrence of T_2 inside T_1 which is implicit.

- Proposition 3.4.2.6 shows that in fact the operation $\square_{T_1,T_2}$ can be expressed as an iterated nonsymmetric composition; we however believe that thinking of it as an insertion is a very helpful bit of intuition.

Example 3.4.2.9. Let $\mathcal{X} = \{a, b\}$. Consider the tree monomial

$T =$  $\in \mathcal{T}(\mathcal{X})(4)$

from Example 3.4.2.5. This monomial has two occurrences of  as a divisor; let us denote the one sharing the root with T by T_1, and the other one by T_2. We have



One very useful feature of the insertion operations is that they allow us to give an explicit description of an ideal generated by a given collection $\mathcal{S}$ in the free operad which is a suitable replacement of the description "the ideal (S) is the linear span of all elements r_1sr_2 for all $r_1, r_2 \in T(X)$, $s \in S$" which we had in the associative case.

Proposition 3.4.2.10. *Let $\mathcal{S} \subset \mathcal{T}(\mathcal{X})$. The ideal $(\mathcal{S})$ generated by $\mathcal{S}$ can be described explicitly as the linear span of all insertions $\square_{T_1,T_2}(f)$, where T_1 is a monomial, T_2 is a divisor of T_1, and $f \in \mathcal{S}(\mathrm{ar}(T_2))$.*

Proof. The ideal $(\mathcal{S})$ is spanned by iterated nonsymmetric compositions where at least one of the elements involved belongs to $\mathcal{S}$; by multilinearity of compositions, we may assume that all other elements are monomials, in which case the corresponding iterated composition is the insertion operation. □

The following proposition is clear from the definition. It expresses another type of associativity exhibited by operads, related to the monadic definition of an operad, see [180].

Proposition 3.4.2.11. *Let*

$$T \in \mathrm{Tree}_{\mathcal{X}}(n), T_1, T_1' \in \mathrm{Tree}_{\mathcal{X}}(n_1), T_2 \in \mathrm{Tree}_{\mathcal{X}}(n_2),$$

and suppose that T_1 is a divisor of T and T_2 is a divisor of T_1'. Then

$$\square_{T,T_1} \circ \square_{T_1',T_2} = \square_{\square_{T,T_1}(T_1'),T_2}. \tag{3.6}$$

In particular, if $T_1 = T_1'$, this simplifies to

$$\square_{T,T_1} \circ \square_{T_1,T_2} = \square_{T,T_2}. \tag{3.7}$$

Let us show that under the insertion operations, the leading monomials change in a controllable way.

Proposition 3.4.2.12. *Suppose that T_1 is a tree monomial, and T_2 is a divisor of T_1. Then for each $g \in \mathcal{T}(\mathcal{X})(\mathrm{ar}(T_2))$, we have*

$$\textsc{lm}(\Box_{T_1,T_2}(g)) = \Box_{T_1,T_2}(\textsc{lm}(g)). \tag{3.8}$$

Proof. Let us first check that for any nonzero elements

$$f_0 \in \mathcal{T}(\mathcal{X})(r), f_1 \in \mathcal{T}(\mathcal{X})(n_1), \ldots, f_r \in \mathcal{T}(\mathcal{X})(n_r),$$

we have

$$\textsc{lm}(f_0 \circ (f_1, \ldots, f_r)) = \textsc{lm}(f_0) \circ (\textsc{lm}(f_1), \ldots, \textsc{lm}(f_r)).$$

Since the composition products on $\mathcal{T}(\mathcal{X})$ are multilinear, the element $f_0 \circ (f_1, \ldots, f_r)$ is equal to a linear combination of elements $m_0 \circ (m_1, \ldots, m_r)$, where $m_p \in \mathrm{supp}(f_p)$. It remains to notice that for each $m_p \neq \textsc{lm}(f_p)$ we have $m_p \prec \textsc{lm}(f_p)$, so by the defining property of monomial orders we have

$$m_0 \circ (m_1, \ldots, m_r) \prec \textsc{lm}(f_0) \circ (\textsc{lm}(f_1), \ldots, \textsc{lm}(f_r)),$$

unless $m_0 = \textsc{lm}(f_0)$, $m_1 = \textsc{lm}(f_1)$, $\ldots$, $m_r = \textsc{lm}(f_r)$.

Now, the element $\Box_{T_1,T_2}(g)$ is obtained from g by an iteration of nonsymmetric compositions, and the result follows. □

Definition 3.4.2.13 (Reduced monomials and polynomials)**.** Let $\mathcal{S}$ be a subset of $\mathcal{T}(\mathcal{X})$. A tree monomial T is said to be *reduced with respect to* $\mathcal{S}$ if $T \notin (\textsc{lm}(\mathcal{S}))$; in other words, if T is not divisible by any of the leading monomials of elements of $\mathcal{S}$.

In general, a tree polynomial f is said to be *reduced with respect to* $\mathcal{S}$ if it is equal to a linear combination of tree monomials which are reduced with respect to $\mathcal{S}$. A subset $\mathcal{S} \subset \mathcal{T}(\mathcal{X})$ is said to be *self-reduced* if each element $s \in \mathcal{S}$ is monic and reduced with respect to $\mathcal{S} \setminus \{s\}$.

Definition 3.4.2.14 (Reduction)**.** Let $f, g \in \mathcal{T}(\mathcal{X})$ be two nonzero elements. We say that f is *reducible with respect to* g if $\textsc{lm}(f)$ is not reduced with respect to $\{g\}$, or, in plain words, if the leading monomial of f is divisible by the leading monomial of g, that is,

$$\textsc{lm}(f) = \Box_{T_1,T_2}(\textsc{lm}(g))$$

for some tree monomials

$$T_1 \in \mathrm{Tree}_{\mathcal{X}}(\mathrm{ar}(\textsc{lm}(f))), \quad T_2 \in \mathrm{Tree}_{\mathcal{X}}(\mathrm{ar}(\textsc{lm}(g))).$$

In that case, the *reduction of f with respect to g*, denoted by $r_g(f)$, is defined by the formula

$$r_g(f) = f - \frac{\textsc{lc}(f)}{\textsc{lc}(g)} \Box_{T_1,T_2}(g).$$

Lemma 3.4.2.15. *For all elements $f, g \in \mathcal{T}(\mathcal{X})$ such that $r_g(f)$ is defined, we have*

$$r_g(f) = 0 \quad \textit{or} \quad \mathrm{LM}(r_g(f)) \prec \mathrm{LM}(f).$$

Proof. Indeed, by construction we have

$$\mathrm{LT}(f) = \mathrm{LT}\left(\frac{\mathrm{LC}(f)}{\mathrm{LC}(g)}\square_{T_1,T_2}(g)\right).$$

□

One can view a reduction as one step of a version of the long division algorithm. We make it more precise as follows.

Algorithm 3.4.2.16 (Long division for nonsymmetric operads)**.**

Input: An element $f \in \mathcal{T}(\mathcal{X})$, and a finite set $\mathcal{S} \subset \mathcal{T}(\mathcal{X})$.

Output: An element $\tilde{f}$, reduced with respect to $\mathcal{S}$, for which $\mathrm{LT}(\tilde{f}) \preceq \mathrm{LT}(f)$ such that $f + (\mathcal{S}) = \tilde{f} + (\mathcal{S})$.

- If $f = 0$, return f.
- Replace $\mathcal{S}$ by its linear self-reduction (Proposition 1.2.1.6).
- If $\mathcal{D} := \{s \in \mathcal{S} \colon \mathrm{LM}(f) \text{ is divisible by } \mathrm{LM}(s)\} \neq \varnothing$, take $s_0 \in \mathcal{D}$ with the least leading monomial (such s_0 is unique since $\mathcal{S}$ is linearly self-reduced), and return the result of long division of $f' := r_s(f)$ by $\mathcal{S}$.
- Otherwise, $\mathrm{LM}(f)$ is reduced with respect to $\mathcal{S}$, so let $\tilde{f}$ be the result of long division of $f' := f - \mathrm{LT}(f)$ by S; return $\mathrm{LT}(f) + \tilde{f}$.

Lemma 3.4.2.17. *For every $f \in \mathcal{T}(\mathcal{X})$, the long division algorithm terminates in a finite number of steps. Its output is an element $\tilde{f}$ reduced with respect to $\mathcal{S}$, for which $\mathrm{LT}(\tilde{f}) \preceq \mathrm{LT}(f)$ and*

$$f + (\mathcal{S}) = \tilde{f} + (\mathcal{S}).$$

Proof. By Lemma 3.4.2.15, the leading monomial of the dividend (the element that the algorithm is applied to) decreases at each step, so termination follows from the fact that Ξ is a well-order. This also proves the second claim about the output. Suppose that for some f the output is not reduced. Let us pick among such f an element with the smallest leading monomial (again using the well-order Ξ). If $\mathrm{LM}(f)$ is not reduced with respect to $\mathcal{S}$, then the first step applies the same algorithm to $f' = r_s(f)$, and by Lemma 3.4.2.15 we have $f' = 0$ or $\mathrm{LM}(f') \prec \mathrm{LM}(f)$, so the output of the long division is reduced. If $\mathrm{LM}(f)$ is reduced, then the second step of the algorithm applies the same algorithm to $f' = f - \mathrm{LT}(f)$, so $f' = 0$ or $\mathrm{LM}(f') \prec \mathrm{LM}(f)$, and the output of the long division is reduced, a contradiction. Finally, note that each reduction subtracts an element in $(\mathcal{S})$, which justifies the claim about the coset, and completes the proof. □

Remark 3.4.2.18. We see that in fact there is nothing particularly problematic if $\mathcal{S}$ is an infinite self-reduced set: it is clear from the proof of Lemma 3.4.2.17 that for the given $f \in \mathcal{T}(\mathcal{X})$ the elements $s \in \mathcal{S}$ which we use at various steps of our computation have decreasing leading monomials, and so there can be only finitely many reductions performed; that is, for each f we never use more than a finite subset of $\mathcal{S}$. While for purposes of implementation this is not particularly important, it will be beneficial for theoretical results where $\mathcal{S}$ may be infinite.

We will now establish that the set of elements that are reduced with respect to $\mathcal{I}$ is a suitable candidate for the set of normal forms for the elements of the quotient $\mathcal{T}(\mathcal{X})/\mathcal{I}$. This is an improvement of Lemma 1.2.1.3 which takes into account the extra structures we have on the underlying vector spaces.

Lemma 3.4.2.19. *Suppose that $\mathcal{I}$ is an ideal of $\mathcal{T}(\mathcal{X})$. Monomials that are reduced with respect to $\mathcal{I}$ form a basis of the quotient $\mathcal{T}(\mathcal{X})/\mathcal{I}$.*

Proof. Let us first prove the spanning property. For that, it is enough to show that the coset $f + \mathcal{I}$ of every element $f \in \mathcal{T}(\mathcal{X})$ contains an element that is reduced with respect to $\mathcal{I}$. This is true, since we can take $\tilde{f}$ to be the result of long division of f with respect to $\mathcal{I}$, which is reduced and satisfies $\tilde{f} + \mathcal{I} = f + \mathcal{I}$.

It remains to prove linear independence. For that, note that if $f \neq 0 \in \mathcal{I}$, then $\mathrm{LM}(f) \in \mathrm{LM}(I)$, so f is not even linearly reduced with respect to $\mathcal{I}$, so $\mathcal{I}$ does not contain nonzero reduced elements. □

It is possible to use long division to find, for each finite set, a finite self-reduced set that generates the same ideal.

Algorithm 3.4.2.20 (Self-reduction for nonsymmetric operads)**.**

Input: A finite subset $\mathcal{S} \subset \mathcal{T}(\mathcal{X})$.

Output: A finite self-reduced subset $\mathcal{S}' \subset \mathcal{T}(\mathcal{X})$ with $(\mathcal{S}) = (\mathcal{S}')$.

- Replace $\mathcal{S}$ by its linear self-reduction.
- If $\mathcal{S}$ is self-reduced, return $\mathcal{S}$.
- Let s be the element of $\mathcal{S}$ with the maximal leading monomial, and compute the self-reduction $\mathcal{S}'$ of $\mathcal{S} \setminus \{s\}$.
- Compute $\tilde{s}$, the result of long division of s by $\mathcal{S}'$.
- Compute the self-reduction of $\mathcal{S}' \cup \{\tilde{s}\}$.

We leave it as an exercise (Exercise 3.1) for the reader to check that for each finite $\mathcal{S}$ this algorithm terminates after finitely many steps (in which case it of course outputs a finite self-reduced set).

3.4.3 Gröbner bases

Proposition 3.4.3.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{T}(\mathcal{X})$. The space of leading terms $\textsc{lt}(\mathcal{I})$ is an ideal of $\mathcal{T}(\mathcal{X})$.*

Proof. By definition, $\textsc{lt}(\mathcal{I})$ is a subspace, so we just have to show that each nonsymmetric composition of several elements belongs to $\textsc{lt}(\mathcal{I})$ whenever at least one of the elements belongs to $\textsc{lt}(\mathcal{I})$. Since the operations are multilinear, it is enough to consider the case of several monomials

$$T_0 \in \mathcal{T}(\mathcal{X})(r), T_1 \in \mathcal{T}(\mathcal{X})(n_1), \ldots, T_r \in \mathcal{T}(\mathcal{X})(n_r),$$

one of which, say, T_1, is the leading monomial of some element f_1 of $\mathcal{I}$. From the proof of Proposition 3.4.2.12, in this case we have

$$\textsc{lm}(T_0 \circ (f_1, T_2, \ldots, T_r)) = T_0 \circ (T_1, \ldots, T_r),$$

and therefore $T_0 \circ (T_1, \ldots, T_r) \in \textsc{lt}(\mathcal{I})$. □

We are now ready to define a Gröbner basis of an ideal.

Definition 3.4.3.2 (Gröbner basis)**.** Let $\mathcal{I}$ be an ideal of $\mathcal{T}(\mathcal{X})$. We say that $\mathcal{G} = \{\mathcal{G}(n) \subset \mathcal{I}(n)\}$ is a *Gröbner basis* of $\mathcal{I}$ with respect to a given monomial order Ξ if the set of leading monomials $\textsc{lm}(\mathcal{G}) := \{\textsc{lm}(g) \colon g \in \mathcal{G}\}$ generates the leading term ideal of the ideal $\mathcal{I}$:

$$\textsc{lt}(\mathcal{I}) = (\textsc{lm}(\mathcal{G})).$$

A Gröbner basis which is a self-reduced subset of $\mathcal{T}(\mathcal{X})$ is said to be *reduced*.

Lemma 3.4.3.3. *A Gröbner basis of an ideal $\mathcal{I} \subset \mathcal{T}(\mathcal{X})$ generates $\mathcal{I}$.*

Proof. Suppose that $\mathcal{G}$ is a Gröbner basis of $\mathcal{I}$, and that $(\mathcal{G})$ is a proper subset of $\mathcal{I}$. (Clearly, $(\mathcal{G}) \subset \mathcal{I}$ since $(\mathcal{G})$ is the smallest ideal containing $\mathcal{G}$.) Let us take $f \in \mathcal{I} \setminus (\mathcal{G})$ with the least possible leading monomial. Since $\textsc{lm}(f) \in \textsc{lt}(\mathcal{I})$, there exists $g \in \mathcal{G}$ for which $\textsc{lm}(f)$ is divisible by $\textsc{lm}(g)$. Then $r_g(f)$ is defined and belongs to $\mathcal{I}$, and by Lemma 3.4.2.15, we have $\textsc{lm}(r_g(f)) \prec \textsc{lm}(f)$, so $r_g(f) \in (\mathcal{G})$ by minimality of f. But this implies $f \in (\mathcal{G})$, since $r_g(f)$ is obtained by subtracting an element of $(\mathcal{G})$ from f, which is a contradiction. □

Proposition 3.4.3.4. *Let $\mathcal{I}$ be an ideal of $\mathcal{T}(\mathcal{X})$. Then $\mathcal{G} \subset \mathcal{I}$ is a Gröbner basis if and only if the cosets of monomials that are reduced with respect to $\mathcal{G}$ form a basis of the quotient $\mathcal{T}(\mathcal{X})/\mathcal{I}$.*

Proof. Let us note that the cosets of monomials that are reduced with respect to $\mathcal{G}$ form a basis of the quotient $\mathcal{T}(\mathcal{X})/\mathcal{I}$ if and only if every coset modulo $\mathcal{I}$ contains a unique element that is reduced with respect to $\mathcal{G}$.

First of all, we remark that if $f \in \mathcal{T}(\mathcal{X})$, then $\tilde{f}$, the result of the long division of f by $\mathcal{G}$, is reduced, and $\tilde{f} + (\mathcal{G}) = f + (\mathcal{G}) \subset f + \mathcal{I}$, so every coset contains at least one reduced element whether $\mathcal{G}$ is a Gröbner basis or not.

Suppose now that $\mathcal{G}$ is a Gröbner basis of $\mathcal{I}$. Suppose that the cosets of reduced monomials are linearly dependent, or, in other words, that the zero coset $\mathcal{I}$ contains a nonzero reduced element f. In that case, $\textsc{lm}(f) \in \textsc{lt}(\mathcal{I})$ is reduced with respect to $\mathcal{G}$, which is a contradiction.

Suppose that $\mathcal{G}$ is not a Gröbner basis. This implies that there exists an element $f \in \mathcal{I}$ for which $\textsc{lm}(f)$ is reduced with respect to $\mathcal{G}$. Let $\tilde{f}$ be the result of the long division of f by $\mathcal{G}$. Clearly, $\tilde{f}$ is a nontrivial linear combination of reduced monomials, so the cosets of reduced monomials are in this case linearly dependent. □

Corollary 3.4.3.5. *Suppose that $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I} \subset \mathcal{T}(\mathcal{X})$. Then the result of long division of $f \in \mathcal{T}(\mathcal{X})$ by $\mathcal{G}$ does not depend on either the choices or the order of the reductions performed.*

Proof. Suppose that two different choices of order of reductions yield two different results. In this case, the coset $f + \mathcal{I}$ contains two different elements that are reduced with respect to $\mathcal{G}$, hence reduced monomials are linearly dependent, a contradiction. □

We summarize Proposition 3.4.3.4 and its corollary as follows.

Theorem 3.4.3.6.

(i) Let $\mathcal{I}$ be an ideal of $\mathcal{T}(\mathcal{X})$. A sequence of subsets $\mathcal{G} \subset \mathcal{I}$ is a Gröbner basis if and only if the normal forms modulo $\mathcal{I}$ are precisely the elements that are reduced with respect to $\mathcal{G}$.

(ii) Suppose that $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I} \subset \mathcal{T}(\mathcal{X})$. Given an element $f \in \mathcal{I}$, its normal form modulo $\mathcal{I}$ can be computed using long division by $\mathcal{G}$. In fact, in this long division the order of reductions can be chosen arbitrarily.

Proposition 3.4.3.7. *Each ideal $\mathcal{I} \subset \mathcal{T}(\mathcal{X})$ has a unique reduced Gröbner basis.*

Proof. Let us first prove uniqueness. If $\mathcal{G}$ is a Gröbner basis, then $\textsc{lt}(\mathcal{I}) = (\textsc{lm}(\mathcal{G}))$; if $\mathcal{G}$, in addition, is reduced, then $\textsc{lm}(\mathcal{G}) \subset \textsc{lm}(\mathcal{I})$ must coincide with the set $\mathcal{M}$ of all elements $T \in \textsc{lm}(\mathcal{I})$ that are not divisible by other elements of $\textsc{lm}(\mathcal{I})$. (In other words, $\mathcal{M}$ is the set of minimal elements of $\textsc{lm}(\mathcal{I})$) with respect to the partial order of divisibility.) Indeed, each $T \in \mathcal{M} \subset \textsc{lm}(\mathcal{I})$ must be divisible by a leading term of an element $g \in \mathcal{G}$, and by definition of $\mathcal{M}$, this can only happen if $\textsc{lm}(g) = T$, so $\mathcal{M} \subset \textsc{lm}(\mathcal{G})$. Also, if

$g \in \textsc{lm}(\mathcal{G})\backslash\mathcal{M}$, then $\textsc{lm}(g)$ is divisible by T' for some $T' \in \textsc{lt}(\mathcal{I})$ by definition of $\mathcal{M}$, and T' is divisible by $\textsc{lt}(g')$ for some $g' \in \mathcal{G}$ by definition of a Gröbner basis, so since $\mathcal{G}$ is reduced, we have $g = g'$, and $\textsc{lm}(g) = T$, a contradiction. Moreover, since $\mathcal{G}$ is reduced, then for each $T \in \mathcal{M} = \textsc{lm}(\mathcal{G})$ there exists a unique element $g \in \mathcal{G}$ with $\textsc{lm}(g) = T$; for such g we have $g = T - h$, where h is reduced with respect to I. Finally, this element h must be equal to the unique element in the coset $T + \mathcal{I}$ that is reduced with respect to $\mathcal{I}$.

Now we will prove existence. As we have just seen, the only feasible candidate for $\mathcal{G}$ is the set of all elements of the form $T - h$, where $T \in \mathcal{M}$, and h is the unique element in the coset $T + \mathcal{I}$ that is reduced with respect to $\mathcal{I}$. This set $\mathcal{G}$ is self-reduced by construction. Note that every element of $\textsc{lm}(\mathcal{I})$ is divisible by some element $T \in \mathcal{M}$; indeed, the smallest element which is not divisible by any element of $\mathcal{M}$ is either not divisible by any other element of $\textsc{lm}(\mathcal{I})$, and hence must be in $\mathcal{M}$, or is divisible by some (smaller) element, and hence has a divisor from $\mathcal{M}$; either way we get a contradiction. Therefore, $\textsc{lt}(\mathcal{I}) = (\mathcal{M}) = (\textsc{lm}(\mathcal{G}))$, which shows that $\mathcal{G}$ is a Gröbner basis. □

3.5 Computing Gröbner bases

In this section, we will explain how to compute Gröbner bases for ideals of $\mathcal{T}(\mathcal{X})$. As in Chapter 2, some ideals have infinite Gröbner bases, so the word “algorithm” should be taken with a grain of salt.

3.5.1 Diamond lemma

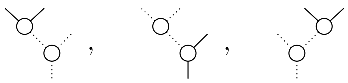
To define S-polynomials for trees, we need to make precise what we mean by overlaps of trees.

Definition 3.5.1.1 (Overlap of planar trees)**.** An *overlap* of two planar trees τ_1 and τ_2 is the data of a nontrivial rooted tree τ and isomorphisms $f_i \colon \tau \to \tau_i'$ where τ_i' is a subtree of τ_i, $i = 1, 2$, satisfying the following properties:

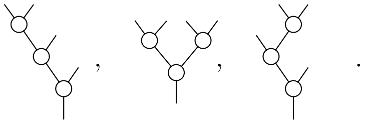
- at least one of τ_i' shares the root with τ_i,
- $f_1^{-1}(\mathrm{Int}(\tau_1)) \cup f_2^{-1}(\mathrm{Int}(\tau_2)) = \mathrm{Int}(\tau)$, but $f_1^{-1}(\mathrm{Int}(\tau_1)) \neq \mathrm{Int}(\tau)$ and $f_2^{-1}(\mathrm{Int}(\tau_2)) \neq \mathrm{Int}(\tau)$, and also $f_1^{-1}(\mathrm{Int}(\tau_1)) \cap f_2^{-1}(\mathrm{Int}(\tau_2)) \neq \varnothing$ (each internal vertex of τ is an internal vertex in at least one of τ_i, not all internal vertices are internal vertices of just one of them, and at least one of internal vertices is an internal vertex of both, so the overlap is nontrivial),
- for each $\ell \in \mathrm{Leaves}(\tau)$, at least one of the $f_1(\ell)$ and $f_2(\ell)$ is a leaf in τ_i,
- at least one of τ_i' is a proper subtree of τ_i.

Two planar rooted trees that have an overlap can be *merged* along it by identifying the vertices of τ_1' with the corresponding vertices of τ_2', and consider the naturally induced parent function and planar structure. The overlap conditions guarantee that the result of that identification is a planar rooted tree again.

Example 3.5.1.2. Let us consider the three trees



from Example 3.4.2.2. Each two of those trees form an overlap (the dashed edges mark the common parts). Merging the first and the second one (respectively, the first and the third one, the second and the third one) along their overlap, we obtain, respectively, the trees



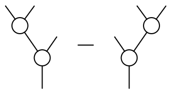
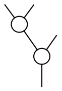
Definition 3.5.1.3 (S-polynomial)**.** Let $g_1, g_2 \in \mathcal{T}(\mathcal{X})$ be two monic polynomials. We say that the leading monomials $\text{LM}(g_1)$ and $\text{LM}(g_2)$ form an *overlap* if they have a *small common multiple*, a tree monomial T and its two proper divisors T_1 and T_2 for which

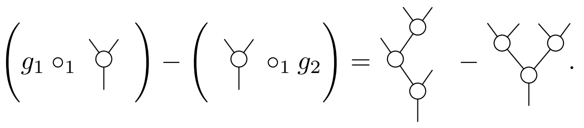
$$\text{LM}(g_1) = T_1, \quad \text{LM}(g_2) = T_2,$$

and the underlying tree of T is the result of merging of the underlying trees of T_1 and T_2 along an overlap. We call the element

$$S_T(g_1, g_2) := \square_{T,T_1}(g_1) - \square_{T,T_2}(g_2)$$

an *S-polynomial* of g_1 and g_2; the common term cancels, since both g_1 and g_2 are monic.

Example 3.5.1.4. Let $g_1 = g_2 =$  , and suppose we are using the `gpathlex` order. Then  is the leading monomial; as we know from Example 3.5.1.2, it has an overlap with itself. The corresponding S-polynomial is equal to



We will now prove the result which is at the core of most feasible ways to check that some subset of an ideal is a Gröbner basis.

Definition 3.5.1.5 (Parameter of a representation)**.** Let $\mathcal{I} = (\mathcal{G})$ be an ideal of $\mathcal{T}(\mathcal{X})$. Consider the representation of an element $f \in \mathcal{I}$ as a combination of insertions of $g_1, \ldots, g_N \in \mathcal{G}$:

$$f = \sum_{i=1}^{N} c_i \square_{\widetilde{T}_i, T_i}(g_i), \tag{3.9}$$

where $T_i = \textsc{lm}(g_i)$. We call $\max(\widetilde{T}_i)$ the *parameter* of this linear combination.

If $f = S_T(g_1, g_2)$ is the S-polynomial of $g_1, g_2 \in \mathcal{G}$ (with all the notation as above in Definition 3.5.1.3), then it has an obvious representation

$$f = \square_{T,T_1}(g_1) - \square_{T,T_2}(g_2),$$

with parameter T. We call a representation of that S-polynomial *nontrivial* if its parameter is smaller than T.

Theorem 3.5.1.6 (Diamond lemma)**.** *Let $\mathcal{G} \subset \mathcal{T}(\mathcal{X})$ be self-reduced, and let $\mathcal{I} = (\mathcal{G})$. The following statements are equivalent:*

(i) *$\mathcal{G}$ is a Gröbner basis of $\mathcal{I}$.*

(ii) *Every S-polynomial $S_T(g_1, g_2)$ has reduced form* 0 *with respect to $\mathcal{G}$.*

(iii) *Every S-polynomial $S_T(g_1, g_2)$ admits a nontrivial representation of the form* (3.9)*.*

(iv) *Every element $f \in \mathcal{I}$ admits a representation of the form* (3.9) *with parameter* $\textsc{lm}(f)$*.*

Proof. We will prove the chain of implications (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (i).

(i) implies (ii): Note that each S-polynomial belongs to $\mathcal{I}$, and each element of $\mathcal{I}$ has reduced form 0 with respect to $\mathcal{G}$ for a Gröbner basis.

(ii) implies (iii): If each S-polynomial has reduced form 0 with respect to $\mathcal{G}$, we record all the steps of long division of $S_T(g_1, g_2)$ by $\mathcal{G}$, and obtain a representation of the desired form.

(iii) implies (iv): This is the hardest part of the proof. Suppose the statement (iv) is not true for some $f \in \mathcal{T}(\mathcal{X})$. If we drop the assumption on the parameter of the representation, then the statement is obvious, since $\mathcal{I} = (\mathcal{G})$. In general, in a representation of the form (3.9), $\textsc{lm}(f)$ may be smaller than $\max_i(\widetilde{T}_i)$ because some leading terms may cancel. Suppose that for each representation of f of that form we have $\textsc{lm}(f) \prec \max_i(\widetilde{T}_i)$. Let us consider the "most economic counterexample"; in other words, we assume:

- that f does not have a representation of the form (3.9) with $\textsc{lm}(f) = \max_i(\widetilde{T}_i)$,

- that among the representations of the form (3.9), we consider the one where the parameter $T = \max_i(\widetilde{T}_i)$ is the least possible;

- that among the representations with the parameter T, the number of i for which $\widetilde{T}_i$ is equal to T is the least possible.

Without the loss of generality, we have $\widetilde{T}_i = T$ for $i = 1, \ldots, k$, and $\widetilde{T}_i \prec T$ for $i > k$. Clearly, $k \geq 2$, in order for the leading monomials of this combination to cancel each other so that the resulting leading monomial is equal to $\textsc{lm}(f)$. Clearly, both $T_{k-1} = \textsc{lm}(g_{k-1})$ and $T_k = \textsc{lm}(g_k)$ are divisors of T. Let us examine the relative position of the underlying trees of those divisors. In general, given two different subtrees of the same tree, one may be a subtree of the other, they may overlap, or they may be disjoint.

The first of these possibilities is especially easy to handle: since $\mathcal{G}$ is assumed self-reduced, this can only happen if $g_{k-1} = g_k$, and the divisors T_{k-1} and T_k coincide. In this case, the two terms $c_{k-1}\square_{T,T_{k-1}}(g_{k-1}) + c_k\square_{T,T_k}(g_k)$ can be merged into a single term $(c_{k-1}+c_k)\square_{T,T_{k-1}}(g_{k-1})$, resulting in a representation for f where either the parameter is smaller (that happens if $k = 2$ and $c_{k-1} + c_k = 0$) or the parameter is the same, but k is smaller, which is a contradiction.

Suppose that T_{k-1} and T_k overlap inside T. Let us denote by T' the corresponding small common multiple; it is still a divisor of T. Let us rewrite the sum

$$c_{k-1}\square_{T,T_{k-1}}(g_{k-1}) + c_k\square_{T,T_k}(g_k)$$

using Equation (3.7):

$$\begin{aligned}
&c_{k-1}\square_{T,T_{k-1}}(g_{k-1}) + c_k\square_{T,T_k}(g_k) = \\
&\qquad c_{k-1}\square_{T,T'} \circ \square_{T',T_{k-1}}(g_{k-1}) + c_k\square_{T,T'} \circ \square_{T',T_k}(g_k) = \\
&\quad \square_{T,T'}\left(c_{k-1}\square_{T',T_{k-1}}(g_{k-1}) + c_k\left(\square_{T',T_{k-1}}(g_{k-1}) - S_{T'}(g_{k-1},g_k)\right)\right) = \\
&\qquad \square_{T,T'}\left((c_{k-1}+c_k)\square_{T',T_{k-1}}(g_{k-1})\right) - c_k\square_{T,T'}(S_{T'}(g_{k-1},g_k)) = \\
&\qquad\qquad (c_{k-1}+c_k)\square_{T,T_{k-1}}(g_{k-1}) - c_k\square_{T,T'}(S_{T'}(g_{k-1},g_k))
\end{aligned} \tag{3.10}$$

We assumed that every S-polynomial has a nontrivial representation

$$S_{T'}(g_{k-1},g_k) = \sum_{i=1}^{N'} c_i'\square_{\widetilde{T}_i{}',T_i'}(g_i),$$

with $\max_i(\widetilde{T}_i{}') \prec T'$. Substituting this into (3.10), we obtain

$$c_{k-1}\square_{T,T_{k-1}}(g_{k-1}) + c_k\square_{T,T_k}(g_k) =$$

$$(c_{k-1}+c_k)\square_{T,T_{k-1}}(g_{k-1}) - c_k\square_{T,T'}\left(\sum_{i=1}^{N'} c_i'\square_{\widetilde{T_i}',T_i'}(g_i)\right). \quad (3.11)$$

Replacing the terms

$$c_{k-1}\square_{T,T_{k-1}}(g_{k-1}) + c_k\square_{T,T_k}(g_k)$$

in the minimal counterexample by the right-hand side of (3.11), we obtain a representation for f where either the parameter is smaller (that happens if $k=2$ and $c_{k-1}+c_k=0$) or the parameter is the same, but k is smaller, which is a contradiction. (To justify that, one should use Equation (3.6) and Proposition 3.4.2.12; we leave it to the reader to fill in the details in Exercise 3.2.)

Suppose that T_{k-1} and T_k are disjoint inside T, so that the bilinear operation

$$\square_{T,T_{k-1},T_k} : \mathcal{T}(\mathcal{X})(\mathrm{ar}(T_{k-1})) \otimes \mathcal{T}(\mathcal{X})(\mathrm{ar}(T_k)) \to \mathcal{T}(\mathcal{X})(\mathrm{ar}(T))$$

inserting arbitrary elements in places of T_1 and T_2 inside T is defined. Note that

$$\begin{gathered}\square_{T,T_k}(g_k) = \square_{T,T_{k-1},T_k}(\textsc{lm}(g_{k-1}), g_k) = \\ \square_{T,T_{k-1},T_k}(g_{k-1}-g_{k-1}', g_k) = \square_{T,T_{k-1},T_k}(g_{k-1}, g_k) - \square_{T,T_{k-1},T_k}(g_{k-1}', g_k) = \\ \square_{T,T_{k-1},T_k}(g_{k-1}, \textsc{lm}(g_k)) + \square_{T,T_{k-1},T_k}(g_{k-1}, g_k') - \square_{T,T_{k-1},T_k}(g_{k-1}', g_k) = \\ \square_{T,T_{k-1}}(g_{k-1}) + \square_{T,T_{k-1},T_k}(g_{k-1}, g_k') - \square_{T,T_{k-1},T_k}(g_{k-1}', g_k),\end{gathered}$$

where we use the notation $g_{k-1} = \textsc{lm}(g_{k-1}) + g_{k-1}'$ and $g_k = \textsc{lm}(g_k) + g_k'$. Therefore,

$$\begin{gathered}c_{k-1}\square_{T,T_{k-1}}(g_{k-1}) + c_k\square_{T,T_k}(g_k) = \\ (c_{k-1}+c_k)\square_{T,T_{k-1}}(g_{k-1}) + c_k\left(\square_{T,T_{k-1},T_k}(g_{k-1}, g_k') - \square_{T,T_{k-1},T_k}(g_{k-1}', g_k)\right)\end{gathered}$$

where the terms

$$\square_{T,T_{k-1},T_k}(g_{k-1}, g_k') - \square_{T,T_{k-1},T_k}(g_{k-1}', g_k),$$

using Equation (3.6) and Proposition 3.4.2.12, can be expanded as a linear combination of elements $\square_{T',T_i}(g_i)$ with the leading monomial smaller than T. Therefore, as in the case of an overlap, we can join together two contributions to the leading monomial T at the cost of increasing the number of terms $\square_{T',T_i}(g_i)$ with the smaller leading monomial, so we obtain a representation for f where either the parameter is smaller (that happens if $k=2$ and $c_{k-1}+c_k=0$) or the parameter is the same, but k is smaller. This contradiction completes the proof of the present implication.

(iv) implies (i): For such a representation of an element f, we have

$$\textsc{lm}(f) = \textsc{lm}(\square_{T,T_i}(g_i)) = \square_{T,T_i}(\textsc{lm}(g_i)),$$

for some i, so $\textsc{lm}(f)$ is divisible by $\textsc{lm}(g_i)$. Since this is assumed true for every $f \in I$, it follows that $\mathcal{G}$ is a Gröbner basis. □

3.5.2 The Buchberger algorithm

Theorem 3.5.1.6 leads naturally to a recipe for computing reduced Gröbner bases: given a set of generators of an ideal, one has to compute all pairwise S-polynomials, adjoin all reduced forms of those to the set of generators, and repeat the same. It is rather a "recipe" than an algorithm since we are not guaranteed termination, but it is nevertheless very useful.

Algorithm 3.5.2.1 (Buchberger algorithm for nonsymmetric operads)**.**

Input: A finite subset $\mathcal{G} \subset \mathcal{T}(\mathcal{X})$ generating an ideal $\mathcal{I} \subset \mathcal{T}(\mathcal{X})$.

Output: If terminates, the output is the reduced Gröbner basis of $\mathcal{I}$.

```
• Set newSpolynomials ← true.
• While newSpolynomials do:
    – Sort $\mathcal{G}$ by gpathlex order of leading monomials: $\mathcal{G} = \{g_1, \dots, g_n\}$.
    – Compute the self-reduction of $\mathcal{G}$.
    – Set Spolynomials ← $\varnothing$.
    – Set newSpolynomials ← false.
    – For $g_1 \in \mathcal{G}$ do for $g_2 \in \mathcal{G}$ do:
        * If $\textsc{lm}(g_1)$ and $\textsc{lm}(g_2)$ form an overlap then:
            1. Compute the S-polynomial $S_T(g_1, g_2)$.
            2. Let $t$ be the result of long division of $S_T(g_1, g_2)$ by $\mathcal{G}$.
            3. If $t \neq 0$ and $t \notin$ Spolynomials then
                * Set newSpolynomials ← true.
                * Set Spolynomials ← Spolynomials $\cup \{t\}$.
    – Set $\mathcal{G} \leftarrow \mathcal{G} \cup$ Spolynomials.
• Return $\mathcal{G}$.
```

Proposition 3.5.2.2. *If Algorithm 3.5.2.1 terminates then its output is the reduced Gröbner basis of $\mathcal{I}$.*

Proof. Immediate corollary to Theorem 3.5.1.6. □

3.5.3 Triangle lemma

Definition 3.5.3.1 (Essential overlap)**.** Let $\mathcal{G}$ be a self-reduced subset of $\mathcal{T}(\mathcal{X})$, and let $g_1, g_2 \in \mathcal{G}$ be two elements for which $\textsc{lm}(g_1)$ and $\textsc{lm}(g_2)$ have an overlap. We call this overlap *essential* if $\text{LM}(g_1)$ and $\text{LM}(g_2)$ are the only two divisors from $\text{LM}(\mathcal{G})$ of the tree monomial obtained by merging these monomials along their overlap.

Proposition 3.5.3.2 (Triangle lemma for nonsymmetric operads)**.** *Let $\mathcal{G}$ be a self-reduced subset of $\mathcal{T}(\mathcal{X})$, and let $g_1, g_2 \in \mathcal{G}$ be two elements for which $\text{LM}(g_1)$ and $\text{LM}(g_2)$ have an overlap. Suppose that this overlap is not essential, so that there exists $g_3 \in G$ for which $\text{LM}(g_3)$ is another divisor of the tree monomial T obtained by merging $\text{LM}(g_1)$ and $\text{LM}(g_2)$ along their overlap. Then:*

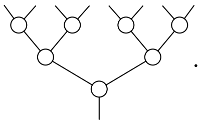
- *The divisors $\text{LM}(g_1)$ and $\text{LM}(g_3)$ of T have an overlap, and the divisors $\text{LM}(g_3)$ and $\text{LM}(g_2)$ of T also have an overlap.*
- *If the S-polynomials $S_{T'}(g_1, g_3)$ and $S_{T''}(g_3, g_2)$ for the corresponding overlaps admit nontrivial representations of the form* (3.9)*, then the S-polynomial $S_T(g_1, g_2)$ also admits a nontrivial representation of that form.*

Proof. Note that since $\mathcal{G}$ is assumed self-reduced, $T_3 = \text{LM}(g_3)$ cannot be a divisor of either $T_1 = \text{LM}(g_1)$ or $T_2 = \text{LM}(g_2)$. Therefore, it has an overlap with both T_1 and T_2. We use the notation T', T'' for the results of the corresponding merging. Note that due to Equation (3.7), we have

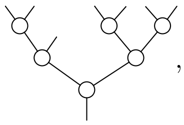
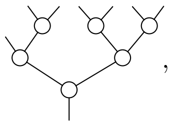
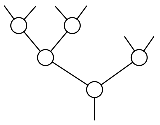
$$\begin{aligned} S_T(g_1, g_2) = \square_{T,T_1}(g_1) - \square_{T,T_2}(g_2) = \\ \square_{T,T_1}(g_1) - \square_{T,T_3}(g_3) + \square_{T,T_3}(g_3) - \square_{T,T_2}(g_2) = \\ \square_{T,T'}(\square_{T',T_1}(g_1) - \square_{T',T_3}(g_3)) + \square_{T,T''}(\square_{T'',T_3}(g_3) - \square_{T'',T_2}(g_2)) = \\ \square_{T,T'}(S_{T'}(g_1, g_3)) + \square_{T,T''}(S_{T''}(g_3, g_2)). \end{aligned}$$

Note that by Proposition 3.4.2.12, applying $\square_{T,T'}$ to a nontrivial representation for the S-polynomial $S_{T'}(g_1, g_3)$, we get an element with parameter less than T, and the same is true if we apply $\square_{T,T''}$ to a nontrivial representation for the S-polynomial $S_{T''}(g_3, g_2)$. This completes the proof. □

It turns out that although we are able to prove an analogue of Proposition 2.4.3.2 in the case of nonsymmetric operads, Corollary 2.4.3.3 does not generalize as easily, as in the case of associative algebras we took something for granted. If a word m in some alphabet X is a small common multiple of two words m_1 and m_2, and m_3 is a divisor of m which is not a subword of either m_1 or m_2, then the small common multiple of m_1 and m_3 is a proper subword of m, and so is the small common multiple of m_3 and m_2, and this allows one to prove Corollary 2.4.3.3 by induction on weight of overlaps. In the case of tree monomials, this is not quite the case, as the following example shows. Consider the free nonsymmetric operad $\mathcal{T}(\mathcal{X})$ with one binary generator, and consider the tree monomial

$T =$  .

Among the divisors of this monomial, consider the following three

$T_1 =$  , $T_2 =$  , $T_3 =$  ,

each sharing the root with the root of T. Note that these are three distinct overlapping divisors of T, none of them is a divisor of either of the two others, and for each pair the result of merging them over their overlap is the tree monomial T. Thus, in the proof of Proposition 3.5.3.2 above, it can easily happen that T' or T'' or both of them actually coincide with T, and we cannot infer a representation for the S-polynomial $S_T(g_1, g_2)$ from representations of "smaller" S-polynomials. Thus, Corollary 2.4.3.3 becomes the following more technical result (which is still occasionally useful for computations).

Corollary 3.5.3.3. *Let $\mathcal{G}$ be a self-reduced set of elements of $\mathcal{T}(\mathcal{X})$. Suppose that for two elements $g_1, g_2 \in \mathcal{G}$ whose leading monomials have an overlap the following holds:*

- *there exists $g_3 \in \mathcal{G}$ for which $\mathrm{LM}(g_3)$ is another divisor of the tree monomial T obtained by merging $\mathrm{LM}(g_1)$ and $\mathrm{LM}(g_2)$ along their overlap,*
- *both the tree monomials T' which is the result of merging $\mathrm{LM}(g_1)$ and $\mathrm{LM}(g_3)$ along their overlap and T'' which is the result of merging $\mathrm{LM}(g_3)$ and $\mathrm{LM}(g_2)$ along their overlap are proper divisors of T.*

Then, while computing the reduced Gröbner basis using Algorithm 3.5.2.1, the S-polynomial $S_T(g_1, g_2)$ may be ignored.

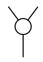
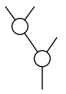
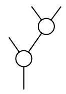
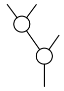
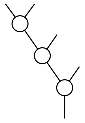
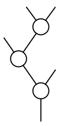
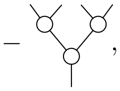
The reader interested in optimizing the algorithms further is encouraged to compare the effects observed in this section (somehow illustrating one important difference between operads and associative algebras) with [75, Sec. 3], and to try and improve Corollary 3.5.3.3 under some extra assumptions on $\mathcal{G}$ using the notion of an Anick numbering from that paper.

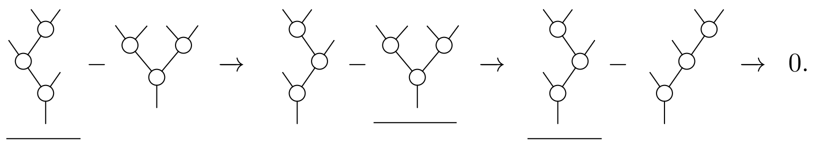
3.6 Examples of Gröbner bases for nonsymmetric operads

In this section, we discuss three simple examples of computations of Gröbner bases for nonsymmetric operads. We would like to make a simple but very important remark. If one views nonsymmetric collections as nonnegatively graded vector spaces, there is no difference between the given nonsymmetric operad $\mathcal{P}$ and the free $\mathcal{P}$-algebra on one generator. (This fails drastically for symmetric operads, but in the nonsymmetric case inserting the generator into all slots of the operation is an isomorphism of graded vector spaces.) However, a nonsymmetric operad has a much richer structure than the corresponding free algebra: an operad allows for all possible substitutions (an expert in the formalism of PI-algebras would say that operad ideals are closer to the so-called T-ideals in free algebras), and therefore presentations obtained using operads are often much more economic than presentations attempting to stay in the universe of algebras. (As a toy model, one can compare the approach of Example 3.6.2.1 below with the approach to dendriform algebras from [56]; this advantage of the operad approach is noted in [182].)

In many computations, instead of explicitly finding the standard form at each step, we will merely underline the leading monomial (which is being reduced).

3.6.1 Associative and q-associative operad

Example 3.6.1.1. The case of the nonsymmetric associative operad, as simple as it may be, actually is very instructional. The computation that we reproduce here is absolutely fundamental in many areas of mathematics, from rather basic algebra to some rather advanced category theory and algebraic topology. The nonsymmetric associative operad As is the quotient of the free operad with binary generator  by the ideal generated by the element  $-$ . Let us consider the gpathlex order of tree monomials. The leading term of the relation is , and the only small common multiple of that element with itself is the tree monomial . The corresponding S-polynomial is computed in Example 3.5.1.4; it is equal to  $-$ , and can be reduced to zero by the following chain of reductions:



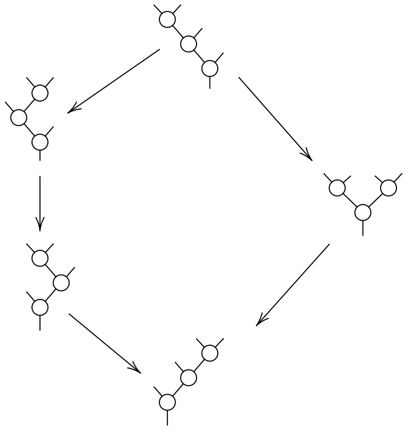
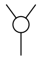
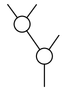
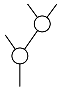
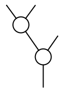
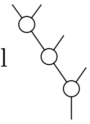
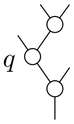
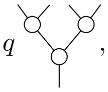


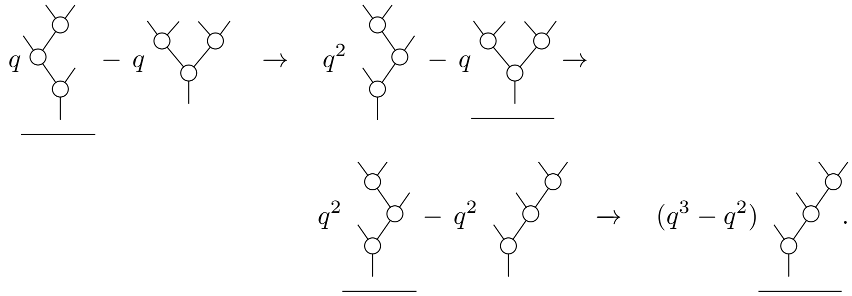
FIGURE 3.1: Stasheff associahedron K_2 arising from the Buchberger algorithm.

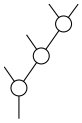
We conclude that the defining relation of As forms a Gröbner basis, and that the normal forms are given by “right combs” (right-growing trees, right-normed products).

Both the computation of the S-polynomial and the process of reducing it to zero are summarized in Figure 3.1. There, each arrow corresponds to a single reduction. The top two reductions are two different reductions of the small common multiple; their difference is the S-polynomial. Instead of reducing the S-polynomial to zero, one may keep reducing the two reductions separately, and check whether or not they reduce to the same element. This is of course equivalent to verifying that the S-polynomial reduces to zero. The diagram thus obtained has the shape of a pentagon, the second Stasheff associahedron K_2 [180, 241].

Example 3.6.1.2. Let q be an element of the ground field. We consider a generalization of the nonsymmetric associative operad, the operad As_q which is the quotient of the free operad with binary generator  by the operadic ideal generated by the element  $-\ q$  . Let us consider the `gpathlex` order of tree monomials. The leading term of the relation is  , and the only small common multiple of that element with itself is the tree monomial  . The corresponding S-polynomial is q  $- q$  ,

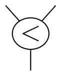
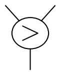
and we have the following chain of reductions:

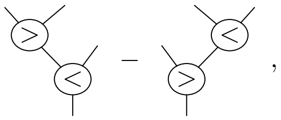


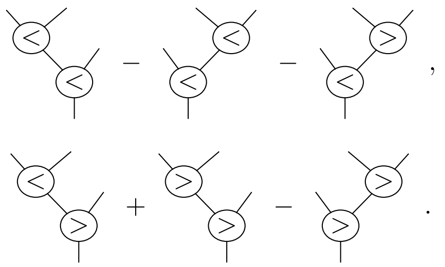
Therefore, for $q^3 = q^2$ (that is, for $q = 0$ or $q = 1$) the defining relation of the operad As_q forms a Gröbner basis, and for other values of q the element  should be adjoined to the set of relations when forming a Gröbner basis. We leave it to the reader to check that all further S-polynomials can be reduced to zero, and to describe the normal forms (Exercise 3.3).

Remark 3.6.1.3. In the particular case $q = -1$, the operad As_q is called the *antiassociative* operad. It is the simplest example of a non-Koszul quadratic operad. See [186] for more properties of that operad.

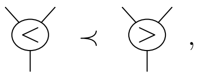
3.6.2 The dendriform operad

Example 3.6.2.1. The nonsymmetric dendriform operad Dend defined in [175] is the quotient of the free operad with two generators  and  by the ideal generated by the elements

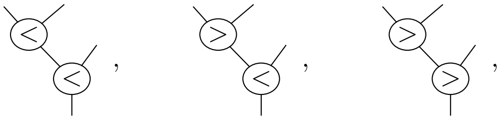




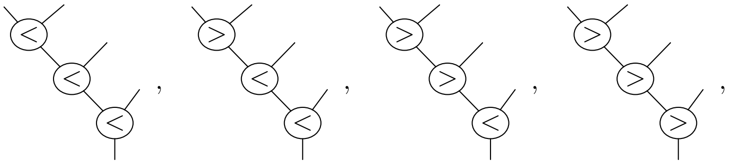
Let us consider the ordering of the generators given by



and the induced `pathdeglex` ordering of tree monomials. For this ordering, the leading terms of the relations are

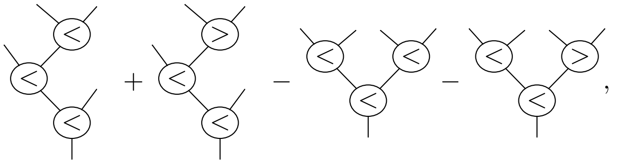


respectively. There are four small common multiples,

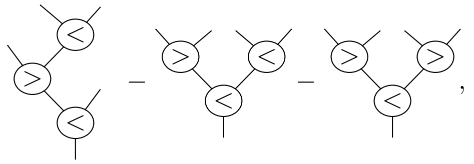


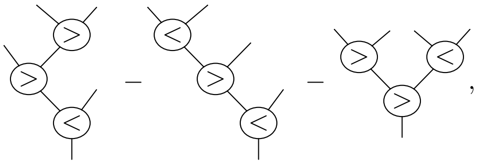
and the corresponding S-polynomials are

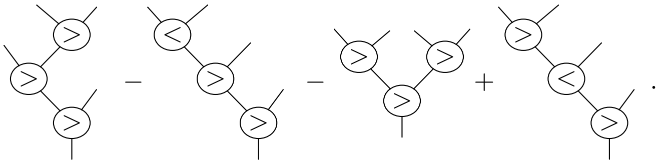
$M_1 =$



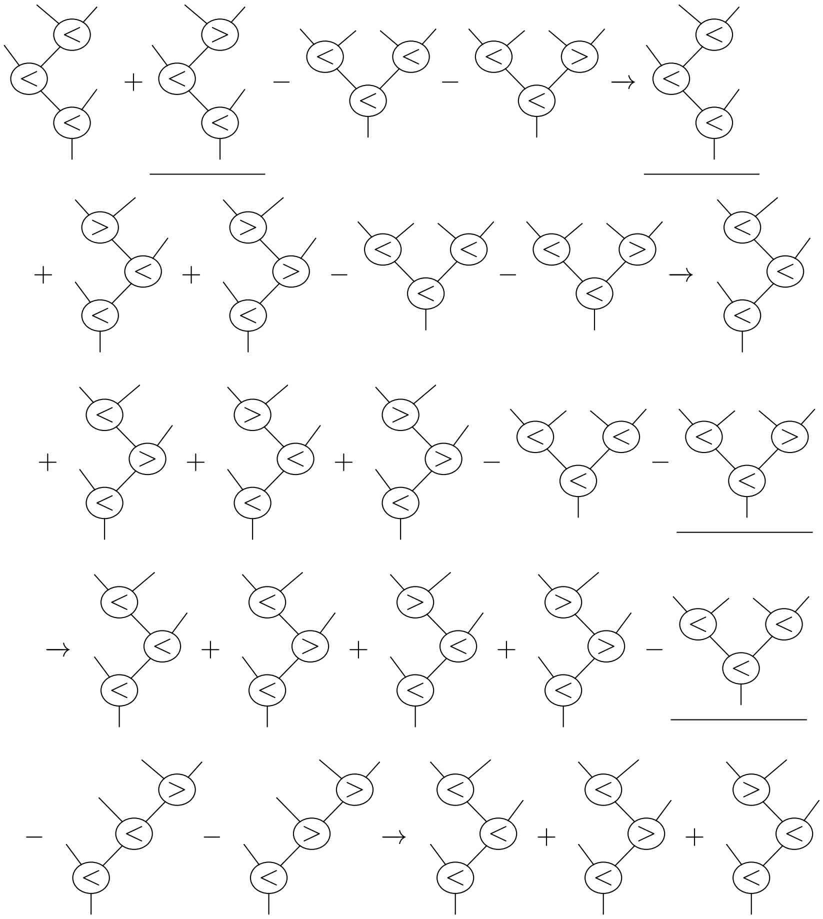
$M_2 =$

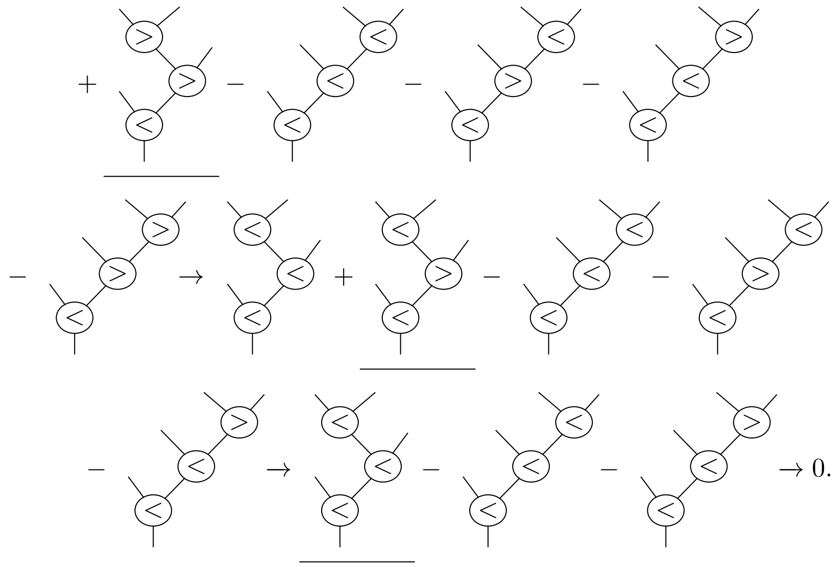


$M_3 =$ 

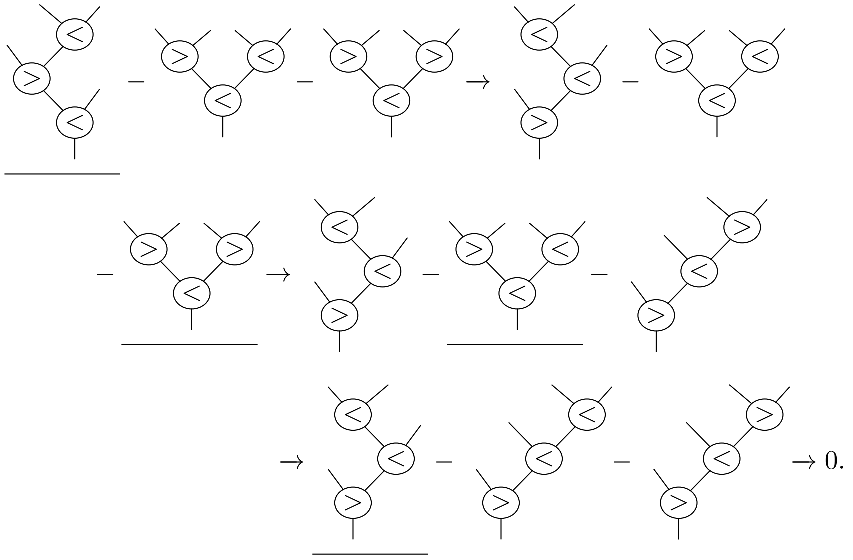
$M_4 =$ 

Let us demonstrate that M_1 can be reduced to zero. We have the following sequence of reductions:

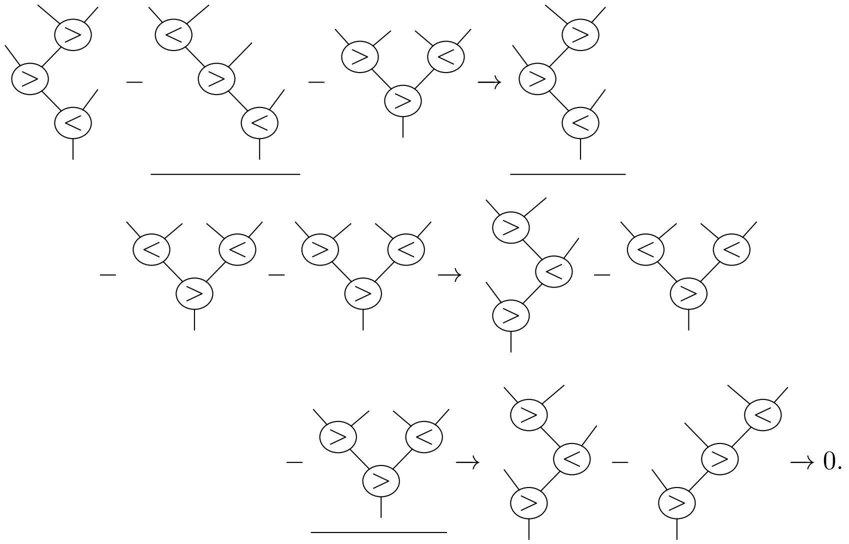




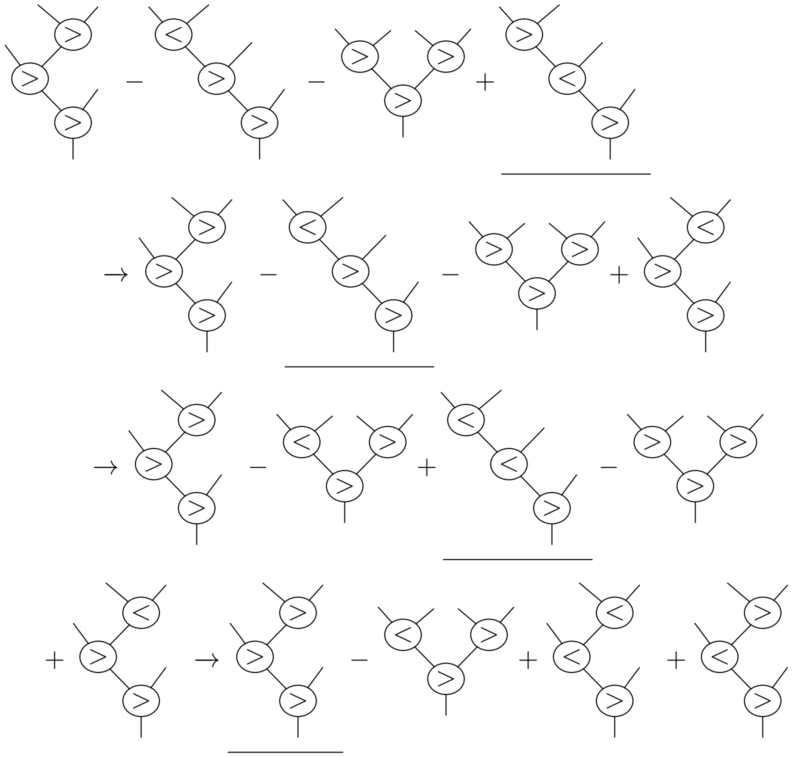
Let us demonstrate that M_2 can be reduced to zero. We have the following sequence of reductions:

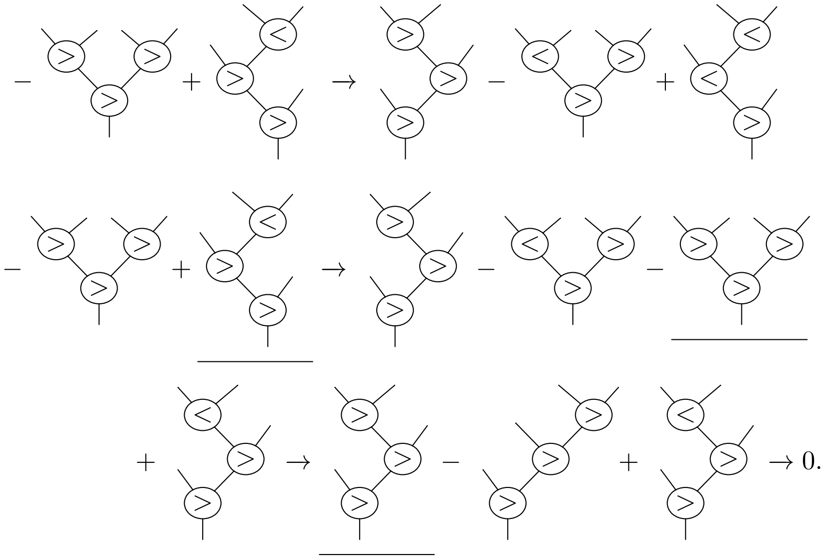


Let us demonstrate that M_3 can be reduced to zero. We have the following sequence of reductions:



Finally, let us demonstrate that M_4 can be reduced to zero. We have the following sequence of reductions:





Therefore, the defining relations of Dend form a Gröbner basis. (This is not the case for the other ordering of generators, as Exercise 3.4 shows.)

3.7 Normal forms for algebras over nonsymmetric operads

In general, finding normal forms for algebras of a given type is a difficult task. For example, if one works with presentations by generators and relations for algebras with two binary operations each of which is an associative product, there is no known way to approach Gröbner bases and normal forms along the lines of Chapter 2, that is by exhibiting a convenient basis of the free algebra, and imposing a monomial order, that is an order of that basis for which both products are increasing functions. In this section, we will explain how operad theory can help to solve these problems.

It turns out that for each nonsymmetric operad $\mathcal{P}$ it is possible to work out normal forms for $\mathcal{P}$-algebras presented by generators and relations. The way we approach this problem may feel a bit bizarre at first sight: we view it as a particular case of a much more complex problem, viewing a $\mathcal{P}$-algebra A as an arity zero component of a certain operad $\mathcal{P} \ltimes A$. It turns out that due to a richer algebraic structure that we use, the latter problem is much easier to approach algorithmically, as we will see below.

3.7.1 Extensions and normal forms in algebras

Let $\mathcal{P} = \mathcal{T}(\mathcal{X})/\mathcal{I}$ be a nonsymmetric operad, and let A be an algebra over $\mathcal{P}$. The following construction is an explicit adaptation for the nonsymmetric case of the construction of the enveloping operad for the pair $(\mathcal{P}, A)$, see [17] and references therein.

Definition 3.7.1.1 (Extension of an operad by an algebra)**.** The *extension of an operad $\mathcal{P}$ by its algebra A*, denoted $\mathcal{P} \ltimes A$, is the operad

$$\mathcal{T}(\mathcal{X} \oplus \overline{A})/(\mathcal{I} \oplus \mathcal{I}_A),$$

where $\overline{A}$ is the same vector space as A but viewed as a collection of operations of arity 0 (for each element $a \in A$, we denote the corresponding element of $\overline{A}$ by $\overline{a}$), and $\mathcal{I}_A$ consists of all the relations

$$\mu \circ (\overline{a}_1, \dots, \overline{a}_n) - \overline{\mu(a_1, \dots, a_n)}$$

for all $\mu \in \mathcal{X}(n)$ and all $a_1, \dots, a_n \in A$.

Remark 3.7.1.2. Once one passes from the algebra A to the collection $\overline{A}$, this construction can be also viewed as an operadic analogue of “split null extensions” [84]. In the case of commutative associative algebras, split null extensions are used in the context of normal forms as well, appearing in the original definition of Gröbner bases for submodules of free modules over polynomial rings [201].

Proposition 3.7.1.3. *We have $(\mathcal{P} \ltimes A)(0) \cong A$.*

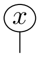
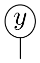
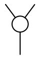
Proof. Using the relations $\mathcal{I}_A$, every element from $\mathcal{T}(\mathcal{X} \oplus \overline{A})(0)$ can be shown equal to an element of $\overline{A}(0) = A$. All these elements are linearly independent since A is a $\mathcal{P}$-algebra, so applying relations $\mathcal{I}_A$ cannot create further linear dependencies. □

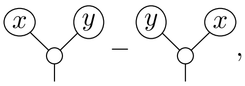
Consequently, it becomes clear how to use Gröbner bases to study algebras over any nonsymmetric operad: one should form the corresponding extension, compute the operadic Gröbner basis, and use it to determine normal forms in arity 0. This results in the following theorem.

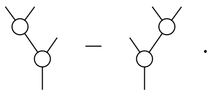
Theorem 3.7.1.4. *Let $\mathcal{P} = \mathcal{T}(\mathcal{X})/\mathcal{I}$ be a nonsymmetric operad, and let A be an algebra over $\mathcal{P}$. If $\mathcal{G}$ is the reduced Gröbner basis of the operad $\mathcal{P} \ltimes A$, then the normal tree monomials of arity zero form a basis of A.*

Proof. This is an immediate corollary of Proposition 3.7.1.3. □

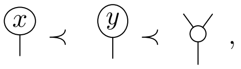
3.7.2 Example of normal forms

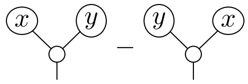
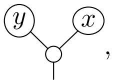
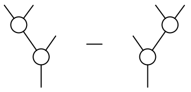
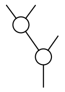
Let us consider the polynomial ring $\mathbb{F}[x, y]$ as an associative algebra $T(x, y)/(xy - yx)$, and let us study that algebra by viewing it as an algebra over the nonsymmetric operad As. This means that we consider the free nonsymmetric operad with two generators  and  of arity zero, and a binary generator . We will study the quotient of this operad by the ideal generated by the elements

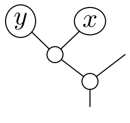
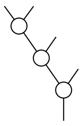




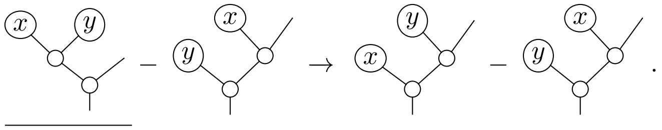
Let us consider the ordering of the generators given by

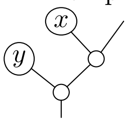
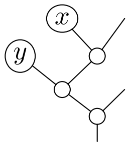


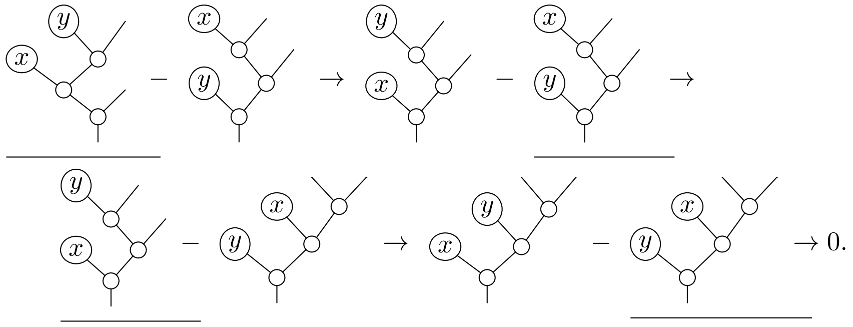
and the corresponding `gpathlex` order of the tree monomials. In that case, the leading monomial of  is , and the leading monomial of  is . These tree monomials have two small common multiples, the tree monomials

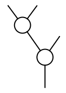
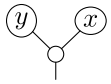
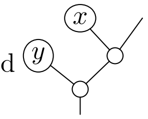
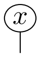
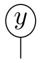
 and .

The first small common multiple gives rise to the S-polynomial and its reduction:



Neither of the monomials appearing in this new element is divisible by the leading terms of the original relations, and therefore this element must be adjoined to the reduced Gröbner basis. The second small common multiple gives rise to an S-polynomial that can be reduced to zero, as we saw previously in Example 3.6.1.1. The leading monomial of the newly adjoined element is , which has no small common multiples with itself, and forms just one small common multiple  with the other leading terms. That small common multiple gives rise to the S-polynomial which is reduced to zero by a sequence of reductions:



(the last reduction uses the element adjoined at the previous step). This means that we found the reduced Gröbner bases. To classify the arity zero normal forms, we note that a normal monomial cannot be divisible by , and so the underlying tree is a "right comb", a tree where a binary vertex can only be a right child of another binary vertex. Also, a normal form cannot have divisors  and , which means that the arity zero generators used in it, listed from the left to the right, must be several copies of the generator , and then several copies of the generator . Overall, this recovers the usual basis $x^i y^j$ in $\mathbb{F}[x,y]$.

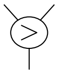
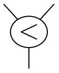
In general, for an associative algebra presented by generators and relations, this approach recovers the normal forms obtained in Chapter 2 (Exercise 3.13). For other nonsymmetric operads, it gives a new approach to normal forms. We shall recall another application in Chapter 6.

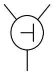
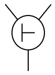
3.8 Exercises

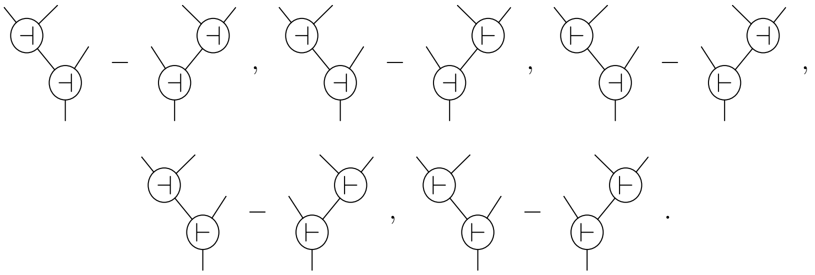
Exercise 3.1. Show that for each finite $\mathcal{S} \subset \mathcal{T}(\mathcal{X})$ Algorithm 3.4.2.20 terminates after finitely many steps.

Exercise 3.2. Use Equation (3.6) and Proposition 3.4.2.12 to fill in the details of the proof of Theorem 3.5.1.6.

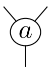
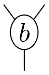
Exercise 3.3. Compute the remaining S-polynomials for Example 3.6.1.2, and describe normal forms in the operad As_q.

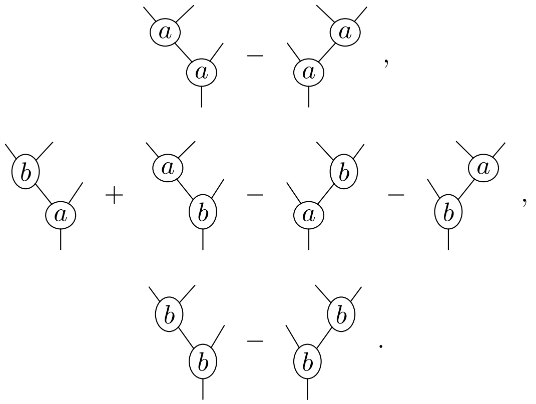
Exercise 3.4 ([182])**.** Consider the ordering  $\prec$  , and compute the corresponding reduced Gröbner basis for the operad Dend.

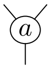
Exercise 3.5. The nonsymmetric diassociative operad Dias (defined in [175]) is the quotient of the free operad with two generators  and  by the ideal generated by the five elements

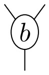


Pick some monomial order, and compute the reduced Gröbner basis for the defining relations of Dias for that order.

Exercise 3.6. The nonsymmetric operad $\mathsf{As}^{\langle 2 \rangle}$ of two linearly compatible associative products (defined in [70]) is the quotient of the free operad with two generators  and  by the ideal generated by the three elements

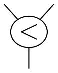
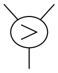


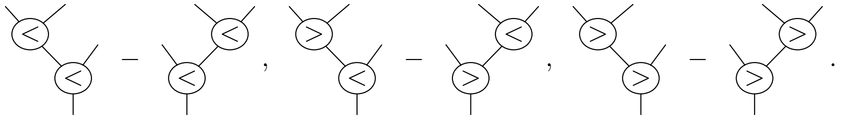
These relations together express the fact that any linear combination of 

and  is associative.

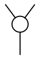
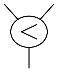
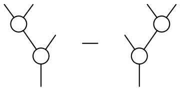
Pick some monomial order, and compute the reduced Gröbner basis for the defining relations of $\mathsf{As}^{\langle 2\rangle}$ for that order.

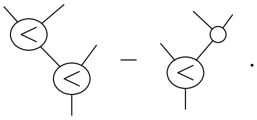
Exercise 3.7. Define the nonsymmetric operad $\mathsf{As}^{\langle k\rangle}$ of k linearly compatible associative products, and find some monomial order for which you can compute the reduced Gröbner basis for the defining relations of $\mathsf{As}^{\langle k\rangle}$ for that order.

Exercise 3.8. The nonsymmetric duplicial operad Dup (defined in [177]) is the quotient of the free operad with two generators  and  by the ideal generated by the three elements

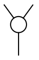
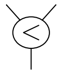
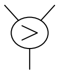


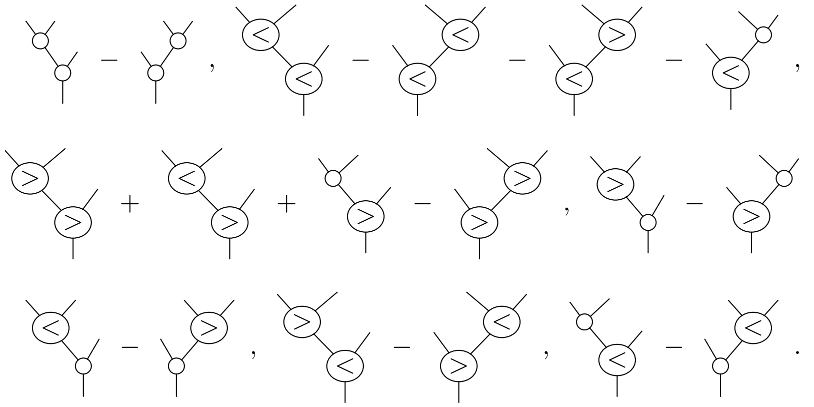
Pick some monomial order, and compute the reduced Gröbner basis for the defining relations of Dup for that order.

Exercise 3.9. The nonsymmetric dipterous operad Dipt (defined in [178]) is the quotient of the free operad with two generators  and  by the ideal generated by the two elements  and



Pick some monomial order, and compute the reduced Gröbner basis for the defining relations of Dipt for that order.

Exercise 3.10. The nonsymmetric tridendriform operad $\mathsf{Tridend}$ (defined in [179]) is the quotient of the free operad with three generators  ,  , and  by the ideal generated by the seven elements



Pick some monomial order, and compute the reduced Gröbner basis for the defining relations of Tridend for that order.

Exercise 3.11. Consult [2] for the definition of the nonsymmetric operad of quadri-algebras. Try to guess, based on the example of the dendriform operad, an optimal monomial order for computing its reduced Gröbner basis. Check your guess, and compare your results with the investigation for several different orders undertaken in [182].

Exercise 3.12. Consult [176] for the definition of a certain diagram of operads called there “the operadic butterfly”, and in particular for the definition of two operads $\mathcal{X}^+$ and $\mathcal{X}^-$. Currently, not much is known about those operads. For instance, it is conjectured in [176] that $\dim \mathcal{X}^+(n) = \dim \mathcal{X}^-(n) = 4^{n-1}$. Check this conjecture for small n by computing the reduced Gröbner basis in low arities, and working out the corresponding normal forms.

Exercise 3.13. Explain how to use the approach of Section 3.7 to recover, for any associative algebra presented by generators and relations, the normal forms obtained in Chapter 2.

Exercise 3.14. Use results of Example 3.6.2.1 to attempt a generalization of Theorem 2.5.3.1 for the dendriform algebras arising as universal enveloping of pre-Lie and brace algebras [52].

Exercise 3.15. Compare the approach to normal forms for dendriform algebras which follows from general results of Section 3.7 to the approach of the preprint [152] (released as the final draft of this book was being prepared).

Chapter 4

Twisted Associative Algebras and Shuffle Algebras

The goal of this chapter is to discuss the algebraic structures that are somewhere in between associative algebras and operads: twisted associative algebras and shuffle algebras. Even though these can in principle be treated in the more general operadic context, this topic is much easier to digest independently, and it serves as a gentle introduction to the philosophy behind shuffle operads that we will discuss later.

4.1 Introduction

When working with the tensor algebra of a vector space V, we use the concatenation of tensors to define products of elements. More precisely, for two decomposable tensors $v_1 \otimes \cdots \otimes v_k$ and $v_{k+1} \otimes \cdots \otimes v_n$, the concatenation product operation takes the factors in the first tensor, and puts them next to the factors of the second tensor, on the left. It is natural to ask what we would obtain if we would be allowed to do more, for example, put the factors of the first and the second tensor together but in a different order.

Why is this viewpoint useful at all? First, it can help when tensor algebras in question have some extra structure. For instance, suppose that the vector space V of which we take tensor powers is a Lie algebra. In that case, there is the adjoint action of that Lie algebra on itself, leading to an action on the tensor algebra $T(V)$. A natural representation-theoretic question would be to study the algebra of invariants of that action. Unlike the symmetric algebra where this question is extremely well understood, at least for, say, finite-dimensional semisimple Lie algebras, in the case of tensor algebras the answer is quite complicated, mainly because the algebra in question is too large. By using extra algebraic structures, one may hope to use fewer elements to generate the algebra of invariants, which would be a useful extra insight. Since the adjoint action of a Lie algebra on its tensor powers commutes with the actions of symmetric group by permutation of factors, it is not too far fetched to assume that the symmetric group actions would play a certain role here.

Second, incorporating actions of symmetric groups allows one to view tensor algebras as algebras where the concatenation products satisfy some sort of obscure commutativity:

$$(v_{k+1}\otimes\cdots\otimes v_n)(v_1\otimes\cdots\otimes v_k)=[(v_1\otimes\cdots\otimes v_k)(v_{k+1}\otimes\cdots\otimes v_n)]\,\sigma_{k,n-k},$$

where $\sigma_{k,n-k}$ denotes the permutation that swaps the two clusters of elements, putting the integers between 1 and n in the order $k{+}1,\ldots,n,1,\ldots,k$. Viewing tensor algebras as algebras that exhibit some sort of commutativity can be used for purposes of noncommutative geometry [106].

However convincing what we just outlined may have been to motivate an algebraist to come up with a definition of a twisted associative algebra, in fact such a definition was first given by topologists.[1] One reason for that is as follows. If we consider the n-sphere S^n as the one-point compactification of $\mathbb{R}^n$, then the canonical product isomorphism

$$\mathbb{R}^n\times\mathbb{R}^m\cong\mathbb{R}^{n+m},\qquad (x_1,\ldots,x_n)\times(y_1,\ldots,y_m)\to(x_1,\ldots,x_n,y_1,\ldots,y_m)$$

induces a homeomorphism

$$\mu_{n,m}\colon S^n\wedge S^m\simeq S^{n+m}.$$

If we consider the action of permutation groups S_n on $\mathbb{R}^n$ by permutations of coordinates, this action compactifies to the action on S^n preserving the basepoint of S^n, and the homeomorphism $\mu_{n,m}$ is $S_n\times S_m$-equivariant. This leads one to a realization of importance of symmetric group actions when thinking of a universal algebraic formalism for Whitehead products [12], or when talking about symmetric spectra as a good playground for stable homotopy theory [137].

4.2 Twisted associative algebras and shuffle algebras

4.2.1 Two definitions of a twisted associative algebra

The most economic definition (which however is not the easiest one for computations) is the following one.

Definition 4.2.1.1 (Classical definition of a twisted associative algebra)**.** A *twisted associative algebra* is a nonnegatively graded associative algebra

[1] To quote the opening sentence of [12], “Several forces have made me take up again the notion of homotopy envelopes, where the milling crowd of generalised Hopf invariants may be reduced to order or at least quieted.”

$\mathcal{A} = \bigoplus_{n\geq 0} \mathcal{A}(n)$ for which each graded component $\mathcal{A}(n)$ is a right S_n-module, and each product map

$$\mathcal{A}(n_1) \otimes \mathcal{A}(n_2) \to \mathcal{A}(n_1 + n_2)$$

is a morphism of $S_{n_1} \times S_{n_2}$-modules (the right-hand side is viewed as an $S_{n_1} \times S_{n_2}$-module through the standard embedding $S_{n_1} \times S_{n_2} \subset S_{n_1+n_2}$).

Let us remark that if only the component $\mathcal{A}(0)$ is nonzero, then there are no symmetric group actions to keep track of, so a twisted associative algebra of that kind is a usual associative algebra. If only the component $\mathcal{A}(1)$ is nonzero, then the product must be zero, since the product of two elements from $\mathcal{A}(1)$ belongs to $\mathcal{A}(2)$.

As we mentioned in the previous section, one important nontrivial example of a shuffle algebra is given by the tensor algebra $T(V)$.

Example 4.2.1.2. Let us equip each homogeneous component $V^{\otimes n}$ of $T(V)$ with the right S_n-action in the usual way:

$$(v_1 \otimes \cdots \otimes v_n).\tau = v_{\tau(1)} \otimes \cdots \otimes v_{\tau(n)}.$$

Then the concatenation of tensors is a morphism of $S_{n_1} \times S_{n_2}$-modules, so we get a twisted associative algebra structure.

Remark 4.2.1.3. At this stage, there are two different ways to make the tensor algebra a shuffle algebra, by making it concentrated in the zeroth component, and by separating the components. Those two are completely different shuffle algebras; we will mostly be using the latter one in our examples.

Let us try to decipher the definition a little bit further. We will take the viewpoint that already emerged in Chapter 3: instead of looking at graded spaces as direct sums, we will think of them as collections of their components. Defining a structure of a graded associative algebra on a nonnegatively graded vector space $\mathcal{A} = \oplus_{n\geq 0}\mathcal{A}(n)$ is equivalent to defining a collection of maps

$$\mu_{n_1,n_2} \colon \mathcal{A}(n_1) \otimes \mathcal{A}(n_2) \to \mathcal{A}(n_1 + n_2)$$

satisfying appropriate associativity conditions

$$\mu_{n_1+n_2,n_3} \circ (\mu_{n_1,n_2} \otimes \mathrm{id}) = \mu_{n_1,n_2+n_3} \circ (\mathrm{id} \otimes \mu_{n_2,n_3}).$$

The condition that such a map is $S_n \times S_m$-equivariant is equivalent to saying that the map

$$\mathcal{A}(n_1) \otimes \mathcal{A}(n_2) \otimes \mathbb{F}S_{n_1+n_2} \to \mathcal{A}(n_1 + n_2) \otimes \mathbb{F}S_{n_1+n_2} \to \mathcal{A}(n_1 + n_2),$$

the composite of $\mu_{n,m} \otimes \mathrm{id}$ and the symmetric group action, factors through the canonical projection

$$(\mathcal{A}(n_1)\otimes\mathcal{A}(n_2))\otimes\mathbb{F}S_{n_1+n_2}\twoheadrightarrow (\mathcal{A}(n_1)\otimes\mathcal{A}(n_2))\otimes_{\mathbb{F}(S_{n_1}\times S_{n_2})}\mathbb{F}S_{n_1+n_2}\cong \mathrm{Ind}_{S_{n_1}\times S_{n_2}}^{S_{n_1+n_2}}(\mathcal{A}(n_1)\otimes\mathcal{A}(n_2)).$$

The last line uses the notion of an induced representation; a reader who needs guidance on that is directed to [97] for details.

This leads to a definition of a twisted associative algebra in the language of "symmetric collections".

Definition 4.2.1.4 (Symmetric collection)**.** A *symmetric collection* is a sequence $\mathcal{V}=\{\mathcal{V}(n)\}_{n\geq 0}$ of vector spaces, where each $\mathcal{V}(n)$ is a right $\mathbb{F}S_n$-module.

A *morphism* between two symmetric collections $\mathcal{V}$ and $\mathcal{W}$ is a sequence of linear maps

$$\phi_n\colon \mathcal{V}(n)\to\mathcal{W}(n),\quad n\geq 0,$$

which commute with the symmetric group actions. If each ϕ_n is injective, we call the collection of their images a *subcollection* of $\mathcal{W}$.

Two most important operations on symmetric collections are direct sums and tensor products, which we will now define.

Definition 4.2.1.5 (Operations on symmetric collections)**.** Let $\mathcal{V}$ and $\mathcal{W}$ be two symmetric collections. The *direct sum* $\mathcal{V}\oplus\mathcal{W}$ is defined by the formula

$$(\mathcal{V}\oplus\mathcal{W})(n)=\mathcal{V}(n)\oplus\mathcal{W}(n).$$

The *tensor product* $\mathcal{V}\otimes\mathcal{W}$ is defined by the formula

$$(\mathcal{V}\otimes\mathcal{W})(n)=\bigoplus_{n_1+n_2=n}\mathrm{Ind}_{S_{n_1}\times S_{n_2}}^{S_n}(\mathcal{V}(n_1)\otimes\mathcal{W}(n_2)).$$

Note that the two collections $\underline{\mathbb{F}}$ and $\mathbb{1}$ which we already discussed in the nonsymmetric case (Definition 3.1.1.2), can be viewed as symmetric collections in a unique way, since for $n=0$ and $n=1$ the symmetric group S_n is trivial.

Proposition 4.2.1.6.

- *The following formula holds:*

$$(\mathcal{V}\otimes\mathcal{W})(n)=\bigoplus_{I_1\sqcup I_2=\{1,\ldots,n\}}\mathcal{V}(|I_1|)\otimes\mathcal{V}(|I_2|).$$

- *The tensor product is associative, so that*

$$(\mathcal{U}\otimes\mathcal{V})\otimes\mathcal{W}\cong\mathcal{U}\otimes(\mathcal{V}\otimes\mathcal{W})$$

for all symmetric collections $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$.

- *We have*

$$\mathcal{V} \otimes \underline{\mathbb{F}} \cong \mathcal{V} \cong \underline{\mathbb{F}} \otimes \mathcal{V}$$

for all symmetric collections $\mathcal{V}$.

Proof. The cosets $(S_{n_1} \times S_{n_2}) \backslash S_{n_1+n_2}$ are known to be represented by (n_1, n_2)-shuffles, that is permutations τ for which

$$\tau^{-1}(1) < \cdots < \tau^{-1}(n_1), \quad \tau^{-1}(n_1+1) < \cdots < \tau^{-1}(n_1+n_2).$$

Now, we have

$$\mathrm{Ind}_{S_{n_1} \times S_{n_2}}^{S_{n_1+n_2}} (\mathcal{V}(n_1) \otimes \mathcal{W}(n_2)) \cong \bigoplus_{\tau \text{ a } (n_1,n_2)-\text{shuffle}} (\mathcal{V}(n_1) \otimes \mathcal{W}(n_2)) \otimes \tau,$$

or in other words

$$(\mathcal{V} \otimes \mathcal{W})(n) = \bigoplus_{I_1 \sqcup I_2 = \{1,\ldots,n\}} \mathcal{V}(|I_1|) \otimes \mathcal{W}(|I_2|),$$

where

$$I_1 = \tau^{-1}\{1, \ldots, n_1\}, \quad I_2 = \tau^{-1}\{n_1+1, \ldots, n_1+n_2\}.$$

The rest of the proof is left as an exercise for the reader (Exercise 4.1). □

This result leads to another definition of a twisted associative algebra.

Definition 4.2.1.7 (Monoidal definition of a twisted associative algebra)**.** A *twisted associative algebra* is a monoid in the category of symmetric collections with respect to the tensor product.

We leave it to the reader (Exercise 4.2) to prove that the two definitions we gave are equivalent, using a simple analysis of our preliminary remarks above. Another consequence of associativity of the tensor product is that we can talk about tensor powers of symmetric collections.

Definition 4.2.1.8 (Tensor power of a symmetric collection)**.** Let $\mathcal{V}$ be a symmetric collection. The *tensor power* $\mathcal{V}^{\otimes n}$ is the tensor product of n copies of $\mathcal{V}$. For $n = 0$, we define $\mathcal{V}^{\otimes 0} := \underline{\mathbb{F}}$.

The monoidal definition of a twisted associative algebra also allows us to give a very concise definition of an ideal in a twisted associative algebra.

Definition 4.2.1.9 (Ideal of a twisted associative algebra)**.** An *ideal* of a twisted associative algebra $\mathcal{A}$ is a symmetric subcollection $\mathcal{I} \subset \mathcal{A}$ for which the image of the structure map $\mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ restricted to $\mathcal{I} \otimes \mathcal{A} + \mathcal{A} \otimes \mathcal{I}$ is contained in $\mathcal{I}$.

4.2.2 Free twisted associative algebras

Similar to the case of associative algebras, a twisted associative algebra can be presented via generators and relations, that is, as a quotient of the free twisted associative algebra $T_\Sigma(\mathcal{M})$, which we will now describe, by some ideal. Unlike the cases of the free associative algebra and the free nonsymmetric operad, we will not discuss free twisted associative algebras in full detail, since we will see that they are not fully suitable for defining Gröbner bases and proving an appropriate diamond lemma (which leads to a suitable replacement, free shuffle algebras, defined in the next section).

Definition 4.2.2.1 (Free twisted associative algebra)**.** The *free twisted associative algebra* $T_\Sigma(\mathcal{M})$ generated by a given symmetric collection $\mathcal{M}$ is the direct sum of all tensor powers of $\mathcal{M}$, including $\mathcal{M}^{\otimes 0} := \underline{\mathbb{F}}$:

$$T_\Sigma(\mathcal{M}) = \underline{\mathbb{F}} \oplus \bigoplus_{k \geq 1} \mathcal{M}^{\otimes k}.$$

Let us make this definition more concrete.

Definition 4.2.2.2 (Partition tensors)**.** Elements of the component $T_\Sigma(\mathcal{M})(n)$ are linear combinations of *partition tensors*. Each partition tensor is a pair (π, m), where

- π is an ordered set partition of $\{1, \ldots, n\}$, $\{1, \ldots, n\} = \bigsqcup_{j=1}^{k} I^{(j)}$;
- m is a decomposable tensor $\mathsf{m}^{(1)} \otimes \mathsf{m}^{(2)} \otimes \ldots \otimes \mathsf{m}^{(k)}$, with $\mathsf{m}^{(j)} \in \mathcal{M}(|I^{(j)}|)$ for every $j = 1, \ldots, k$.

The product μ_{n_1,n_2} of two partition tensors (π_1, m_1) and (π_2, m_2) is the partition tensor (π, m), where $\pi = \pi_1 \sqcup \imath_{n_1}(\pi_2)$, $\mathsf{m} = \mathsf{m}_1\mathsf{m}_2$. (The map $\imath_{n_1} \colon \{1, \ldots, n_2\} \to \{n_1 + 1, \ldots, n_1 + n_2\}$ is the bijection adding n_1 to all elements.) This product extends to a unique bilinear product on $T_\Sigma(\mathcal{M})$.

Example 4.2.2.3. Let us consider the free twisted associative algebra generated by the symmetric collection $\mathbb{1}$. We note that every subset I_j in Definition 4.2.2.1 has to consist of one element, and therefore allowed ordered partitions are just permutations (and the tensor part does not carry any additional information, since the vector space $\mathbb{1}(1)$ is one-dimensional). Therefore, each component of the free twisted associative algebra generated by $\mathbb{1}$ has a basis of permutations, and can thus be identified, as vector spaces, with the group algebra of the respective symmetric group.

The particular case of the free algebra $T_\Sigma(\mathbb{1})$ which we just discussed is quite sufficient to illustrate a major problem that arises because of symmetric group actions.

Proposition 4.2.2.4. *It is impossible to define a total ordering of basis elements of* $T_\Sigma(\mathbb{1})$ *which would lead to normal forms in quotient shuffle algebras.*

Proof. Let us consider the subspace of $T_\Sigma(\mathbb{1})(2)$ spanned by the element

$$r = 12 - 21,$$

the difference of the two permutations of two elements. We can consider the ideal generated by this element, which is the span of all elements obtained from this one by iterations of products and permutations. Such elements can be easily seen to be all elements of the form

$$i_1 i_2 \cdots i_k i_{k+1} \cdots i_n - i_1 i_2 \cdots i_{k+1} i_k \cdots i_n,$$

that is differences of permutations that differ from each other by a transposition of two elements in neighboring places. It follows that the quotient twisted associative algebra $T_\Sigma(\mathbb{1})/(r)$ has one-dimensional components; in fact, it is the tensor algebra $T(x)$ viewed as a twisted associative algebra according to Example 4.2.1.2. On the other hand, suppose that it were possible to have normal forms for elements of quotient algebras based on leading terms of ideals of relations. In this case, the leading term of r would be either 12 or 21. In both cases, our plan fails, since the ideal generated by either of them (which of course would be contained by the ideal of leading terms) contains the other due to being a symmetric subcollection, so a collection of S_n-invariant subspaces. Thus, there would be no normal monomials in the second component at all, a contradiction. □

We will now define a different kind of algebras, the so-called shuffle algebras. This would allow us to resolve the problem on normal forms by completely ignoring the symmetric group action whenever possible.

4.2.3 Shuffle algebras

To define shuffle algebras, we will use nonsymmetric collections (Definition 3.1.1.1) instead of symmetric ones; for those, there is a direct sum construction and a version of the tensor product construction that is motivated by the first formula of Proposition 4.2.1.6.

Definition 4.2.3.1 (Operations on nonsymmetric collections)**.** Let $\mathcal{V}$ and $\mathcal{W}$ be two nonsymmetric collections. The *direct sum* $\mathcal{V} \oplus \mathcal{W}$ is defined by the formula

$$(\mathcal{V} \oplus \mathcal{W})(n) = \mathcal{V}(n) \oplus \mathcal{W}(n).$$

The *shuffle tensor product* $\mathcal{V} \boxtimes \mathcal{W}$ is defined by the formula

$$(\mathcal{V} \boxtimes \mathcal{W})(n) := \bigoplus_{I_1 \sqcup I_2 = \{1,\ldots,n\}} \mathcal{V}(|I_1|) \otimes \mathcal{W}(|I_2|),$$

where the sum is taken over all partitions of $\{1, \ldots, n\}$ into two disjoint subsets I_1 and I_2.

Proposition 4.2.3.2.

- *The shuffle tensor product is associative, so that*
$$(\mathcal{U} \boxtimes \mathcal{V}) \boxtimes \mathcal{W} \cong \mathcal{U} \boxtimes (\mathcal{V} \boxtimes \mathcal{W})$$
for all nonsymmetric collections $\mathcal{U}$*,* $\mathcal{V}$*,* $\mathcal{W}$*.*
- *We have*
$$\mathcal{V} \boxtimes \underline{\mathbb{F}} \cong \mathcal{V} \cong \underline{\mathbb{F}} \boxtimes \mathcal{V}$$
for all nonsymmetric collections $\mathcal{V}$*.*

Proof. This is straightforward:

$$\begin{aligned} ((\mathcal{U} \boxtimes \mathcal{V}) \boxtimes \mathcal{W})(n) &= \bigoplus_{I_1 \sqcup I_2 \sqcup I_3 = \{1,\dots,n\}} (\mathcal{U}(|I_1|) \otimes \mathcal{V}(|I_2|)) \otimes \mathcal{W}(|I_3|) \\ &\cong \bigoplus_{I_1 \sqcup I_2 \sqcup I_3 = \{1,\dots,n\}} \mathcal{U}(|I_1|) \otimes (\mathcal{V}(|I_2|) \otimes \mathcal{W}(|I_3|)) = \mathcal{U} \boxtimes (\mathcal{V} \boxtimes \mathcal{W}), \end{aligned}$$

and

$$\begin{aligned} (\mathcal{V} \boxtimes \underline{\mathbb{F}})(n) &= \bigoplus_{I_1 \sqcup I_2 = \{1,\dots,n\}} \mathcal{V}(|I_1|) \otimes \underline{\mathbb{F}}(|I_2|) = V(n), \\ (\underline{\mathbb{F}} \boxtimes \mathcal{V})(n) &= \bigoplus_{I_1 \sqcup I_2 = \{1,\dots,n\}} \underline{\mathbb{F}}(|I_1|) \otimes \mathcal{V}(|I_2|) = V(n). \end{aligned}$$

□

This result allows us to define shuffle algebras as monoids, mimicking Definition 4.2.1.7.

Definition 4.2.3.3 (Shuffle algebra)**.** A *shuffle algebra* is a monoid in the category of nonsymmetric collections with respect to the shuffle tensor product.

More concretely, the datum of a shuffle algebra on a nonsymmetric collection $\mathcal{A}$ is a collection of maps

$$\mu_{I_1,I_2} \colon \mathcal{A}(n_1) \otimes \mathcal{A}(n_2) \to \mathcal{A}(n)$$

for each partition $\{1,\dots,n\} = I_1 \sqcup I_2$ with $|I_1| = n_1$, $|I_2| = n_2$, and a unit element $e \in \mathcal{A}(0)$ satisfying the following properties:

- *associativity*: for each partition
$$\{1,\dots,n\} = I_1 \sqcup I_2 \sqcup I_3 \quad \text{with} \quad |I_1| = n_1,\ |I_2| = n_2,\ |I_3| = n_3,$$
the following two maps from $\mathcal{A}(n_1) \otimes \mathcal{A}(n_2) \otimes \mathcal{A}(n_3)$ to $\mathcal{A}(n)$ are equal to each other:
$$\mu_{I_1 \sqcup I_2, I_3} \circ (\mu_{I_1,I_2} \otimes \mathrm{id}) = \mu_{I_1, I_2 \sqcup I_3} \circ (\mathrm{id} \otimes \mu_{I_2,I_3}),$$

- *unit axiom*: for any $n \geq 0$, the following maps from $\mathcal{A}(n)$ to $\mathcal{A}(n)$ are equal to each other:

$$\mu_{\varnothing,\{1,\ldots,n\}}(e \otimes \mathrm{id}) = \mu_{\{1,\ldots,n\},\varnothing}(\mathrm{id} \otimes e) = \mathrm{id}\,.$$

Remark 4.2.3.4. It is quite common in the literature to use the term "shuffle algebra" for a very particular commutative associative algebra structure on the underlying vector space of the tensor algebra $T(V)$ obtained as a sum of all individual shuffle products. We do not expect this to lead to a confusion, but nevertheless feel that this should be mentioned.

Similar to the case of twisted associative algebras, we can use the monoidal definition of shuffle algebras to define ideals.

Definition 4.2.3.5 (Ideal of a shuffle algebra)**.** An *ideal* of a shuffle algebra $\mathcal{A}$ is a nonsymmetric subcollection $\mathcal{I} \subset \mathcal{A}$ for which the image of the structure map $\mathcal{A} \boxtimes \mathcal{A} \to \mathcal{A}$ restricted to $\mathcal{I} \otimes \mathcal{A} + \mathcal{A} \otimes \mathcal{I}$ is contained in $\mathcal{I}$.

Since the shuffle tensor product is associative, we can talk about shuffle tensor powers of nonsymmetric collections.

Definition 4.2.3.6 (Shuffle tensor power)**.** The *shuffle tensor power* $\mathcal{V}^{\boxtimes n}$ is the tensor product of n copies of $\mathcal{V}$. For $n = 0$, we define $\mathcal{V}^{\boxtimes 0} := \underline{\mathbb{F}}$.

4.3 Free shuffle algebras

4.3.1 Monomials and polynomials

The following definition of free shuffle algebras is completely analogous to that of twisted associative algebras.

Definition 4.3.1.1 (Free shuffle algebra)**.** The *free shuffle algebra* $T_{\text{Ш}}(\mathcal{M})$ generated by a given nonsymmetric collection $\mathcal{M}$ is the direct sum of all shuffle tensor powers of $\mathcal{M}$, including $\mathcal{M}^{\otimes 0} := \underline{\mathbb{F}}$:

$$T_{\text{Ш}}(\mathcal{M}) = \underline{\mathbb{F}} \oplus \bigoplus_{k \geq 1} \mathcal{M}^{\boxtimes k}.$$

Remark 4.3.1.2. The Cyrillic letter Ш (pronounced "sha") is the first letter in the Russian transliteration "шафл" of the word "shuffle".

Let us make this definition more explicit by exhibiting a combinatorial basis of the free shuffle algebra that generalizes the basis of words in the tensor algebra of a vector space.

Definition 4.3.1.3 (Shuffle monomial)**.** Let $\mathcal{X} = \{\mathcal{X}(n)\}_{n\geq 0}$ be an operation alphabet. A *shuffle monomial* in $\mathcal{X}$ is a pair $T = (\pi, \mathsf{m})$, where

- π is an ordered partition of $\{1, \ldots, n\}$ into subsets, $\{1, \ldots, n\} = \bigsqcup_{j=1}^{k} I^{(j)}$;
- m is a decomposable tensor $\mathsf{m}^{(1)} \otimes \mathsf{m}^{(2)} \otimes \cdots \otimes \mathsf{m}^{(k)}$, with $\mathsf{m}^{(j)} \in \mathcal{X}_{|I^{(j)}|}$ for every $j = 1, \ldots, k$.

The shuffle monomial for which $n = k = 0$ is called the *empty shuffle monomial.*

The *arity* of a shuffle monomial T as above, denoted $\mathrm{ar}(T)$, is equal to n, and the *weight* of such monomial, denoted $\mathrm{wt}(T)$, is equal to k. The set of all shuffle monomials in $\mathcal{X}$ of arity n is denoted $\text{Ш}_{\mathcal{X}}(n)$. The collection of all these sets for all $n \geq 0$ is denoted $\text{Ш}_{\mathcal{X}}$.

Remark 4.3.1.4. In Chapter 3 where the notion of an operation alphabet was introduced, we really dealt with operations in a nonsymmetric operad. In the context of shuffle algebras, the elements of $\mathcal{X}(n)$ are not representing n-ary operations. Nevertheless, using the same language in this context does highlight some similarities between different algebraic structures we discuss throughout the book, so this choice of terminology, even if surprising, is fully intentional.

Example 4.3.1.5. Let us consider the free shuffle algebra generated by the nonsymmetric collection $\mathbb{1}$. Similar to Example 4.2.2.3, we note that every subset I_j in Definition 4.3.1.3 has to consist of one element, and therefore allowed ordered partitions are just permutations (and the tensor part does not carry any additional information, since the vector space $\mathbb{1}(1)$ is one-dimensional). Therefore, each component of the free shuffle algebra generated by $\mathbb{1}$ has a basis of permutations, and can thus be identified, as vector spaces, with the group algebra of the respective symmetric group.

Definition 4.3.1.6 (Shuffle polynomial)**.** Let $\mathcal{X} = \{\mathcal{X}(n)\}_{n\geq 0}$ be an operation alphabet. A *shuffle polynomial* in $\mathcal{X}$ with coefficients in $\mathbb{F}$ is a linear combination of shuffle monomials of the same arity. The *support* of a shuffle polynomial f, denoted $\mathrm{supp}(f)$, is the set of all shuffle monomials that appear in f with nonzero coefficients.

We denote the vector space of all shuffle polynomials of arity n by $T_{\text{Ш}}(\mathcal{X})(n)$; of course we have $T_{\text{Ш}}(\mathcal{X})(n) = \mathbb{F}\text{Ш}_{\mathcal{X}}(n)$.

Definition 4.3.1.7 (Explicit construction of the free shuffle algebra)**.** Suppose that

$$T_1 = (\pi_1, \mathsf{m}_1) \in \text{Ш}_{\mathcal{X}}(n_1), \quad T_2 = (\pi_2, \mathsf{m}_2) \in \text{Ш}_{\mathcal{X}}(n_2).$$

For each partition $\{1, \ldots, n_1+n_2\} = I_1 \sqcup I_2$ with $|I_1| = n_1$, $|I_2| = n_2$, we define the partition $\tilde{\pi}_k$ of I_k, $k = 1, 2$, using the unique order preserving bijection $I_k \cong \{1, \ldots, n_k\}$. The *shuffle* (I_1, I_2)*-product*

$$\mu_{I_1,I_2}(T_1, T_2) \in \text{Ш}_{\mathcal{X}}(n)$$

is the shuffle monomial (π, m), where $\pi = \tilde{\pi}_1 \sqcup \tilde{\pi}_2$, $\mathsf{m} = \mathsf{m}_1\mathsf{m}_2$.

These operations μ_{I_1,I_2} may be extended to unique bilinear operations

$$\mu_{I_1,I_2} \colon T_{\text{Ш}}(\mathcal{X})(n_1) \otimes T_{\text{Ш}}(\mathcal{X})(n_2) \to T_{\text{Ш}}(\mathcal{X})(n).$$

Equipped with these operations, $T_{\text{Ш}}(\mathcal{X})$ is the *free shuffle algebra generated by* $\mathcal{X}$. In addition to the notation $T_{\text{Ш}}(\mathcal{X})$, we will use the notation $T_{\text{Ш}}(\mathcal{M})$, where $\mathcal{M} = \{\mathcal{M}(n)\}_{n\geq 0}$ is a collection of vector spaces for which $\mathcal{M}(n) = \text{span}(\mathcal{X}(n))$ for all $n \geq 0$.

Example 4.3.1.8. Let us consider the free shuffle algebra $T_{\text{Ш}}(\mathbb{1})$ from Example 4.3.1.5. The four different shuffle products defined for the shuffle monomial $321 \in T_{\text{Ш}}(\mathbb{1})(3)$ and the shuffle monomial $1 \in T_{\text{Ш}}(\mathbb{1})(1)$, in this order, are:

$$\begin{aligned}
\mu_{\{1,2,3\},\{4\}}(321, 1) &= 3214,\\
\mu_{\{1,2,4\},\{3\}}(321, 1) &= 4213,\\
\mu_{\{1,3,4\},\{2\}}(321, 1) &= 4312,\\
\mu_{\{2,3,4\},\{1\}}(321, 1) &= 4321.
\end{aligned}$$

One of the six different shuffle products of the shuffle monomial $12 \in T_{\text{Ш}}(\mathbb{1})(2)$ with the shuffle monomial $21 \in T_{\text{Ш}}(\mathbb{1})(2)$ is

$$\mu_{\{1,3\},\{2,4\}}(12, 21) = 1342.$$

We leave it to the reader as an exercise (Exercise 4.3) to compute the remaining five shuffle products of these elements.

4.3.2 Presentation by generators and relations

The analogue of First Homomorphism Theorem holds for shuffle algebras, and we may utilise it to define presentations of shuffle algebras. Suppose that a shuffle algebra $\mathcal{A}$ is generated by a collection of elements $\alpha_i \in \mathcal{A}(n_i)$. In that case, we can consider the collection $\mathcal{X}$ of operations $\kappa_i \in \mathcal{X}(n_i)$, one operation for each generator of $\mathcal{A}$. There is a surjective homomorphism from $T_{\text{Ш}}(\mathcal{X})$ onto $\mathcal{A}$ sending κ_i to α_i which is uniquely defined by the universal property of the free shuffle algebra. By the First Homomorphism Theorem, that homomorphism is the canonical map onto the quotient of $T_{\text{Ш}}(\mathcal{X})$ by some ideal $\mathcal{I}$.

Definition 4.3.2.1 (Ideal generated by a subset)**.** Let $\mathcal{A}$ be a shuffle algebra, and suppose that $\mathcal{S} \subset \mathcal{A}$ is a nonsymmetric subcollection. The *ideal of* $\mathcal{A}$ *generated by* $\mathcal{S}$, denoted by $(\mathcal{S})$, is the smallest (by inclusion) ideal of $\mathcal{A}$ containing $\mathcal{S}$.

Definition 4.3.2.2 (Presentation by generators and relations)**.** Suppose that the shuffle algebra $\mathcal{P}$ is a quotient of the free shuffle algebra $T_{\text{Ш}}(\mathcal{A})$ by some ideal $\mathcal{I}$, and that the ideal $\mathcal{I}$ is generated by the collection $\mathcal{S}$. In this case, we will say that the shuffle algebra $\mathcal{A}$ is *presented by generators $\mathcal{X}$ and relations $\mathcal{S}$.*

4.3.3 Twisted associative algebras as shuffle algebras

As we mentioned before, our main reason to deal with shuffle algebras is that they allow us to solve the problem of finding normal forms in twisted associative algebras presented by generators and relations. Let us explain why this is the case.

Definition 4.3.3.1 (Forgetful functor)**.** To each symmetric collection $\mathcal{P}$ we can associate a nonsymmetric collection $\mathcal{P}^f$; it is the same collection of vector spaces but without symmetric group actions. As we already mentioned earlier, there is no real difference between $\underline{\mathbb{F}}^f$ and $\underline{\mathbb{F}}$, nor between $\mathbb{1}^f$ and $\mathbb{1}$, since the symmetric groups S_n are trivial for $n < 2$; thus in those cases forgetting about the symmetries makes absolutely no difference, and we will suppress the subscript ^{f}. The assignment $\mathcal{P} \mapsto \mathcal{P}^f$ will be sometimes referred to as the *forgetful functor* from the category of symmetric collections to the category of nonsymmetric ones.

It turns out that the shuffle tensor product is precisely the kind of operation one needs to ignore symmetries of symmetric collections without losing information about their tensor products. More precisely, "the forgetful functor is monoidal", as the following result shows.

Proposition 4.3.3.2. *Let $\mathcal{V}$ and $\mathcal{W}$ be two symmetric collections. Then we have*

$$(\mathcal{V} \otimes \mathcal{W})^f \cong \mathcal{V}^f \boxtimes \mathcal{W}^f.$$

Proof. Let us examine the n-th component for both sides. By the formula for the tensor product of two symmetric collections,

$$(\mathcal{V} \otimes \mathcal{W})(n) = \bigoplus_{n_1+n_2=n} \operatorname{Ind}_{S_{n_1}\times S_{n_2}}^{S_{n_1+n_2}} (\mathcal{V}(n_1) \otimes \mathcal{W}(n_2)).$$

By Proposition 4.2.1.6, the latter is naturally identified with

$$\bigoplus_{I_1 \sqcup I_2 = \{1,\ldots,n\}} \mathcal{V}(|I_1|) \otimes \mathcal{W}(|I_2|).$$

Meanwhile, the formula for the shuffle tensor product gives

$$(\mathcal{V}^f \boxtimes \mathcal{W}^f)(n) := \bigoplus_{I_1 \sqcup I_2 = \{1,\ldots,n\}} \mathcal{V}^f(|I_1|) \otimes \mathcal{W}^f(|I_2|),$$

which is precisely the former formula without the symmetric group actions. □

The following corollary is, in some sense, the central result of this chapter. It shows that any twisted associative algebra, when studied as a shuffle algebra, needs the same number of generators and relations to be defined. Thus, any approach to normal forms for shuffle algebras leads to normal forms for twisted associative algebras as well.

Corollary 4.3.3.3. *Let $\mathcal{M}$ be a symmetric collection. Then we have an isomorphism of shuffle algebras*

$$T_{\text{Ш}}(\mathcal{M}^f) \cong (T_\Sigma(\mathcal{M}))^f.$$

Moreover, if $\mathcal{I} \subset T_\Sigma(\mathcal{M})$ is an ideal, then, under the identification that we made, $\mathcal{I}^f$ is an ideal of $T_{\text{Ш}}(\mathcal{M}^f)$, and

$$T_{\text{Ш}}(\mathcal{M}^f)/\mathcal{I}^f \cong (T_\Sigma(\mathcal{M})/\mathcal{I})^f.$$

Proof. All the notions in question, that is free twisted associative algebras, shuffle algebras, and ideals in those algebras, are defined using tensor products, so Proposition 4.3.3.2 applies. □

Example 4.3.3.4. We consider the free shuffle algebra $T_\Sigma(\mathbb{1})^f \cong T_{\text{Ш}}(\mathbb{1})$ from Example 4.3.1.5, and the ideal generated by the element $r' = 21$ in its second component $T_{\text{Ш}}(\mathbb{1})(2)$ (this ideal is not an ideal of the form $\mathcal{I}^f$). This ideal is the span of all elements obtained from r' by iterations of shuffle products μ_{I_1,I_2}. Such elements can be easily seen to be all elements of the form

$$i_1 i_2 \cdots i_k i_{k+1} \cdots i_n,$$

with $i_k > i_{k+1}$ for some k. Therefore, all components of the quotient shuffle algebra are one-dimensional spanned by $\{1, \ldots, n\}$. As a nonsymmetric collection, this is the same as the tensor algebra $T(x)$ viewed as a shuffle algebra according to Example 4.2.1.2, and hints that the problem we exhibited in Proposition 4.2.2.4 is naturally fixed in the context of shuffle algebras.

4.4 Normal forms

4.4.1 Monomial orders

Let us generalize the definition of a monomial order to the case of shuffle monomials.

Definition 4.4.1.1 (Monomial order)**.** A collection of total orders Ξ_n of $\text{Ш}_{\mathcal{X}}(n)$, $n \geq 0$, is said to be a *monomial order* if the following two conditions are satisfied:

- each Ξ_n is a well-order;
- each shuffle product is a strictly increasing function in each of its arguments; that is, for all $T_1, T_1' \in Ш_{\mathcal{X}}(n_1)$, $T_2, T_2' \in Ш_{\mathcal{X}}(n_2)$, and all partitions $\{1, \ldots, n_1 + n_2\} = I_1 \sqcup I_2$, $|I_1| = n_1$, $|I_2| = n_2$, we have

$$\mu_{I_1,I_2}(T_1, T_2) \prec \mu_{I_1,I_2}(T_1', T_2) \text{ if } T_1 \prec T_1',$$
$$\mu_{I_1,I_2}(T_1, T_2) \prec \mu_{I_1,I_2}(T_1, T_2') \text{ if } T_2 \prec T_2'.$$

Unless otherwise specified, throughout this chapter, we will give definitions as well as state and prove all theoretical results for an arbitrary monomial order Ξ.

We will now outline one construction of monomial orders in free shuffle algebras. We denote $X := \bigsqcup_{n\geq 0} \mathcal{X}(n)$. For the purpose of the following definition, let us establish the following convention. We will encode k-element subsets of $\{1, \ldots, n\}$ by k-tuples of integers, listing elements of a subset in the increasing order. Once that is done, we can compare those sequences using the graded lexicographic order, thus obtaining a total order on all finite subsets of the set of natural numbers, which actually is even a well-order.

Definition 4.4.1.2 (Partition extension of a monomial order)**.** Suppose that Ξ is a monomial order on X^*. The *partition extension of* Ξ is defined as follows. Let $T_1 = (\pi_1, \mathsf{m}_1)$, where π_1 is a set partition $\{1, \ldots, n_1\} = \bigsqcup_{j=1}^{k_1} I_1^{(j)}$, and $\mathsf{m}_1 = \mathsf{m}_1^{(1)} \otimes \mathsf{m}_1^{(2)} \otimes \cdots \otimes \mathsf{m}_1^{(k_1)}$, and $T_2 = (\pi_2, \mathsf{m}_2)$, where π_2 is a set partition $\{1, \ldots, n_2\} = \bigsqcup_{j=1}^{k_2} I_2^{(j)}$, and $\mathsf{m}_2 = \mathsf{m}_2^{(1)} \otimes \mathsf{m}_2^{(2)} \otimes \cdots \otimes \mathsf{m}_2^{(k_2)}$, be two shuffle monomials. We say that $T_1 \prec T_2$ if and only if

- $n_1 < n_2$, or
- $n_1 = n_2$ and $k_1 < k_2$, or
- $n_1 = n_2$, $k_1 = k_2$, and for the first j for which $I_1^{(j)} \neq I_2^{(j)}$ we have $I_1^{(j)} \prec I_2^{(j)}$, or
- $n_1 = n_2$, $k_1 = k_2$, $\pi_1 = \pi_2$, and $\mathsf{m}_1 \prec \mathsf{m}_2$.

Proposition 4.4.1.3. *The partition extension of any monomial order Ξ, viewed as an order of shuffle monomials, is a monomial order.*

Proof. Since this order is a superposition of several graded lexicographic orders and the order Ξ that is assumed to be a total well-order, both the total order property and the well-order property follow. Finally, each shuffle product μ_{I_1,I_2} is strictly increasing in each of its arguments because of the way that product is defined: it uses an order-preserving bijection between I_k and $\{1, \ldots, n_k\}$, and hence does not alter the result of comparison for partitions. For the comparison on the level of words, the order is not altered since Ξ is a monomial order. □

Definition 4.4.1.4 (Graded partition lexicographic order)**.** Let us fix some order Ξ of $X := \bigsqcup_{n\geq 0} \mathcal{X}(n)$. The *graded partition lexicographic order* of shuffle monomials, denoted `gpartlex`, is the partition extension of the `glex` order induced by Ξ.

4.4.2 Long division

In the case of both associative algebras and nonsymmetric operads, it was crucial to have two views of divisibility of monomials, both in terms of structure operations of an algebra and a combinatorial one. Let us give a combinatorial definition of divisibility for shuffle monomials.

Definition 4.4.2.1 (Divisibility of shuffle monomials)**.** A shuffle monomial $T_1 = (\pi_1, \mathsf{m}_1)$, where π_1 is a partition $\{1, \ldots, n_1\} = \bigsqcup_{j=1}^{k_1} I_1^{(j)}$, and $\mathsf{m}_1 = \mathsf{m}_1^{(1)} \otimes \mathsf{m}_1^{(2)} \otimes \cdots \otimes \mathsf{m}_1^{(k_1)}$, is *divisible* by a (nontrivial) shuffle monomial $T_2 = (\pi_2, \mathsf{m}_2)$, where π_2 is a partition $\{1, \ldots, n_2\} = \bigsqcup_{j=1}^{k_2} I_2^{(j)}$, and $\mathsf{m}_2 = \mathsf{m}_2^{(1)} \otimes \mathsf{m}_2^{(2)} \otimes \cdots \otimes \mathsf{m}_2^{(k_2)}$, if there exists an integer p satisfying $1 \leq p \leq p + k_2 - 1 \leq k_1$ for which a unique order preserving bijection

$$\sigma\colon \bigsqcup_{j=p}^{p+k_1-1} I_1^{(j)} \cong \{1, \ldots, n_2\}$$

induces the partition π_2, and

$$\mathsf{m}_1^{(p)} \otimes \mathsf{m}_1^{(p+1)} \otimes \cdots \otimes \mathsf{m}_1^{(p+k_1-1)} = \mathsf{m}_2^{(1)} \otimes \mathsf{m}_2^{(2)} \otimes \cdots \otimes \mathsf{m}_2^{(k_2)}.$$

Example 4.4.2.2. Consider the element $4312 \in T_{\text{Ш}}(\mathbb{1})(4)$. It has two different divisors of weight 3, 321, and 312. The first of them occurs in the beginning, since the relative order of entries in 431 is the same as in 321, and the second one occurs in the end. In comparison, the two divisors of length 3 of the monomial 4321 both are occurrences of the monomial 321 as a divisor.

Proposition 4.4.2.3. *Let $T_1 = (\tau_1, \mathsf{x}_1)$ and $T_2 = (\tau_2, \mathsf{x}_2)$ be two shuffle monomials. Then T_1 is divisible by T_2 if and only if it can be obtained from T_2 by iterated shuffle products with elements of $T_{\text{Ш}}(\mathcal{X})$.*

Proof. Exercise 4.4. □

Definition 4.4.2.4 (Insertion into a shuffle monomial)**.** Suppose that T_1 and T_2 are shuffle monomials, and T_1 is divisible by T_2. In this case, there is an *insertion* operation

$$\square_{T_1,T_2}\colon T_{\text{Ш}}(\mathcal{X})(\operatorname{ar}(S_2)) \to T_{\text{Ш}}(\mathcal{X})(\operatorname{ar}(S_1)).$$

If $T = (\pi, \mathsf{m})$ is a shuffle monomial of the same arity n_2 as T_2, the insertion operation replaces the part $\bigsqcup_{j=p}^{p+k_1-1} I_1^{(j)}$ of π_1 by $\tilde{\pi}$, the partition obtained from π by the bijection σ^{-1}, and also replaces the subword $\mathsf{m}_1^{(p)} \otimes \mathsf{m}_1^{(p+1)} \otimes \cdots \otimes \mathsf{m}_1^{(p+k_1-1)}$ of m_1 by m. Then, this operation is extended by linearity to all shuffle polynomials of the same arity.

Remark 4.4.2.5. Our notation is not completely precise, since there may be several different divisors T_2 inside T_1. We always assume that the operation $\square_{T_1,T_2}$ inserts everything at a particular occurrence of T_2 inside T_1 which is implicit.

Example 4.4.2.6. Consider the shuffle monomial $T = 4321 \in T_{\text{Ш}}(\mathbb{1})$ from Example 4.4.2.2. This monomial has two occurrences of 321 as a divisor; let us denote the one in the beginning by T_1, and the one in the end by T_2. We have

$$\square_{T,T_1}(213) = 3241 \quad \text{and} \quad \square_{T,T_2}(213) = 4213.$$

One very useful feature of the insertion operations is that they allow us to give an explicit description of an ideal generated by a given collection $\mathcal{S}$ in the free shuffle algebra which is a suitable replacement of the description "the ideal (S) is the linear span of all elements $r_1 s r_2$ for all $r_1, r_2 \in T(X)$, $s \in S$" which we had in the associative case. While in the case of shuffle algebras it is possible to furnish a more elementary description, we stick to the formalism of insertions because of its general applicability.

Proposition 4.4.2.7. *Let $\mathcal{S} \subset T_{\text{Ш}}(\mathcal{X})$. The ideal $(\mathcal{S})$ generated by $\mathcal{S}$ can be described explicitly as the linear span of all insertions $\square_{T_1,T_2}(f)$, where T_1 is a monomial, T_2 is a divisor of T_1, and $f \in \mathcal{S}(\operatorname{ar}(T_2))$.*

Proof. The ideal $(\mathcal{S})$ is spanned by iterated shuffle products where at least one of the elements involved belongs to $\mathcal{S}$; by bilinearity of shuffle products, we may assume that all other elements are monomials, in which case the corresponding iterated product is the insertion operation. □

The following proposition is clear from the definition. It is an analogue of "monadic associativity" for operads from Proposition 3.4.2.11.

Proposition 4.4.2.8. *Let $T \in \text{Ш}_{\mathcal{X}}(n)$, $T_1, T_1' \in \text{Ш}_{\mathcal{X}}(n_1)$, $T_2 \in \text{Ш}_{\mathcal{X}}(n_2)$, and suppose that T_1 is a divisor of T and T_2 is a divisor of T_1'. Then*

$$\square_{T,T_1} \circ \square_{T_1',T_2} = \square_{\square_{T,T_1}(T_1'),T_2}. \tag{4.1}$$

In particular, if $T_1 = T_1'$, this simplifies to

$$\square_{T,T_1} \circ \square_{T_1,T_2} = \square_{T,T_2}. \tag{4.2}$$

Let us show that under the insertion operations, the leading monomials change in a controllable way.

Proposition 4.4.2.9. *Suppose that T_1 is a shuffle monomial, and T_2 is a divisor of T_1. Then for each $g \in T_{\text{Ш}}(\mathcal{X})(\mathrm{ar}(T_2))$, we have*

$$\mathrm{LM}(\Box_{T_1,T_2}(g)) = \Box_{T_1,T_2}(\mathrm{LM}(g)). \tag{4.3}$$

Proof. Let us first check that for any two nonzero elements

$$f_1 \in T_{\text{Ш}}(\mathcal{X})(n_1), \quad f_2 \in T_{\text{Ш}}(\mathcal{X})(n_2),$$

and all partitions

$$\{1, \dots, n_1 + n_2\} = I_1 \sqcup I_2, \quad |I_1| = n_1, \quad |I_2| = n_2,$$

we have

$$\mathrm{LM}(\mu_{I_1,I_2}(f_1, f_2)) = \mu_{I_1,I_2}(\mathrm{LM}(f_1), \mathrm{LM}(f_2)).$$

Since the product on $T_{\text{Ш}}(\mathcal{X})$ is bilinear, the element $\mu_{I_1,I_2}(f_1, f_2)$ is equal to a linear combination of elements $\mu_{I_1,I_2}(m_1, m_2)$, where $m_p \in \mathrm{supp}(f_p)$. It remains to notice that for each $m_p \neq \mathrm{LM}(f_p)$ we have $m_p \prec \mathrm{LM}(f_p)$, so the defining property of monomial orders implies that

$$\mu_{I_1,I_2}(m_1, m_2) \prec \mu_{I_1,I_2}(\mathrm{LM}(f_1), \mathrm{LM}(f_2)),$$

unless $m_1 = \mathrm{LM}(f_1)$, $m_2 = \mathrm{LM}(f_2)$. Now, the element $\Box_{T_1,T_2}(g)$ is obtained from g by an iteration of shuffle products, and the result follows. □

Definition 4.4.2.10 (Reduced monomials and polynomials)**.** Let $\mathcal{S}$ be a subset of $T_{\text{Ш}}(\mathcal{X})$. A shuffle monomial T is said to be *reduced with respect to $\mathcal{S}$* if $T \notin (\mathrm{LM}(\mathcal{S}))$; in other words, if T is not divisible by any of the leading monomials of elements of $\mathcal{S}$. In general, a shuffle polynomial f is said to be *reduced with respect to $\mathcal{S}$*, if it is equal to a linear combination of shuffle monomials which are reduced with respect to $\mathcal{S}$. A subset $\mathcal{S} \subset T_{\text{Ш}}(\mathcal{X})$ is said to be *self-reduced* if each element $T \in \mathcal{S}$ is monic and reduced with respect to $\mathcal{S} \setminus \{T\}$.

Definition 4.4.2.11 (Reduction)**.** Let $f, g \in T_{\text{Ш}}(\mathcal{X})$ be two nonzero elements. We say that f is *reducible with respect to g* if $\mathrm{LM}(f)$ is not reduced with respect to $\{g\}$, or, in plain words, if the leading monomial of f is divisible by the leading monomial of g, $\mathrm{LM}(f) = \Box_{T_1,T_2}(\mathrm{LM}(g))$ for some $T_1 \in \text{Ш}_{\mathcal{X}}(\mathrm{ar}(\mathrm{LM}(f)))$, $T_2 \in \text{Ш}_{\mathcal{X}}(\mathrm{ar}(\mathrm{LM}(g)))$. In that case, the *reduction of f with respect to g*, denoted by $r_g(f)$, is defined by the formula

$$r_g(f) = f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \Box_{T_1,T_2}(g).$$

Lemma 4.4.2.12. *For all elements $f, g \in T_{\text{Ш}}(\mathcal{X})$ such that $r_g(f)$ is defined, we have*

$$r_g(f) = 0 \quad \textit{or} \quad \mathrm{LM}(r_g(f)) \prec \mathrm{LM}(f).$$

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.2.15. □

One can view a reduction as one step of a version of the long division algorithm. We make it more precise as follows.

Algorithm 4.4.2.13 (Long division for shuffle algebras)**.**

Input: An element $f \in T_{\sha}(\mathcal{X})$, and a finite set $\mathcal{S} \subset T_{\sha}(\mathcal{X})$.

Output: An element $\tilde{f}$, reduced with respect to $\mathcal{S}$, for which $\textsc{lt}(\tilde{f}) \preceq \textsc{lt}(f)$ such that $f + (\mathcal{S}) = \tilde{f} + (\mathcal{S})$.

- If $f = 0$, return f.
- Replace $\mathcal{S}$ by its linear self-reduction (Proposition 1.2.1.6).
- If $\mathcal{D} := \{s \in \mathcal{S} \colon \textsc{lm}(f) \text{ is divisible by } \textsc{lm}(s)\} \neq \varnothing$, take $s_0 \in \mathcal{D}$ with the least leading monomial (such s_0 is unique since $\mathcal{S}$ is linearly self-reduced), and return the result of long division of $f' := r_s(f)$ by $\mathcal{S}$.
- Otherwise, $\textsc{lm}(f)$ is reduced with respect to $\mathcal{S}$, so let $\tilde{f}$ be the result of long division of $f' := f - \textsc{lt}(f)$ by $\mathcal{S}$; return $\textsc{lt}(f) + \tilde{f}$.

Lemma 4.4.2.14. *For every $f \in T_{\sha}(\mathcal{X})$, the long division algorithm terminates in a finite number of steps. Its output is an element $\tilde{f}$ reduced with respect to $\mathcal{S}$, for which $\textsc{lt}(\tilde{f}) \preceq \textsc{lt}(f)$ and $f + (\mathcal{S}) = \tilde{f} + (\mathcal{S})$.*

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.2.17. □

Remark 4.4.2.15. We see that in fact there is nothing particularly problematic if $\mathcal{S}$ is an infinite self-reduced set: it is clear from the proof of Lemma 4.4.2.14 that for the given $f \in T_{\sha}(\mathcal{X})$ the elements $s \in \mathcal{S}$ which we use at various steps of our computation have decreasing leading monomials, and so there can be only finitely many reductions performed; that is, for each f we never use more than a finite subset of $\mathcal{S}$. While for purposes of implementation this is not particularly important, it will be beneficial for theoretical results where $\mathcal{S}$ may be infinite.

We will now establish that the set of elements that are reduced with respect to $\mathcal{I}$ is a suitable candidate for the set of normal forms for the elements of the quotient $T_{\sha}(\mathcal{X})/\mathcal{I}$. This is an improvement of Lemma 1.2.1.3 which takes into account the extra structures we have on the underlying vector spaces.

Lemma 4.4.2.16. *Suppose that $\mathcal{I}$ is an ideal of $T_{\sha}(\mathcal{X})$. Monomials that are reduced with respect to $\mathcal{I}$ form a basis of the quotient $T_{\sha}(\mathcal{X})/\mathcal{I}$.*

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.2.19. □

It is possible to use long division to find, for each finite set, a finite self-reduced set that generates the same ideal.

Algorithm 4.4.2.17 (Self-reduction for shuffle algebras)**.**

Input: A finite subset $\mathcal{S} \subset T_{\text{Ш}}(\mathcal{X})$.

Output: A finite self-reduced subset $\mathcal{S}' \subset T_{\text{Ш}}(\mathcal{X})$ with $(\mathcal{S}) = (\mathcal{S}')$.

- Replace $\mathcal{S}$ by its linear self-reduction.
- If $\mathcal{S}$ is self-reduced, return $\mathcal{S}$.
- Let s be the element of $\mathcal{S}$ with the maximal leading monomial, and compute the self-reduction $\mathcal{S}'$ of $\mathcal{S} \setminus \{s\}$.
- Compute $\tilde{s}$, the result of long division of s by $\mathcal{S}'$.
- Compute the self-reduction of $\mathcal{S}' \cup \{\tilde{s}\}$.

We leave it as an exercise (Exercise 4.5) for the reader to check that for each finite $\mathcal{S}$ this algorithm terminates after finitely many steps.

4.4.3 Gröbner bases

In general, there are several different reduced forms one may obtain when doing reductions with respect to a set $\mathcal{S}$; however, there is a *canonical* form with respect to the ideal $(\mathcal{S})$, namely the corresponding normal form. In this section, we will explain how to fix this discrepancy.

Proposition 4.4.3.1. *Let $\mathcal{I}$ be an ideal of $T_{\text{Ш}}(\mathcal{X})$. The space of leading terms $\textsc{lt}(\mathcal{I})$ is an ideal of $T_{\text{Ш}}(\mathcal{X})$.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.4.3.1. □

We are now ready to define a Gröbner basis of an ideal.

Definition 4.4.3.2 (Gröbner basis)**.** Let $\mathcal{I}$ be an ideal of $T_{\text{Ш}}(\mathcal{X})$. We say that $\mathcal{G} = \{\mathcal{G}(n) \subset \mathcal{I}(n)\}$ is a *Gröbner basis* of $\mathcal{I}$ with respect to a given monomial order Ξ if the set of leading monomials $\textsc{lm}(\mathcal{G}) := \{\textsc{lm}(g) \colon g \in \mathcal{G}\}$ generates the leading term ideal of the ideal $\mathcal{I}$:

$$\textsc{lt}(\mathcal{I}) = (\textsc{lm}(\mathcal{G})).$$

A Gröbner basis which is a self-reduced subset of $T_{\text{Ш}}(\mathcal{X})$ is said to be *reduced*.

Lemma 4.4.3.3. *A Gröbner basis of an ideal $\mathcal{I} \subset T_{\text{Ш}}(\mathcal{X})$ generates $\mathcal{I}$.*

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.3.3. □

Proposition 4.4.3.4. *Let $\mathcal{I}$ be an ideal of $T_{Ш}(\mathcal{X})$. Then $\mathcal{G} \subset \mathcal{I}$ is a Gröbner basis if and only if the cosets of monomials that are reduced with respect to $\mathcal{G}$ form a basis of the quotient $T_{Ш}(\mathcal{X})/\mathcal{I}$.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.4.3.4. □

Corollary 4.4.3.5. *Suppose that $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I} \subset T_{Ш}(\mathcal{X})$. Then the result of long division of $f \in T_{Ш}(\mathcal{X})$ by $\mathcal{G}$ does not depend on either the choices or the order of the reductions performed.*

Proof. Same (*mutatis mutandis*) as the proof of Corollary 3.4.3.5. □

We summarize Proposition 4.4.3.4 and its corollary as follows.

Theorem 4.4.3.6.

(i) Let $\mathcal{I}$ be an ideal of $T_{Ш}(\mathcal{X})$. A subset $\mathcal{G} \subset \mathcal{I}$ is a Gröbner basis if and only if the normal forms modulo $\mathcal{I}$ are precisely the elements that are reduced with respect to $\mathcal{G}$.

(ii) Suppose that $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I} \subset T_{Ш}(\mathcal{X})$. Given an element $f \in \mathcal{I}$, its normal form modulo $\mathcal{I}$ can be computed using long division by $\mathcal{G}$. In fact, in this long division the order of reductions can be chosen arbitrarily.

Proposition 4.4.3.7. *Each ideal $\mathcal{I} \subset T_{Ш}(\mathcal{X})$ has a unique reduced Gröbner basis.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.4.3.7. □

4.5 Computing Gröbner bases

In this section, we will explain how to compute Gröbner bases for ideals of $T_{Ш}(\mathcal{X})$. As in Chapter 2, some ideals have infinite Gröbner bases, so the word "algorithm" below should be taken with a grain of salt.

4.5.1 Diamond lemma

Definition 4.5.1.1 (S-polynomial)**.** Let $g_1, g_2 \in T_{Ш}(\mathcal{X})$ be two monic polynomials. We say that the shuffle monomials $T_1 := \text{LM}(g_1)$ and $T_2 := \text{LM}(g_2)$ *form an overlap* if there exist nonempty shuffle monomials T_1' and T_2' for which $\mu_{I_1,I_2}(T_1, T_1') = \mu_{J_1,J_2}(T_2', T_2)$, and T_2 is not a divisor of T_1'. In this case, we consider the corresponding *small common multiple* $T := \mu_{I_1,I_2}(T_1, T_1') = \mu_{J_1,J_2}(T_2', T_2)$, and call the element

$$S_T(g_1, g_2) := \square_{T,T_1}(g_1) - \square_{T,T_2}(g_2)$$

an *S-polynomial* of g_1 and g_2; the common term cancels, since both g_1 and g_2 are monic.

Example 4.5.1.2. Consider the shuffle monomial $321 \in T_{\text{Ш}}(\mathbb{1})(3)$. This monomial forms two different overlaps with itself: we have

$$4321 = \mu_{\{2,3,4\},\{1\}}(321, 1) = \mu_{\{4\},\{1,2,3\}}(1, 321)$$

and

$$54321 = \mu_{\{3,4,5\},\{1,2\}}(321, 21) = \mu_{\{4,5\},\{1,2,3\}}(21, 321).$$

In this case, there is one small common multiple of weight 4, and one small common multiple of weight 5. However, the situation might be very different, as the shuffle monomial $312 \in T_{\text{Ш}}(\mathbb{1})(3)$ demonstrates. This monomial does not have an overlap of weight 4 with itself: if the permutation $abcd$ is a small common multiple of weight 4, then $b < c < a$ and $c < d < b$, so we have $b < c$ and $c < b$, a contradiction. At the same time, there are three different small common multiples of weight 5, namely 51423, 52413, and 53412.

We will now prove the result which is at the core of most feasible ways to check that some subset of an ideal is a Gröbner basis.

Definition 4.5.1.3 (Parameter of a representation)**.** Let $\mathcal{I} = (\mathcal{G})$ be an ideal of $T_{\text{Ш}}(\mathcal{X})$. Consider the representation of an element $f \in \mathcal{I}$ as a combination of insertions of $g_1, \ldots, g_N \in \mathcal{G}$:

$$f = \sum_{i=1}^{N} c_i \Box_{\tilde{T}_i, T_i}(g_i), \tag{4.4}$$

where $T_i = \text{LM}(g_i)$. We call $\max(\tilde{T}_i)$ the *parameter* of this linear combination.

If $f = S_T(g_1, g_2)$ is the S-polynomial of $g_1, g_2 \in \mathcal{G}$ (with all the notation as above in Definition 4.5.1.1), then it has an obvious representation

$$f = \Box_{T,T_1}(g_1) - \Box_{T,T_2}(g_2),$$

with parameter T. We call a representation of that S-polynomial *nontrivial* if its parameter is smaller than T.

Theorem 4.5.1.4 (Diamond lemma)**.** *Let $\mathcal{G} \subset T_{\text{Ш}}(\mathcal{X})$ be self-reduced, and let $\mathcal{I} = (\mathcal{G})$. The following statements are equivalent:*

(i) *$\mathcal{G}$ is a Gröbner basis of $\mathcal{I}$.*

(ii) *Every S-polynomial $S_T(g_1, g_2)$ has reduced form* 0 *with respect to $\mathcal{G}$.*

(iii) *Every S-polynomial $S_T(g_1, g_2)$ admits a nontrivial representation of the form* (4.4)*.*

(iv) *Every element $f \in \mathcal{I}$ admits a representation of the form* (4.4) *with parameter* $\text{LM}(f)$*.*

Proof. Same (*mutatis mutandis*) as the proof of Theorem 3.5.1.6. □

4.5.2 The Buchberger algorithm

Theorem 4.5.1.4 leads naturally to a recipe for computing reduced Gröbner bases: given a set of generators of an ideal, one has to compute all pairwise S-polynomials, adjoin all reduced forms of those to the set of generators, and repeat the same.

Algorithm 4.5.2.1 (Buchberger algorithm for shuffle algebras)**.**

```
    Input: A finite subset $\mathcal{G} \subset T_{\text{Ш}}(\mathcal{X})$ generating an ideal $\mathcal{I} \subset T_{\text{Ш}}(\mathcal{X})$.

    Output: If terminates, the output is the reduced Gröbner basis of $\mathcal{I}$.

• Set newSpolynomials $\leftarrow$ true.
• While newSpolynomials do:
    – Sort $\mathcal{G}$ by gpartlex order of leading monomials:
      $\mathcal{G} = \{g_1, \dots, g_n\}$.
    – Compute the self-reduction of $\mathcal{G}$.
    – Set Spolynomials $\leftarrow \varnothing$.
    – Set newSpolynomials $\leftarrow$ false.
    – For $g_1 \in \mathcal{G}$ do for $g_2 \in \mathcal{G}$ do:
        ∗ If $\text{LM}(g_1)$ and $\text{LM}(g_2)$ form an overlap then:
            1. Compute the S-polynomial $S_T(g_1, g_2)$.
            2. Let $t$ be the result of long division of $S_T(g_1, g_2)$ by $\mathcal{G}$.
            3. If $t \neq 0$ and $t \notin$ Spolynomials then
                ∗ Set newSpolynomials $\leftarrow$ true.
                ∗ Set Spolynomials $\leftarrow$ Spolynomials $\cup \{t\}$.
    – Set $\mathcal{G} \leftarrow \mathcal{G} \cup$ Spolynomials.
• Return $\mathcal{G}$.
```

Proposition 4.5.2.2. *If Algorithm 4.5.2.1 terminates then its output is the reduced Gröbner basis of $\mathcal{I}$.*

Proof. Immediate corollary to Theorem 4.5.1.4. □

4.5.3 Triangle lemma

Definition 4.5.3.1 (Essential overlap)**.** Let $\mathcal{G}$ be a self-reduced subset of $T_{\text{Ш}}(\mathcal{X})$, and let $g_1, g_2 \in \mathcal{G}$ be two elements for which $\text{LM}(g_1)$ and $\text{LM}(g_2)$ form an overlap. We call this overlap *essential* if $\text{LM}(g_1)$ and $\text{LM}(g_2)$ are the only two divisors from $\text{LM}(\mathcal{G})$ of the corresponding small common multiple.

Proposition 4.5.3.2 (Triangle lemma for shuffle algebras)**.** *Let $\mathcal{G}$ be a self-reduced subset of $T_{Ш}(\mathcal{X})$, and let $g_1, g_2 \in \mathcal{G}$ be two elements for which $\text{LM}(g_1)$ and $\text{LM}(g_2)$ form an overlap. Suppose that this overlap is not essential, so that there exists $g_3 \in G$ for which $\text{LM}(g_3)$ is another divisor of the corresponding small common multiple T. Then:*

- *The divisors $\text{LM}(g_1)$ and $\text{LM}(g_3)$ of T form an overlap, and the divisors $\text{LM}(g_3)$ and $\text{LM}(g_2)$ of T also form an overlap.*
- *If the S-polynomials $S_{T'}(g_1, g_3)$ and $S_{T''}(g_3, g_2)$ for the corresponding overlaps admit nontrivial representations of the form* (4.4)*, then the S-polynomial $S_T(g_1, g_2)$ also admits a nontrivial representation of that form.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.5.3.2. □

Remarkably, the technical issues that we observed in the case of nonsymmetric operads do not arise for shuffle algebras, and Corollary 2.4.3.3 can be adapted for shuffle algebras in its full generality, giving the following result that often simplifies computations quite drastically.

Corollary 4.5.3.3. *Let $\mathcal{G}$ be a self-reduced set of elements of $T_{Ш}(\mathcal{X})$.*

(i) If each S-polynomial of two elements of $\mathcal{G}$ corresponding to an essential overlap has reduced form 0 *with respect to $\mathcal{G}$, then $\mathcal{G}$ is the reduced Gröbner basis of* $(\mathcal{G})$*.*

(ii) While computing the reduced Gröbner basis using Algorithm 4.5.2.1, we may ignore all non-essential overlaps.

Example 4.5.3.4. Let $q \in \mathbb{F}$, and consider the element

$$R_q = 321 + q\,312 + q\,231 + q^2\,213 + q^2\,132 + q^3\,123$$

in $T_{Ш}(\mathbb{1})(3)$. It turns out that for the `gpartlex` order the element R_q forms a Gröbner basis of the ideal it generates (Exercise 4.7).

As we know from Example 4.5.1.2, in principle there are two small common multiples of the leading term 321 of R_q with itself: 4321 and 54321. However, the second one is non-essential, so we only have to deal with the first one. This observation simplifies the Gröbner basis verification most drastically (without it, one needs to compute and reduce the second S-polynomial, which is an element of a 120-dimensional space).

4.6 Examples of shuffle algebras and their applications

4.6.1 Shuffle algebras and patterns in permutations

In the case of associative algebras, monomials that are reduced with respect to a given set are precisely monomials whose divisors do not occur on the given list of words. (Those would be “obscene” words for real-life applications.) In the case of shuffle algebras, the notion of divisibility is a bit more complex. However, it turns out that in the particular case of the free shuffle algebra $T_{Ш}(\mathbb{1})$ the notion of divisibility of monomials arises naturally in the theory of consecutive permutation patterns [88, 149, 243].

Definition 4.6.1.1 (Consecutive patterns in permutations)**.** To every sequence s of length k consisting of k distinct numbers, we associate a (unique) permutation $\mathrm{st}(s) \in S_k$ called the *standardization* of s; it satisfies the constraints $\mathrm{st}(s)_i < \mathrm{st}(s)_j$ if and only if $s_i < s_j$. For example, $\mathrm{st}(153) = 132$. In other words, $\mathrm{st}(s)$ is the permutation whose relative order of entries is the same as that of s. We say that a permutation $\sigma \in S_n$ *contains the given permutation $\tau \in S_k$ as a consecutive pattern* if there exists $i \leq n - k + 1$ for which

$$\mathrm{st}(\sigma_i\sigma_{i+1}\ldots\sigma_{i+k-1}) = \tau;$$

otherwise we say that σ *avoids τ as a consecutive pattern.*

The relationship between consecutive patterns in permutations and divisibility of monomials in $T_{Ш}(\mathbb{1})$ is summarized by the following result.

Theorem 4.6.1.2 ([76])**.**

(i) *A permutation $\sigma \in S_n$ contains the given permutation $\tau \in S_k$ as a consecutive pattern if and only if σ, viewed as a shuffle monomial from $T_{Ш}(\mathbb{1})$, is divisible by τ.*

(ii) *For every set P of permutation patterns, let us define the shuffle algebra $\mathcal{A}^P$ as the quotient of the algebra $T_{Ш}(\mathbb{1})$ by the ideal generated by all patterns from P. Then the cosets of permutations avoiding all patterns from P form a basis of $\mathcal{A}^P$.*

Proof. Since the products in $T_{Ш}(\mathbb{1})$ are essentially defined via concatenations, it is clear that the ideal generated by P is spanned by permutations containing patterns from P, so the first part of the theorem is clear. The second part is an immediate corollary to the first one. □

4.6.2 Antisymmetrizer shuffle algebras

Example 4.6.2.1. Let V be a finite-dimensional vector space. Let us consider the associative algebra

$$A_k(V) := T(V)/(\Lambda^k(V)),$$

that is the algebra whose relations are all antisymmetrized k-fold products of elements of V. This algebra is called the *k-th antisymmetrizer algebra*. It is one of the first examples of k-Koszul algebras [19]. This algebra depends on V in a functorial way, and by Schur–Weyl duality [97] it corresponds to a symmetric collection $\mathcal{A}_k = \{\mathcal{A}_k(n)\}_{n\geq 0}$, so that

$$A_k(V) = \bigoplus_{n\geq 0} \mathcal{A}_k(n) \otimes_{\mathbb{F}S_n} V^{\otimes n}.$$

It turns out that $\mathcal{A}_k$ has a natural structure of a twisted associative algebra; the kernel of the natural map from $T_\Sigma(\mathbb{1})$ to $\mathcal{A}_k$ coming from Schur–Weyl duality is an ideal, so the twisted associative algebra structure descends to $\mathcal{A}_k$. Moreover, it is very easy to describe the ideal of relations of $\mathcal{A}_k$ precisely: it is generated by a single element

$$R_k = \sum_{\sigma\in S_k} (-1)^\sigma \sigma.$$

To apply our methods, we may consider the corresponding shuffle algebra $\mathcal{A}_k^f$. It is a quotient of the free shuffle algebra $T_{\text{Ш}}(\mathbb{1})$ by the ideal generated by the same element R_k viewed now as an element of $T_{\text{Ш}}(\mathbb{1})(k)$. It is possible to check that this element forms a Gröbner basis of the corresponding ideal for the `gpartlex` order; we leave it as a (not very easy) exercise for the reader (Exercise 4.9). It turns out that one can convert normal forms for $\mathcal{A}_k$ into normal forms for $A_k(V)$, thus solving the problem for all vector spaces at once.

4.6.3 Twisted commutative algebras and shuffle algebras

An important class of twisted associative algebras is given by their commutative versions; those algebras have recently been prominently featured in stable representation theory [225, 222, 223, 224, 239]. They appear to share some properties with classical commutative algebras, although their Noetherianity in general remains an important open problem which is only resolved in particular cases; see, e.g., [203].

Recall from the introduction to this chapter the notation $\sigma_{k,n-k}$ for the permutation of $1,\ldots,n$ that swaps the clusters $1,\ldots,k$ and $k+1,\ldots,n$, putting the integers between 1 and n in the order $k+1,\ldots,n,1,\ldots,k$.

Definition 4.6.3.1 (Twisted commutative algebra)**.** A *twisted commutative algebra $\mathcal{A}$* is a twisted associative algebra for which we have

$$\mu(a_2,a_1) = \mu(a_1,a_2).\sigma_{k,n-k}$$

whenever $k\geq 0$, $a_1\in\mathcal{A}(k)$, $a_2\in\mathcal{A}(n-k)$.

Of course, this notion admits a counterpart in the universe of shuffle algebras.

Definition 4.6.3.2 (Commutative shuffle algebra)**.** A shuffle algebra $\mathcal{A}$ for which

$$\mu_{I_1,I_2}(a_1,a_2) = \mu_{I_2,I_1}(a_2,a_1)$$

whenever $\{1,\ldots,n\} = I_1 \sqcup I_2$, $a_1 \in \mathcal{A}(|I_1|)$, $a_2 \in \mathcal{A}(|I_2|)$, is said to be *commutative*.

The most important example of a twisted commutative algebra is the tensor algebra of a vector space.

Proposition 4.6.3.3. *The tensor algebra $T(V)$ with its shuffle algebra structure is commutative. In fact, it is free as a commutative shuffle algebra.*

Proof. The first statement is trivially true; it is essentially explained in the introduction to this chapter. The second statement is left as an exercise for the reader (Exercise 4.10). □

We expect that methods explained in this book can be beneficial for dealing with twisted commutative algebras. They are related to "Gröbner methods" of [222], but provide a somewhat different angle, where the primary focus comes from a wider noncommutative setup.

Let us conclude this section by outlining a very promising direction of research of twisted commutative algebras in the context of representation theory that has not received enough attention so far.

Definition 4.6.3.4 (Algebra of tensor invariants)**.** Suppose that $V = \mathfrak{g}$ is a Lie algebra. Then, since the adjoint $\mathfrak{g}$-action on tensor powers commutes with the action of symmetric groups, the $\mathfrak{g}$-invariants in tensor powers form a symmetric subcollection of $T(V)$, which moreover is a twisted associative subalgebra. We call that subalgebra the *tensor invariant algebra* of $\mathfrak{g}$.

As an associative algebra, the tensor invariant algebra is usually quite far from being finitely generated. However, in a range of examples (explored in unpublished work of the second author and J. Griffin), it is finitely generated as a twisted associative algebra, or equivalently as a shuffle algebra. It would be interesting to obtain an explicit presentation of that algebra by generators and relations, and we believe that methods of this paper can be used for that purpose. Some related questions are discussed in Exercise 4.11.

4.7 Exercises

Exercise 4.1. Complete the proof of Proposition 4.2.1.6.

Exercise 4.2. Prove that our two definitions of twisted associative algebras are indeed equivalent.

Exercise 4.3. Compute the six different shuffle products of the shuffle monomial $12 \in T_{Ш}(\mathbb{1})(2)$ with the shuffle monomial $21 \in T_{Ш}(\mathbb{1})(2)$, completing the computation started in Example 4.3.1.8.

Exercise 4.4. Prove Proposition 4.4.2.3.

Exercise 4.5. Show that for each finite $\mathcal{S} \subset T_{Ш}(\mathcal{X})$ Algorithm 4.4.2.17 terminates after finitely many steps.

Exercise 4.6. Use Equation (4.1) and Proposition 4.4.2.9 to fill in the details of the proof of Theorem 4.5.1.4.

Exercise 4.7.

(i) Consider the element

$$R = 321 + c_1\, 312 + c_2\, 231 + c_3\, 213 + c_4\, 132 + c_5\, 123$$

in $T_{Ш}(\mathbb{1})(3)$. Show that the element R forms a Gröbner basis of the ideal (R) for the `gpartlex` order if and only if there exists $q \in \mathbb{F}$ for which $c_1 = c_2 = q$, $c_3 = c_4 = q^2$, and $c_5 = q^3$.

(ii) Try to generalize the result of (i) to the case of an element $R \in T_{Ш}(\mathbb{1})(4)$ for which $\text{LT}(R) = 4321$, and to the case of any $n \geq 3$.

Exercise 4.8. Generalize the approach of Section 4.6.1 to include more general free shuffle algebras. As a starting point, consider the free shuffle algebra with one generator of each arity $n \geq 1$. Divisibility of monomials in this algebra leads to a somewhat natural notion of "consecutive patterns in surjective maps".

Exercise 4.9.

(i) Prove the claim made in Example 4.6.2.1 that the defining relation

$$R_k = \sum_{\sigma \in S_k} (-1)^{\sigma} \sigma.$$

of the shuffle algebra $\mathcal{A}_k^f$ forms a Gröbner basis of its ideal of relations.

(ii) Consider the algebra

$$B_k(V) := T(V)/(S^k(V)),$$

the quotient of the tensor algebra by the ideal generated by all *symmetrized* k-fold products. Explain why, even though this algebra depends on V functorially, converting normal forms for the corresponding shuffle algebra $\mathcal{B}_k^f$ into normal forms for $B_k(V)$ is much harder than it was for $A_k(V)$ in Example 4.6.2.1.

Exercise 4.10.

(i) Explain why the quotient of $T_{\text{Ш}}(\mathcal{X})$ by the ideal generated by $\mu_{I_1,I_2}(x_1,x_2) = \mu_{I_2,I_1}(x_2,x_1)$ for all $x_1 \in \mathcal{X}(|I_1|)$, $x_2 \in \mathcal{X}(|I_2|)$ is the free commutative shuffle algebra generated by $\mathcal{X}$.

(ii) Pick a monomial order of shuffle monomials, and compute the reduced Gröbner basis for the defining relations of the free commutative shuffle algebra.

(iii) Show that the tensor algebra of V with its shuffle algebra structure is the free commutative shuffle algebra generated by the collection $\mathbb{1} \otimes V$ for which

$$(\mathbb{1} \otimes V)(n) = \begin{cases} V, & n = 1, \\ 0, & n \neq 1. \end{cases}$$

Exercise 4.11. In this exercise, we assume $\mathbb{F} = \mathbb{Q}$.

(i) Consider the collection of tensor invariants of the Lie algebra $\mathfrak{sl}_2$ (Exercise 2.11); this collection has components

$$\left((\mathfrak{sl}_2)^{\otimes n}\right)^{\mathfrak{sl}_2};$$

it is a particular case of the general construction of the algebra of tensor invariants (Definition 4.6.3.4). Prove that as a twisted associative algebra it is generated by two elements: the Casimir element

$$K \in S^2(\mathfrak{sl}_2)^{\mathfrak{sl}_2} \subset \left((\mathfrak{sl}_2)^{\otimes 2}\right)^{\mathfrak{sl}_2}$$

and the invariant 3-form

$$\Omega \in \Lambda^3(\mathfrak{sl}_2)^{\mathfrak{sl}_2} \subset \left((\mathfrak{sl}_2)^{\otimes 3}\right)^{\mathfrak{sl}_2}.$$

(ii) Generalize this result for the case of $\mathfrak{sl}_3$.

(iii) Generalize this result for the case of $\mathfrak{sl}_n$.

(iv) Find the defining relations of the corresponding twisted associative algebra (at least for $\mathfrak{sl}_2$; the authors do not know the answer for $n > 2$).

Chapter 5

Symmetric Operads and Shuffle Operads

5.1 Introduction

This chapter continues developing methods for handling operations with several arguments. In Chapter 3, we used nonsymmetric operads, which allowed us to deal with substitutions of operations. In that chapter, we remarked that the language of nonsymmetric operads is rich enough to express properties like associativity, where all arguments appear in the same order, but is insufficient for the properties like the Jacobi identity in Lie algebras. If one attempts to combine substitutions of operations with permutations of arguments, the natural notion to deal with is that of a symmetric operad.

Symmetric operads were invented by Peter May for purely topological reasons (to study spectra); see [193, 242] for some historical (and even prehistorical) background. (It is worth remarking that, though invented and, until 1990s, almost exclusively used by topologists, operads could have been rediscovered by experts in combinatorics in the context of combinatorial species [142], as monoids in species with respect to the partitional composition [94, 141].) Notably, similar to the phenomenon we observed for twisted associative algebras in Chapter 4, the presence of symmetries makes it more difficult to have a working formalism of normal forms. The solution to this problem is similar to the one we exhibited for twisted associative algebras; we will explain how to ignore the symmetries for most purposes by dealing with shuffle operads instead of symmetric operads.

Our account of symmetric operads is fairly minimalistic; our goal is to give just about enough definitions to explain our methods and formulate clearly all the questions that we are going to address using the methods developed. A reader who is interested in learning more about algebraic aspects of the theory of symmetric operads is directed to [180] for a detailed account of the state-of-art in that theory, and to [187] for extra context and applications of algebraic operads.

5.2 Symmetric operads and shuffle operads

5.2.1 Two definitions of a symmetric operad

In this section, we outline two definitions of a symmetric operad which are parallel to the two definitions of a twisted associative algebra from Chapter 4. One of them views a symmetric operad as a nonsymmetric operad whose components have symmetric group actions for which the compositions are reasonably equivariant, the other one defines it as a monoid. The monoidal definition is the one that turns out to be easy to adapt, obtaining a more general definition of a shuffle operad, better suited for normal forms.

The following definition is motivated by looking at the endomorphism operad again. It is clear that besides substituting multilinear operations into one another, we can also permute arguments of an operation; this extra structure is in some way compatible with the nonsymmetric operad structure, and spelling out the compatibility explicitly, we arrive at a definition of a symmetric operad. Note that graphically the composition $f \circ (g_1, \ldots, g_r)$ is represented by a tree of depth two, that is trees with two levels of internal vertices, the first level consisting of the only vertex v directly connected to root, and the second level being the elements of $\mathrm{Parent}^{-1}(v)$. This leads to two different types of symmetry: the first-level symmetry which arises from permuting elements of $\mathrm{Parent}^{-1}(v)$, and the second-level symmetry which arises from permuting elements of $\mathrm{Parent}^{-1}(v_i)$, where $v_i \in \mathrm{Parent}^{-1}(v)$.

Definition 5.2.1.1 (Classical definition of a symmetric operad)**.** A *symmetric operad* is a symmetric collection $\mathcal{O} = \{\mathcal{O}(n)\}_{n\geq 0}$ with a nonsymmetric operad structure given by a set of maps

$$\gamma^{(r)}_{n_1,\ldots,n_r} \colon \mathcal{O}(r) \otimes \mathcal{O}(n_1) \otimes \cdots \otimes \mathcal{O}(n_r) \to \mathcal{O}(n_1 + \cdots + n_r)$$

and an element $\mathrm{id} \in \mathcal{O}(1)$ which satisfy the associativity and the unit axiom for nonsymmetric operads (Definition 3.2.1.1), and in addition satisfy the following equivariance axioms:

- *first-level symmetry:* the map

  $$\bigoplus_{n_1,\ldots,n_r} \gamma^{(r)}_{n_1,\ldots,n_r} \colon \mathcal{O}(r) \otimes \Big(\bigoplus \mathcal{O}(n_1) \otimes \cdots \otimes \mathcal{O}(n_r)\Big) \to \mathcal{O}(n) \qquad (5.1)$$

  factors through the tensor product over $\mathbb{F}S_r$ (the direct sum is over all r-tuples $(n_1, \ldots, n_r)$ with $n_1 + \cdots + n_r = n$, and the action of S_r on the direct sum $\bigoplus\limits_{n_1+\cdots+n_r=n} \mathcal{O}(n_1) \otimes \cdots \otimes \mathcal{O}(n_r)$ is by permuting factors in tensor products);

- *second-level symmetry:* the map $\gamma^{(r)}_{n_1,\ldots,n_r}$ is a morphism of $S_{n_1} \times \cdots \times S_{n_r}$-modules (here the target of this map is viewed as an $S_{n_1} \times \cdots \times S_{n_r}$-module through the obvious embedding $S_{n_1} \times \cdots \times S_{n_r} \subset S_{n_1+\cdots+n_r}$).

Similarly to the case of twisted associative algebras, it is possible to rephrase the definition of a symmetric operad in a slightly more conceptual way, as an associative algebra for a certain product on symmetric collections.

Definition 5.2.1.2 (Symmetric composition product)**.** Let $\mathcal{V}$ and $\mathcal{W}$ be two symmetric collections. We define their *symmetric composition product* $\mathcal{V} \circ_\Sigma \mathcal{W}$ as the symmetric collection $\mathcal{V} \circ_\Sigma \mathcal{W}$ with the components

$$(\mathcal{V} \circ_\Sigma \mathcal{W})(n) = \bigoplus_{r \geq 0} \mathcal{V}(r) \otimes_{\mathbb{F}S_r} \mathcal{W}^{\otimes r}(n),$$

where the action of S_r on the components $\mathcal{W}^{\otimes r}(n)$ of the r-th tensor power of the collection $\mathcal{W}$ (Definition 4.2.1.8) is by permuting factors in tensor products.

Remark 5.2.1.3. Using Definition 4.2.1.5 and basic properties of induced representations, one can easily prove the formula

$$\mathcal{W}^{\otimes r}(n) = \bigoplus_{n_1 + \cdots + n_r = n} \mathrm{Ind}_{S_{n_1} \times \cdots \times S_{n_r}}^{S_n} \mathcal{W}(n_1) \otimes \cdots \otimes \mathcal{W}(n_r).$$

The following proposition is an analogue of Proposition 4.2.1.6 for the case of symmetric operads.

Proposition 5.2.1.4.

- *The following formula for symmetric composition products holds:*

$$(\mathcal{V} \circ_\Sigma \mathcal{W})(n) = \bigoplus_{r \geq 0} \mathcal{V}(r) \otimes_{\mathbb{F}S_r} \left(\bigoplus_{\pi} \mathcal{W}(|I^{(1)}|) \otimes \cdots \otimes \mathcal{W}(|I^{(r)}|) \right),$$

  where π ranges in all set partitions $\{1, \ldots, n\} = \bigsqcup_{j=1}^{r} I^{(j)}$.

- *The symmetric composition product is associative, so that*

$$(\mathcal{U} \circ_\Sigma \mathcal{V}) \circ_\Sigma \mathcal{W} \cong \mathcal{U} \circ_\Sigma (\mathcal{V} \circ_\Sigma \mathcal{W})$$

  for all symmetric collections $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$.

- *We have*

$$\mathcal{V} \circ_\Sigma \mathbb{1} \cong \mathcal{V} \cong \mathbb{1} \circ_\Sigma \mathcal{V}$$

  for all symmetric collections $\mathcal{V}$.

Proof. The first statement follows directly from Proposition 4.2.1.6. The rest of the proof is left as an exercise for the reader (Exercise 5.1). □

This result leads to another definition of a symmetric operad.

Definition 5.2.1.5 (Monoidal definition of a symmetric operad)**.** A *symmetric operad* is a monoid in the category of symmetric collections with respect to the symmetric composition product.

We leave it to the reader (Exercise 5.2) to prove that the two definitions we gave are equivalent.

Using the monoidal definition of a symmetric operad, we can give a very concise definition of an ideal.

Definition 5.2.1.6 (Ideal of a symmetric operad)**.** An *ideal* of a symmetric operad $\mathcal{O}$ is a symmetric subcollection $\mathcal{I} \subset \mathcal{O}$ for which the image of the structure map $\mathcal{O} \circ_\Sigma \mathcal{O} \to \mathcal{O}$ restricted to $\mathcal{I} \circ_\Sigma \mathcal{O} + \mathcal{O} \circ_\Sigma \mathcal{I}$ is contained in $\mathcal{I}$.

As a consequence of associativity of the composition product, we can define composition powers of symmetric collections.

Definition 5.2.1.7 (Composition power of a symmetric collection)**.** Let $\mathcal{V}$ be a symmetric collection. The *composition power* $\mathcal{V}^{\circ_\Sigma n}$ is the symmetric composition product of n copies of $\mathcal{V}$. For $n = 0$, we define $\mathcal{V}^{\circ_\Sigma 0} := \mathbb{1}$.

5.2.2 Free symmetric operads

Similarly to the case of nonsymmetric operads, a symmetric operad can be presented via generators and relations, that is, as a quotient of the free symmetric operad $\mathcal{T}_\Sigma(\mathcal{M})$. The latter is also defined using decorated trees. As was the case with twisted associative algebras, we will not discuss free symmetric operads in full detail, since we will see that they are not fully suitable for defining Gröbner bases and proving an appropriate diamond lemma (which leads to a suitable replacement, free shuffle operads, defined in the next section).

Unlike the case of twisted associative algebras where the free algebra was just the sum of tensor powers, taking the sum of composition powers is not enough to define the free symmetric operad. The reason for that is that the composition product is highly nonlinear in its second argument, and computing the sum of composition powers would not allow us any natural way to implement partial compositions. For that reason, we forcefully adjoin the unit, and then factor out the relations needed for the unit axiom to hold.

Definition 5.2.2.1 (Free symmetric operad)**.** The *free symmetric operad* $\mathcal{T}_\Sigma(\mathcal{M})$ generated by a given symmetric collection $\mathcal{M}$ is the quotient of the direct sum

$$\bigoplus_{k\geq 1} (\mathbb{1} \oplus \mathcal{M})^{\circ_\Sigma k}$$

by the identifications

$$\mathbb{1} \circ_\Sigma \mathcal{M} \cong \mathcal{M} \cong \mathcal{M} \circ_\Sigma \mathbb{1} \quad \text{and} \quad \mathbb{1} \circ_\Sigma \mathbb{1} \cong \mathbb{1}$$

of Proposition 5.2.1.4.

Definition 5.2.2.2 (Tree tensors)**.** Let us develop a more concrete way to represent elements of $\mathcal{T}_\Sigma(\mathcal{M})$. Similarly to how the composition $f \circ (g_1, \ldots, g_r)$ may be represented by trees of depth two, for any symmetric collection $\mathcal{Q}$, elements that span the symmetric collection $\mathcal{Q}^{\circ_\Sigma k}$ can be viewed as equivalence classes of *tree tensors*, that is triples $(\tau, \mathsf{x}, \mathsf{n})$, where

- τ is a "fully grown rooted tree" (a tree for which all leaves are of the same depth k) with n leaves;
- x is a labelling of all internal vertices of τ by elements of $\mathcal{M}$, where each vertex v must have a label $\mathsf{x}_v \in \mathcal{X}(|\operatorname{Parent}^{-1}(v)|)$;
- n is a numbering of $\operatorname{Leaves}(\tau)$ by integers $\{1, \ldots, n\}$.

(Basically, the label x_v of an internal vertex v of depth $p \leq k$ comes from the p-th factor $\mathcal{Q}$ in $\mathcal{Q}^{\circ_\Sigma k}$.)

The equivalence relation on these is generated by two kinds of relations. First of all, x should be understood as a tensor, linear in each of the labels x_v. Second, isomorphisms of trees are related to symmetric group actions: if $v \in \operatorname{Vert}(\tau)$, and $\operatorname{Parent}^{-1}(v) = \{v_1, \ldots, v_k\}$, then for each $\sigma \in S_k$ we can obtain another rooted tree τ^σ by changing, for each $i = 1, \ldots, k$ and each $u \in \operatorname{Parent}^{-1}(v_i)$, the value of $\operatorname{Parent}(u)$ to $\sigma^{-1}(i)$, and we can obtain another labelling x^σ by (only) changing the value x_v to $\mathsf{x}_v.\sigma$. By definition, we say that $(\tau, \mathsf{x}, \mathsf{n}) \equiv (\tau^\sigma, \mathsf{x}^\sigma, \mathsf{n})$.

In our particular case, we have $\mathcal{Q} = \mathbb{1} \oplus \mathcal{M}$, and the identifications

$$\mathbb{1} \circ_\Sigma \mathcal{M} \cong \mathcal{M} \cong \mathcal{M} \circ_\Sigma \mathbb{1} \quad \text{and} \quad \mathbb{1} \circ_\Sigma \mathbb{1} \cong \mathbb{1}$$

merely allow to ignore the vertices with labels from $\mathbb{1}$, which just means that we work with all trees with labels from $\mathcal{M}$, not only fully grown ones.

To define compositions in the free symmetric operad, we need to tweak a little bit Definition 3.3.3.1 of full grafting of planar rooted trees so that we can take leaf labels into account.

Definition 5.2.2.3 (Composition product of tree tensors)**.** Suppose that

$$T_0 = (\tau_0, \mathsf{x}_0, \mathsf{n}_0) \in \mathcal{T}_\Sigma(\mathcal{M})(r) \text{ and } T_i = (\tau_i, \mathsf{x}_i, \mathsf{n}_i) \in \mathcal{T}_\Sigma(\mathcal{M})(n_i), \quad i = 1, \ldots, r,$$

are tree tensors. We define the *nonsymmetric composition product* $T_0 \circ (T_1, \ldots, T_r)$ to be the tree tensor $(\tau, \mathsf{x}, \mathsf{n})$, where

$$\operatorname{Root}(\tau) = \operatorname{Root}(\tau_0),$$
$$\operatorname{Int}(\tau) = \bigsqcup_{i=0}^{r} \operatorname{Int}(\tau_i),$$
$$\operatorname{Leaves}(\tau) = \bigsqcup_{i=1}^{r} \operatorname{Leaves}(\tau_i).$$

The parent function and the planar structure on the thus defined set of vertices are induced by the respective parent functions and planar structures of τ_i, $0 \leq i \leq r$, with the following exceptions. For each $j = 1, \ldots, r$, for the only vertex v_j in $\mathrm{Parent}^{-1}_{\tau_j}(\mathrm{Root}(\tau_j))$, we define

$$\mathrm{Parent}_{\tau}(v_j) := \mathrm{Parent}_{\tau_0}(\ell_j),$$

where $\ell_j = \mathsf{n}_0^{-1}(j)$ is the leaf of τ_0 numbered by j. This means that

$$\mathrm{Parent}^{-1}_{\tau}(\mathrm{Parent}_{\tau_0}(\ell_j)) = \{v_j\} \sqcup \mathrm{Parent}^{-1}_{\tau_0}(\mathrm{Parent}_{\tau_0}(\ell_j)) \setminus \{\ell_j\};$$

the total order needed by the planar structure puts v_j in the place of ℓ_j.

The labelling x of $\mathrm{Int}(\tau) = \bigsqcup_{i=0}^{r} \mathrm{Int}(\tau_i)$ is given by the disjoint union of labellings x_j, $1 \leq j \leq r$.

The numbering n of $\mathrm{Leaves}(\tau) = \bigsqcup_{i=1}^{r} \mathrm{Leaves}(\tau_i)$ is given by an appropriate shift of the numbering n_j:

$$\mathsf{n}(\ell) = n_1 + \ldots + n_{j-1} + \mathsf{n}_j(\ell), \quad \ell \in \mathrm{Leaves}(\tau_j).$$

This operation extends to a unique multilinear operation

$$\gamma\colon \mathcal{T}_{\Sigma}(\mathcal{M})(r) \otimes \mathcal{T}_{\Sigma}(\mathcal{M})(n_1) \otimes \cdots \otimes \mathcal{T}_{\Sigma}(\mathcal{M})(n_r) \to \mathcal{T}_{\Sigma}(\mathcal{M})(n_1 + \cdots + n_r).$$

Equipped with these operations and with the symmetric group action on the numberings of leaves, $\mathcal{T}_{\Sigma}(\mathcal{M})$ is the free symmetric operad generated by $\mathcal{M}$.

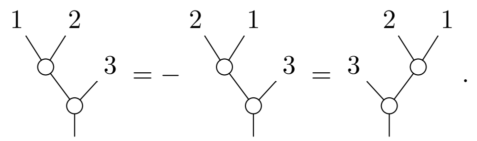
The following example may make our general description more clear.

Example 5.2.2.4. Let us consider the symmetric collection $\mathcal{L}$ for which

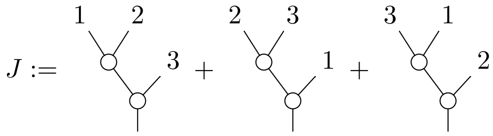
$$\mathcal{L}(n) = \begin{cases} \mathrm{sign}_2, & n = 2, \\ 0, & n \neq 2 \end{cases}$$

(here sign_2 is the sign representation of S_2). Since $\mathcal{L}(n) = 0$ for $n \neq 2$, all the tree tensors we may use are based on binary trees, that is trees τ for which $|\mathrm{Parent}^{-1}(v)| = 2$ for each $v \in \mathrm{Int}(\tau)$.

There need not be any labels of internal vertices since the vector space $\mathcal{L}(2)$ is one-dimensional; the only equivalence on such tensors we have to implement is that exchanging two children of an internal vertex results in multiplying the corresponding term by -1. For example,



In particular, this means that we now have a proper vocabulary to represent the Jacobi identity in Lie algebras: it is the element

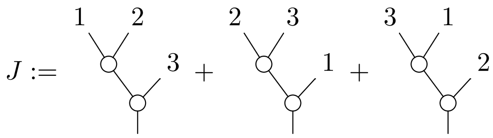


of the free operad $\mathcal{T}_\Sigma(\mathcal{L})$. Furthermore, the quotient $\mathcal{T}_\Sigma(\mathcal{L})/(J)$ is the operad Lie; its component $\mathsf{Lie}(n)$ consists of all n-ary operations that are canonically defined on any Lie algebra. (This is straighforward: taking the quotient by an ideal amounts to imposing all algebraic identities between operations represented by elements of the ideal.)

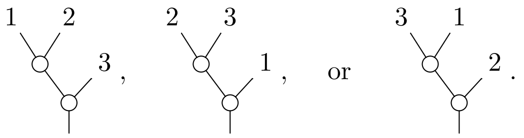
The particular case of the free algebra $\mathcal{T}_\Sigma(\mathcal{L})$ which we just discussed is quite sufficient to illustrate a major problem that arises because of symmetric group actions.

Proposition 5.2.2.5. *It is impossible to define a total ordering of basis elements of $\mathcal{T}_\Sigma(\mathcal{L})$ which would lead to normal forms in quotient symmetric operads.*

Proof. Let us consider the subspace of $\mathcal{T}_\Sigma(\mathcal{L})(3)$ spanned by the element



that we discussed above, and the ideal (J) generated by this element, which is the span of all elements obtained from this one by iterations of partial compositions and permutations. As we just mentioned above, the quotient operad is the operad Lie of Lie algebras. Suppose that it were possible to have normal forms for elements of quotient operads based on leading terms of ideals of relations. In this case, the leading term of J would be one of the three elements



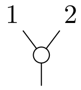
In each of the cases, our plan fails, since the ideal generated by any one of these (which of course would be contained by the ideal of leading terms) contains both others due to being a symmetric subcollection, so a collection of S_n-invariant subspaces. Moreover, all the basis elements of arity 3 belong to the same orbit of S_3, so there would be no normal monomials in the arity three component at all, a contradiction. (Of course, $\mathsf{Lie}(3)$ is two-dimensional, since the Jacobi identity is just one linear dependency between the three elements above.) □

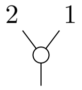
The way we are going to resolve this problem is similar to the one from Chapter 4: we will define a different kind of operads, the so-called shuffle operads. This will allow us to work out normal forms by completely ignoring the symmetric group action whenever possible. Before doing that, let us present one more example of a symmetric operad.

Example 5.2.2.6. Consider the symmetric collection $\mathcal{U}$ for which

$$\mathcal{U}(n) = \begin{cases} \mathbb{F}S_2, & n = 2, \\ 0, & n \neq 2. \end{cases}$$

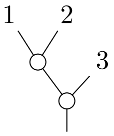
Since $\mathcal{U}(n) = 0$ for $n \neq 2$, all the tree tensors we may use are based on binary trees, similarly to Example 5.2.2.4. Although $\mathcal{U}(2)$ is two-dimensional, a conventional way to avoid labelling internal vertices in this particular case is to consider planar trees; in this case there are two different orders on $\mathrm{Parent}^{-1}(v)$ for each $v \in \mathrm{Int}(v)$, and a two-dimensional space of labels, so one can use a planar structure instead of a labelling. (This also leads to an important observation that every operad generated by a single binary operation may be viewed as a quotient of $\mathcal{T}_\Sigma(\mathcal{U})$.) For instance, the component $\mathcal{T}_\Sigma(\mathcal{U})(2) \cong \mathcal{U}(2) = \mathbb{F}S_2$ this way acquires a basis consisting of the two elements

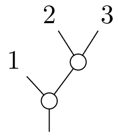


and


.

The best known operad with one binary generator is the symmetric associative operad Ass. When viewed as a quotient of $\mathcal{T}_\Sigma(\mathcal{U})$, its ideal of defining relations is generated by the element

$A :=$


$-$


;

note that in the case of symmetric operads, generating an ideal by an element amounts to finding the smallest symmetric subcollection containing this element and closed under compositions; in particular, the orbit of the symmetric group on A must be included in (A).

Remark 5.2.2.7. Throughout this chapter, we mainly use examples of operads generated by binary operations. In that particular case, the number of internal vertices and the number of leaves in the underlying tree of every tree tensor are related: the latter always exceeds the former by one. For general trees, there is no obvious relationship between the two.

5.2.3 Shuffle operads

In this section, we spell out the definition of a shuffle operad, originally defined in [74]. To define shuffle operads, we will use nonsymmetric collections (Definition 3.1.1.1) instead of symmetric ones; for those, there is a version of the composition product construction which will prove very useful. That product is only meaningful under a certain restriction, for so-called reduced collections.

Definition 5.2.3.1 (Reduced collection)**.** A (symmetric or nonsymmetric) collection $\mathcal{V}$ is said to be *reduced* if $\mathcal{V}(0) = 0$.

We are now ready to define the shuffle composition product.

Definition 5.2.3.2 (Shuffle composition product)**.** The *shuffle composition product* $\mathcal{V} \circ_{\text{III}} \mathcal{W}$ of two reduced nonsymmetric collections $\mathcal{V}$ and $\mathcal{W}$ is defined by the formula

$$(\mathcal{V} \circ_{\text{III}} \mathcal{W})(n) = \bigoplus_{r\geq 1} \mathcal{V}(r) \otimes \bigoplus_{\pi} \mathcal{W}(|I^{(1)}|) \otimes \cdots \otimes \mathcal{W}(|I^{(r)}|),$$

where π ranges in all set partitions $\{1, \ldots, n\} = \bigsqcup_{j=1}^{r} I^{(j)}$ for which all parts $I^{(j)}$ are nonempty and $\min(I_1) < \cdots < \min(I_r)$.

Proposition 5.2.3.3.

- *The shuffle composition product is associative, so that*

$$(\mathcal{U} \circ_{\text{III}} \mathcal{V}) \circ_{\text{III}} \mathcal{W} \cong \mathcal{U} \circ_{\text{III}} (\mathcal{V} \circ_{\text{III}} \mathcal{W})$$

  for all reduced nonsymmetric collections $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$.

- *We have $\mathcal{V} \circ_{\text{III}} \mathbb{1} \cong \mathcal{V} \cong \mathbb{1} \circ_{\text{III}} \mathcal{V}$ for all reduced nonsymmetric collections $\mathcal{V}$.*

Proof. Exercise 5.3. □

This result allows us to define shuffle operads as monoids, mimicking Definition 5.2.1.5.

Definition 5.2.3.4 (Shuffle operad)**.** A *shuffle operad* is a monoid in the category of reduced nonsymmetric collections with respect to the shuffle composition product.

More concretely, the datum of a shuffle operad on a reduced nonsymmetric collection $\mathcal{O}$ is a collection of maps

$$\gamma_\pi : \mathcal{O}(r) \otimes \mathcal{O}(n_1) \otimes \cdots \otimes \mathcal{O}(n_r) \to \mathcal{O}(n)$$

for each partition π of $\{1, \ldots, n\}$ of the form $\displaystyle\bigsqcup_{j=1}^{r} I^{(j)}$ with $|I^{(j)}| = n_j$, and $\min(I^{(1)}) < \cdots < \min(I^{(r)})$, and an identity element $\mathrm{id} \in \mathcal{O}(1)$ satisfying the following properties:

- *associativity*:

$$\gamma_\pi(f;\gamma_{\pi_1}(g_1;h_1^{(1)},\dots,h_{q_1}^{(1)}),\dots,\gamma_{\pi_r}(g_r;h_1^{(r)},\dots,h_{q_r}^{(r)}))= \\ =\gamma_{\tilde\pi}(\gamma_\pi(f;g_1,\dots,g_r);h_1,\dots,h_q), \quad (5.2)$$

  where for each $j=1,\dots,r$, π_j is a partition of the individual part $I^{(j)}$ of π into q_j parts, $\tilde\pi$ is the partition of $\{1,\dots,n\}$ obtained by putting together the individual parts of all π_j and ordering them globally according to the minimal elements in those parts, $q=q_1+\cdots+q_r$, and $(h_1,\dots,h_q)$ is a reordering of $(h_1^{(1)},\dots,h_{q_1}^{(1)},\dots,h_1^{(r)},\dots,h_{q_r}^{(r)})$ according to the reordering of all the individual parts of all π_j that we imposed.

- *unit axiom*:

$$\gamma_{\{1,\dots,n\}}(\mathrm{id};\alpha)=\alpha,\quad \gamma_{\{1\},\dots,\{n\}}(\alpha;\mathrm{id},\dots,\mathrm{id})=\alpha. \quad (5.3)$$

As usual, we can utilize the monoidal definition of shuffle operads to define ideals.

Definition 5.2.3.5 (Ideal of a shuffle operad)**.** Suppose that $\mathcal{O}$ is a shuffle operad. An *ideal* $\mathcal{I}$ of $\mathcal{O}$ is a nonsymmetric subcollection $\mathcal{I}\subset\mathcal{O}$ for which the images of structure maps restricted to both $\mathcal{I}\circ_{Ш}\mathcal{O}$ and $\mathcal{O}\circ_{Ш}\mathcal{I}$ are contained in $\mathcal{I}$.

As a consequence of associativity of the shuffle composition product, we can define shuffle composition powers of reduced nonsymmetric collections.

Definition 5.2.3.6 (Composition power of a nonsymmetric collection)**.** Let $\mathcal{V}$ be a reduced nonsymmetric collection. The *composition power* $\mathcal{V}^{\circ_{Ш} n}$ is the shuffle composition product of n copies of $\mathcal{V}$. For $n=0$, we define $\mathcal{V}^{\circ_{Ш} 0}:=\mathbb{1}$.

5.3 Free shuffle operads

5.3.1 Tree monomials and tree polynomials

One can define free shuffle operads analogously to free symmetric operads.

Definition 5.3.1.1 (Free shuffle operad)**.** The *free shuffle operad* $\mathcal{T}_\Sigma(\mathcal{M})$ generated by a given reduced nonsymmetric collection $\mathcal{M}$ is the quotient of the direct sum

$$\bigoplus_{k\geq 1}(\mathbb{1}\oplus\mathcal{M})^{\circ_{Ш} k}$$

by the identifications

$$\mathbb{1}\circ_{Ш}\mathcal{M}\cong\mathcal{M}\cong\mathcal{M}\circ_{Ш}\mathbb{1} \quad\text{and}\quad \mathbb{1}\circ_{Ш}\mathbb{1}\cong\mathbb{1}$$

of Proposition 5.2.3.3.

Let us describe an explicit construction of the free shuffle operad with a given set of generators.

Definition 5.3.1.2 (Shuffle tree monomial)**.** Let $\mathcal{X} = \{\mathcal{X}(n)\}_{n\geq 1}$ be a reduced operation alphabet. A *shuffle tree monomial* in $\mathcal{X}$ is a triple $T = (\tau, \mathsf{x}, \mathsf{n})$, where

- τ is a planar rooted tree all of whose endpoints are leaves;
- x is a labelling of all internal vertices of τ by elements of $\mathcal{X}$; each vertex v must have a label $x_v \in \mathcal{X}(|\operatorname{Parent}^{-1}(v)|)$;
- n is a numbering of leaves of τ by integers $1, \ldots, |\operatorname{Leaves}(\tau)|$ satisfying the following *local increasing condition* stated as follows.

  Any numbering n of leaves induces a numbering n_* of all vertices of τ: we put $\mathsf{n}_*(v)$ to be the number of the smallest leaf of the subtree of τ with the root v. The local increasing condition for n states that for each vertex u, the ordering of the set $\operatorname{Parent}^{-1}(u)$ according to the numbering n_* of its elements is precisely the ordering given by the planar structure of τ.

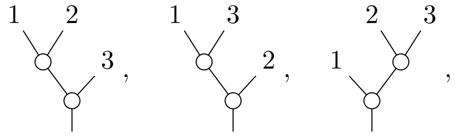
The tree monomial for which the underlying tree τ is the trivial tree is called the *trivial tree monomial*, or the *empty tree monomial*.

The *arity* of a shuffle tree monomial T, denoted $\operatorname{ar}(T)$, is the number of leaves of τ, and its *weight*, denoted $\operatorname{wt}(T)$, is the number of internal vertices of τ.

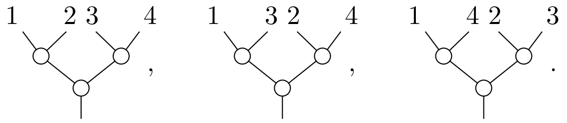
The set of all shuffle tree monomials in $\mathcal{X}$ of arity n is denoted $\text{Ш}\mathrm{Tree}_{\mathcal{X}}(n)$. The collection of all these sets for all $n \geq 1$ is denoted $\text{Ш}\mathrm{Tree}_{\mathcal{X}}$.

In simple words, shuffle tree monomials are planar tree monomials for which each internal vertex has at least one input edge, all leaves are numbered, and for each internal vertex, the minimal leaves of the subtrees grafted at that vertex increase from the left to the right in the usual graphical representation.

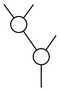
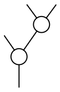
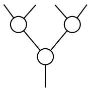
Example 5.3.1.3. Suppose that $\mathcal{X}(2) = \{*\}$, and $\mathcal{X}(n) = \varnothing$ for $n \neq 2$. In this case we can suppress the vertex labels of trees since they do not carry any new information. The following elements form a basis in $\text{Ш}\mathrm{Tree}_{\mathcal{X}}(3)$:

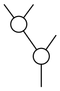
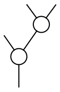


and the following elements are examples of basis elements in the vector space $\text{Ш}\mathrm{Tree}_{\mathcal{X}}(4)$ (which in fact is 15-dimensional):



Note that for the underlying trees

 ,  , and 

we listed all shuffle tree monomials of that shape; the local increasing condition implies, for instance, that there are two different shuffle tree monomials of the shape  but only one such monomial of the shape  .

Definition 5.3.1.4 (Shuffle tree polynomial). Let $\mathcal{X} = \{\mathcal{X}(n)\}_{n\geq 1}$ be a reduced operation alphabet. A *shuffle tree polynomial* in $\mathcal{X}$ with coefficients in $\mathbb{F}$ is a linear combination of shuffle tree monomials of the same arity. The *support* of a shuffle tree polynomial f, denoted $\operatorname{supp}(f)$, is the set of all nonsymmetric tree monomials that appear in f with nonzero coefficients.

We denote the vector space of all nonsymmetric tree polynomials of arity n by $\mathcal{T}_{\text{Ш}}(\mathcal{X})(n)$; of course we have $\mathcal{T}_{\text{Ш}}(\mathcal{X})(n) = \mathbb{F}\text{ШTree}_{\mathcal{X}}(n)$.

Definition 5.3.1.5 (Explicit construction of the free shuffle operad). Suppose that

$$T_0 = (\tau_0, \mathsf{x}_0, \mathsf{n}_0) \in \text{ШTree}_{\mathcal{X}}(r), T_i = (\tau_i, \mathsf{x}_i, \mathsf{n}_i) \in \text{ШTree}_{\mathcal{X}}(n_i), i = 1, \dots, r.$$

For each partition π of $\{1, \dots, n_1 + \cdots + n_r\}$ of the form

$$\bigsqcup_{j=1}^{r} I^{(j)} \text{ with } |I^{(j)}| = n_j, \text{ and } \min(I^{(1)}) < \cdots < \min(I^{(r)}),$$

we define the *shuffle composition* $\gamma_\pi(T_0; T_1, \dots, T_r)$ to be the shuffle tree monomial $(\tau, \mathsf{x}, \mathsf{n})$, where

$$\begin{aligned} \operatorname{Root}(\tau) &= \operatorname{Root}(\tau_0), \\ \operatorname{Int}(\tau) &= \bigsqcup_{i=0}^{r} \operatorname{Int}(\tau_i), \\ \operatorname{Leaves}(\tau) &= \bigsqcup_{i=1}^{r} \operatorname{Leaves}(\tau_i). \end{aligned}$$

The parent function and the planar structure on the thus defined set of vertices are induced by the respective parent functions and planar structures of τ_i, $0 \leq i \leq r$, with the following exceptions. For each $j = 1, \dots, r$, for the only vertex v_j in $\operatorname{Parent}_{\tau_j}^{-1}(\operatorname{Root}(\tau_j))$, we define

$$\operatorname{Parent}_\tau(v_j) := \operatorname{Parent}_{\tau_0}(\ell_j),$$

where $\ell_j = \mathsf{n}_0^{-1}(j)$ is the leaf of τ_0 numbered by j. This means that

$$\mathrm{Parent}_{\tau}^{-1}(\mathrm{Parent}_{\tau_0}(\ell_j)) = \{v_j\} \sqcup \mathrm{Parent}_{\tau_0}^{-1}(\mathrm{Parent}_{\tau_0}(\ell_j)) \setminus \{\ell_j\};$$

the total order needed by the planar structure puts v_j in the place of ℓ_j. The labelling x of $\mathrm{Int}(\tau) = \bigsqcup_{i=0}^{r} \mathrm{Int}(\tau_i)$ is given by the disjoint union of labellings x_j, $1 \leq j \leq r$, and the numbering n of $\mathrm{Leaves}(\tau) = \bigsqcup_{i=1}^{r} \mathrm{Leaves}(\tau_i)$ is given by numbering the leaves of each τ_j via the composition of the only order preserving bijection of $\sigma_j \colon \{1, \ldots, n_j\} \cong I^{(j)}$ with the numbering n_j:

$$\mathsf{n}(\ell) = \sigma_j(\mathsf{n}_j(\ell)), \quad \ell \in \mathrm{Leaves}(\tau_j).$$

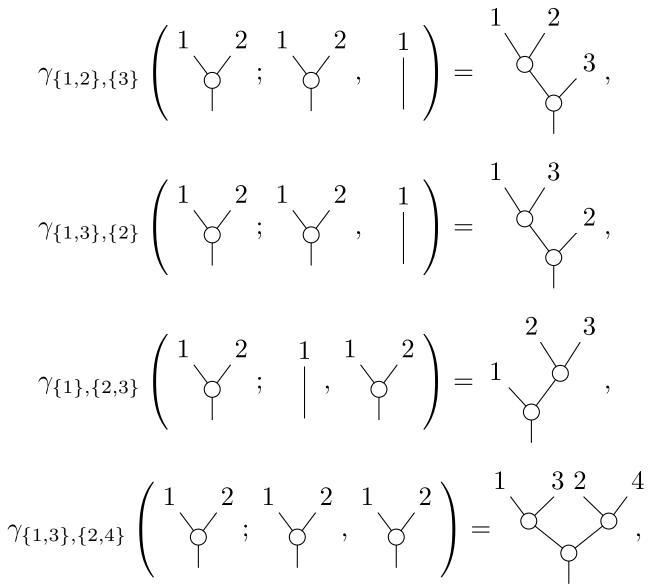
These shuffle compositions may be extended by multilinearity to the collection $\mathcal{T}_{\text{Ш}}(\mathcal{X}) = \{\mathcal{T}_{\text{Ш}}(\mathcal{X})(n)\}_{n \geq 1}$ of all shuffle tree polynomials of all arities, giving operations

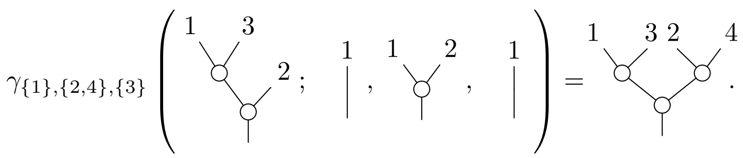
$$\gamma_\pi \colon \mathcal{T}_{\text{Ш}}(\mathcal{X})(r) \otimes \mathcal{T}_{\text{Ш}}(\mathcal{X})(n_1) \otimes \cdots \otimes \mathcal{T}_{\text{Ш}}(n_r) \to \mathcal{T}_{\text{Ш}}(\mathcal{X})(n_1 + \cdots + n_r).$$

Equipped with these operations, $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ is the *free shuffle operad generated by $\mathcal{X}$*. In addition to the notation $\mathcal{T}_{\text{Ш}}(\mathcal{X})$, we will use the notation $\mathcal{T}_{\text{Ш}}(\mathcal{M})$, where $\mathcal{M} = \{\mathcal{M}(n)\}_{n \geq 1}$ is a nonsymmetric collection for which $\mathcal{M}(n) = \mathrm{span}(\mathcal{X}(n))$ for all $n \geq 1$.

Throughout this chapter, we mainly consider shuffle tree monomials and polynomials, so we will occasionally drop the word "shuffle", hoping that it does not lead to confusion.

Example 5.3.1.6. Let us consider the free shuffle operad $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ from Example 5.3.1.3. The following are examples of shuffle compositions in that operad:





5.3.2 Presentation by generators and relations

The analogue of First Homomorphism Theorem holds for shuffle operads, and we may utilize it to define presentations of operads. Suppose that a shuffle operad $\mathcal{P}$ is generated by a collection of operations $\alpha_i \in \mathcal{P}(n_i)$. In that case, we can consider the collection $\mathcal{X}$ of operations $\kappa_i \in \mathcal{X}(n_i)$, one operation for each generator of $\mathcal{P}$. There is a surjective homomorphism from $\mathcal{T}_{\text{III}}(\mathcal{X})$ onto $\mathcal{P}$ sending κ_i to α_i which is uniquely defined by the universal property of the free operad. By the First Homomorphism Theorem, that homomorphism is the canonical map onto the quotient of $\mathcal{T}_{\text{III}}(\mathcal{X})$ by some ideal $\mathcal{I}$.

Definition 5.3.2.1 (Ideal generated by a subcollection)**.** Let $\mathcal{P}$ be a shuffle operad, and suppose that $\mathcal{S} \subset \mathcal{P}$ is a subcollection. The *ideal of $\mathcal{P}$ generated by $\mathcal{S}$*, denoted by $(\mathcal{S})$, is the smallest (by inclusion) ideal of $\mathcal{P}$ containing $\mathcal{S}$.

Definition 5.3.2.2 (Presentation by generators and relations)**.** Suppose that the shuffle operad $\mathcal{P}$ is a quotient of the free operad $\mathcal{T}_{\text{III}}(\mathcal{X})$ by some ideal $\mathcal{I}$, and that the ideal $\mathcal{I}$ is generated by the collection $\mathcal{S}$. In this case, we will say that the operad $\mathcal{P}$ is *presented by generators $\mathcal{X}$ and relations $\mathcal{S}$*.

5.3.3 Symmetric operads as shuffle operads

As we mentioned before, our main reason to deal with shuffle algebras is that they allow us to solve the problem of finding normal forms in twisted associative algebras presented by generators and relations. Let us explain why this is the case. Similarly to Chapter 4, we will use the forgetful functor that assigns to each symmetric collection $\mathcal{V}$ the same collection of vector spaces viewed as a nonsymmetric collection (Definition 4.3.3.1).

The following result is analogous to Proposition 4.3.3.2; it confirms that the shuffle tensor product is precisely the kind of operation one needs to ignore symmetries of symmetric collections without losing information about their composition products.

Proposition 5.3.3.1. *Let $\mathcal{V}$ and $\mathcal{W}$ be two reduced symmetric collections. Then we have*

$$(\mathcal{V} \circ_\Sigma \mathcal{W})^f \cong \mathcal{V}^f \circ_{\text{III}} \mathcal{W}^f.$$

Proof. Let us examine the n-th component for both sides. By Proposition 5.2.1.4,

$$(\mathcal{V} \circ_\Sigma \mathcal{W})(n) = \bigoplus_{r \geq 1} \mathcal{V}(r) \otimes_{\mathbb{F}S_r} \bigoplus_{\pi} \mathcal{W}(|J^{(1)}|) \otimes \cdots \otimes \mathcal{W}(|J^{(r)}|)$$

(we can write the direct sum for $r \geq 1$ since $\mathcal{V}$ is reduced), where π ranges in all set partitions $\{1, \ldots, n\} = \bigsqcup_{j=1}^{r} I^{(j)}$ (we may assume all $I^{(j)}$ nonempty since $\mathcal{W}$ is reduced). At the same time, by definition of shuffle composition products,

$$(\mathcal{V}^f \circ_{\text{III}} \mathcal{W}^f)(n) = \bigoplus_{r\geq 1} \mathcal{V}^f(r) \otimes \bigoplus_{\pi} \mathcal{W}^f(|I^{(1)}|) \otimes \cdots \otimes \mathcal{W}^f(|I^{(r)}|),$$

where π ranges in all set partitions $\{1, \ldots, n\} = \bigsqcup_{j=1}^{r} I^{(j)}$ for which all parts $I^{(j)}$ are nonempty and $\min(I_1) < \cdots < \min(I_r)$. It remains to note that the direct sum

$$\bigoplus_{\substack{J^{(1)}\sqcup\cdots\sqcup J^{(r)}=\{1,\ldots,n\},\\ J^{(k)}\neq\varnothing}} \mathcal{W}(|J^{(1)}|) \otimes \cdots \otimes \mathcal{W}(|J^{(r)}|)$$

is a free left $\mathbb{F}S_r$-module: it is a direct sum over all ordered partitions of $\{1, \ldots, n\}$ into r nonempty parts, and each unordered partition gives rise to exactly $n!$ different ordered partitions, so the action of $\mathbb{F}S_r$ on the direct sum is the regular action. It remains to recall that for any associative $\mathbb{F}$-algebra A, any left A-module M, and any free right A-module N, we have a vector space isomorphism

$$M \otimes_A N \cong M \otimes U,$$

where U is any space of free generators of N. In our case, we can take

$$\bigoplus_{\substack{J^{(1)}\sqcup\cdots\sqcup J^{(r)}=\{1,\ldots,n\}, J^{(k)}\neq\varnothing,\\ \min(J_1)<\cdots<\min(J_r)}} \mathcal{W}(|J^{(1)}|) \otimes \cdots \otimes \mathcal{W}(|J^{(r)}|)$$

as the space of generators: for every r-fold tensor product there exists a unique permutation of factors making it a tensor product where minimal elements of parts increase as the number of the part increases, and we get precisely the desired formula once we forget about the symmetric group actions. □

Remark 5.3.3.2. Note that the assumption on $\mathcal{W}$ being reduced is absolutely crucial; without that assumption, the direct sum

$$\bigoplus_{J^{(1)}\sqcup\cdots\sqcup J^{(r)}=\{1,\ldots,n\}} \mathcal{W}(|J^{(1)}|) \otimes \cdots \otimes \mathcal{W}(|J^{(r)}|)$$

is certainly not a free S_r-module, and the key step of the proof fails.

The following corollary is, in some sense, the central result of this chapter. It shows that any symmetric operad, when studied as a shuffle operad, needs the same number of generators and relations to be defined. Thus, any approach to normal forms for shuffle operads leads to normal forms for symmetric operads as well.

Corollary 5.3.3.3. *Let $\mathcal{M}$ be a symmetric collection. Then we have an isomorphism of shuffle operads*

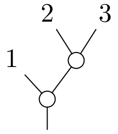
$$\mathcal{T}_{\text{Ш}}(\mathcal{M}^f) \cong (\mathcal{T}_\Sigma(\mathcal{M}))^f.$$

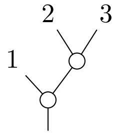
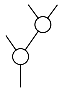
Moreover, if $\mathcal{I} \subset \mathcal{T}_\Sigma(\mathcal{M})$ is an ideal, then, under the identification that we made, $\mathcal{I}^f$ is an ideal of $\mathcal{T}_{\text{Ш}}(\mathcal{M}^f)$, and

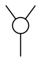
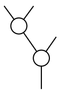
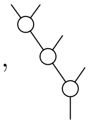
$$\mathcal{T}_{\text{Ш}}(\mathcal{M}^f)/\mathcal{I}^f \cong (\mathcal{T}_\Sigma(\mathcal{M})/\mathcal{I})^f.$$

Proof. All the notions in question, that is free symmetric operads, free shuffle operads, and ideals in those operads, are defined using composition products, so Proposition 5.3.3.1 applies. □

Example 5.3.3.4. Let us consider the free shuffle operad $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ from Example 5.3.1.3. Note that it is isomorphic to $\mathcal{T}_\Sigma(\mathcal{L})^f$, where $\mathcal{L}$ is the symmetric collection from Example 5.2.2.4: indeed, $\mathcal{T}_\Sigma(\mathcal{L})^f \cong \mathcal{T}_{\text{Ш}}(\mathcal{L}^f)$, and $\mathcal{L}(2)$ is one-dimensional, so $\mathcal{X}(2)$ can be identified with the only basis element of $\mathcal{L}^f(2)$. Consider, in this operad, the ideal generated by the element

$J' :=$ 

(this ideal is not an ideal of the form $\mathcal{I}^f$). This ideal is the span of all elements obtained from J' by iterations of shuffle compositions. Such elements are precisely all the elements $(\tau, \mathsf{x}, \mathsf{n})$ for which the tree τ has at least one "right branch", that is an internal vertex v which is not the smallest element of $\text{Parent}^{-1}(\text{Parent}(v))$. This happens because, as we mentioned in Example 5.3.1.3, the shuffle tree monomial  is the only shuffle tree monomial with the underlying tree . Therefore, a basis in the quotient $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ is formed by all shuffle tree monomials T without right branches. The underlying trees of such tree monomials are "left combs"

 ,  ,  , . . . ,

and the only condition on the numbering of leaves required to satisfy the local increasing condition is that the leftmost leaf is numbered by 1. Thus, for each n there are $(n-1)!$ basis elements; this agrees with the known formula for the dimension of the n-th component of the operad Lie [180]. Thus, on the level of nonsymmetric collections we have

$$\mathcal{T}_{\text{Ш}}(\mathcal{X})/(J') \cong \mathsf{Lie}^f;$$

this hints that the problem we exhibited in Proposition 5.2.2.5 is naturally fixed in the context of shuffle operads.

5.3.4 Applying the forgetful functor

Let us follow the example we just discussed with a further discussion of how to apply the forgetful functor to symmetric operads.

In the case of twisted associative algebras and shuffle algebras, the combinatorial constructions of free algebras were the same, so we could just, say, take an element of $T_\Sigma(\mathbb{1})$, a linear combination of permutations, and view it as an element of $T_{\text{Ш}}(\mathbb{1})$ without any pre-processing.

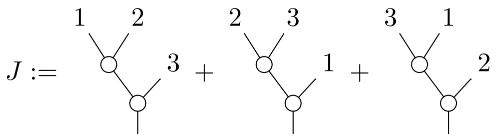
In the case of symmetric operads and shuffle operads, the situation is slightly different. The free shuffle operad has a basis of shuffle tree monomials, whereas the free symmetric operad has a spanning set of tree tensors, and some of these are identified with each other by the symmetric group action. The isomorphism of Proposition 5.3.3.1 chooses representatives of elements, and this is what we also have to do when regarding a symmetric operad as a shuffle operad.

Proposition 5.3.4.1. *Let $\mathcal{M}$ be a reduced symmetric collection, and let $\mathcal{X}$ be a reduced operation alphabet such that for each $n \geq 1$ the set $\mathcal{X}(n)$ forms a basis of $\mathcal{M}^f(n)$. Then the shuffle tree monomials from $\mathcal{T}_{\text{Ш}}(\mathcal{X})$, which, if the planar structure is ignored, can be viewed as elements in $\mathcal{T}_\Sigma(\mathcal{M})$, form a basis of $\mathcal{T}_\Sigma(\mathcal{M})$.*

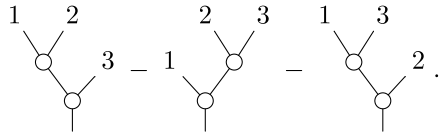
Proof. This is a mere reformulation of the isomorphism of Proposition 5.3.3.1. □

Let us consider two examples.

Example 5.3.4.2. Let us consider the operad Lie as defined in Example 5.2.2.4. As we already discussed in Example 5.3.3.4, we can take the operation alphabet $\mathcal{X}$ for which $\mathcal{X}(2)$ consists of one element and $\mathcal{X}(n)$ is empty for $n \neq 2$ as the basis collection for $\mathcal{L}^f$. The Jacobi identity



is an element of the free operad $\mathcal{T}_\Sigma(\mathcal{L})$; we would like to view it as an element of $\mathcal{T}_\Sigma(\mathcal{L})^f \cong \mathcal{T}_{\text{Ш}}(\mathcal{X})$. For that, we use the equivalence of tree tensors coming from the symmetric group actions on the space of generators to rewrite all the elements involved as combinations of shuffle tree monomials, obtaining the element

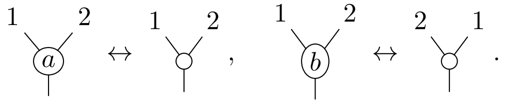


This element generates the ideal of relations defining the operad Lie^f as a quotient of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$.

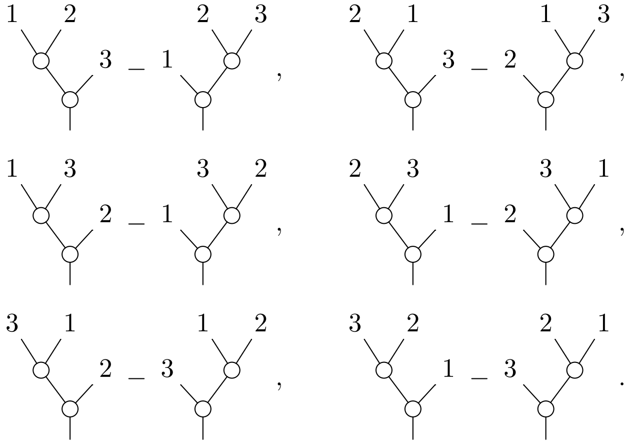
Example 5.3.4.3. Let us consider the symmetric operad Ass as defined in Example 5.2.2.6. We can take the operation alphabet $\mathcal{X}$ for which

$$\mathcal{X}(2) = \{a, b\} \text{ and } \mathcal{X}(n) = \varnothing \text{ for } n \neq 2$$

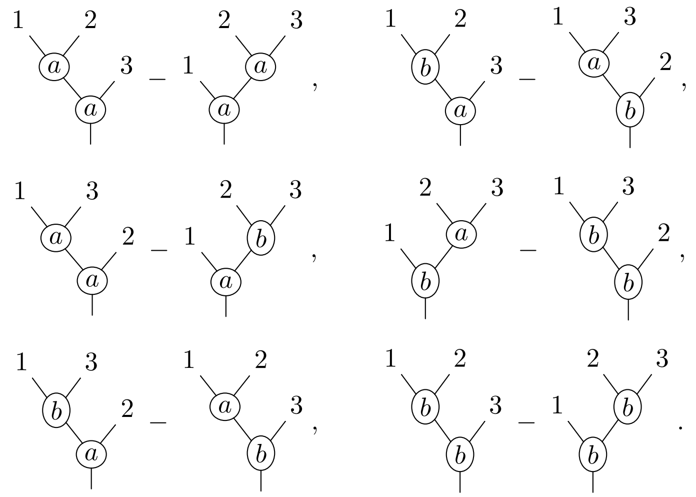
as the basis collection for $\mathcal{U}^f$. We identify $\mathcal{X}$ with a basis of $\mathcal{U}^f$, which leads to identification of bases of $\mathcal{T}_{\text{Ш}}(\mathcal{X})(2)$ and $\mathcal{T}_\Sigma(\mathcal{U})^f(2)$ as follows:



The symmetric group orbit of the defining relation of the operad Ass in $\mathcal{T}_\Sigma(\mathcal{U})(3)$ is



To convert these to elements of $\mathcal{T}_\Sigma(\mathcal{U})^f \cong \mathcal{T}_{\text{Ш}}(\mathcal{X})$, we use the equivalence of tree tensors coming from the symmetric group actions on the space of generators, obtaining the corresponding elements



These elements generate the ideal of relations defining the operad Ass^f as a quotient of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$.

5.4 Normal forms

5.4.1 Monomial orders

The definition of a monomial order can be easily adapted to the case of shuffle tree monomials.

Definition 5.4.1.1 (Monomial order)**.** A collection of total orders Ξ_n of $\text{Ш}\mathrm{Tree}_{\mathcal{X}}(n)$, $n \geq 1$, is said to be a *monomial order* if the following two conditions are satisfied:

- each Ξ_n is a well-order;
- each shuffle composition is a strictly increasing function in each of its arguments; that is if

  $$T_0, T_0' \in \text{Ш}\mathrm{Tree}_{\mathcal{X}}(r), T_1, T_1' \in \text{Ш}\mathrm{Tree}_{\mathcal{X}}(n_1), \ldots, T_r, T_r' \in \text{Ш}\mathrm{Tree}_{\mathcal{X}}(n_r),$$

  and π is a partition of $\{1, \ldots, n_1 + \cdots + n_r\}$ of the form

  $$\bigsqcup_{j=1}^{r} I^{(j)} \text{ with } |I^{(j)}| = n_j, \text{ and } \min(I^{(1)}) < \cdots < \min(I^{(r)}),$$

then

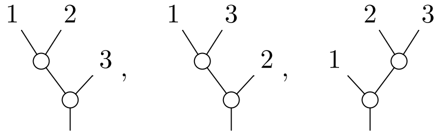
$$\gamma_\pi(T_0; T_1, \dots, T_r) \prec \gamma_\pi(T_0'; T_1, \dots, T_r) \text{ if } T_0 \prec T_0',$$
$$\gamma_\pi(T_0; T_1, \dots, T_i, \dots, T_r) \prec \gamma_\pi(T_0; T_1, \dots, T_i, \dots, T_r) \text{ if } T_i \prec T_i'.$$

Let us now outline an important construction of monomial orders. We denote $X := \bigsqcup_{n\geq 1} \mathcal{X}(n)$.

We will first explain how to replace every tree monomial by a sequence of words in the alphabet X that transform in a controllable way under composition. The path sequences we define are similar to those of Definition 3.4.1.2, and we somewhat suggestively use the same notation for them.

Definition 5.4.1.2 (Path sequence of a shuffle tree monomial)**.** Let $T = (\tau, \mathsf{x}, \mathsf{n})$ be a shuffle tree monomial. For each leaf ℓ of τ in the total order induced by the numbering n, we record the labels of internal vertices of the path from the root of τ to ℓ, forming a word in the alphabet X. The sequence of these words, denoted $\mathrm{Path}(T)$, is called the *path sequence* of the tree monomial T.

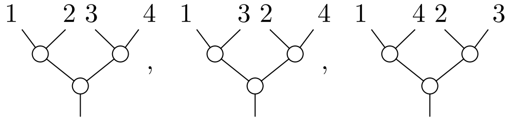
Example 5.4.1.3. Suppose that $\mathcal{X}(2) = \{*\}$. The path sequences of the tree monomials



from Example 5.3.1.3 are, respectively,

$$(**, **, *), \quad (**, *, **), \quad (*, **, **).$$

Note that however unlike the case of nonsymmetric operads the path sequence does not determine a monomial uniquely. For instance, each of the tree monomials



from the same example has the path sequence

$$(**, **, **, **).$$

There is a way to fix the issue of non-injectivity of path sequences.

Definition 5.4.1.4 (Leaf permutation of a shuffle tree monomial)**.** Let $T = (\tau, \mathsf{x}, \mathsf{n})$ be a shuffle tree monomial. The *leaf permutation* of T is the permutation $\sigma(T)$ for which $\sigma(T)(j) = \mathsf{n}(\ell_j)$, where ℓ_j is the j-th leaf of τ in the total planar order of leaves (Definition 3.3.1.3).

The *path-permutation data* of a shuffle tree monomial T is the pair $(\mathrm{Path}(T), \sigma(T))$.

Lemma 5.4.1.5. *A tree monomial* $T = (\tau, \mathsf{x}, \mathsf{n})$ *is uniquely determined by its path-permutation data.*

Proof. Let us rearrange the words in $\mathrm{Path}(T)$ according to the permutation $\sigma(T)^{-1}$; this would list the paths from the root to the leaves according to the total planar order of leaves. By Lemma 3.4.1.4 we can uniquely reconstruct a nonsymmetric tree monomial out of that path sequence. It remains to use $\sigma(T)$ to number the leaves of that tree monomial, obtaining the original shuffle tree monomial. □

Definition 5.4.1.6 (Path-permutation extension)**.** Suppose that Ξ is a monomial order on X^*.

The *path-permutation extension of* Ξ is the degree-lexicographic order on path-permutation data that is derived from Ξ. More precisely, it is defined as follows:

- if for two shuffle tree monomials $T_1 = (\tau_1, \mathsf{x}_1, \mathsf{n}_1)$ and $T_2 = (\tau_2, \mathsf{x}_2, \mathsf{n}_2)$ the number of leaves of τ_1 is less than the number of leaves of τ_2, we put $T_1 \prec T_2$;
- if τ_1 and τ_2 have the same numbers of leaves, we compare the sequences $\mathrm{Path}(T_1)$ and $\mathrm{Path}(T_2)$ word by word, comparing words using the order Ξ;
- if τ_1 and τ_2 have the same numbers of leaves, and $\mathrm{Path}(T_1) = \mathrm{Path}(T_2)$, we compare the permutations $\sigma(T_1)$ and $\sigma(T_2)$ using the lexicographic order.

Proposition 5.4.1.7. *The path-permutation extension of any monomial order* Ξ*, viewed as an order of shuffle tree monomials, is a monomial order.*

Proof. From Lemma 5.4.1.5 it follows immediately that the path extension is a total order of tree monomials. The fact that it is a well-order is clear from the same assumption on the order Ξ. Finally, let us prove that each shuffle composition is strictly increasing in each of its arguments.

Let us take some shuffle tree monomials

$$T_0 = (\tau_0, \mathsf{x}_0, \mathsf{n}_0) \in ⧢\mathrm{Tree}_{\mathcal{X}}(r), T_i = (\tau_i, \mathsf{x}_i, \mathsf{n}_i) \in ⧢\mathrm{Tree}_{\mathcal{X}}(n_i), i = 1, \dots, r,$$

and suppose that π is a partition π of $\{1, \dots, n_1 + \cdots + n_r\}$ of the form

$$\bigsqcup_{j=1}^{r} I^{(j)} \text{ with } |I^{(j)}| = n_j, \text{ and } \min(I^{(1)}) < \cdots < \min(I^{(r)}).$$

The path sequence $\gamma_\pi(T_0; T_1, \dots, T_r)$ is computed as follows. First, one computes appropriate concatenations of words of individual path sequences:

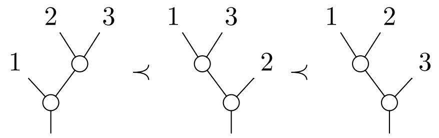
- the words obtained by concatenating the word corresponding to the leaf ℓ of T_0 with $\mathsf{n}_0(\ell) = 1$ with each of the words of $\mathrm{Path}(T_1)$,

- the words obtained by concatenating the word corresponding to the leaf ℓ of T_0 with $\mathsf{n}_0(\ell) = 2$ with each of the words of $\mathrm{Path}(T_2)$,
- $\ldots$
- the words obtained by concatenating the word corresponding to the leaf ℓ of T_0 with $\mathsf{n}_0(\ell) = r$ with each of the words of $\mathrm{Path}(T_r)$.

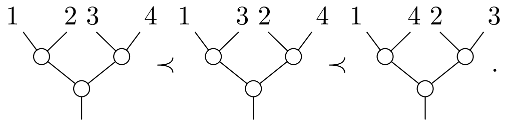
Then, these words are arranged in the order prescribed by the permutation $\sigma(\gamma_\pi(T_0; T_1, \ldots, T_r))$, or, equivalently, according to the permutation obtained by listing the permutations of subsets $I^{(j)}$ induced by the permutations $\sigma(T_j)$ in the order of j according to the permutation $\sigma(T_0)$. Replacing one of the elements T_i by a larger one (of the same arity, for the shuffle composition to be defined) would either lead to an increase in the path sequence, or an increase in the permutation for that element (and no other changes); thus, combining the arguments of Propositions 3.4.1.6 and 4.4.1.3 essentially concludes the proof. We leave it as an exercise for the reader to fill in the details (Exercise 5.6). □

Definition 5.4.1.8 (Graded path-permutation lexicographic order)**.** Let us fix some order Ξ of $X := \bigsqcup_{n\geq 0} \mathcal{X}(n)$. The *graded path-permutation lexicographic order* of tree monomials, denoted `gpathpermlex`, is the path extension of the `glex` order induced by Ξ.

Example 5.4.1.9. Let $\mathcal{X}(2) = \{*\}$. For the `gpathpermlex` order, we have



and



This follows from comparing the corresponding path-permutation data

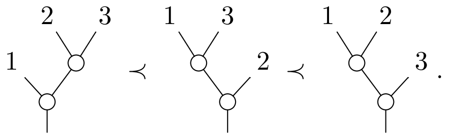
$$((*, **, **), 123) \prec ((**, *, **), 132) \prec ((**, **, *), 123)$$

and

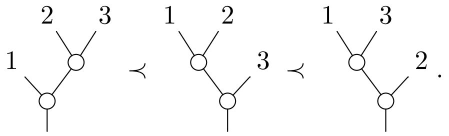
$$((**, **, **, **), 1234) \prec ((**, **, **, **), 1324) \prec ((**, **, **, **), 1423).$$

Remark 5.4.1.10. Suppose that a reduced operation alphabet $\mathcal{X}$ is such that $\mathcal{X}(1) = \varnothing$, and that for each n the set $\mathcal{X}(n)$ is finite. Under this assumption, if for a total order Ξ of words in the alphabet X the concatenation product is increasing in each argument, then the path extension of Ξ is a monomial order even if Ξ is not a well-order. The reason for that is that under our assumption there are only finitely many tree monomials with the given number of endpoints, and so the well-order property of the path-permutation extension is obtained for free.

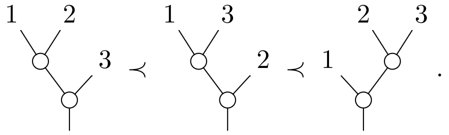
Example 5.4.1.11. Let $\mathcal{X}(2) = \{*\}$. We already saw that for the `gpathpermlex` order, we have



Note that if we alter the definition of the order so that we first compare the permutation and then the path sequence, then



Also, using Remark 5.4.1.10 with the order on words which makes shorter words larger (and compares words of the same length lexicographically), we get



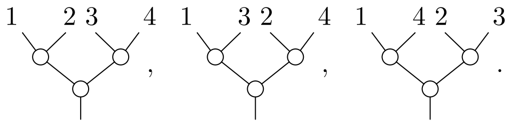
In particular, each of the three shuffle tree monomials of arity 3 can be made a leading monomial by an appropriate change of a monomial order.

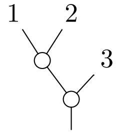
5.4.2 Long division

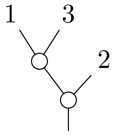
We already discussed in the previous chapters that for the algorithmic aspects of dealing with normal forms it is crucial to have two views of divisibility of monomials, both in terms of structure operations and a combinatorial one. Let us give a combinatorial definition of divisibility for shuffle tree monomials. Recall from Definition 5.3.1.2 that for each shuffle tree monomial $T = (\tau, \mathsf{x}, \mathsf{n})$, we have an induced numbering n_* of all vertices of τ such that $\mathsf{n}_*(v)$ is the number of the smallest leaf of the subtree of τ with the root v.

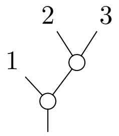
Definition 5.4.2.1 (Divisibility of shuffle tree monomials)**.** A shuffle tree monomial $T_1 = (\tau_1, \mathsf{x}_1, \mathsf{n}_1)$ is *divisible* by a (nontrivial) shuffle tree monomial $T_2 = (\tau_2, \mathsf{x}_2, \mathsf{n}_2)$ if the tree τ_1 contains a subtree τ_1' isomorphic to the tree τ_2, the labels of internal vertices of that subtree in the monomial T_1 match the labels of τ_2 in the monomial T_2, and finally the numbering $(\mathsf{n}_1)_*$ of leaves of that subtree matches the numbering n_2 (is order-isomorphic to it).

Example 5.4.2.2. Consider the shuffle tree monomials



from Example 5.3.1.3. The monomial 

is a divisor of the first one but not of the two others, due to mismatch in leaf labels. The monomial 

is a divisor of the second and the last one. The monomial 

is a divisor of all the three trees.

Proposition 5.4.2.3. *Let $T_1 = (\tau_1, \mathsf{x}_1)$ and $T_2 = (\tau_2, \mathsf{x}_2)$ be two shuffle tree monomials. Then T_1 is divisible by T_2 if and only if it can be obtained from T_2 by iterated shuffle products with elements of $T_{\text{Ш}}(\mathcal{X})$.*

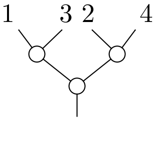
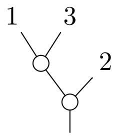
Proof. Exercise 5.7. □

Definition 5.4.2.4 (Insertion into a shuffle tree monomial)**.** Suppose that T_1 and T_2 are shuffle tree monomials, and T_1 is divisible by T_2. In this case, there is an *insertion* operation

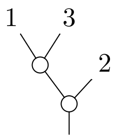
$$\square_{T_1,T_2} \colon \mathcal{T}_{\text{Ш}}(\mathcal{X})(\operatorname{ar}(T_2)) \to \mathcal{T}_{\text{Ш}}(\mathcal{X})(\operatorname{ar}(T_1)).$$

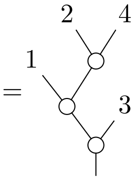
If $T = (\tau, \mathsf{x}, \mathsf{n})$ is a shuffle tree monomial of the same arity as T_2, the insertion operation replaces the subtree τ_1' by τ (ensuring that each subtree of τ_1 that was grafted at a leaf ℓ of τ_1' gets grafted at the respective leaf $\mathsf{n}^{-1}(\mathsf{n}_2(\ell))$ of τ), and changing labels of internal vertices accordingly. Then, this operation is extended by linearity to all shuffle tree polynomials of the same arity.

Example 5.4.2.5. Consider the shuffle tree monomial

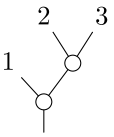
$T_1 =$  from Example 5.4.2.2, and its divisor T_2 = 

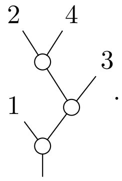
. We may insert any other element with three leaves in place of T_2; for instance, we have

$\Box_{T_1,T_2}$ (

) = 

,

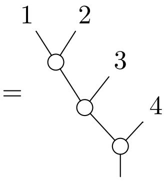
$\Box_{T_1,T_2}$ (

) = 

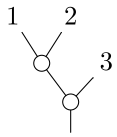
.

Remark 5.4.2.6. Our notation is not completely precise, since there may be several different divisors T_2 inside T_1. We always assume that the operation $\Box_{T_1,T_2}$ inserts everything at a particular occurrence of T_2 inside T_1 which is implicit.

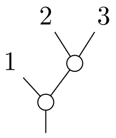
Example 5.4.2.7. Let us consider the shuffle tree monomial

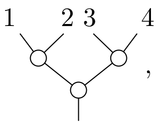
T = 

.

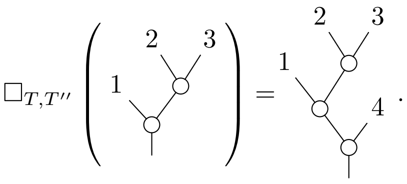
It has two different ternary divisors, each of those divisors is the monomial 

. Let us denote these divisors T' and T'', where T' shares the root with T, and T'' does not. We have

$\Box_{T,T'}$ (

) = 

,



One very useful feature of the insertion operations is that they allow us to give an explicit description of an ideal generated by a given collection $\mathcal{S}$ in the free shuffle operad which is a suitable replacement of the description "the ideal (S) is the linear span of all elements r_1sr_2 for all $r_1, r_2 \in T(X)$, $s \in S$" which we had in the associative case.

Proposition 5.4.2.8. *Let $\mathcal{S} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$. The ideal $(\mathcal{S})$ generated by $\mathcal{S}$ can be described explicitly as the linear span of all insertions $\square_{T_1,T_2}(f)$, where T_1 is a shuffle tree monomial, T_2 is a divisor of T_1, and $f \in \mathcal{S}(\operatorname{ar}(T_2))$.*

Proof. The ideal $(\mathcal{S})$ is spanned by iterated shuffle compositions where at least one of the elements involved belongs to $\mathcal{S}$; by multilinearity of shuffle compositions, we may assume that all other elements are monomials, in which case the corresponding iterated composition is the insertion operation. □

The following proposition is clear from the definition. It is analogous to the monadic associativity for nonsymmetric operads from Proposition 3.4.2.11.

Proposition 5.4.2.9. *Suppose that for the tree monomials*

$$T \in \text{Ш}\mathrm{Tree}_{\mathcal{X}}(n), \quad T_1, T_1' \in \text{Ш}\mathrm{Tree}_{\mathcal{X}}(n_1), \quad T_2 \in \text{Ш}\mathrm{Tree}_{\mathcal{X}}(n_2),$$

T_1 is a divisor of T and T_2 is a divisor of T_1'. Then

$$\square_{T,T_1} \circ \square_{T_1',T_2} = \square_{\square_{T,T_1}(T_1'),T_2}. \tag{5.4}$$

In particular, if $T_1 = T_1'$, this simplifies to

$$\square_{T,T_1} \circ \square_{T_1,T_2} = \square_{T,T_2}. \tag{5.5}$$

Let us show that under the insertion operations, the leading monomials change in a controllable way.

Proposition 5.4.2.10. *Suppose that T_1 is a tree monomial, and T_2 is a divisor of T_1. Then for each $g \in \mathcal{T}_{\text{Ш}}(\mathcal{X})(\operatorname{ar}(T_2))$, we have*

$$\mathrm{LM}(\square_{T_1,T_2}(g)) = \square_{T_1,T_2}(\mathrm{LM}(g)). \tag{5.6}$$

Proof. Let us first check that for any nonzero elements

$$f_0 \in \mathcal{T}_{\text{Ш}}(\mathcal{X})(r), f_1 \in \mathcal{T}_{\text{Ш}}(\mathcal{X})(n_1), \ldots, f_r \in \mathcal{T}_{\text{Ш}}(\mathcal{X})(n_r),$$

and for each partition π of $\{1,\dots,n_1+\cdots+n_r\}$ of the form $\bigsqcup_{j=1}^{r} I^{(j)}$ with $|I^{(j)}|=n_j$, and $\min(I^{(1)})<\cdots<\min(I^{(r)})$, we have

$$\textsc{lm}(\gamma_\pi(f_0;f_1,\dots,f_r))=\gamma_\pi(\textsc{lm}(f_0);\textsc{lm}(f_1),\dots,\textsc{lm}(f_r)).$$

Since the shuffle composition products on $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ are multilinear, the element $\gamma_\pi(f_0;f_1,\dots,f_r)$ is equal to a linear combination of elements

$$\gamma_\pi(m_0;m_1,\dots,m_r),\ \text{ where } m_p\in\operatorname{supp}(f_p).$$

It remains to notice that for each $m_p\neq\textsc{lm}(f_p)$ we have $m_p\prec\textsc{lm}(f_p)$, so by the defining property of monomial orders we have

$$\gamma_\pi(m_0;m_1,\dots,m_r)\prec\gamma_\pi(\textsc{lm}(f_0);\textsc{lm}(f_1),\dots,\textsc{lm}(f_r)),$$

unless

$$m_0=\textsc{lm}(f_0),m_1=\textsc{lm}(f_1),\dots,m_r=\textsc{lm}(f_r).$$

Now, the element $\square_{T_1,T_2}(g)$ is obtained from g by an iteration of shuffle compositions, and the result follows. □

Definition 5.4.2.11 (Reduced monomials and polynomials)**.** Let $\mathcal{S}$ be a subset of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$. A shuffle tree monomial T is said to be *reduced with respect to* $\mathcal{S}$ if $T\notin(\textsc{lm}(\mathcal{S}))$; in other words, if T is not divisible by any of the leading monomials of elements of $\mathcal{S}$.

In general, a shuffle tree polynomial f is said to be *reduced with respect to* $\mathcal{S}$, if it is equal to a linear combination of shuffle tree monomials which are reduced with respect to $\mathcal{S}$.

A subset $\mathcal{S}\subset\mathcal{T}_{\text{Ш}}(\mathcal{X})$ is said to be *self-reduced* if each element $s\in\mathcal{S}$ is monic and reduced with respect to $\mathcal{S}\setminus\{s\}$.

Definition 5.4.2.12 (Reduction)**.** Let $f,g\in\mathcal{T}_{\text{Ш}}(\mathcal{X})$ be two nonzero elements. We say that f is *reducible with respect to* g if $\textsc{lm}(f)$ is not reduced with respect to $\{g\}$, or, in plain words, if the leading monomial of f is divisible by the leading monomial of g, $\textsc{lm}(f)=\square_{T_1,T_2}(\textsc{lm}(g))$ for some

$$T_1\in\text{ШTree}_{\mathcal{X}}(\operatorname{ar}(\textsc{lm}(f))),\qquad T_2\in\text{ШTree}_{\mathcal{X}}(\operatorname{ar}(\textsc{lm}(g))).$$

In that case, the *reduction of f with respect to g*, denoted by $r_g(f)$, is defined by the formula

$$r_g(f)=f-\frac{\textsc{lc}(f)}{\textsc{lc}(g)}\square_{T_1,T_2}(g).$$

Lemma 5.4.2.13. *For all elements $f,g\in\mathcal{T}_{\text{Ш}}(\mathcal{X})$ such that $r_g(f)$ is defined, we have*

$$r_g(f)=0\qquad \textit{or}\qquad \textsc{lm}(r_g(f))\prec\textsc{lm}(f).$$

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.2.15. □

One can view a reduction as one step of a version of the long division algorithm. We make it more precise as follows.

Algorithm 5.4.2.14 (Long division for shuffle operads)**.**

Input: An element $f \in \mathcal{T}_{\text{Ш}}(\mathcal{X})$, and a finite set $\mathcal{S} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$.

Output: An element $\tilde{f}$, reduced with respect to $\mathcal{S}$, for which $\mathrm{LT}(\tilde{f}) \preceq \mathrm{LT}(f)$ such that $f + (\mathcal{S}) = \tilde{f} + (\mathcal{S})$.

- If $f = 0$, return f.
- Replace $\mathcal{S}$ by its linear self-reduction (Proposition 1.2.1.6).
- If $\mathcal{D} := \{s \in \mathcal{S} \colon \mathrm{LM}(f) \text{ is divisible by } \mathrm{LM}(s)\} \neq \varnothing$, take $s_0 \in \mathcal{D}$ with the least leading monomial (such s_0 is unique since $\mathcal{S}$ is linearly self-reduced), and return the result of long division of $f' := r_s(f)$ by $\mathcal{S}$.
- Otherwise, $\mathrm{LM}(f)$ is reduced with respect to $\mathcal{S}$, so let $\tilde{f}$ be the result of long division of $f' := f - \mathrm{LT}(f)$ by S; return $\mathrm{LT}(f) + \tilde{f}$.

Lemma 5.4.2.15. *For every $f \in \mathcal{T}_{\text{Ш}}(\mathcal{X})$, the long division algorithm terminates in a finite number of steps. Its output is an element $\tilde{f}$ reduced with respect to $\mathcal{S}$, for which $\mathrm{LT}(\tilde{f}) \preceq \mathrm{LT}(f)$ and*

$$f + (\mathcal{S}) = \tilde{f} + (\mathcal{S}).$$

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.2.17. □

Remark 5.4.2.16. We see that in fact there is nothing particularly problematic if $\mathcal{S}$ is an infinite self-reduced set: it is clear from the proof of Lemma 5.4.2.15 that for the given $f \in \mathcal{T}_{\text{Ш}}(\mathcal{X})$ the elements $s \in \mathcal{S}$ which we use at various steps of our computation have decreasing leading monomials, and so there can be only finitely many reductions performed; that is, for each f we never use more than a finite subset of $\mathcal{S}$. While for purposes of implementation this is not particularly important, it will be beneficial for theoretical results where $\mathcal{S}$ may be infinite.

We will now establish that the set of elements that are reduced with respect to $\mathcal{I}$ is a suitable candidate for the set of normal forms for the elements of the quotient shuffle operad $\mathcal{T}_{\text{Ш}}(\mathcal{X})/\mathcal{I}$. This is an improvement of Lemma 1.2.1.3 which takes into account the extra structures we have on the underlying vector spaces.

Lemma 5.4.2.17. *Suppose that $\mathcal{I}$ is an ideal of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$. Monomials that are reduced with respect to $\mathcal{I}$ form a basis of the quotient $\mathcal{T}_{\text{Ш}}(\mathcal{X})/\mathcal{I}$.*

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.2.19. □

It is possible to use long division to find, for each finite set, a finite self-reduced set that generates the same ideal.

Algorithm 5.4.2.18 (Self-reduction for shuffle operads)**.**

Input: A finite subset $\mathcal{S} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$.

Output: A finite self-reduced subset $\mathcal{S}' \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$ with $(\mathcal{S}) = (\mathcal{S}')$.

- Replace $\mathcal{S}$ by its linear self-reduction.
- If $\mathcal{S}$ is self-reduced, return $\mathcal{S}$.
- Let s be the element of $\mathcal{S}$ with the maximal leading monomial, and compute the self-reduction $\mathcal{S}'$ of $\mathcal{S} \setminus \{s\}$.
- Compute $\tilde{s}$, the result of long division of s by $\mathcal{S}'$.
- Recursively call the algorithm to compute the self-reduction of $\mathcal{S}' \cup \{\tilde{s}\}$.

We leave it as an exercise (Exercise 5.8) for the reader to check that for each finite $\mathcal{S}$ this algorithm terminates after finitely many steps.

5.4.3 Gröbner bases

In general, there are several different reduced forms one may obtain when doing reductions with respect to a set $\mathcal{S}$; however, there is a *canonical* form with respect to the ideal $(\mathcal{S})$, namely the corresponding normal form. In this section, we will explain how to fix this discrepancy.

Proposition 5.4.3.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$. The space of leading terms $\textsc{lt}(\mathcal{I})$ is an ideal of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.4.3.1. □

We are now ready to define a Gröbner basis of an ideal.

Definition 5.4.3.2 (Gröbner basis)**.** Let $\mathcal{I}$ be an ideal of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$. We say that $\mathcal{G} = \{\mathcal{G}(n) \subset \mathcal{I}(n)\}$ is a *Gröbner basis* of $\mathcal{I}$ with respect to a given monomial order Ξ if the set of leading monomials $\textsc{lm}(\mathcal{G}) := \{\textsc{lm}(g) \colon g \in \mathcal{G}\}$ generates the leading term ideal of the ideal $\mathcal{I}$:

$$\textsc{lt}(\mathcal{I}) = (\textsc{lm}(\mathcal{G})).$$

A Gröbner basis which is a self-reduced subset of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ is said to be *reduced*.

Lemma 5.4.3.3. *A Gröbner basis of an ideal $\mathcal{I} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$ generates $\mathcal{I}$.*

Proof. Same (*mutatis mutandis*) as the proof of Lemma 3.4.3.3. □

Proposition 5.4.3.4. *Let $\mathcal{I}$ be an ideal of $\mathcal{T}_{\text{III}}(\mathcal{X})$. Then $\mathcal{G} \subset \mathcal{I}$ is a Gröbner basis if and only if the cosets of monomials that are reduced with respect to $\mathcal{G}$ form a basis of the quotient $\mathcal{T}_{\text{III}}(\mathcal{X})/\mathcal{I}$.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.4.3.4. □

Corollary 5.4.3.5. *Suppose that $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I} \subset \mathcal{T}_{\text{III}}(\mathcal{X})$. Then the result of long division of $f \in \mathcal{T}_{\text{III}}(\mathcal{X})$ by $\mathcal{G}$ does not depend on either the choices or the order of the reductions performed.*

Proof. Same (*mutatis mutandis*) as the proof of Corollary 3.4.3.5. □

We summarize Proposition 5.4.3.4 and its corollary as follows.

Theorem 5.4.3.6.

(i) Let $\mathcal{I}$ be an ideal of $\mathcal{T}_{\text{III}}(\mathcal{X})$. A subset $\mathcal{G} \subset \mathcal{I}$ is a Gröbner basis if and only if the normal forms modulo $\mathcal{I}$ are precisely the elements that are reduced with respect to $\mathcal{G}$.

(ii) Suppose that $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I} \subset \mathcal{T}_{\text{III}}(\mathcal{X})$. Given an element $f \in \mathcal{I}$, its normal form modulo $\mathcal{I}$ can be computed using long division by $\mathcal{G}$. In fact, in this long division the order of reductions can be chosen arbitrarily.

Proposition 5.4.3.7. *Each ideal $\mathcal{I} \subset \mathcal{T}_{\text{III}}(\mathcal{X})$ has a unique reduced Gröbner basis.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.4.3.7. □

5.5 Computing Gröbner bases

In this section, we will explain how to compute Gröbner bases for ideals of $\mathcal{T}_{\text{III}}(\mathcal{X})$. As in Chapter 2, some ideals have infinite Gröbner bases, so the word "algorithm" below should be taken with a grain of salt.

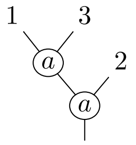
5.5.1 Diamond lemma

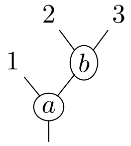
Definition 5.5.1.1 (S-polynomial)**.** Let $g_1, g_2 \in \mathcal{T}_{\text{III}}(\mathcal{X})$ be two monic polynomials. We say that the leading monomials $\text{LM}(g_1)$ and $\text{LM}(g_2)$ form an *overlap* if they have a *small common multiple*, a tree monomial T and its two proper divisors T_1 and T_2 for which $\text{LM}(g_1) = T_1$, $\text{LM}(g_2) = T_2$, and the underlying tree of T is the result of merging of the underlying trees of T_1 and T_2 along an overlap. We call the element

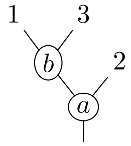
$$S_T(g_1, g_2) := \square_{T,T_1}(g_1) - \square_{T,T_2}(g_2)$$

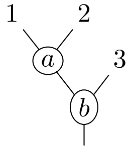
an *S-polynomial* of g_1 and g_2; the common term cancels, since both g_1 and g_2 are monic.

Example 5.5.1.2. Let us consider the shuffle associative operad Ass^f discussed in Example 5.3.4.3, and the following two of its six defining relations:

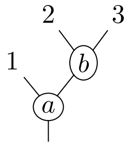
$g_1 =$ 

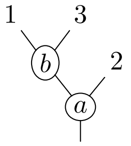
$-$ 

and $g_2 =$ 

$-$ 

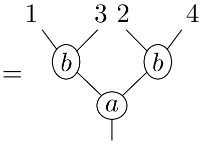
.

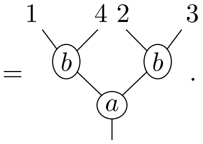
Let us consider, for the purpose of this example, the following ordering: to compare two shuffle tree monomials T and T' of the same arity, we compare the number of internal vertices labelled by b, then if those numbers are the same, compare T and T' using the order `gpathpermlex` for $b \prec a$. In this case, the leading monomials of the elements above are 

and 

.

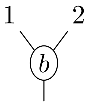
These two shuffle tree monomials have two small common multiples,

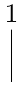
$T_1 =$ 

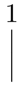
and $T_2 =$ 

.

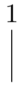
The corresponding S-polynomials are

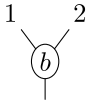
$S_{T_1}(-g_1, g_2) = \gamma_{\{1,3\},\{2\},\{4\}} \Bigg(-g_1,$ 

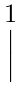
, 

, 

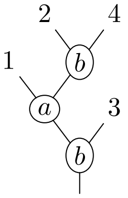
$\Bigg)$

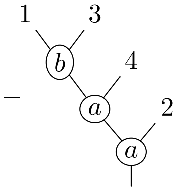
$- \gamma_{\{1\},\{2,4\},\{3\}} \Bigg(g_2,$ 

, 

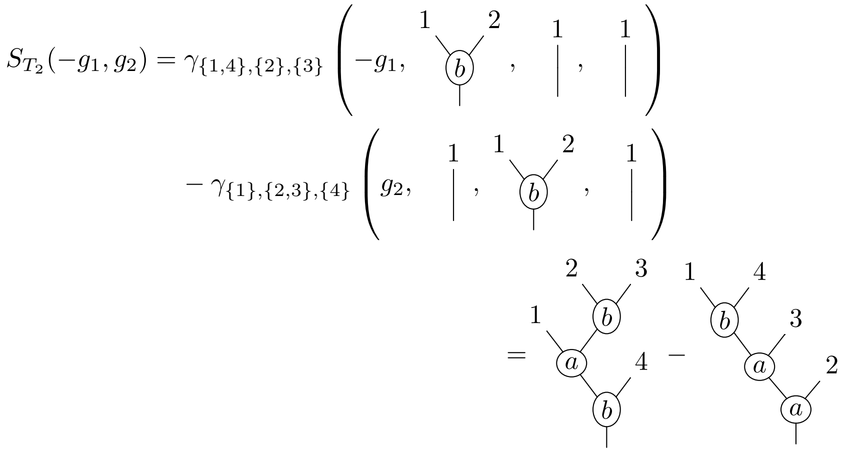
, 

$\Bigg)$

$=$ 

$-$ 

and


$S_{T_2}(-g_1, g_2) = \gamma_{\{1,4\},\{2\},\{3\}}$
$-g_1,$
1
2
b
1
1
$- \gamma_{\{1\},\{2,3\},\{4\}}$
$g_2,$
1
1
2
b
1
=
2
3
1
b
a
4
b
−
1
4
b
3
a
2
a

(we write $-g_1$ in both cases to make the polynomial monic); here γ is the shuffle composition from Definition 5.3.1.5.

We will now prove the result which is at the core of most feasible ways to check that some subset of an ideal is a Gröbner basis.

Definition 5.5.1.3 (Parameter of a representation)**.** Let $\mathcal{I} = (\mathcal{G})$ be an ideal of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$. Consider the representation of an element $f \in \mathcal{I}$ as a combination of insertions of $g_1, \ldots, g_N \in \mathcal{G}$:

$$f = \sum_{i=1}^{N} c_i \square_{\tilde{T}_i, T_i}(g_i), \tag{5.7}$$

where $T_i = \textsc{lm}(g_i)$. We call $\max(\tilde{T}_i)$ the *parameter* of this linear combination.

If $f = S_T(g_1, g_2)$ is the S-polynomial of $g_1, g_2 \in \mathcal{G}$ (with all the notation as above in Definition 5.5.1.1), then it has an obvious representation

$$f = \square_{T,T_1}(g_1) - \square_{T,T_2}(g_2),$$

with parameter T. We call a representation of that S-polynomial *nontrivial* if its parameter is smaller than T.

Theorem 5.5.1.4 (Diamond lemma)**.** *Let $\mathcal{G} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$ be self-reduced, and let $\mathcal{I} = (\mathcal{G})$. The following statements are equivalent:*

(i) *$\mathcal{G}$ is a Gröbner basis of $\mathcal{I}$.*

(ii) *Every S-polynomial $S_T(g_1, g_2)$ has reduced form 0 with respect to $\mathcal{G}$.*

(iii) *Every S-polynomial $S_T(g_1, g_2)$ admits a nontrivial representation of the form* (5.7)*.*

(iv) *Every element $f \in \mathcal{I}$ admits a representation of the form* (5.7) *with parameter $\textsc{lm}(f)$.*

Proof. Same (*mutatis mutandis*) as the proof of Theorem 3.5.1.6. □

5.5.2 The Buchberger algorithm

Theorem 5.5.1.4 leads naturally to a recipe for computing reduced Gröbner bases: given a set of generators of an ideal, one has to compute all pairwise S-polynomials, adjoin all reduced forms of those to the set of generators, and repeat the same. It is rather a "recipe" than an algorithm since we are not guaranteed termination, but it is nevertheless very useful.

Algorithm 5.5.2.1 (Buchberger algorithm for shuffle operads)**.**

```
    Input: A finite subset $\mathcal{G} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$ generating an ideal $\mathcal{I} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$.

    Output: If terminates, the output is the reduced Gröbner basis of $\mathcal{I}$.

• Set newSpolynomials ← true.
• While newSpolynomials do:
    – Sort $\mathcal{G}$ by gpathpermlex order of leading monomials: $\mathcal{G} = \{g_1, \dots, g_n\}$.
    – Compute the self-reduction of $\mathcal{G}$.
    – Set Spolynomials ← $\varnothing$.
    – Set newSpolynomials ← false.
    – For $g_1 \in \mathcal{G}$ do for $g_2 \in \mathcal{G}$ do:
        ∗ If $\text{LM}(g_1)$ and $\text{LM}(g_2)$ form an overlap then:
            1. Compute the S-polynomial $S_T(g_1, g_2)$.
            2. Let $t$ be the result of long division of $S_T(g_1, g_2)$ by $\mathcal{G}$.
            3. If $t \neq 0$ and $t \notin$ Spolynomials then
                ∗ Set newSpolynomials ← true.
                ∗ Set Spolynomials ← Spolynomials $\cup \{t\}$.
    – Set $\mathcal{G} \leftarrow \mathcal{G} \cup$ Spolynomials.
• Return $\mathcal{G}$.
```

Proposition 5.5.2.2. *If Algorithm 5.5.2.1 terminates then its output is the reduced Gröbner basis of $\mathcal{I}$.*

Proof. Immediate corollary to Theorem 5.5.1.4. □

5.5.3 Triangle lemma

Definition 5.5.3.1 (Essential overlap)**.** Let $\mathcal{G}$ be a self-reduced subset of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$, and let $g_1, g_2 \in \mathcal{G}$ be two elements for which $\text{LM}(g_1)$ and $\text{LM}(g_2)$ have an overlap. We call this overlap *essential* if $\text{LM}(g_1)$ and $\text{LM}(g_2)$ are the only two divisors from $\text{LM}(\mathcal{G})$ of the corresponding small common multiple.

Proposition 5.5.3.2 (Triangle lemma for shuffle operads)**.** *Let $\mathcal{G}$ be a self-reduced subset of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$, and let $g_1, g_2 \in \mathcal{G}$ be two elements for which $\text{LM}(g_1)$ and $\text{LM}(g_2)$ have an overlap. Suppose that this overlap is not essential, so that there exists $g_3 \in G$ for which $\text{LM}(g_3)$ is another divisor of the corresponding small common multiple T. Then:*

- *The divisors $\text{LM}(g_1)$ and $\text{LM}(g_3)$ of T have an overlap, and the divisors $\text{LM}(g_3)$ and $\text{LM}(g_2)$ of T also have an overlap.*
- *If the S-polynomials $S_{T'}(g_1, g_3)$ and $S_{T''}(g_3, g_2)$ for the corresponding overlaps admit nontrivial representations of the form* (5.7)*, then the S-polynomial $S_T(g_1, g_2)$ also admits a nontrivial representation of that form.*

Proof. Same (*mutatis mutandis*) as the proof of Proposition 3.5.3.2. □

Similarly to the case of nonsymmetric operads, Corollary 2.4.3.3 cannot be fully generalized to the case of shuffle operads, and only admits the following partial generalization, analogous to Corollary 3.5.3.3.

Corollary 5.5.3.3. *Let $\mathcal{G}$ be a self-reduced set of elements of $\mathcal{T}_{\text{Ш}}(\mathcal{X})$. Suppose that for two elements $g_1, g_2 \in \mathcal{G}$ whose leading monomials have an overlap the following holds:*

- *there exists $g_3 \in \mathcal{G}$ for which $\text{LM}(g_3)$ is another divisor of the tree monomial T obtained by merging $\text{LM}(g_1)$ and $\text{LM}(g_2)$ along their overlap,*
- *both the tree monomials T' which is the result of merging $\text{LM}(g_1)$ and $\text{LM}(g_3)$ along their overlap and T'' which is the result of merging $\text{LM}(g_3)$ and $\text{LM}(g_2)$ along their overlap are proper divisors of T.*

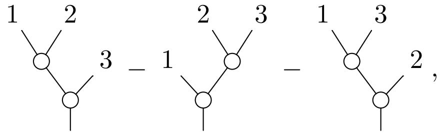
Then, while computing the reduced Gröbner basis using Algorithm 5.5.2.1, the S-polynomial $S_T(g_1, g_2)$ may be ignored.

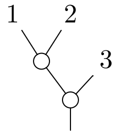
Similarly to the case of nonsymmetric operads, this can be improved under some extra assumptions on $\mathcal{G}$ using the notion of an Anick ordering from[75, Sec. 3]; we invite the reader to come up with such improvements.

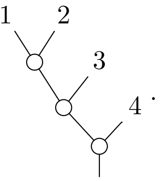
5.6 Examples of Gröbner bases for shuffle operads

5.6.1 Shuffle Lie and associative operads

Example 5.6.1.1. Let us consider the example of the shuffle operad Lie^f discussed in Example 5.3.4.2. Its ideal of relations is generated by the element

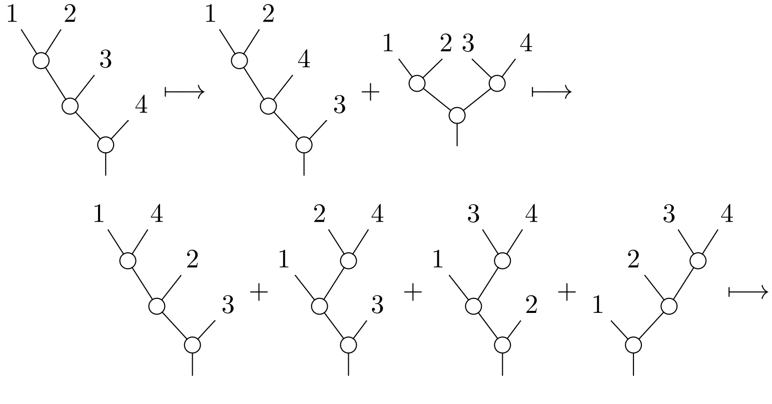


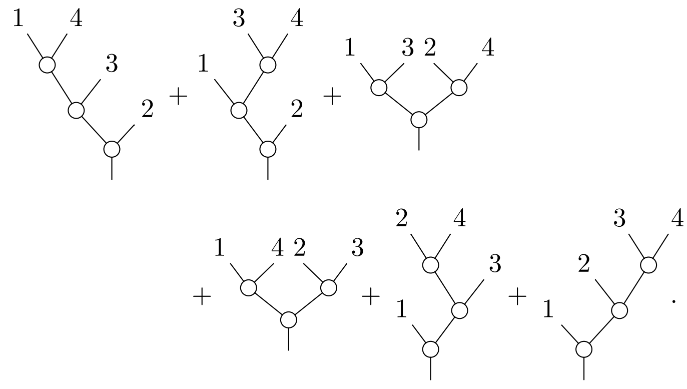
whose leading monomial, for the `gpathpermlex` order, is  (Example 5.4.1.9). This monomial has exactly one small common multiple with itself, the monomial

$T :=$  .

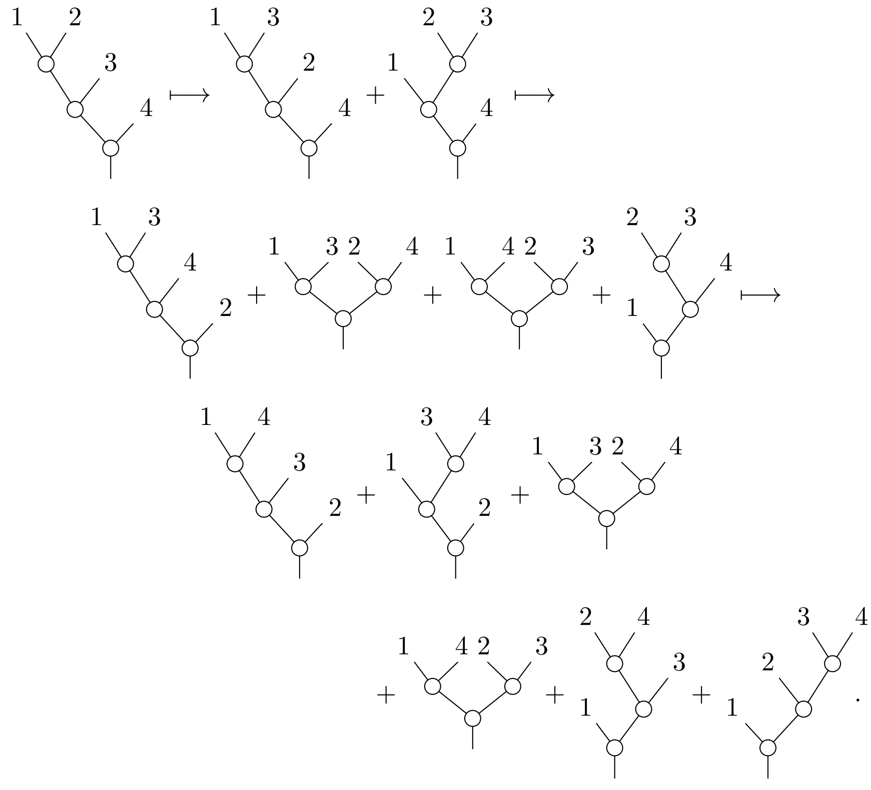
Instead of the usual computation of the S-polynomial and its reduction, let us compute separately the two different ways to rewrite this monomial as a linear combination of reduced monomials; this computation, even though a lot of intrinsic structures can be observed in the terms that arise in it, involves manipulations with many terms, and mixing them together within one S-polynomial would be a tougher task for the reader.

For the rewriting using the divisor T_1 sharing the root with T, we obtain



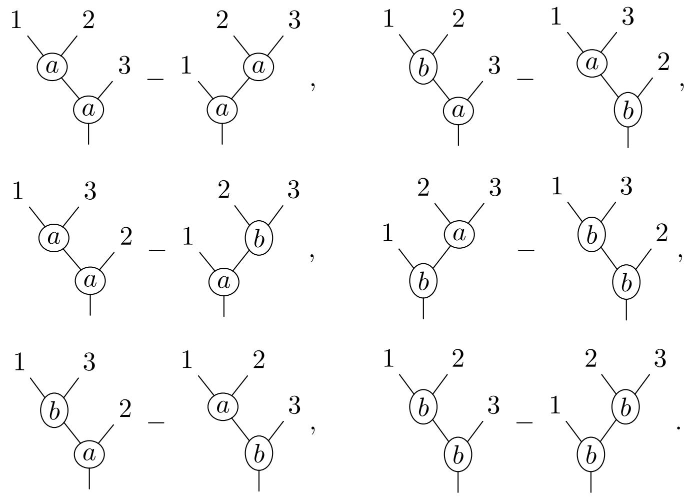


For the rewriting using the other divisor T_2, we obtain:

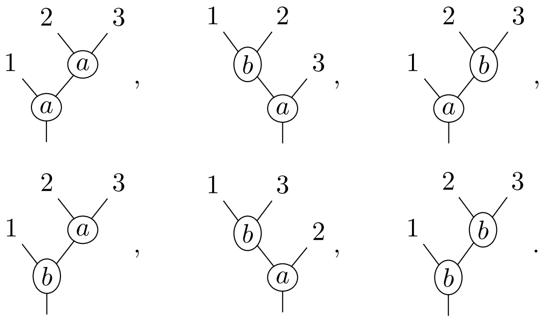


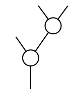
(In each of these cases, each arrow represents several rewritings of all non-reduced monomials in one go.) We see that the results are the same, so the corresponding S-polynomial can be reduced to zero, and the defining relation of the operad Lie^f is the reduced Gröbner basis. A similar computation shows that in this case for each of the monomials in the defining relation, and any choice of order (e.g., the choices from Example 5.4.1.11) making that monomial the leading monomial, the defining relation of the operad Lie^f is a Gröbner basis.

Example 5.6.1.2. Let us consider the shuffle associative operad Ass^f discussed in Example 5.3.4.3. Its ideal of relations is generated by the six elements



As one can infer from Example 5.5.1.2, in this case, depending on the choice of an order, there may be many S-polynomials involved, and so in order to compute the reduced Gröbner basis one has to either be extremely diligent or have access to computer software for computing Gröbner bases for shuffle operads. At the moment when the second author was looking at this question for the first time, there was no computer software available, and his diligence had its limitations, so he came up with the following shortcut. Let us consider the path-permutation extension of the monomial order on $\{a,b\}^*$ which first compares two words in the *reverse* order of length, and if the lengths are equal, compares them lexicographically, assuming $a \prec b$ (this extension is a monomial order on $\text{Ш}\mathrm{Tree}_{\mathcal{X}}$, see Remark 5.4.1.10). The leading monomials of the relations for this order are, respectively,



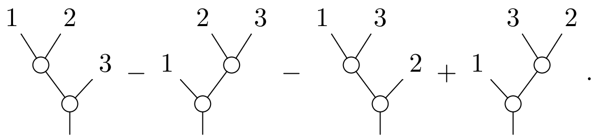
Let us examine the set of reduced monomials with respect to this set. Since this set contains all the four shuffle tree monomials with the underlying tree  , a reduced monomial is necessarily a "left comb" (we already encountered a similar situation in Example 5.3.3.4). By direct inspection of the two remaining leading terms that we have not accounted for yet, among the 2^{n-1} ways of labelling the internal vertices of the n-ary left comb by letters a and b, the ones that lead to non-reduced monomials are those for which there exist a pair of vertices v, $v' = \text{Parent}(v)$ such that $\mathsf{x}_v = b$, $\mathsf{x}_{v'} = a$. Therefore, allowed labellings are those for which the labels on the path from the root to leaf number 1 are $b, \dots, b, a, \dots, a$ (in this order). We conclude that there are exactly $n! = n \cdot (n-1)!$ reduced monomials of arity n: first, there are $(n-1)!$ ways to number the leaves of the left comb with n leaves (Example 5.3.3.4), second, there are n different ways to label internal vertices of the left comb with n leaves, as we just established. This means that the number of normal monomials for Ass^f is at most $n!$: in principle, the leading monomials of the reduced Gröbner basis will contain the six monomials that we already have, and possibly some other monomials. But the n-th component of Ass is of dimension $n!$, since there are $n!$ different ways to compute the associative product of n elements, one for each permutation in S_n. Therefore, there must be $n!$ normal monomials, and the defining relations of Ass^f form its reduced Gröbner basis for our chosen order.

5.6.2 Symmetric and shuffle operad PreLie

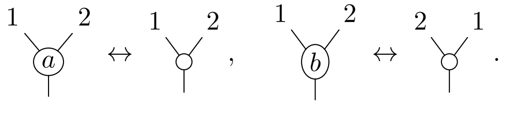
Example 5.6.2.1. Consider the symmetric collection $\mathcal{U}$ for which

$$\mathcal{U}(n) = \begin{cases} \mathbb{F}S_2, & n = 2, \\ 0, & n \neq 2. \end{cases}$$

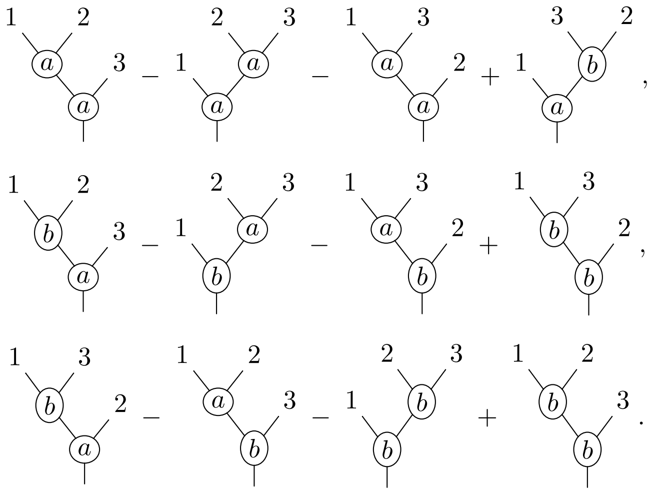
The symmetric operad PreLie of (right) pre-Lie algebras (first defined in [100, 255]) is the quotient of $\mathcal{T}_\Sigma(\mathcal{U})$ by the ideal generated by the element

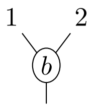
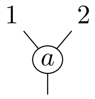


We can take the operation alphabet $\mathcal{X}$ for which $\mathcal{X}(2) = \{a, b\}$ and $\mathcal{X}(n)$ is empty for $n \neq 2$ as the basis collection for $\mathcal{U}^f$. We identify $\mathcal{X}$ with a basis of $\mathcal{U}^f$, which leads to identification of bases of $\mathcal{T}_{\text{Ш}}(\mathcal{X})(2)$ and $\mathcal{T}_\Sigma(\mathcal{U})^f(2)$ as follows:



It is easy to see that the ideal of relations of operad PreLie^f is generated by the following elements:


1 2 a 3 a − 1 2 3 a a − 1 3 a 2 a + 1 3 2 b a ,
1 2 b 3 a − 1 2 3 a b − 1 3 a 2 b + 1 3 b 2 b ,
1 3 b 2 a − 1 2 a 3 b − 1 2 3 b b + 1 2 b 3 b .

For the `gpathpermlex` order with  $\prec$  , this set of elements forms a Gröbner basis (Exercise 5.10; another explanation for that will be given in Example 6.3.3.5).

5.6.3 Symmetric operads as nonsymmetric operads

Every symmetric operad can be regarded as a nonsymmetric operad: we can not only forget about symmetric group actions, but also restrict ourselves to compositions

$$\gamma_{\{x_{k_1+1},\ldots,x_{k_1+n_1}\},\{x_{k_2+1},\ldots,x_{k_2+n_2}\},\ldots,\{x_{k_r+1},\ldots,x_{k_r+n_r}\}},$$

where $k_i = n_1 + \cdots + n_{i-1}$, that is precisely all nonsymmetric compositions $\gamma^{(r)}_{n_1,\ldots,n_r}$ from Definition 3.2.1.1. The corresponding nonsymmetric operad may still carry some information about the original operad, e.g., of its defining relations, or may go to a different end of the spectrum and end up being a free nonsymmetric operad on some set of generators. In this paragraph, we establish a criterion for that latter possibility, and prove that it holds for the operad Lie.

Definition 5.6.3.1 (Decomposable and prime tree monomials)**.** Let T be a shuffle tree monomial, v an internal vertex of the underlying tree of T, and T' the maximal subtree of T rooted at v. We say that T is *decomposable at v* if the set of leaf labels of T' form an interval in the set of leaf labels.

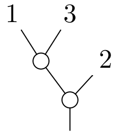
A tree monomial is said to be *prime* if there is no vertex v at which it is decomposable.

Theorem 5.6.3.2. *Let $\mathcal{P} = \mathcal{F}(\mathcal{X})/(\mathcal{R})$ be a shuffle operad for which all leading terms of its Gröbner basis $\mathcal{G}$ are prime tree monomials. Then $\mathcal{P}$ is free as a nonsymmetric operad.*

Proof. We leave it as an exercise to the reader (Exercise 5.12) to show that prime tree monomials that are reduced with respect to $\mathcal{G}$ freely generate $\mathcal{P}$ as a nonsymmetric operad; both the spanning property and the linear independence follow easily from the definition. □

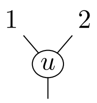
The following result was first proved in [221].

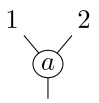
Theorem 5.6.3.3. *The operads* Lie *is free as a nonsymmetric operad.*

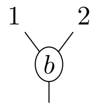
Proof. Let us consider the modification of `gpathpermlex` discussed in Example 5.4.1.11; we first compare the permutations lexicographically, and in the case when the permutations are equal, compare the path sequences. It is easy to check that the defining relation of Lie forms the reduced Gröbner basis of relations. The leading term 

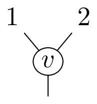
is clearly a prime tree monomial, so Theorem 5.6.3.2 applies. □

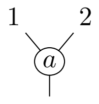
5.6.4 The operad PreLie as a Lie-module

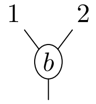
Example 5.6.4.1. Let us consider a different presentation of the operad PreLie, using its symmetric generator 

$=$ 

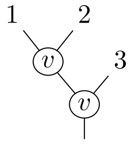
$+$ 

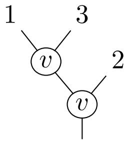
and its antisymmetric generator 

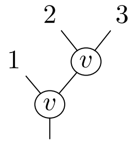
$=$ 

$+$ 

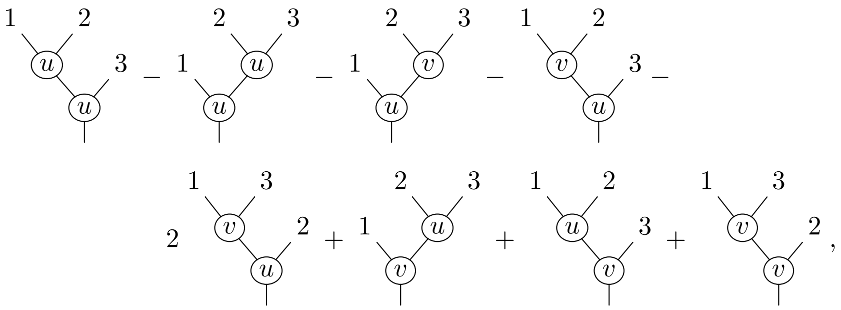
. It is easy to check (Exercise 5.16) that the defining relations of PreLie^f for this system of generators are



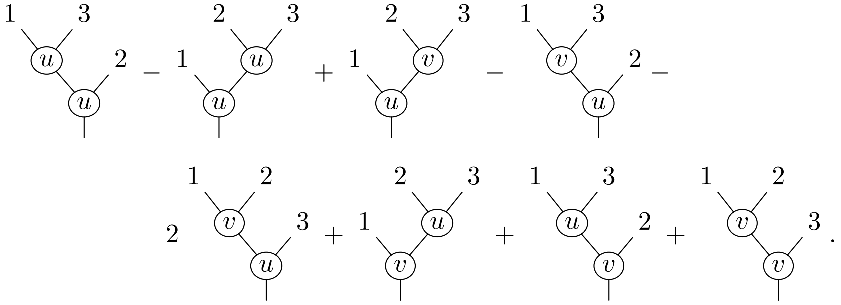
$-$ 

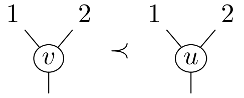
$-$ 

$= 0,$

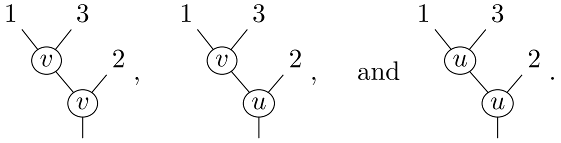


and



Let us consider the following monomial order. We set 

and modify the `gpathpermlex` order in a way that we first compare the permutations of leaves using the lexicographic order, and then compare the path sequences. The set of relations is not linearly self-reduced; after making it linearly self-reduced, the leading monomials of relations are the tree monomials



It is easy to see that both S-polynomials corresponding to common multiples of these tree monomials have reduced form zero. (Alternatively, a version of the argument from Example 6.3.3.5 can be used.) This provides a description of normal forms for elements of PreLie that has an interesting feature. Namely, let us denote by $\mathcal{M}$ the nonsymmetric collection spanned by reduced monomials for which the internal vertex of the underlying tree that is adjacent to the root is labelled u. Then the natural map

$$\mathsf{Lie}^f \circ_{\text{III}} \mathcal{M} \to \mathsf{PreLie}^f$$

is an isomorphism (Exercise 5.15). Since the forgetful functor is monoidal, this implies that there exists a symmetric subcollection $\mathcal{N} \subset \mathsf{PreLie}$ for which the natural map

$$\mathsf{Lie} \circ_{\Sigma} \mathcal{N} \to \mathsf{PreLie}$$

is an isomorphism. From this, it follows, for instance, that free pre-Lie algebras are free as Lie algebras [53].

5.7 Exercises

Exercise 5.1. Complete the proof of Proposition 5.2.1.4.

Exercise 5.2. Prove that the two definitions of a symmetric operad (Definitions 5.2.1.1 and 5.2.1.5) are equivalent.

Exercise 5.3. Prove Proposition 5.2.3.3.

Exercise 5.4. Our definitions of symmetric and shuffle operads adapt the classical definition of a nonsymmetric operad (Definition 3.2.1.1). Determine the axioms that adapt the partial definition of a nonsymmetric operad (Definition 3.2.2.3) in each of the cases.

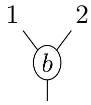
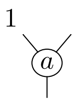
Exercise 5.5. Suppose that $\mathcal{X}(2)$ consists of one element $*$, and that $\mathcal{X}(n)$ is empty for $n \neq 2$. Write down the 15 tree monomials that form a basis in $\text{Ш}\mathrm{Tree}_{\mathcal{X}}(4)$.

Exercise 5.6. Fill in the details of the proof of Proposition 5.4.1.7.

Exercise 5.7. Prove Proposition 5.4.2.3. (*Hint*: modify the proof of Proposition 3.4.2.6.)

Exercise 5.8. Show that for each finite $\mathcal{S} \subset \mathcal{T}_{\text{Ш}}(\mathcal{X})$ Algorithm 5.4.2.18 terminates after finitely many steps.

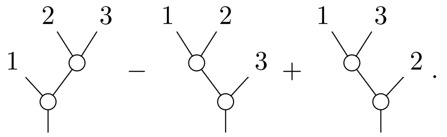
Exercise 5.9. Use Equation (5.4) and Proposition 5.4.2.10 to fill in the details of the proof of Theorem 5.5.1.4.

Exercise 5.10. For the `gpathpermlex` order with  $\prec$  , show that the defining relations of the operad PreLie (Example 5.6.2.1) forms a Gröbner basis.

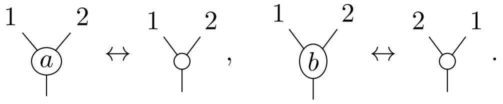
Exercise 5.11. Consider the symmetric collection $\mathcal{U}$ for which

$$\mathcal{U}(n) = \begin{cases} \mathbb{F}S_2, & n = 2, \\ 0, & n \neq 2. \end{cases}$$

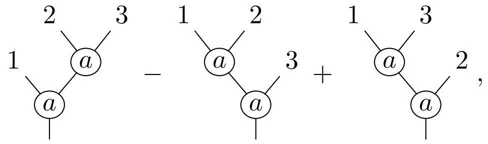
The symmetric operad Leib of (right) Leibniz algebras (first defined in [173]) is the quotient of $\mathcal{T}_\Sigma(\mathcal{U})$ by the ideal generated by the element

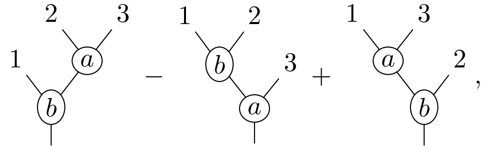


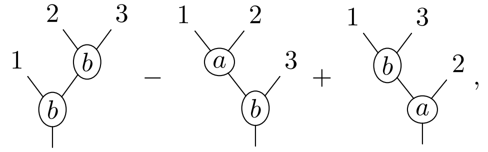
We can take the operation alphabet $\mathcal{X}$ for which $\mathcal{X}(2) = \{a, b\}$ and $\mathcal{X}(n)$ is empty for $n \neq 2$ as the basis collection for $\mathcal{U}^f$. We identify $\mathcal{X}$ with a basis of $\mathcal{U}^f$, which leads to identification of bases of $\mathcal{T}_{\text{Ш}}(\mathcal{X})(2)$ and $\mathcal{T}_\Sigma(\mathcal{U})^f(2)$ as follows:

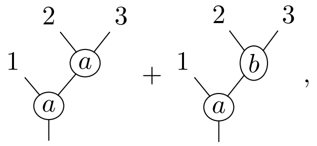


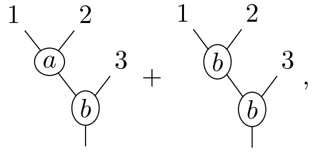
(i) Check that the ideal of relations of operad Leib^f is generated by the following elements:

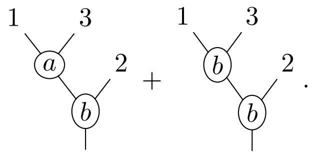










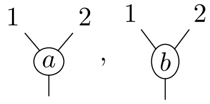


(ii) Pick an ordering of tree monomials, and compute the reduced Gröbner basis of Leib^f.

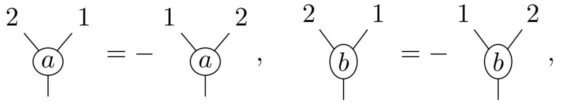
Exercise 5.12. Prove Theorem 5.6.3.2.

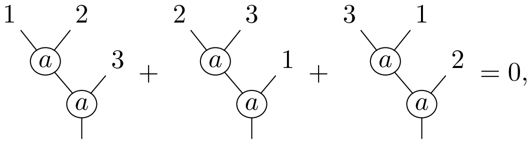
Exercise 5.13. Modify the proof of Theorem 5.6.3.3 to establish that the operad PreLie is free as a nonsymmetric operad.

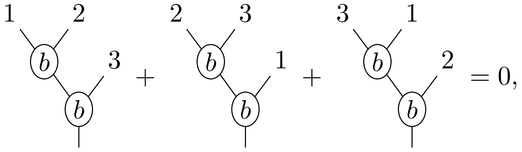
Exercise 5.14. The symmetric operad $\mathsf{Lie}^{\langle 2\rangle}$ (first defined in [73]) controls *linearly compatible Lie brackets*. It is a symmetric operad with two generators



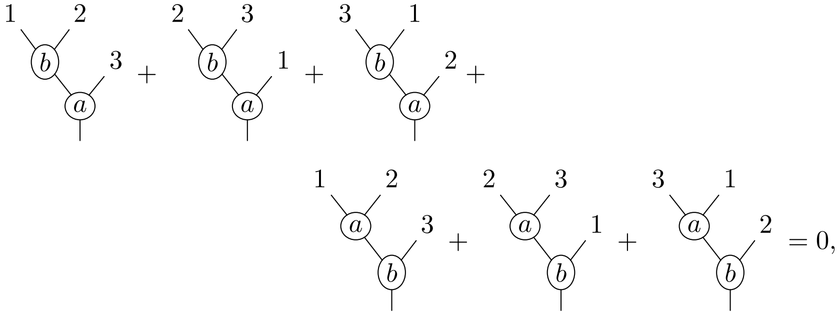
for which

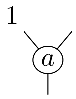


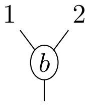




so these operations are Lie brackets, and



which implies that 

$+$ 

is also a Lie bracket. Modify the proof of Theorem 5.6.3.3 to establish that the operad $\mathsf{Lie}^{\langle 2\rangle}$ is free as a nonsymmetric operad.

Exercise 5.15. Use the Gröbner basis of the operad PreLie^f discussed in Example 5.6.4.1 to justify that the natural map

$$\mathsf{Lie}^f \circ_{\text{III}} \mathcal{M} \to \mathsf{PreLie}^f$$

is an isomorphism.

Exercise 5.16. Verify the claim on the defining relations of the operad PreLie^f from Example 5.6.4.1.

Exercise 5.17. Similarly to the way it is done for the operad PreLie^f in Example 5.6.4.1, one can consider the symmetric and antisymmetric generators for any operad with binary generators; this process is referred to as *polarization* in [185]. The most celebrated example is the symmetric associative operad Ass. It is well known (and probably first was observed in an unpublished manuscript of Livernet and Loday) that if we introduce, for the symmetric operad Ass, the new generators $[a_1, a_2] = a_1a_2 - a_2a_1$ and $a_1 \cdot a_2 = a_1a_2 + a_2a_1$, then the corresponding symmetric operad has the following defining relations:

$$\begin{gathered}[a_1,[a_2,a_3]] + [a_2,[a_3,a_1]] + [a_3,[a_1,a_2]] = 0,\\ [a_1 \cdot a_2, a_3] = a_1 \cdot [a_2,a_3] + [a_1,a_3] \cdot a_2,\\ (a_1 \cdot a_2) \cdot a_3 - a_1 \cdot (a_2 \cdot a_3) = [a_2,[a_1,a_3]].\end{gathered}$$

(i) Describe the shuffle operad obtained from the above presentation after applying the forgetful functor.

(ii) Find a monomial order for which the shuffle operad from part (i) has a quadratic Gröbner basis.

(iii) Prove in two different ways (using (ii) or, as an alternative, using Corollary 2.5.3.2) that the map $\mathsf{Lie} \to \mathsf{Ass}$ sending the generator of Lie to $[a_1, a_2] = a_1a_2 - a_2a_1$ is an embedding.

(iv) Show that the operation $a_1 \cdot a_2 = a_1a_2 + a_2a_1$ in every associative algebra satisfies the *multilinear Jordan identity*

$$\begin{aligned}&((a_1 \cdot a_2) \cdot a_3) \cdot a_4 + ((a_1 \cdot a_4) \cdot a_3) \cdot a_2 + a_1 \cdot ((a_2 \cdot a_4) \cdot a_3) =\\ &\quad ((a_1 \cdot a_2) \cdot (a_3 \cdot a_4)) + ((a_1 \cdot a_3) \cdot (a_2 \cdot a_4)) + ((a_1 \cdot a_4) \cdot (a_2 \cdot a_3)).\end{aligned}$$

(v) It turns out that the identity of (iv) does not generate the operadic ideal of the identities satisfied by the operation $a_1 \cdot a_2 = a_1a_2 + a_2a_1$; this was first discovered by Glennie [110, 111] who established that the lowest arity in which new identities appear is 8. Try to use operadic Gröbner bases to find identities in higher arities.

Exercise 5.18. Modify the argument of Example 5.6.4.1 to establish that there exists a symmetric subcollection $\mathcal{N} \subset \mathsf{Lie}^{\langle 2\rangle}$ for which the natural map

$$\mathsf{Lie} \circ_\Sigma \mathcal{N} \to \mathsf{Lie}^{\langle 2\rangle}$$

is an isomorphism.

Exercise 5.19. The *two-step Lie nilpotent associative operad* $\mathcal{N}_2\,\mathsf{Ass}$ is obtained from the symmetric operad Ass by imposing the relation $[[a_1, a_2], a_3]$ in its presentation from Exercise 5.17. In other words, this symmetric operad has a presentation

$$\begin{gathered}
[[a_1, a_2], a_3] = 0, \\
[a_1 \cdot a_2, a_3] = a_1 \cdot [a_2, a_3] + [a_1, a_3] \cdot a_2, \\
(a_1 \cdot a_2) \cdot a_3 - a_1 \cdot (a_2 \cdot a_3) = 0.
\end{gathered}$$

Prove that the dimension of the component $\mathcal{N}_2\,\mathsf{Ass}(n)$ is equal to 2^{n-1} over any ground field $\mathbb{F}$. (One possible strategy is to use Gröbner bases; it is possible to find an infinite Gröbner basis that has enough structure to be useful, see [71] for details. For other approaches to this operad, see [35, 79, 89, 92, 160, 166].)

Exercise 5.20. Consider the symmetric operad $\mathcal{Q}$ generated by a skew-symmetric binary operation $a_1, a_2 \mapsto [a_1, a_2]$ and a symmetric binary operation $a_1, a_2 \mapsto a_1 \cdot a_2$ subject to the following relations:

$$\begin{gathered}
[[a_1, a_2], a_3] + [[a_1, a_3], a_2] = 0, \\
[a_1 \cdot a_2, a_3] = a_1 \cdot [a_2, a_3] + [a_1, a_3] \cdot a_2, \\
(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3).
\end{gathered}$$

Prove that over any field $\mathbb{F}$ of characteristic different from two, $\dim \mathcal{Q}(n) = 2^n - n$. (Similarly to Exercise 5.19, one possible strategy is to use Gröbner bases; it is possible to find an infinite Gröbner basis that has enough structure to be useful, see [71] for details.)

Chapter 6

Operadic Homological Algebra and Gröbner Bases

Many natural examples of operads are operads whose components are chain complexes, or at least homologically graded vector spaces. In fact, there are two conceptually important sources of examples of that sort. Some algebraic operads, like the celebrated operad of Gerstenhaber algebras [100], are the homology operads of some operad whose components are topological spaces (and composition maps are continuous). Some other algebraic operads, like the operad of L_∞-algebras [227], or the operad of A_∞-algebras [241], are operads where classical identities, like the Jacobi identity, or associativity, are relaxed up to a system of coherent homotopies. This is crucial for the questions on homotopy categories of algebras over operads, a nonabelian analogue of the questions on derived categories of modules over algebras that we discussed in Theorem 2.1.2.3.

In many ways, the title of our book may be most applicable to this particular chapter, which we regard as a bridge that would assist someone with only very limited experience with homological and homotopical algebra in working through the book of Loday and Vallette [180], for which one of the main motivations is developing a range of methods specifically for operadic homological and homotopical algebra. A thorough reader will notice that the number of references to Loday and Vallette increases visibly in this chapter; the sole reason for this is to highlight important topics that can be made a bit more accessible by methods presented in our book.

6.1 Introduction

6.1.1 Symmetry isomorphisms and the Koszul sign rule

Definition 6.1.1.1 (Chain complexes and their morphisms)**.** The datum of a *chain complex* is a pair (V, d), where V is a sequence of vector spaces $\{V_i\}_{i\in\mathbb{Z}}$, and d, referred to as a *boundary map*, or the *differential* of V, is a sequence of maps $d_i\colon V_i \to V_{i-1}$ satisfying the condition $d_{i-1}d_i = 0$ for all i, which is usually abbreviated to $d^2 = 0$.[1]

Definition 6.1.1.2 (Homological degree of an element)**.** Let V be a chain complex. For an element $v \in V_i$, we say that the *homological degree* of v is equal to i, and write $|v| = i$.

Definition 6.1.1.3 (Homological degree of a map)**.** Let (V, d) and (V', d') be chain complexes. A *map of homological degree* k between V and V' is a sequence of maps $f_i\colon V_i \to V'_{i+k}$.

Example 6.1.1.4. The differential of a chain complex is a map from that chain complex to itself of degree -1.

The space of maps of homological degree k from (V, d) to (V', d') is conventionally denoted by $\mathrm{Hom}(V, V')_k$ (the boundary maps are implicit in this notation). Thus,

$$\mathrm{Hom}(V, V')_k = \prod_{i\in\mathbb{Z}} \mathrm{Hom}(V_i, V'_{i+k}).$$

The following proposition is well known.

Proposition 6.1.1.5. *The sequence of maps*

$$\delta_k\colon \mathrm{Hom}(V, V')_k \to \mathrm{Hom}(V, V')_{k-1}$$

defined by

$$(\delta_k f)_i(v) = d'_{i+k}(f_i(v)) - (-1)^k f_{i-1} d_i(v)$$

makes the sequence $\mathrm{Hom}(V, V')_k$ *a chain complex.*

Suppose that we consider the collection End_V for a chain complex V, rather than a vector space V. As everyone who ever took a basic course in homological algebra knows, this creates various signs in formulas. What often remains unexplained in those homological algebra courses is that all those signs come from one and only one change, the symmetry isomorphisms in tensor products.

Definition 6.1.1.6 (Koszul sign rule)**.** We adopt the following *Koszul sign rule convention*: for two chain complexes V and W, the isomorphism

$$\sigma_{V,W}\colon V \otimes W \to W \otimes V$$

depends on homological degrees of elements as follows:

$$\sigma_{V,W}(v \otimes w) = (-1)^{|v|\cdot|w|} w \otimes v.$$

[1] Henri Cartan, upon receiving the degree of *Doctor Honoris Causa* from the University of Oxford, said, in particular, "...if I could only understand the beautiful consequence following from the concise proposition $d^2 = 0$."

One of the origins of this definition is hidden in various computations in algebraic topology and differential geometry, where these signs take care of orientations of simplices when computing simplicial or singular cohomology, and are in a sense forced by wedge products of differential forms when computing the de Rham cohomology. A reader whose background is closer to varieties of algebras and representation theory would benefit from the observation that Koszul signs are closely related to the signs that are used when working with enveloping algebras of Lie superalgebras [11, 197, 199, 202]. Similarly, a reader whose background comes from geometry may recognize these signs from the context of superanalysis [16, 159, 171]. However, a conceptual leap that these readers must undertake is that throughout this chapter multilinear operations sometimes have nonzero degrees as well, and this creates extra signs that would not generally be visible in the conventional superalgebra and superanalysis contexts.

Algebraically, this definition means that there are “Koszul signs” in all formulas one writes down: whenever two objects are exchanged, this exchange creates a factor -1 if both objects are of odd homological degree. Consequences of that rule are easy to foresee in the case of formulas like $[a_1, a_2] = a_1a_2 - a_2a_1$; of course, such a formula must become $[a_1, a_2] = a_1a_2 - (-1)^{|a_1||a_2|}a_2a_1$ in this setting (since we change the order of the arguments a_1 and a_2). However, it takes more effort to handle the signs of composite multilinear operations in a consistent way. (In particular, a sizeable proportion of papers on operads, at least before the publication of [180], either did not make the signs explicit enough for concrete computations, or handled them with inaccuracies, ranging from minor to drastic; see Remark 6.3.1.8 below.) In order to have a consistent way to deal with signs, one has to view, for a multilinear operation $\omega \in \mathrm{End}_V(n)$ and n vectors $v_1, \dots, v_n \in V$, the result of evaluation $\omega(v_1, \dots, v_n)$ as the result of computing the evaluation map

$$\mathrm{End}_V(n) \otimes V^{\otimes n} \to V, \quad \omega \otimes v_1 \otimes \cdots \otimes v_n \mapsto \omega(v_1, \dots, v_n).$$

6.2 First instances of Koszul signs for graded operads

6.2.1 Determinant operad and operadic suspension

Prior to discussing the impact of signs on graded operads in general, let us consider a very important example of an operad which features in most formulas needed for operadic Koszul duality.

Definition 6.2.1.1 (Suspension symbol and determinant operad)**.** We consider a formal symbol s of homological degree 1, the *suspension variable*, and the *desuspension variable*, a formal symbol s^{-1} of homological degree -1. The vector space $\mathbb{F}s$ will be viewed as a chain complex with zero differential and the only nonzero component being the ground field $\mathbb{F}$ concentrated in degree 1. We define the *determinant operad* as the endomorphism operad of $\mathbb{F}s$:

$$\mathcal{S} := \mathrm{End}_{\mathbb{F}s}\,.$$

Later we will also use the operad denoted $\mathcal{S}^{-1}$:

$$\mathcal{S}^{-1} := \mathrm{End}_{\mathbb{F}s^{-1}}\,.$$

We will now consider an example of a computation in the determinant operad.

Example 6.2.1.2. Since the vector space $\mathbb{F}s$ is one-dimensional, each component $\mathcal{S}(n) = \mathrm{End}_{\mathbb{F}s}(n)$ is one-dimensional; it is spanned by the operation μ_n which is uniquely determined by the property $\mu_n(s^{\otimes n}) = s$; this property shows that $|\mu_n| = 1 - n$. Let us compare the two operations

$$\mu_2 \circ_1 \mu_2 \quad \text{and} \quad \mu_2 \circ_2 \mu_2.$$

We have

$$(\mu_2 \circ_1 \mu_2)(s \otimes s \otimes s) = \mu_2(\mu_2(s \otimes s), s) = s,$$
$$(\mu_2 \circ_2 \mu_2)(s \otimes s \otimes s) = -\mu_2(s, \mu_2(s \otimes s)) = -s.$$

The minus sign in the second line arises as follows: the evaluation of the composite map $\mu_2 \circ_2 \mu_2$ on $s \otimes s \otimes s$ is the result of applying two evaluation maps to an element $\mu_2 \otimes \mu_2 \otimes s \otimes s \otimes s$ of $\mathrm{End}_{\mathbb{F}s}(2) \otimes \mathrm{End}_{\mathbb{F}s}(2) \otimes (\mathbb{F}s)^{\otimes 3}$. For that particular composition, we should rewrite that tensor product as $\mathrm{End}_{\mathbb{F}s}(2) \otimes \mathbb{F}s \otimes \mathrm{End}_{\mathbb{F}s}(2) \otimes (\mathbb{F}s)^{\otimes 2}$, compute the evaluation map on the last three factors, and then compute the evaluation map again. The rewriting of the tensor product utilizes one symmetry isomorphism $\mathrm{id} \otimes \sigma_{\mathrm{End}_{\mathbb{F}s}(2),\mathbb{F}s} \otimes \mathrm{id} \otimes \mathrm{id}$, and since $\mathrm{End}_{\mathbb{F}s}(2)$ is concentrated in homological degree -1, a Koszul sign $(-1)^{(-1)\cdot 1} = -1$ arises.

Definition 6.2.1.3 (Suspension)**.** For every chain complex V, we define its *suspension* sV as $\mathbb{F}s \otimes V$.

Example 6.2.1.4. As we saw above, in $\mathrm{End}_{\mathbb{F}s}$ we have

$$\delta_2 \circ_1 \delta_2 + \delta_2 \circ_2 \delta_2 = 0.$$

Moreover, we have $\delta_2 \circ_1 \delta_2 = \delta_3$, and more generally $\delta_n \circ_1 \delta_m = \delta_{n+m-1}$. From this, it easily follows that the nonsymmetric operad $\mathrm{End}_{\mathbb{F}s}$ is generated by one binary operation μ of degree -1 subject to the relation

$$\mu \circ_1 \mu + \mu \circ_2 \mu = 0.$$

We leave it as an exercise for the reader (Exercise 6.2). Note that for an operation ν of degree 0, the property $\nu \circ_1 \nu + \nu \circ_2 \nu = 0$ is usually referred to as the *antiassociative law* [186]; this law does not have specific "nice" properties. However, as we see now, for an operation of degree -1 this is rather a *suspended associative law*; it shows an algebraic property that emerges if we have the associative property on a vector space V, and then use it to define a binary operation on the vector space sV.

6.2.2 Koszul signs in axioms of an operad

The examples we just considered should convince the reader that various signs tend to arise from applying operations to arguments, and those signs can be recovered easily from the respective evaluation maps $\mathrm{End}_V(n) \otimes V^{\otimes n} \to V$. It is possible to avoid these signs almost completely by writing algebraic identities without arguments, and only recalling signs arising from evaluations when absolutely necessary. However, there is one more important source of signs that remains; this source will feature quite prominently in our computations of this chapter.

Proposition 6.2.2.1. *Suppose that V is a homologically graded chain complex. For all $\alpha \in \mathrm{End}_V(n)$, $\beta \in \mathrm{End}_V(m)$, $\gamma \in \mathrm{End}_V(r)$, we have*

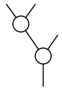
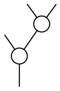
$$(\alpha \circ_i \beta) \circ_j \gamma = \begin{cases} \alpha \circ_i (\beta \circ_{j-i+1} \gamma), & i \leq j \leq i+m-1, \\ (-1)^{|\beta||\gamma|} (\alpha \circ_j \gamma) \circ_{i+r-1} \beta, & 1 \leq j \leq i-1, \\ (-1)^{|\beta||\gamma|} (\alpha \circ_{j-m+1} \gamma) \circ_i \beta, & i+m \leq j \leq n+m-1. \end{cases}$$

The first formula here is identical to the sequential axiom (*Equation* (3.3))*, while the two other formulas differ from the parallel axioms* (*Equation* (3.4)) *by signs.*

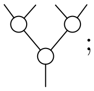
Proof. The respective evaluation operations require, in addition to rearranging arguments of operations, swapping β with γ, hence the sign. □

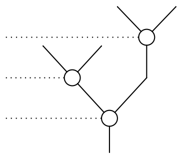
These formulas altogether are precisely what one has to use when defining nonsymmetric operads whose components are homologically graded vector spaces. This does not affect any results on free operads and normal forms with the exception of the fact that we always have to pick, among many ways to draw a tree monomial in the plane, a particular choice where all vertices have different levels.

Definition 6.2.2.2 (Levelization of a tree)**.** Let τ be a planar tree. A *levelization* of τ is a total order of internal vertices of τ which extends the partial order $v \prec v'$ if v belongs to the path from the root to v'.

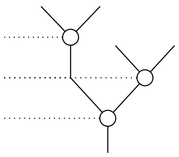
Example 6.2.2.3. For each of the binary trees  and , there is a unique levelization, since the partial order above is already a total order.

Once a choice of a levelization of a planar tree τ is made, a tree monomial whose underlying tree is τ is defined precisely, and not up to a sign. A "local" change of the choice of levels (swapping the order of two vertices with the same parent, see Equation (3.2)) now comes, according to the formulas above, at a cost of the sign $(-1)^{|\beta||\gamma|}$.

Example 6.2.2.4. The smallest binary tree for which there is no obvious choice of levels is ; the two possible choices of levelization correspond to the following two ways of drawing that tree:



and



.

There is another important difference to have in mind. When components of the given operad are chain complexes, it makes sense to require the differentials to be compatible with the operad structure. This leads to the definition of a differential graded operad.

Definition 6.2.2.5 (Differential graded operad)**.** A symmetric operad $\mathcal{P}$ whose components are chain complexes is called a *differential graded operad* if the differentials of its components are equivariant with respect to the symmetric group actions and agree with the operad compositions:

$$d(\alpha \circ_i \beta) = d(\alpha) \circ_i \beta + (-1)^{|\alpha|} \alpha \circ_i d(\beta).$$

In the examples that follow, we will use partial compositions, not trees, to represent monomials in the free operad. There are two main reasons for that: in both cases, we will deal with operations with many arguments, and, on the second occasion, infinitely many relations emerge; in such situations, writing formulas is much easier to handle than drawing pictures, especially when keeping track of levels is required.

6.2.3 Totally associative operad

Let us start with a toy model where it becomes very clear how signs emerge when computing Gröbner bases.

Definition 6.2.3.1 (Graded totally associative operad)**.** Let $N \geq 2$. The *totally associative N-ary operad in degree d*, denoted $\mathsf{tAs}_d^{(N)}$, is the nonsymmetric operad with one generator μ of arity N and homological degree d, and relations

$$\mu \circ_p \mu = \mu \circ_N \mu \quad \text{for all} \quad p \leq N-1.$$

We will now apply the Buchberger algorithm to the operad $\mathsf{tAs}_d^{(N)}$ using the `gpathlex` order. From the common multiple

$$(\mu \circ_1 \mu) \circ_1 \mu = \mu \circ_1 (\mu \circ_1 \mu)$$

of the leading monomial $\mu \circ_1 \mu$ with itself, we compute the S-polynomial

$$(\mu \circ_N \mu) \circ_1 \mu - \mu \circ_1 (\mu \circ_N \mu).$$

We can perform the following chain of reductions (with leading monomials underlined):

$$\begin{gathered}
(\mu \circ_N \mu) \circ_1 \mu - \underline{\mu \circ_1 (\mu \circ_N \mu)} = \\
(\mu \circ_N \mu) \circ_1 \mu - \underline{(\mu \circ_1 \mu) \circ_N \mu} \longmapsto \underline{(\mu \circ_N \mu) \circ_1 \mu} - (\mu \circ_N \mu) \circ_N \mu = \\
(-1)^{d^2} \underline{(\mu \circ_1 \mu) \circ_{2N-1} \mu} - (\mu \circ_N \mu) \circ_N \mu \longmapsto (-1)^{d^2} (\mu \circ_N \mu) \circ_{2N-1} \mu - \\
\underline{(\mu \circ_N \mu) \circ_N \mu} = (-1)^{d^2} (\mu \circ_N \mu) \circ_{2N-1} \mu - \underline{\mu \circ_N (\mu \circ_1 \mu)} \longmapsto \\
(-1)^{d^2} (\mu \circ_N \mu) \circ_{2N-1} \mu - \mu \circ_N (\mu \circ_N \mu) = \\
((-1)^{d^2} - 1)(\mu \circ_N \mu) \circ_{2N-1} \mu.
\end{gathered}$$

In this computation, the only time that we used Koszul signs was the parallel composition axiom

$$(\mu \circ_N) \circ_1 \mu = (-1)^{d^2} (\mu \circ_1 \mu) \circ_{2N-1} \mu.$$

We observe that for even d, the corresponding S-polynomial has the reduced form zero, while for odd d, the monomial $(\mu \circ_N \mu) \circ_{2N-1} \mu$ cannot be reduced further, and we recover the relation $(\mu \circ_N \mu) \circ_{2N-1} \mu = 0$ discovered in [186]. We leave it to the reader to complete the computation of the reduced Gröbner basis, depending on d and N (Exercise 6.3).

6.2.4 Normal forms and higher Koszul duality

In this section, we will explain, following [78], how to use normal forms for nonsymmetric operads and algebras over nonsymmetric operads to obtain some results relevant in higher Koszul duality for associative algebras. Let us recall basics of the N-homogeneous Koszul duality which originates in [19].

Definition 6.2.4.1 (N-homogeneous dual algebra)**.** Let V be a finite-dimensional space, and let $A = T(V)/(R)$ be an N-homogeneous algebra, that is an associative algebra with $R \subset V^{\otimes N}$. The *N-homogeneous dual algebra $A^\vee$* of A is defined by the formula

$$A^\vee := T(V^*)/(R^\perp),$$

where $R^\perp \subset (V^*)^{\otimes N}$ is the annihilator of R under the natural pairing of vector spaces $(V^*)^{\otimes N} \otimes V^{\otimes N} \to \mathbb{F}$.

At this stage, the reader can recall Definition 2.1.2.1, according to which for $N = 2$ the algebra $A^\vee$ is denoted by $A^!$ and called the Koszul dual algebra of A. However, in the case $N > 2$, only some of the homogeneous components of $A^\vee$ are used for purposes of homological and homotopical algebra, that is, in defining higher analogues of the Koszul complex.

Definition 6.2.4.2 (N-homogeneous Koszul dual syzygy space)**.** We define the graded vector space $A^!$, the *Koszul dual syzygy space* of A, by the formula

$$A^!_m := \begin{cases} A^\vee_m, & m \equiv 0, 1 \pmod N, \\ 0, & \text{otherwise,} \end{cases}$$

where in addition to being of weight m, $A^\vee_m$ is assigned the homological degree $\frac{2m}{N}$ if $m \equiv 0 \pmod N$ and the homological degree $\frac{2(m-1)}{N} + 1$ is $m \equiv 1 \pmod N$.

It turns out that for a general $N > 2$ there are two meaningful operations on the Koszul dual syzygy space [126].

Definition 6.2.4.3 (N-homogeneous Koszul dual algebra)**.** The associative product on $A^\vee$ induces operations μ_2 and μ_N on $A^!$ as follows. We let

$$\mu_2 \colon \begin{cases} {A^!}_{iN} \otimes {A^!}_{jN} \cong {A^\vee}_{iN} \otimes {A^\vee}_{jN} \to {A^\vee}_{(i+j)N} \cong {A^!}_{(i+j)N}, \\ {A^!}_{iN+1} \otimes {A^!}_{jN} \cong {A^\vee}_{iN+1} \otimes {A^\vee}_{jN} \to {A^\vee}_{(i+j)N+1} \cong {A^!}_{(i+j)N+1}, \\ {A^!}_{iN} \otimes {A^!}_{jN+1} \cong {A^\vee}_{iN} \otimes {A^\vee}_{jN+1} \to {A^\vee}_{(i+j)N+1} \cong {A^!}_{(i+j)N+1}, \end{cases}$$

$$\begin{aligned} \mu_N \colon {A^!}_{k_1N+1} \otimes \cdots \otimes {A^!}_{k_NN+1} &\cong {A^\vee}_{k_1N+1} \otimes \cdots \otimes {A^\vee}_{k_NN+1} \\ &\to {A^\vee}_{(k_1+\cdots+k_N+1)N} \cong {A^!}_{(k_1+\cdots+k_N+1)N} \end{aligned}$$

be derived from the product in $A^\vee$, and let these operations be zero for all other choices of arguments. With these operations, the space $A^!$ is called the *Koszul dual algebra* of A.

In [78], the full system of identities satisfied by the operations μ_2 and μ_N independently of the algebra A was determined. Let us explain and prove that result.

Definition 6.2.4.4 (The operad $\mathcal{NA}_{2,N}$)**.** The nonsymmetric operad $\mathcal{NA}_{2,N}$ is the quotient of the free nonsymmetric operad generated by a binary operation μ_2 of homological degree 0 and an N-ary operation μ_N of homological degree $2 - N$ modulo the ideal generated by the $N + 2$ elements

$$\mu_2 \circ_1 \mu_2 - \mu_2 \circ_2 \mu_2, \tag{6.1}$$

$$\mu_2 \circ_1 \mu_N + (-1)^{N-1} \mu_2 \circ_2 \mu_N + \sum_{i=1}^{N} (-1)^{i-1+N} \mu_N \circ_i \mu_2, \tag{6.2}$$

$$\mu_N \circ_i \mu_N, \quad \text{for } \; i = 1, \ldots, N \, . \tag{6.3}$$

Let us define an order of the space of generators by putting $\mu_N \prec \mu_2$, and consider the corresponding `gpathlex` order. It turns out that the reduced Gröbner basis of the operad $\mathcal{NA}_{2,N}$ is infinite but manageable. To state the result, let us introduce the following operations $\mu_2^{(k)} \in \mathcal{T}(\mu_2, \mu_N)(k{+}1)$ defined inductively:

$$\mu_2^{(0)} = \mathrm{id}, \qquad \mu_2^{(k+1)} = \mu_2 \circ_2 \mu_2^{(k)}.$$

In other words, such an operation is a right-normed product made of k copies of μ_2.

Theorem 6.2.4.5. *The reduced Gröbner basis of the operad $\mathcal{NA}_{2,N}$ is obtained by adjoining to its generators* (6.1)*,* (6.2)*, and* (6.3) *the elements*

$$R_{i,k} := \mu_N \circ_i (\mu_2^{(k)} \circ_{k+1} \mu_N) - (-1)^{N(i-1)} (\mu_N \circ_N (\mu_2 \circ_2 \mu_N)) \circ_i \mu_2^{(k-1)} \quad (6.4)$$

for each $k \geq 1$ and for each $i = 1, \ldots, N-1$.

Proof. By Theorem 3.5.1.6, it is enough to prove that all S-polynomials coming from overlaps of leading terms of the listed elements can be reduced to zero. We will prove it by doing explicit computations in low arities, and outlining how further computations are modeled on those for low arities.

The leading term $\mu_2 \circ_1 \mu_2$ of (6.1) has a nontrivial small common multiple with itself; the resulting S-polynomial can be reduced to zero using just that relation (see Example 3.6.1.1 where we checked exactly that statement). The S-polynomial that arises from the small common multiple of the leading terms $\mu_2 \circ_1 \mu_2$ and $\mu_2 \circ_1 \mu_N$ of (6.1) and (6.2), respectively, can as well be reduced to zero using only those relations and nothing else; this is a result of a more tedious but very straightforward computation. However, the leading term $\mu_2 \circ_1 \mu_N$ of the relation (6.2) forms n small common multiples with the relations $\mu_N \circ_i \mu_N$, and the corresponding S-polynomials cannot be reduced using only the defining relations of the operad $\mathcal{NA}_{2,N}$; that is where new elements of the reduced Gröbner basis start showing up.

For the small common multiple $(\mu_2 \circ_1 \mu_N) \circ_1 \mu_N = \mu_2 \circ_1 (\mu_N \circ_1 \mu_N)$ the corresponding S-polynomial can be, using the relations $\mu_N \circ_i \mu_N = 0$, reduced to

$$\begin{aligned}
&(-1)^N (\mu_2 \circ_2 \mu_N) \circ_1 \mu_N - (\mu_N \circ_1 \mu_2) \circ_1 \mu_N \\
&\qquad = (-1)^{N+N^2} (\mu_2 \circ_1 \mu_N) \circ_{N+1} \mu_N - \mu_N \circ_1 (\mu_2 \circ_1 \mu_N) \\
&\qquad \to (-1)^N (\mu_N \circ_N \mu_2) \circ_{N+1} \mu_N - (-1)^N (\mu_N \circ_1 \mu_2) \circ_2 \mu_N \\
&\qquad\qquad = (-1)^N \mu_N \circ_N (\mu_2 \circ_2 \mu_N) - (-1)^N \mu_N \circ_1 (\mu_2 \circ_2 \mu_N),
\end{aligned}$$

where the first equality comes from the parallel and the sequential composition properties of nonsymmetric operads, the second one is the computation of the reduced forms using only the defining relations (6.2) and (6.3), and the last equality comes from the sequential composition properties; the end result is proportional to the element $R_{1,1}$.

For $1 < i \leq N$, the small common multiple

$$(\mu_2 \circ_1 \mu_N) \circ_i \mu_N = \mu_2 \circ_1 (\mu_N \circ_i \mu_N)$$

gives rise to the S-polynomial

$$\mu_N \circ_{i-1} (\mu_2 \circ_2 \mu_N) - \mu_N \circ_i (\mu_2 \circ_1 \mu_N). \tag{6.5}$$

If we are only allowed to use the defining relations of the operad, then the reduced form of this element is

$$\mu_N \circ_{i-1} (\mu_2 \circ_2 \mu_N) - (-1)^N \mu_N \circ_i (\mu_2 \circ_2 \mu_N). \tag{6.6}$$

However, this reduced form is precisely $R_{i-1,1} - (-1)^N R_{i,1}$, so it can be reduced to zero. The S-polynomials corresponding to the small common multiples of the monomial relations $\mu_N \circ_i \mu_N = 0$ and $\mu_N \circ_j \mu_N = 0$ are trivially zero, so there is nothing to check.

All the S-polynomials corresponding to the small common multiples of the leading monomials of the defining relations have now been treated. Let us now study the small common multiples of the leading monomials of the defining relations with the leading terms of elements (6.4).

All the small common multiples of the leading monomial of the elements $R_{i,1}$ with the monomial relations $\mu_N \circ_j \mu_N$ can be easily reduced to zero without using any new elements. The same is true for the small common multiple

$$(\mu_N \circ_i (\mu_2 \circ_2 \mu_N)) \circ_i \mu_N = (-1)^{N^2} (\mu_N \circ_i ((\mu_2 \circ_1 \mu_N) \circ_{N+1} \mu_N))$$

of the leading monomial of $R_{i,1}$ with the leading monomial of (6.2).

It is also easy to see that no new elements are needed to reduce all the S-polynomials arising from the small common multiples of the leading monomials of the elements $R_{i,1}$ and $R_{j,1}$. Indeed, there are two combinatorially different kinds of small common multiples of that sort. The small common multiple

$$(\mu_N \circ_i (\mu_2 \circ_2 \mu_N)) \circ_{j+N} (\mu_2 \circ_2 \mu_N) = (-1)^{N^2} (\mu_N \circ_j (\mu_2 \circ_2 \mu_N)) \circ_i (\mu_2 \circ_2 \mu_N)$$

for $1 \leq i < j \leq N-1$ leads to the S-polynomial

$$\begin{multline*}(-1)^{N(i-1)} (\mu_N \circ_N (\mu_2 \circ_2 \mu_N)) \circ_{j+N} (\mu_2 \circ_2 \mu_N) \\ - (-1)^{N+N(j-1)} (\mu_N \circ_N (\mu_2 \circ_2 \mu_N)) \circ_i (\mu_2 \circ_2 \mu_N),\end{multline*}$$

which can be reduced to zero using the elements $R_{k,1}$ for various k. The small common multiple

$$(\mu_N \circ_i (\mu_2 \circ_2 \mu_N)) \circ_{i+j} (\mu_2 \circ_2 \mu_N) = \mu_N \circ_i (\mu_2 \circ_2 (\mu_N \circ_j (\mu_2 \circ_2 \mu_N)))$$

for $1 \leq i \leq j \leq N-1$ leads to the S-polynomial

$$\begin{multline*}(-1)^{N(i-1)} (\mu_N \circ_N (\mu_2 \circ_2 \mu_N)) \circ_{i+j} (\mu_2 \circ_2 \mu_N) \\ - (-1)^{N(j-1)} \mu_N \circ_i (\mu_2 \circ_2 (\mu_N \circ_N (\mu_2 \circ_2 \mu_N))),\end{multline*}$$

where the second term is immediately reduced to

$$(-1)^{N(j-1)+N(i-1)+N(i-1)}\mu_N \circ_N (\mu_2 \circ_2 (\mu_N \circ_N (\mu_2 \circ_2 \mu_N))) =$$
$$= (-1)^{N(j-1)}\mu_N \circ_N (\mu_2 \circ_2 (\mu_N \circ_N (\mu_2 \circ_2 \mu_N))),$$

using the relation $R_{i,1}$ twice, while the first term is reduced to the same result through a lengthier sequence of reductions (depending on $i+j$ being less than, equal to, or greater than N).

The small common multiple $(\mu_N \circ_i (\mu_2 \circ_2 \mu_N)) \circ_i \mu_2$ of the leading monomial of the relation $R_{i,1}$ with the leading monomial of the left-hand side of (6.1) creates an S-polynomial that can be reduced to $R_{i,2}$, and hence can be reduced to zero using our candidate for the reduced Gröbner basis.

The last computation at this stage is that for the S-polynomial coming from yet another small common multiple of the leading monomials of the elements $R_{i,1}$ and (6.2), that is

$$\mu_2 \circ_1 (\mu_N \circ_i (\mu_2 \circ_2 \mu_N)) = (\mu_2 \circ_1 \mu_N) \circ_i (\mu_2 \circ_2 \mu_N).$$

This S-polynomial can be reduced completely using the defining relations of the operad $\mathcal{NA}_{2,N}$ and the elements $R_{i,1}$ and $R_{i,2}$.

The way the elements $R_{i,3}$, etc., arise is similar, and our system of elements can be shown to be sufficient to reduce to zero all arising S-polynomials. □

Corollary 6.2.4.6. *Normal monomials for the operad $\mathcal{NA}_{2,N}$ can be described as follows. The identity map* id $\in \mathcal{NA}_{2,N}(1)$ *is normal, and for every normal monomial b, the monomial $\mu_2 \circ_2 b$ is normal and also the monomial*

$$\mu_N \circ (\mu_2^{(i_1)}, \mu_2^{(i_2)}, \dots, \mu_2^{(i_{N-1})}, \mu_2 \circ_2 b)$$

is normal for each choice of nonnegative integers $i_1, \dots, i_{N-1}$. Each normal monomial is obtained from id *by repeated application of these rules.*

Let us now pair Theorem 6.2.4.5 with the approach to normal forms in algebras over nonsymmetric operads from Section 3.7 to study certain $\mathcal{NA}_{2,N}$-algebras arising in higher Koszul duality for associative algebras.

Proposition 6.2.4.7 ([78])**.** *The Koszul dual algebra of any N-homogeneous algebra A equipped with the operations μ_2 and μ_N is an $\mathcal{NA}_{2,N}$-algebra.*

Theorem 6.2.4.8. *For each N-homogeneous algebra A, we have an isomorphism of $\mathcal{NA}_{2,N}$-algebras*

$$A^! \cong \mathcal{NA}_{2,N}(V^*)/(\mu_2(V^*, V^*), \mu_N(R^\perp)), \tag{6.7}$$

where $\mu_N(R^\perp)$ is viewed as a subspace of $\mu_N(V^*, V^*, \dots, V^*)$.

Proof. Let us first examine the case $R = V^{\otimes N}$. In this case, the algebra $D := \mathcal{NA}_{2,N}(V^*)/(\mu_2(V^*, V^*))$ on the right-hand side of (6.7) is "the biggest possible": all the algebras appearing on the right-hand side for various R are quotients of D.

Lemma 6.2.4.9. *The statement of Theorem 6.2.4.8 is true for $R = V^{\otimes N}$.*

Proof. We will use Theorem 3.7.1.4, and study the corresponding extension $\mathcal{NA}_{2,N} \ltimes D$ of the operad $\mathcal{NA}_{2,N}$. If we fix some basis $e_1, \ldots, e_k$ of V^*, the relations we need to adjoin to the defining relations of $\mathcal{NA}_{2,N}$ in order to obtain a presentation of the extension are $\mu_2(e_i, e_j) = 0$. Similarly to what we saw in Section 3.7.2, the small common multiple of the associativity relation (6.1) and the new relation $\mu_2(e_i, e_j) = 0$ produces the relation $\mu_2(e_i, \mu_2(e_j, \mathrm{id})) = 0$. This extra relation has no small common multiples with the other relations.

Applying Theorem 3.7.1.4, in the view of Theorem 6.2.4.5 and Corollary 6.2.4.6, we immediately conclude that a basis for the algebra D can be defined inductively as follows. It has elements of two types, which we call even and odd; all generators $e_1, \ldots, e_k$ are odd basis elements, and we have the following rules of forming new elements:

- for each odd basis element b, and for all $1 \leq i_1, \ldots, i_{N-1} \leq k$, the element $\mu_N(e_{i_1}, e_{i_2}, \ldots, e_{i_{N-1}}, b)$ is an even basis element;

- for each even basis element b, and all $1 \leq j \leq k$, the element $\mu_2(e_j, b)$ is an odd basis element.

In particular, this algebra has nonzero elements only of weight divisible by N or congruent to 1 modulo N, and for each such weight there exists exactly one type of basis element of that weight. Combinatorially, the corresponding trees are alternating "towers" of operations with all the compositions using the last slot of operations only. This gives a vector space identification of

$$D \cong V^* \oplus \mu_N(V^*, \ldots, V^*) \oplus (\mu_2 \circ_2 \mu_N)(V^*, \ldots, V^*) \oplus \cdots$$

with the Koszul dual algebra

$$A^! = V^* \oplus V^{*\otimes N} \oplus V^{*\otimes (N+1)} \oplus \cdots$$

of the algebra $A = T(V)/(V^{\otimes N})$. Comparing the operations of D with those of Definition 6.2.4.3, we see that the corresponding $\mathcal{NA}_{2,N}$-algebras are isomorphic. □

Let us return to the case of a general set of relations R. In the proof of Lemma 6.2.4.9 above, for the case of the algebra D corresponding to $R = V^{\otimes N}$, we obtained a basis where we alternate the operations μ_2 and μ_N, computing all compositions at the last slot, and then substitute into the resulting operation an arbitrary word in $e_1, \ldots, e_k$. Now, the defining relation (6.2), together with the vanishing of all the elements (6.4), (6.5), and (6.6) mean that in our alternating towers, the only operation we plug in at each level can be freely moved between the slots.

If we now impose the additional relations $\mu_N(R^\perp) = 0$ and use the identification $D \cong V^* \oplus V^{*\otimes N} \oplus V^{*\otimes (N+1)} \oplus \cdots$ discussed above, it becomes clear that the underlying vector space of $\mathcal{NA}_{2,N}(V^*)/(\mu_2(V^*, V^*), \mu_N(R^\perp))$

is a quotient of $A^!$. However, from Definition 6.2.4.3 and Proposition 6.2.4.7 it is apparent that $A^!$ is an $\mathcal{NA}_{2,N}$-algebra in which the relations $\mu_2(V^*, V^*) = 0$ and $\mu_N(R^\perp) = 0$ are satisfied, so it is a quotient of $\mathcal{NA}_{2,N}(V^*)/(\mu_2(V^*, V^*), \mu_N(R^\perp))$, which is the universal algebra in which these relations are satisfied. Since V is assumed finite-dimensional, the weight graded components of these algebras are finite-dimensional spaces, and existence of surjections in both directions is sufficient to conclude that the algebras are isomorphic. This completes the proof of Theorem 6.2.4.8. □

6.3 Koszul duality for operads

We recall the basics of Koszul duality for operads. We deal specifically with the case of symmetric operads. The cases of nonsymmetric and shuffle operads are analogous, and just require to replace free symmetric operads by free nonsymmetric / shuffle operads; we discuss a couple of examples of those below.

In Section 5.2.2 we recalled an explicit construction, for a symmetric collection $\mathcal{V}$, of the free symmetric operad $\mathcal{T}_\Sigma(\mathcal{V})$. It is spanned by tree tensors, and has appropriate composition products. A notion dual to the notion of an operad is that of a *cooperad*; it is essentially a symmetric collection $\mathcal{C}$ together with a coassociative map $\mathcal{C} \to \mathcal{C} \circ_\Sigma \mathcal{C}$ (plus a counit satisfying appropriate conditions). For a symmetric collection $\mathcal{V}$, the cofree conilpotent operad generated by $\mathcal{V}$, denoted $\mathcal{T}^c_\Sigma(\mathcal{V})$, has the same underlying collection as $\mathcal{T}(\mathcal{V})$, but different structure, a "decomposition coproduct".

Let us denote by $\mathcal{T}_\Sigma(\mathcal{V})^{(k)}$ the collection of tree tensors of weight k, that is, tree tensors whose underlying trees have k internal vertices.

6.3.1 Quadratic operads and cooperads

Definition 6.3.1.1 (Quadratic operad and cooperad)**.** Let $\mathcal{V}$ be a symmetric collection, and $\mathcal{R} \subset \mathcal{T}_\Sigma(\mathcal{V})^{(2)}$ be a subcollection. We will call the pair $(\mathcal{V}, \mathcal{R})$ *quadratic data.* To a choice of quadratic data one can associate the *quadratic operad with generators* $\mathcal{V}$ *and relations* $\mathcal{R}$,

$$\mathcal{P} = \mathcal{P}(\mathcal{V}, \mathcal{R}) := \mathcal{T}_\Sigma(\mathcal{V})/(\mathcal{R}).$$

In other words, $\mathcal{P}(\mathcal{V}, \mathcal{R})$ is the largest quotient operad $\mathcal{O}$ of $\mathcal{T}_\Sigma(\mathcal{V})$ for which the composite

$$\mathcal{R} \hookrightarrow \mathcal{T}_\Sigma(\mathcal{V})^{(2)} \hookrightarrow \mathcal{T}_\Sigma(\mathcal{V}) \twoheadrightarrow \mathcal{O}$$

is zero. Also, to a choice of quadratic data one can associate the *quadratic cooperad with cogenerators* $\mathcal{V}$ *and corelations* $\mathcal{R}$

$$\mathcal{Q} = \mathcal{Q}(\mathcal{V}, \mathcal{R}),$$

the largest subcooperad $\mathcal{C} \subset \mathcal{T}^c_\Sigma(\mathcal{V})$ for which the composite

$$\mathcal{Q} \hookrightarrow \mathcal{T}^c_\Sigma(\mathcal{V}) \twoheadrightarrow \mathcal{T}^c_\Sigma(\mathcal{V})^{(2)} \twoheadrightarrow \mathcal{T}^c_\Sigma(\mathcal{V})^{(2)}/\mathcal{R}$$

is zero.

The most elegant and conceptual way to handle Koszul duality is to have a duality between operads and cooperads [180].

Definition 6.3.1.2 (Koszul duality between operads and cooperads)**.** Let $(\mathcal{V}, \mathcal{R})$ be a choice of quadratic data. The Koszul duality for operads assigns to an operad $\mathcal{P} = \mathcal{P}(\mathcal{V}, \mathcal{R})$ its *Koszul dual cooperad*

$$\mathcal{P}^{¡} := \mathcal{Q}(s\mathcal{V}, s^2\mathcal{R}),$$

and to a cooperad $\mathcal{Q} = \mathcal{Q}(\mathcal{V}, \mathcal{R})$ its *Koszul dual operad*

$$\mathcal{Q}^{¡} := \mathcal{P}(s^{-1}\mathcal{V}, s^{-2}\mathcal{R}).$$

However, it is commonly acknowledged that psychologically it is somewhat harder to work with cooperads than with operads, so we will also present a definition that only uses operads, by passing to dual vector spaces whenever working with operads. For that, however, one important notion should be introduced.

Definition 6.3.1.3 (Hadamard product of symmetric collections)**.** Let $\mathcal{V}$ and $\mathcal{W}$ be two symmetric collections. The *Hadamard product* $\mathcal{V} \underset{\mathrm{H}}{\otimes} \mathcal{W}$ is the following symmetric collection:

$$(\mathcal{V} \underset{\mathrm{H}}{\otimes} \mathcal{W})(n) := \mathcal{V}(n) \otimes \mathcal{W}(n),$$

with the diagonal symmetric group action.

Definition 6.3.1.4 (Operadic suspension)**.** The *operadic suspension* of a (symmetric or nonsymmetric) collection of chain complexes $\mathcal{L}$ is the Hadamard tensor product with $\mathcal{S}$:

$$\mathcal{S}\mathcal{L} := \mathcal{S} \underset{\mathrm{H}}{\otimes} \mathcal{L}.$$

Definition 6.3.1.5. Let $\mathcal{P}$ be a quadratic operad. Its *Koszul dual operad* is the operad

$$\mathcal{P}^! := (\mathcal{S}^c \underset{\mathrm{H}}{\otimes} \mathcal{P}^{¡})^*.$$

Here $\mathcal{S}^c$ is the determinant cooperad $(\mathcal{S}^{-1})^*$.

Remark 6.3.1.6. This definition, when applied to associative algebras viewed as operads with generators of arity 1, gives a definition which is slightly different from Definition 2.1.2.1. We leave it to the reader to examine the two definitions and identify the differences (Exercise 6.4).

Proposition 6.3.1.7. *For any quadratic operad $\mathcal{P} = \mathcal{P}(\mathcal{V}, \mathcal{R})$ generated by a reduced symmetric collection $\mathcal{V}$ of finite dimension in each arity, we have*

$$\mathcal{P}^! \cong \mathcal{P}(s^{-1}\mathcal{S}^{-1} \underset{\mathrm{H}}{\otimes} \mathcal{V}^*, s^{-2}\mathcal{R}^{\perp}),$$

where $\mathcal{R}^{\perp}$ is the annihilator of $\mathcal{R}$ under the natural pairing

$$\mathcal{T}_{\Sigma}\left(\mathcal{S}^{-1} \underset{\mathrm{H}}{\otimes} \mathcal{V}^*\right)^{(2)} \otimes \mathcal{T}_{\Sigma}(\mathcal{V})^{(2)} \to \mathcal{S}^{-1} \underset{\mathrm{H}}{\otimes} \mathcal{T}_{\Sigma}\left(\mathcal{V}^*\right)^{(2)} \otimes \mathcal{T}_{\Sigma}(\mathcal{V})^{(2)} \to \mathbb{F},$$

where the first map comes from composing elements from $\mathcal{S}^{-1}$.

Proof. See [180, Prop. 7.2.1]. □

Remark 6.3.1.8. Note that the arity 2 space of the collection $s^{-1}\mathcal{S}^{-1}$ is concentrated in degree 0, but in general the arity n space of that collection is concentrated in homological degree $n - 2$. An immediate consequence of that is the following observation that unfortunately escaped some early literature on Koszul duality [112, 113, 114, 115] (rendering many results obtained in those papers wrong): for an operad generated by operations of homological degree zero, the Koszul dual operad is generated by operations of degree zero only if all the operations are binary. For example, if an operad is generated by ternary operations of degree 0, its Koszul dual is generated by ternary operations of degree 1.

It is worth noting that for the purpose of computing Koszul signs it is just the parity of the homological degree that matters. However, collapsing all degrees modulo 2 and working with $\mathbb{Z}/2\mathbb{Z}$-graded vector spaces is almost never a good strategy, as it loses more refined information about graded pieces of a chain complex. For example, doing that may make a chain complex with finite-dimensional components into a $\mathbb{Z}/2\mathbb{Z}$-graded vector space with infinite-dimensional components without any extra structure; among many other things, this would make dual spaces and tensor products completely unmanageable.

As we mentioned above, the same definitions and results may be used in the case of nonsymmetric operads and shuffle operads.

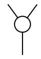
6.3.2 Examples of Koszul dual operads

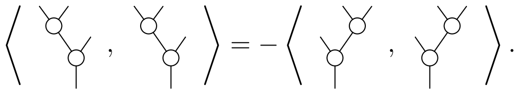
Example 6.3.2.1. Consider the q-associative nonsymmetric operad 3.6.1.2. According to Proposition 6.3.1.7, the pairing

$$\mathcal{T}\left(\mathcal{S}^{-1} \underset{\mathrm{H}}{\otimes} \mathcal{V}^*\right)^{(2)} \otimes \mathcal{T}(\mathcal{V})^{(2)} \to \mathbb{F}$$

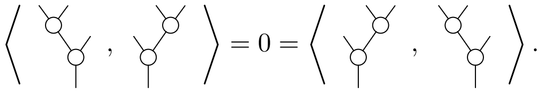
differs from the "naive" pairing

$$\mathcal{T}\left(\mathcal{V}^*\right)^{(2)} \otimes \mathcal{T}(\mathcal{V})^{(2)} \to \mathbb{F}$$

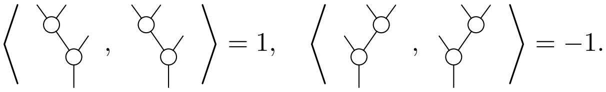
by the signs that come from compositions in $\mathcal{S}^{-1}$. Therefore, if we denote the generator of As_q and the generator of $\mathsf{As}_q^!$ by the same symbol  , the pairing in question satisfies



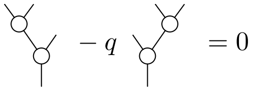
In addition, we of course have



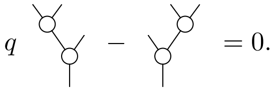
The usual convention is to put



In this case, the dual of the defining relation

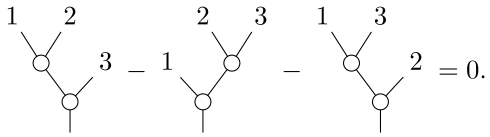


of As_q is the relation

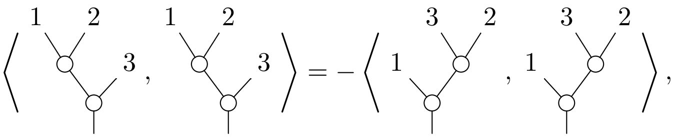


In other words, $\mathsf{As}_q^! \cong \mathsf{As}_{q^{-1}}$ (for $q \neq 0$).

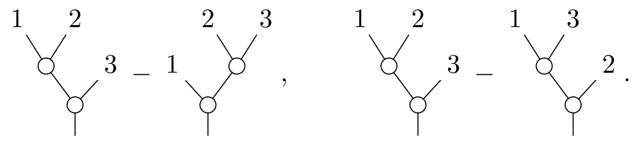
Example 6.3.2.2. Consider the shuffle operad Lie^f which, as we know from Example 5.3.4.2, is the operad with just one defining relation



In the shuffle case, in addition to the property highlighted in Example 6.3.2.1, we also have



as computing the corresponding compositions in the shuffle operad $\mathcal{S}^{-1}$ instantly demonstrates (Exercise 6.5). Therefore, the annihilator of the defining relation of the operad Lie^f is spanned by the two elements



It is easy to see that this operad is the operad Com^f, where Com is the operad of associative commutative algebras.

Example 6.3.2.3. Let us consider the operad $\mathsf{tAs}_d^{(N)}$ (Definition 6.2.3.1) with its relations

$$\mu \circ_p \mu = \mu \circ_N \mu \quad \text{for all} \quad p \leq N-1.$$

Note that in the operad $\mathcal{S}$ we have

$$\mu_n \circ_i \mu_m = (-1)^{(i-1)(m-1)} \mu_{n+m-1};$$

this is established in the same way as a particular way of this formula is established in Example 6.2.1.2. The same signs would come from the compositions in the operad $\mathcal{S}^{-1}$: the parities of homological degrees in these operads are the same, so while their basis elements are of different degrees, these operads have the same structure constants. Therefore, the dual operad of the operad $\mathsf{tAs}_d^{(N)}$ is the operad with one generator ν of degree $-d+N-2$, and the following defining relation:

$$\sum_{i=1}^{N} (-1)^{(i-1)(N-1)} \nu \circ_i \nu = 0.$$

This operad is called the operad of *partially associative N-ary algebras in degree $-d+N-2$*, and is denoted by $\mathsf{pAs}_{-d+N-2}^{(N)}$.

6.3.3 The Koszul property of a quadratic operad

Recall that the Koszul complex of a quadratic operad $\mathcal{P}$ is the symmetric collection $\mathcal{P}^{¡} \circ_\Sigma \mathcal{P}$ equipped with a certain differential coming from a "twisting morphism"

$$\varkappa \colon \mathcal{C}(s\mathcal{V}, s^2\mathcal{R}) \twoheadrightarrow s\mathcal{V} \to \mathcal{V} \hookrightarrow \mathcal{P}(\mathcal{V}, \mathcal{R}),$$

see [180, Sec. 7.4] for details.

Definition 6.3.3.1 (Koszul operad). A quadratic operad $\mathcal{P}$ is said to be *Koszul* if its Koszul complex is acyclic, so that the inclusion

$$\mathbb{1} \hookrightarrow \mathcal{P}^{¡} \circ_\Sigma \mathcal{P}$$

induces an isomorphism in the homology.

The following theorem is currently the most efficient and general way to prove Koszulness of an operad.

Theorem 6.3.3.2. *Let $\mathcal{P}$ be a symmetric operad for which the shuffle operad $\mathcal{P}^f$ admits a quadratic Gröbner basis. Then the operad $\mathcal{P}$ is Koszul.*

Proof. See Proposition 6.4.1.3 and Corollary 6.4.3.2 below. □

From our examples 5.6.1.1 and 5.6.1.2 it instantly follows that the symmetric operads Lie and Ass are Koszul. Exercises from Chapter 5 prove Koszulness of some other operads in the exact same way.

Remark 6.3.3.3. This theorem also holds for nonsymmetric operads: a nonsymmetric operad that admits a quadratic Gröbner basis is Koszul. In particular, it follows from Example 3.6.1.2 that the operad As_q is Koszul for $q = 0, 1$; we will see below in Example 6.3.4.5 that for other values of q that operad is not Koszul.

Let $\mathcal{P} = \mathcal{T}_\Sigma(\mathcal{V})/(\mathcal{R})$ be a quadratic operad. Let us choose a basis $\mathcal{X}$ of $\mathcal{V}$, and take the dual basis $\mathcal{X}^\vee$ in $\mathcal{S}^{-1} \underset{\mathrm{H}}{\otimes} \mathcal{V}^*$, the space of generators of $\mathcal{P}^!$. We identify these bases as sets, pairing each element with its dual. Let us fix some monomial order of $\mathcal{T}_\Sigma(\mathcal{X})^f$, and the opposite (under our identification of bases) order of $\mathcal{T}_\Sigma(\mathcal{X}^\vee)^f$.

Proposition 6.3.3.4 ([70, 135])**.** *Let us denote by $\mathcal{B}$ the linearly self-reduced basis of $\mathcal{R} \subset \mathcal{T}_\Sigma(\mathcal{X})^f$, and by $\mathcal{B}^\perp$ the linearly self-reduced basis of $s^{-2}\mathcal{R}^\perp \subset \mathcal{T}_\Sigma(\mathcal{X}^\vee)^f$.*

(i) *We have $\mathrm{LM}(\mathcal{B}) \sqcup \mathrm{LM}(\mathcal{B}^\perp) = Ш\mathrm{Tree}^{(2)}_{\mathcal{X}}$.*

(ii) *The set of tree monomials for which every quadratic divisor belongs to $\mathrm{LM}(\mathcal{B})$ spans the Koszul dual operad $\mathcal{P}^!$; the number of such monomials of arity n gives an upper bound on $\dim \mathcal{P}^!(n)$. This upper bound is sharp for all n such that $\mathcal{T}_\Sigma(\mathcal{X})(n)^{(3)} \neq 0$ if and only if the operad $\mathcal{P}^!$ has a quadratic Gröbner basis.*

(iii) *The operad $\mathcal{P}$ has a quadratic Gröbner basis if and only if the operad $\mathcal{P}^!$ has a quadratic Gröbner basis.*

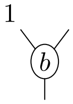
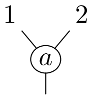
Proof. Statement (i) follows from basic linear algebra and is left as an exercise (Exercise 6.8).

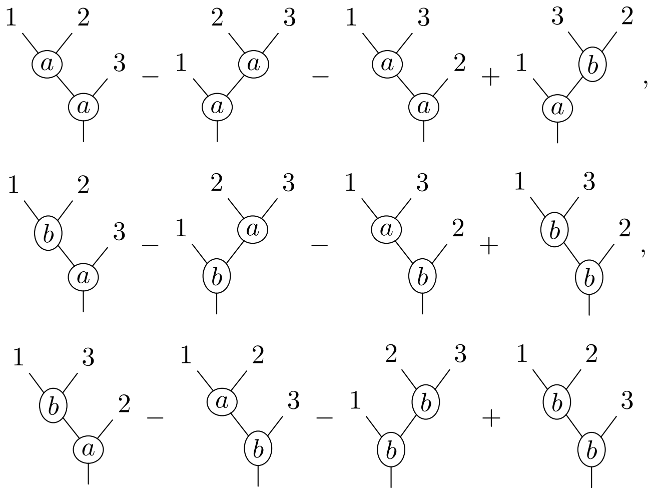
To prove (ii), note that according to (i), the set of tree monomials for which every quadratic divisor belongs to $\mathrm{LM}(\mathcal{B})$ is precisely the set of tree monomials that are reduced with respect to $\mathcal{B}^\perp$. In general, for a linearly self-reduced set $\mathcal{G}$ of quadratic elements in the free shuffle operad, the cosets of monomials of weight three that are reduced with respect to $\mathcal{G}$ span the quotient by $(\mathcal{G})$; they are linearly independent if and only if $\mathcal{G}$ is a Gröbner basis (Proposition 5.4.3.4). It is enough to verify the linear independence of elements of weight 3, since it would ensure that all S-polynomials that arise in Algorithm 5.5.2.1 have reduced form zero.

Finally, to prove (iii), the easiest way is to consider the bar complex of $\mathcal{P}$ [180], and the filtration on it induced by the monomial order that we consider. Using that filtration, it is easy to check that if $\mathcal{P}$ has a Gröbner basis, then a basis of $\mathcal{P}^!$ is formed by elements that are reduced with respect to $\mathcal{B}^\perp$ [135], and (ii) applies. □

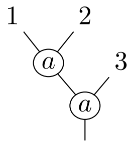
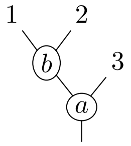
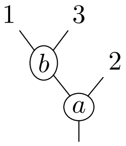
Example 6.3.3.5. Let us consider the operad PreLie of pre-Lie algebras from Example 5.6.2.1. It is known that its Koszul dual operad $\mathsf{PreLie}^! = \mathsf{Perm}$ is generated by one operation $a_1, a_2 \mapsto a_1 \cdot a_2$ which satisfies the relations

$$(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3),$$
$$a_1 \cdot (a_2 \cdot a_3) = a_1 \cdot (a_3 \cdot a_2),$$

moreover, $\dim \mathsf{Perm}(n) = n$: a basis element of Perm is completely determined by its first factor a_i, $i = 1, \dots, n$. This easily allows to justify the Gröbner basis from Example 5.6.2.1. Indeed, for the `gpathpermlex` order with  $\prec$  , the leading monomials of the defining relations


1 2 a 3 a − 1 2 3 a a − 1 3 a 2 a + 1 3 2 b a ,
1 2 b 3 a − 1 2 3 a b − 1 3 a 2 b + 1 3 b 2 b ,
1 3 b 2 a − 1 2 a 3 b − 1 2 3 b b + 1 2 b 3 b

are

 ,  , and  .

The monomials of arity n, for which each divisor is one of these monomials, are left combs for which the labels on the path from the root to the leaf number 1 are either $a, a, \dots, a$ or $a, a, \dots, a, b$ (in this order). In the first case, the only numbering of leaves that is allowed is $1, 2, \dots, n$ (in the planar order of leaves), and in the second case, each numbering $1, k, 2, \dots, k-1, k+1, \dots, n$ is allowed. Altogether we have $n = 1+(n-1)$ monomials, which coincides with $\dim \mathsf{Perm}(n)$. We conclude that our set of relations forms a Gröbner basis.

6.3.4 The Ginzburg–Kapranov criterion

Let us recall a functional equation due to Ginzburg and Kapranov which also can be used as a test of whether an operad is Koszul.

Definition 6.3.4.1 (Hilbert series for symmetric collections)**.** Let $\mathcal{P}$ be a reduced symmetric collection whose components have an extra weight grading, $\mathcal{P}(n) = \bigoplus_{k\ge 0} \mathcal{P}(n)^{(k)}$. Suppose that all components $\mathcal{P}(n)^{(k)}$ are finite-dimensional, and $\mathcal{P}$ is connected, that is

$$\mathcal{P}(k)^{(0)} = \begin{cases} \mathbb{F}, & k = 1, \\ 0, & k \neq 1. \end{cases}$$

We define the *operadic Hilbert–Poincaré series* of $\mathcal{P}$ by the formula

$$HP^{\Sigma}_{\mathcal{P}}(t,x) = \sum_{n\ge 1, s\ge 0} \frac{\dim \mathcal{P}(n)^{(k)}}{n!} t^n x^k.$$

Proposition 6.3.4.2. *Let $\mathcal{P}$ and $\mathcal{Q}$ be two reduced symmetric collections equipped with weight gradings for which they are connected. In this case, the composition $\mathcal{P} \circ_\Sigma \mathcal{Q}$ has a natural weight grading with respect to which it is connected, and*

$$HP^{\Sigma}_{\mathcal{P}\circ_\Sigma \mathcal{Q}}(t,x) = H^{\Sigma}_{\mathcal{P}}(H^{\Sigma}_{\mathcal{Q}}(t,x),x).$$

Proof. Exercise 6.6. □

The following result appeared for the first time in the seminal paper of Ginzburg and Kapranov [105]; it generalizes a result for quadratic algebras that had been known for at least a decade prior to that [10].

Theorem 6.3.4.3 (Ginzburg–Kapranov functional equation)**.** *Suppose that $\mathcal{P}$ is a finitely generated quadratic operad whose generating operations are all of homological degree 0. Consider its natural weight grading by the number of internal vertices of a tree.*

- *If $\mathcal{P}$ is Koszul, then*

$$HP^{\Sigma}_{\mathcal{P}^{¡}}(HP^{\Sigma}_{\mathcal{P}}(t,-x),x) = t.$$

- *Suppose that $\mathcal{P}$ is generated by operations of the same arity $N \geq 2$ and of homological degree zero. In that case $H_{\mathcal{P}}(t) = tf(t^{N-1})$ for some power series f; if $\mathcal{P}$ is Koszul, then*
$$H^{\Sigma}_{\mathcal{P}^{\mathsf{i}}}(\widetilde{H^{\Sigma}_{\mathcal{P}}}(t)) = t,$$
where the "sign modified series" $\widetilde{H^{\Sigma}_{\mathcal{P}}}(t)$ is defined by the formula $\widetilde{H^{\Sigma}_{\mathcal{P}}}(t) = tf(-t^{N-1})$.

Proof. The first part follows from the definition of the Koszul complex, Proposition 6.3.4.2, and the observation that the homological degree in the Koszul complex comes from the weight grading. The second part follows from the first part after letting $x = 1$ and noticing that in case all the generators are of the same arity $N \geq 2$, elements of weight k are precisely elements of arity $1 + k(N-1)$. □

The most common use of this result is for proving that some operads are not Koszul.

Corollary 6.3.4.4 (Ginzburg–Kapranov criterion)**.** *Suppose that $\mathcal{P}$ is a finitely generated quadratic operad whose generating operations are all of the same arity $N \geq 2$ and of homological degree 0. Suppose that the composition inverse of the sign modified series $\left(\widetilde{H^{\Sigma}_{\mathcal{P}}}\right)^{\langle -1\rangle}(t)$ has at least one negative coefficient. Then $\mathcal{P}$ is not Koszul.*

Proof. If $\mathcal{P}$ is Koszul, we have $\left(\widetilde{H^{\Sigma}_{\mathcal{P}}}\right)^{\langle -1\rangle}(t) = H_{\mathcal{P}^{\mathsf{i}}}(t)$. Thus, this series (the exponential generating series of dimensions of components $\mathcal{P}^{\mathsf{i}}(n)$) cannot have negative coefficients. □

The same results hold for nonsymmetric operads if one considers Hilbert and Hilbert–Poincaré series without factorials in denominators.

Example 6.3.4.5. Consider the q-associative operad As_q for $q \neq 0, 1$. We know from Example 3.6.1.2 that
$$\dim \mathsf{As}_q(n) = \begin{cases} 1, & n \leq 3, \\ 0, & n \geq 4. \end{cases}$$

We have $H_{\mathsf{As}_q}(t) = t + t^2 + t^3$, and therefore
$$\left(\widetilde{H_{\mathsf{As}_q}}\right)^{\langle -1\rangle}(t) = (t - t^2 + t^3)^{\langle -1\rangle} = t + t^2 + t^3 - 4t^5 + O(t^6).$$

We conclude that As_q is not Koszul for $q \neq 0, 1$.

6.3.5 Filtered distributive laws between quadratic operads

In this section, we discuss filtered distributive laws, a method in Koszul duality for operads which is somewhere on the way from symmetric to shuffle operads. It is based on dealing with normal forms with respect to a certain partial order for tree monomials, and is a minor extension of the rewriting method of [180, Sec. 8.3]. We will however see that shuffle operads will be useful for upgrading proofs based on this method to proofs which do not depend on the characteristic of the ground field.

For two symmetric subcollections $\mathcal{U}_1$ and $\mathcal{U}_2$ of the same symmetric operad $\mathcal{O}$, let us denote by $\mathcal{J}(\mathcal{U}_1,\mathcal{U}_2)$ the subcollection of $\mathcal{O}$ spanned by all elements $\phi \circ_i \psi$ with $\phi \in \mathcal{U}_1$, $\psi \in \mathcal{U}_2$.

Definition 6.3.5.1 (Distributing rewriting rule)**.** Let $\mathcal{A} = \mathcal{F}(\mathcal{V})/(\mathcal{R})$ and $\mathcal{B} = \mathcal{F}(\mathcal{W})/(\mathcal{S})$ be two symmetric quadratic operads. The data of two maps of symmetric collections

$$s\colon \mathcal{R} \to \mathcal{J}(\mathcal{W},\mathcal{V}) \oplus \mathcal{J}(\mathcal{V},\mathcal{W}) \oplus \mathcal{J}(\mathcal{W},\mathcal{W}) \tag{6.8}$$

and

$$d\colon \mathcal{J}(\mathcal{W},\mathcal{V}) \to \mathcal{J}(\mathcal{V},\mathcal{W}) \oplus \mathcal{J}(\mathcal{W},\mathcal{W}) \tag{6.9}$$

is called a *distributing rewriting rule.*

Definition 6.3.5.2 (Operads from distributing rewriting rules)**.** Every distributing rewriting rule gives rise to a quadratic operad $\mathcal{E}$ with generators $\mathcal{U} = \mathcal{V} \oplus \mathcal{W}$ and relations $\mathcal{T} = \mathcal{Q} \oplus \mathcal{D} \oplus \mathcal{S}$, where

$$\mathcal{Q} = \{x - s(x) \mid x \in \mathcal{R}\}, \quad \mathcal{D} = \{x - d(x) \mid x \in \mathcal{J}(\mathcal{W},\mathcal{V})\}. \tag{6.10}$$

Remark 6.3.5.3.

(i) Basically, a distributing rewriting rule amounts to joining generators of $\mathcal{A}$ and $\mathcal{B}$ together, keeping the relations of $\mathcal{B}$, deforming relations of $\mathcal{A}$ by adding to them "lower terms" of degree at most 1 in generators of $\mathcal{A}$, and imposing a rewriting rule transforming $\mathcal{J}(\mathcal{W},\mathcal{V})$ into a combination of terms from $\mathcal{J}(\mathcal{V},\mathcal{W})$ and "lower terms" of degree 0 in generators of $\mathcal{A}$.

(ii) Note that using the rewriting rule $x \mapsto d(x)$, one can replace s by

$$s'\colon \mathcal{R} \to \mathcal{J}(\mathcal{V},\mathcal{W}) \oplus \mathcal{J}(\mathcal{W},\mathcal{W}). \tag{6.11}$$

From now on we will denote by s that modified mapping.

Lemma 6.3.5.4. *The natural projections of symmetric collections*

$$\pi_1\colon \mathcal{V} \oplus \mathcal{W} \twoheadrightarrow \mathcal{V}, \quad \pi_2\colon \mathcal{V} \oplus \mathcal{W} \twoheadrightarrow \mathcal{W}$$

extend to surjections of operads

$$(\pi_1)_*\colon \mathcal{E} \twoheadrightarrow \mathcal{A}, \quad (\pi_2)_*\colon \mathcal{E} \twoheadrightarrow \mathcal{B}.$$

The surjection $(\pi_2)_*$ always splits, while the surjection $(\pi_1)_*$ may split or not depending on the ground field $\mathbb{F}$.

Proof. Only the last statement is not quite obvious. The splitting of $(\pi_2)_*$ comes from the inclusion of the direct summand $\mathcal{W} \hookrightarrow \mathcal{V} \oplus \mathcal{W}$. For the case of $(\pi_1)_*$, let us consider the symmetric operad Ass over a field of characteristic 3, and its presentation

$$\begin{gathered}[a_1,[a_2,a_3]]+[a_2,[a_3,a_1]]+[a_3,[a_1,a_2]]=0,\\ [a_1\cdots a_2,a_3]=a_1\cdot[a_2,a_3]+[a_1,a_3]\cdot a_2,\\ (a_1\star a_2)\star a_3-a_1\star(a_2\star a_3)=[a_2,[a_1,a_3]].\end{gathered}$$

from Exercise 5.17. It is clear that this presentation may be viewed as a distributing rewriting rule between the operads Com and Lie. However, the surjection $\mathsf{Ass}(3) \twoheadrightarrow \mathsf{Com}(3)$ does not split: the only subspace of $\mathsf{Ass}(3) \cong \mathbb{F}S_3$ where the trivial representation is realized is $\sum_{\sigma\in S_3}\sigma$, and this element projects to zero in $\mathsf{Com}(3)$ when the characteristic of $\mathbb{F}$ divides 6. □

Definition 6.3.5.5 (Split distributing rewriting rule)**.** A distributing rewriting rule is said to be *split* if the projection $(\pi_1)_*$ from Lemma 6.3.5.4 splits.

In characteristic zero every distributing rewriting rule is split. In positive characteristic it happens, for instance, whenever $s = 0$, so that the relations of $\mathcal{A}$ remain undeformed.

Lemma 6.3.5.6. *For every split distributing rewriting rule, the composite of natural mappings*

$$\mathcal{F}_\Sigma(\mathcal{V})\circ\mathcal{F}_\Sigma(\mathcal{W}) \hookrightarrow \mathcal{F}_\Sigma(\mathcal{V}\oplus\mathcal{W}) \twoheadrightarrow \mathcal{F}_\Sigma(\mathcal{V}\oplus\mathcal{W})/(\mathcal{T})$$

gives rise to a surjection of symmetric collections

$$\xi\colon \mathcal{A}\circ_\Sigma\mathcal{B} \twoheadrightarrow \mathcal{E}. \qquad (6.12)$$

Proof. First, using the defining relations $\mathcal{T}$ as rewriting rules, every tree tensor $\mathcal{F}_\Sigma(\mathcal{V}\oplus\mathcal{W})$ can be rewritten as a combination of elements from the subcollection $\mathcal{F}_\Sigma(\mathcal{V})\circ\mathcal{F}_\Sigma(\mathcal{W})$. Next, we consider the filtration of the free operad by the number of labels from $\mathcal{V}$ of a tree tensor. Passing to the graded object with respect to this filtration turns the set of relations $\mathcal{Q}$ into $\mathcal{R}$. Together with the assumption on splitting of $(\pi_1)_*$, these two observations guarantee a surjective map $\mathcal{A}\circ_\Sigma\mathcal{B}$ to $\mathcal{E}$. □

Definition 6.3.5.7 (Filtered distributive law)**.** We say that a split distributing rule is a *filtered distributive law* between the operads $\mathcal{A}$ and $\mathcal{B}$ if the restriction of ξ to weight 3 elements

$$\xi_3\colon (\mathcal{A}\circ_\Sigma\mathcal{B})^{(3)} \to \mathcal{E}^{(3)} \qquad (6.13)$$

is an isomorphism.

The following result (generalizing the distributive law criterion for operads that was first stated in [183]) was proved in [69] using the set operad filtration method of [147] and in [254] using a filtration on the Koszul complex; however, both proofs rely on the Künneth formula for symmetric collections and thus are not available in positive characteristic because in that case the group algebras $\mathbb{F}S_n$ are not semisimple.

Theorem 6.3.5.8 (Split filtered distributive law criterion)**.** *Assume that the operads $\mathcal{A}$ and $\mathcal{B}$ are Koszul, and that they are related by a split distributing rewriting rule which is a filtered distributive law. Then the corresponding operad $\mathcal{E}$ from Definition 6.3.5.2 is Koszul, and the symmetric collections $\mathcal{A}\circ_\Sigma\mathcal{B}$ and $\mathcal{E}$ are isomorphic.*

Proof. Let us first note that either of the characteristic zero proofs mentioned above (set operad filtration; filtration on the Koszul complex) works for shuffle operads for arbitrary characteristic, since the Künneth formula over a field is always available. Also, a symmetric operad $\mathcal{O}$ is Koszul if and only if the shuffle operad $\mathcal{O}^f$ is Koszul, which proves the first statement of the theorem. To prove the second statement, we observe that on the level of nonsymmetric collections we have an isomorphism $\mathcal{E}^f \simeq \mathcal{A}^f\circ_{\text{III}}\mathcal{B}^f \simeq (\mathcal{A}\circ_\Sigma\mathcal{B})^f$, and for symmetric collections we have a surjection $\mathcal{A}\circ_\Sigma\mathcal{B}\twoheadrightarrow\mathcal{E}$. Since the forgetful functor does not change the underlying vector spaces, the surjection in question has to be an isomorphism. □

6.4 Models for operads from Gröbner bases

The main application of Koszul duality in homotopical algebra is for constructing minimal models of operads. Let us recall the corresponding definitions, and explain how Gröbner bases enter this circle of questions, following [75].

6.4.1 Models for operads

The following definition is an extension from [81] of the original definition from [184]; this extension is needed to accommodate an important case of operads with nontrivial unary operations.

Definition 6.4.1.1 (Quasi-free operad, model, minimal model)**.** A differential graded operad is said to be *quasi-free* if it is free if viewed as an operad whose components are graded vector spaces (without differential). A *model* of an operad $\mathcal{O}$ whose components are graded vector spaces is a quasi-free operad $(\mathcal{T}_\Sigma(\mathcal{U}), d)$ equipped with a surjective map $(\mathcal{T}_\Sigma(\mathcal{U}), d)\twoheadrightarrow\mathcal{O}$ which induces an isomorphism on the homology. A quasi-free operad $(\mathcal{T}_\Sigma(\mathcal{U}), d)$ is *minimal* if its differential is decomposable, that is $d(\mathcal{U}) \subset \mathcal{T}_\Sigma(\mathcal{U})^{(\geq 2)}$, and its collection of generators admits a direct sum decomposition $\mathcal{U} = \bigoplus_{k\geq 1}\mathcal{U}^{[k]}$ satisfying the *Sullivan triangulation condition*

$$d(\mathcal{U}^{[k+1]}) \subset \mathcal{T}_\Sigma(\bigoplus_{i=1}^{k}\mathcal{U}^{[i]}).$$

The same definitions apply in the case of associative algebras, nonsymmetric operads, shuffle operads, etc. In particular, the following statement holds.

Proposition 6.4.1.2. *Suppose that $(\mathcal{T}_\Sigma(\mathcal{U}), d)$ is a model of a symmetric operad $\mathcal{O}$. Then*

$$(\mathcal{T}_\Sigma(\mathcal{U}), d)^f = (\mathcal{T}_\Sigma(\mathcal{U})^f, d^f) \cong (\mathcal{T}_{\text{Ш}}(\mathcal{U}^f), d^f)$$

is a model of the shuffle operad $\mathcal{O}^f$.

Proof. It is obvious from Corollary 5.3.3.3. □

Models for operads are related to operadic Koszul duality. More precisely, the following statement is true.

Proposition 6.4.1.3.

(i) *If an operad $\mathcal{O}$ has a minimal model, that minimal model is unique up to an isomorphism.*

(ii) *A symmetric operad $\mathcal{O}$ is Koszul if and only if it admits a minimal model $(\mathcal{T}_\Sigma(\mathcal{U}), d)$ with a* quadratic *differential, that is $d(\mathcal{U}) \subset \mathcal{T}_\Sigma(\mathcal{U})^{(2)}$.*

(iii) *A symmetric operad $\mathcal{O}$ is Koszul if and only if the shuffle operad $\mathcal{O}^f$ admits a minimal model $(\mathcal{T}_{\text{Ш}}(\mathcal{U}), d)$ with a* quadratic *differential, that is $d(\mathcal{U}) \subset \mathcal{T}_{\text{Ш}}(\mathcal{U})^{(2)}$.*

Proof. Statement (i) is Theorem 6.3.4 of [180]. Statement (ii) is closely related to Theorem 6.6.1 of [180], and we leave it as an exercise for the reader to fill in the details (Exercise 6.14). Finally, (iii) is a direct consequence of (i), (ii), and Proposition 6.4.1.2. □

Propositions 6.4.1.2 and 6.4.1.3 imply that while applying the forgetful functor does lose some data, it retains some information about the shape of the differential of the minimal model of a given operad. In some cases, like the Koszul duality, retaining that knowledge is completely sufficient. In some other cases, external information may be used to arrive at a complete answer (like it is done, independently from [81], for the operad of Batalin–Vilkovisky algebras in [75]).

Definition 6.4.1.4 (Syzygy degree)**.** In the context of models for operads and algebras, we will refer to the homological degree in the model as *syzygy degree*; an operad itself may have elements of different homological degrees, in which case there will be more than one homological degree for elements of the model.

6.4.2 Resolution for monomial relations

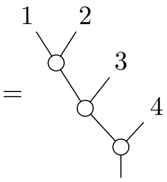
Assume that the shuffle operad $\mathcal{O} = \mathcal{T}_{\text{Ш}}(\mathcal{X})/(\mathcal{G})$ is generated by an operation alphabet $\mathcal{X}$, and that $\mathcal{G}$ consists of shuffle tree monomials. We will now explain how to construct a model of $\mathcal{O}$ which is often minimal.

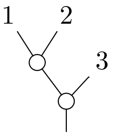
Our first step is to construct a quasi-free shuffle operad $\mathcal{A}_{\mathcal{X}}$ which does not take into account the relations of $\mathcal{O}$; it is a somewhat universal object for operads generated by $\mathcal{X}$, various suboperads of $\mathcal{A}_{\mathcal{X}}$ will be used as resolutions for various choices of $\mathcal{G}$.

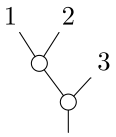
Definition 6.4.2.1 (The inclusion–exclusion operad)**.** Let T be a tree monomial, and let $\Lambda(\mathsf{s}_1, \ldots, \mathsf{s}_q)$ be the exterior algebra generated by the symbols $\mathsf{s}_1, \ldots, \mathsf{s}_q$ of syzygy degree 1 which are in one-to-one correspondence with divisors of T. We denote by $\mathcal{A}_{\mathcal{X}}(T)$ the vector space $\mathbb{F}T \otimes \Lambda(\mathsf{s}_1, \ldots, \mathsf{s}_q)$. We will refer to T as the *underlying tree monomial* for elements of this vector space. The degree -1 derivations ∂_i on the exterior algebra defined by the rule $\partial_i(\mathsf{s}_j) = \delta_{ij}$ anticommute, and the differential $d = \sum_{i=1}^{q} \partial_i$ makes $\mathcal{A}_{\mathcal{X}}(T)$ into a chain complex isomorphic to the augmented chain complex of a $(q-1)$-dimensional simplex Δ^{q-1}. By definition, the chain complex $\mathcal{A}_{\mathcal{X}}(n)$ is the direct sum of complexes $\mathcal{A}_{\mathcal{X}}(T)$ over all tree monomials T with n leaves. There is a natural shuffle operad structure on the nonsymmetric collection $\mathcal{A}_{\mathcal{X}} = \{\mathcal{A}_{\mathcal{X}}(n)\}_{n\geq 1}$; the operadic composition composes the trees, and computes the wedge product of symbols labelling their divisors. The shuffle operad $\mathcal{A}_{\mathcal{X}}$ equipped with the differential d is called the *inclusion–exclusion operad*.

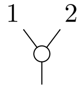
Let us emphasize that the symbols s_{i_r} correspond to divisors, i.e., mark *occurrences of tree monomials in* T rather than monomials themselves. In particular, even though we have $\mathsf{s}_i^2 = 0$ in the exterior algebra, but a composition of an element of our operad with itself is never equal to zero.

Example 6.4.2.2. Recall the shuffle tree monomial

$T =$ 

from Example 5.4.2.7; it has two different ternary divisors, each of those divisors is the monomial  . Let us denote these divisors T' and T'',

where T' shares the root with T, and T'' does not. Let us also consider the shuffle tree monomial $T_1 =$ 

, and denote its only ternary divisor by T_1'. The following examples illustrate computations in the operad $\mathcal{A}_{\mathcal{X}}$ for $\mathcal{X} = \Bigg\{$ 

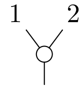
$\Bigg\}$. The chain complex $\mathcal{A}_{\mathcal{X}}(T)$ is

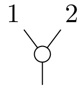
$$\mathbb{F}T \otimes 1 \leftarrow \mathbb{F}T \otimes T' \oplus \mathbb{F}T \otimes T'' \leftarrow \mathbb{F}T \otimes T' \wedge T'',$$

with the differential

$$d(T\otimes 1) = 0, \quad d(T\otimes T') = d(T\otimes T'') = T\otimes 1, \quad d(T\otimes T'\wedge T'') = T\otimes T'' - T\otimes T.$$

We have

$(T_1 \otimes T_1') \circ_1$ 

$= T \otimes T',$ 

$\circ_1 (T_1 \otimes T_1') = T \otimes T''.$

Proposition 6.4.2.3. *The dg operad $\mathcal{A}_{\mathcal{X}}$ is quasi-free.*

Proof. Indeed, let us call an element $T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$, $q \geq 0$, indecomposable, if it cannot be written as a shuffle composition of two elements of the same type in the operad $\mathcal{A}_{\mathcal{X}}$. (This means that each "internal edge", that is an edge between the two internal vertices of T, is an internal edge of at least one of the divisors $\mathsf{s}_{i_1}, \ldots, \mathsf{s}_{i_q}$.) It is easy to see that $\mathcal{A}$ is freely generated by indecomposable elements; those are elements $x \otimes 1$ with $x \in \mathcal{X}$, and indecomposable monomials $T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$, $q \geq 1$. For any other element $\alpha = T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$, we note that there exists at least one internal edge of T that is not an internal edge of either of $\mathsf{s}_{i_1}, \ldots, \mathsf{s}_{i_q}$. Such an edge gives rise to a factorization of α as a shuffle composition (Exercise 6.15); moreover, the set of all such edges leads to a unique decomposition of α as a composition of indecomposable elements. □

So far we have not used the relations $\mathcal{G}$ of the given operad $\mathcal{O}$. The dg operad $(\mathcal{A}_{\mathcal{X},\mathcal{G}}, d)$ is defined similarly to $\mathcal{A}_{\mathcal{X}}$, but with the additional restriction that every symbol s_k corresponds to a divisor of T which is an element of $\mathcal{G}$. The differential d is the restriction of the differential defined above.

Theorem 6.4.2.4. *The shuffle differential graded operad $(\mathcal{A}_{\mathcal{X},\mathcal{G}}, d)$ is a model of the operad $\mathcal{O} = \mathcal{T}_{\text{Ш}}(\mathcal{X})/(\mathcal{G})$.*

Proof. Similarly to the case of the operad $\mathcal{A}_{\mathcal{X}}$, the operad $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ is freely generated by its elements $m \otimes 1$ with $m \in \mathcal{M}$ and all indecomposable monomials $T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$, $q \geq 1$, where each of the divisors s_{i_k} is in $\mathcal{G}$.

Let us prove that $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ provides a model for $\mathcal{O}$. Since the differential d only omits wedge factors but does not change the tree monomial, the chain complex $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ is isomorphic to the direct sum of chain complexes $\mathcal{A}_{\mathcal{X},\mathcal{G}}(T)$ spanned by the elements for which the first tensor factor is the given tree monomial T. If T is not divisible by any relation, the complex $\mathcal{A}_{\mathcal{X},\mathcal{G}}(T)$ is concentrated in degree 0 and is spanned by $T \otimes 1$. Thus, to prove the theorem, we should show that $\mathcal{A}_{\mathcal{X},\mathcal{G}}(T)$ is acyclic whenever T is divisible by some relation g_i.

Assume that there are exactly k divisors of T which are relations of $\mathcal{O}$. We immediately see that the complex $\mathcal{A}_{\mathcal{X},\mathcal{G}}(T)$ is isomorphic to the chain complex of a simplex Δ^{k-1} which is acyclic whenever $k > 0$. □

6.4.3 Resolution for general relations

Let us now consider a shuffle operad $\widetilde{\mathcal{O}} = \mathcal{T}_{\text{Ш}}(\mathcal{X})/(\widetilde{\mathcal{G}})$, and let $\mathcal{O} = \mathcal{T}_{\text{Ш}}(\mathcal{X})/(\mathcal{G})$ be its "monomial replacement", that is, $\widetilde{\mathcal{G}}$ is the reduced Gröbner basis of relations, and $\mathcal{G}$ consists of all leading monomials of $\widetilde{\mathcal{G}}$. By Theorem 6.4.2.4 above, $(\mathcal{A}_{\mathcal{X},\mathcal{G}}, d)$ is a model of $\mathcal{O}$.

Let ϕ be the canonical homomorphism from $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ to its homology $\mathcal{O}$ (it kills all generators of positive syzygy degree, and on elements of syzygy degree 0 is the canonical projection from $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ to its quotient $\mathcal{O}$). The latter canonical projection sends a tree monomial T to its coset modulo $\mathcal{G}$; this coset is zero if T has a divisor from $\mathcal{G}$, and is a basis element of $\mathcal{O}$ otherwise. We define a map $\pi\colon \mathcal{A}_{\mathcal{X},\mathcal{G}} \to \mathcal{A}_{\mathcal{X},\mathcal{G}}$ as the composition of ϕ with the obvious section $\mathcal{O} \to \mathcal{A}_{\mathcal{X},\mathcal{G}}$; π annihilates all elements of positive syzygy degree and all tree monomials of syzygy degree 0 which have divisors from $\mathcal{G}$, and is identical on all other tree monomials. Since $(\mathcal{A}_{\mathcal{X},\mathcal{G}}, d)$ is a model of $\mathcal{O}$, there exists a homotopy map h for which $(dh)|_{\ker d} = \mathrm{id} - \pi$ (in fact, below we will specify a particular choice for such a homotopy map).

Our goal now will be to "deform" the situation described in the previous paragraph in the following sense. Let $\widetilde{\phi}$ be the homomorphism from $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ to $\widetilde{\mathcal{O}}$ that kills all generators of positive syzygy degree, and on elements of syzygy degree 0 is the canonical projection from $\mathcal{T}_{\text{Ш}}(\mathcal{X})$ to its quotient $\widetilde{\mathcal{O}}$. By Lemma 5.4.2.17, shuffle tree monomials that are reduced with respect to $\mathcal{G}$ form a basis of $\widetilde{\mathcal{O}}$, and we define a map $\widetilde{\pi}\colon \mathcal{A}_{\mathcal{X},\mathcal{G}} \to \mathcal{A}_{\mathcal{X},\mathcal{G}}$ as the composition of $\widetilde{\phi}$ with the corresponding section; $\widetilde{\pi}$ annihilates all elements of positive syzygy degree, and sends each element of syzygy degree zero to the result of its long division by $\widetilde{\mathcal{G}}$, a combination of tree monomials that are reduced with respect to $\mathcal{G}$.

We will prove the following result, which is essentially nothing but homological perturbation in the same way as it is used in the case of free resolutions of trivial modules over augmented associative algebras in [3, 151, 165].

Theorem 6.4.3.1. *There exists a "deformed" differential D on $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ and a homotopy*

$$H\colon \ker D \to \mathcal{A}_{\mathcal{X},\mathcal{G}}$$

such that

$$H(\mathcal{A}_{\mathcal{X},\mathcal{G}}, D) \cong \widetilde{\mathcal{O}} \quad \textit{and} \quad (DH)|_{\ker D} = \mathrm{id} - \widetilde{\pi}.$$

Proof. We will construct D and H simultaneously by induction. Let us introduce a partial ordering of basis elements in $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ which just compares the underlying tree monomials. This partial ordering suggests the following definition: for an element $u \in \mathcal{A}_{\mathcal{X},\mathcal{G}}$, its leading term $\textsc{lt}(u)$ is the part of the expansion of u as a combination of basis elements consisting of the basis elements $T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$ with maximal possible T.

If L is a homogeneous linear operator on $\mathcal{A}_{\mathcal{X},\mathcal{G}}$ of some fixed syzygy degree of homogeneity (like D, H, d, h), we denote by L_k the operator L acting on elements of syzygy degree k. We will define the operators D and H by induction: we define the pair (D_{k+1}, H_k) assuming that all previous pairs are defined. At each step, we will also be proving that

$$D(m) = d(\textsc{lt}(m)) + \text{lower terms}, \quad H(m) = h(\textsc{lt}(m)) + \text{lower terms},$$

where the words "lower terms" refers to the partial order we defined above, meaning a linear combination of basis elements whose underlying tree monomial is smaller than the underlying tree monomial of $\textsc{lt}(m)$.

Basis of induction: $k = 0$, so we have to define D_1 and H_0 (note that $D_0 = 0$ because there are no elements of negative syzygy degree). In general, to define D_l, we should only consider the case when our element is a generator of $\mathcal{A}_{\mathcal{X},\mathcal{G}}$, since in a differential graded operad the differential is defined by images of generators. For $l = 1$, this means that we should consider the case where our generator corresponds to a leading monomial $T = \textsc{lm}(g)$ of some relation g, and is of the form $T \otimes \mathsf{s}$ where s corresponds to the divisor of T equal to T itself. Letting $D_1(T \otimes \mathsf{s}) = g$, we see that $D_1(T \otimes S) = T +$ lower terms, as required. Note that $g = \square_{T,\mathsf{s}}(g)$, so we can rewrite the above as

$$D_1(T \otimes \mathsf{s}) = \square_{T,\mathsf{s}}(g). \tag{6.14}$$

By direct inspection, this also holds when s is an arbitrary divisor of T, not necessarily the divisor equal to T itself.

To define H_0, we use yet another inductive argument, decreasing the monomials on which we want to define H_0. First of all, if a tree monomial T is not divisible by any of the leading terms of relations, we put $H_0(T) = 0$. Assume that T is divisible by some leading terms of relations, and $\mathsf{s}_{i_1}, \ldots, \mathsf{s}_{i_p}$ are the corresponding divisors. Then on $\mathcal{A}_{\mathcal{X},\mathcal{G}}(T)$ we can use $\alpha \mapsto \mathsf{s}_{i_1} \wedge \alpha$ as a homotopy for d, so $h_0(T) = T \otimes \mathsf{s}_{i_1}$. We put

$$H_0(T) = h_0(T) + H_0(T - D_1 h_0(T)).$$

Here the leading term of $T - D_1 h_0(T)$ is smaller than T (since we already know that the leading term of $D_1 h_0(T)$ is $d_1 h_0(T) = T$), so induction on the leading term applies. Note that by induction the leading term of $H_0(T)$ is $h_0(T)$.

Suppose that $k > 0$, that we know the pairs (D_{l+1}, H_l) for all $l < k$, and that in these degrees

$$D(m) = d(\text{LT}(m)) + \text{lower terms}, \quad H(m) = h(\text{LT}(m)) + \text{lower terms}.$$

To define D_{k+1}, we should, as above, only consider the case of generators. In this case, we put

$$D_{k+1}(m) = d_{k+1}(m) - H_{k-1}D_k d_{k+1}(m).$$

The property $D_{k+1}(m) = d_{k+1}(\text{LT}(m)) + \text{lower terms}$ now easily follows by induction. To define H_k, we proceed in a way very similar to what we did for the induction basis. Assume that $u \in \ker D_k$, and that we know H_k on all elements of $\ker D_k$ whose leading term is less than $\text{LT}(u)$. Since $D_k(u) = d_k(\text{LT}(u)) + \text{lower terms}$, we see that $u \in \ker D_k$ implies $\text{LT}(u) \in \ker d_k$. Then $h_k(\text{LT}(u))$ is defined, and we put

$$H_k(u) = h_k(\text{LT}(u)) + H_k(u - D_{k+1}h_k(\text{LT}(u))).$$

Here $u - D_{k+1}h_k(\text{LT}(u)) \in \ker D_k$ and its leading term is smaller than $\text{LT}(u)$, so induction on the leading term applies (and it is easy to check that by induction $H_{k+1}(m) = h_{k+1}(\text{LT}(m)) + \text{lower terms}$).

Let us check that the mappings D and H defined by these formulas satisfy, for each $k > 0$, $D_k D_{k+1} = 0$ and $(D_{k+1}H_k)|_{\ker D_k} = \text{id} - \widetilde{\pi}$. A computation checking that is somewhat similar to the way D and H were constructed. Let us prove both statements simultaneously by induction. If $k = 0$, the first statement is obvious. Let us prove the second one and establish that $D_1 H_0(T) = (\text{id} - \widetilde{\pi})(T)$ for each tree monomial T. Slightly rephrasing that, we will prove that for each tree monomial T we have $D_1 H_0(T) = T - \overline{T}$ where $\overline{T}$ is the result of long division of T by $\widetilde{\mathcal{G}}$. We will prove this statement by induction on T. If T is not divisible by any leading terms of relations, we have $H_0(T) = 0 = T - \overline{T}$. Let T have divisors $\mathsf{s}_{i_1}, \ldots, \mathsf{s}_{i_p}$. We have $H_0(T) = h_0(T) + H_0(T - D_1 h_0(T))$, so

$$D_1 H_0(T) = D_1 h_0(T) + D_1 H_0(T - D_1 h_0(T)).$$

By induction, we may assume that

$$D_1 H_0(T - D_1 h_0(T)) = T - D_1 h_0(T) - \overline{(T - D_1 h_0(T))}.$$

Also,

$$D_1 h_0(T) = D_1(T \otimes \mathsf{s}_{i_1}) = \square_{T, \mathsf{s}_{i_1}}(g) = T - r_g(T),$$

due to Equation (6.14).

Combining the three previous equations, we obtain,

$$D_1 H_0(T) = T - r_g(T) + \Big((T - D_1 h_0(T)) - \overline{(T - D_1 h_0(T))}\Big) =$$

$$= T - r_g(T) + (r_g(T) - \overline{r_g(T)}) = T - \overline{r_g(T)} = T - \overline{T},$$

since for a Gröbner basis the residue does not depend on a choice of reductions.

Assume that $k > 0$, and that our statement is true for all $l < k$. We have $D_k D_{k+1}(m) = 0$ since

$$\begin{aligned} D_k D_{k+1}(m) &= D_k(d_{k+1}(m) - H_{k-1} D_k d_{k+1}(m)) = \\ &= D_k d_{k+1}(m) - D_k H_{k-1} D_k d_{k+1}(m) = D_k d_{k+1}(m) - D_k d_{k+1}(m) = 0, \end{aligned}$$

because $D_k d_{k+1} k \in \ker D_{k-1}$, and so $D_k H_{k-1}(D_k(y)) = D_k(y)$ by induction. Also, for $u \in \ker D_k$ we have

$$D_{k+1} H_k(u) = D_{k+1} h_k(\textsc{lt}(u)) + D_{k+1} H_k(u - D_{k+1} h_k(\textsc{lt}(u))),$$

and by the induction on $\textsc{lt}(u)$ we may assume that

$$D_{k+1} H_k(u - D_{k+1} h_k(\textsc{lt}(u))) = u - D_{k+1} h_k(\textsc{lt}(u))$$

(on elements of positive syzygy degree, $\widetilde{\pi} = 0$), so

$$D_{k+1} H_k(u) = D_{k+1} h_k(\textsc{lt}(u)) + u - D_{k+1} h_k(\textsc{lt}(u)) = u,$$

which is exactly what we need. □

We outline one most immediate application of the result of this section, leaving it to the reader to explore various examples of their choice.

Corollary 6.4.3.2. *A shuffle operad with a quadratic Gröbner basis is Koszul.*

Proof. If the relations $\mathcal{G}$ are monomial, then the model of Section 6.4.2 has a quadratic differential: for an indecomposable element $T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$, every divisor s_{i_k} shares exactly one internal edge with T, and every internal edge determines the corresponding s_{i_k} uniquely, so the differential maps such an element to a sum of elements that decompose into exactly two parts.

If the relations are not monomial, then each generator of positive syzygy degree q of the model of Section 6.4.3 has $q = \mathrm{wt} - 1$. Therefore, the differential of an indecomposable element $T \otimes \mathsf{s}_{i_1} \wedge \cdots \wedge \mathsf{s}_{i_q}$ maps it to a sum of elements that decompose into exactly two parts: otherwise, the syzygy degrees of these elements would not add to $q - 1$. □

6.5 Exercises

Exercise 6.1. For $(V, d) = (V', d')$, the formula for the map δ_k from Proposition 6.1.1.5 becomes $\delta f = [d, f] = d \circ f - (-1)^k f \circ d$, according to the Koszul sign rule. Explain why this implies that $\delta^2 = 0$. (*Hint*: $d^2 = \frac{1}{2}[d, d]$.)

Exercise 6.2. Show that the nonsymmetric operad $\mathcal{S} = \mathrm{End}_{\mathbb{F}s}$ is generated by one binary operation μ of degree -1 subject to the relation

$$\mu \circ_1 \mu + \mu \circ_2 \mu = 0.$$

Exercise 6.3. Complete the computation of the reduced Gröbner basis of the operad $\mathsf{tAs}_d^{(N)}$ from Section 6.2.3.

Exercise 6.4. Let $A = T(V)/(R)$ be a quadratic associative algebra. Viewing A as an operad with generators of arity 1, we may apply either Definition 6.3.1.5 or Definition 2.1.2.1. Compare the Koszul dual algebras that those recipes produce, and explain how they are related.

Exercise 6.5. Viewing $\mathcal{S} = \mathrm{End}_{\mathbb{F}s}$ as a shuffle operad, compute the composition

$$\gamma_{\{1,3\},\{2\}}(\mu_2, \mu_2),$$

and explain how this is relevant for the computation in Example 6.3.2.2.

Exercise 6.6. Prove Proposition 6.3.4.2. (*Hint*: define the weight as the sum of weights coming from tensor factors.)

Exercise 6.7. Using Exercise 6.3, Corollary 6.3.4.4, and Theorem 6.3.3.2, investigate for which values of N and d the nonsymmetric operad $\mathsf{tAs}_d^{(N)}$ is Koszul. For some values of N and d this question becomes very hard, since the Gröbner basis is not quadratic and the Ginzburg–Kapranov criterion seems to be inconclusive [186]; in the upcoming paper [77], this question is resolved (it turns out that the corresponding operads are not Koszul).

Exercise 6.8. Prove part (i) of Proposition 6.3.3.4.

Exercise 6.9. Verify the claim $\mathsf{PreLie}^! = \mathsf{Perm}$ from Example 6.3.3.5.

Exercise 6.10. Show that the operad Leib from Exercise 5.11 is Koszul. (*Hint*: if you are not sure which order to choose for a quadratic Gröbner basis, it may help to know that the Koszul dual operad of Leib, called the operad of Zinbiel algebras and denoted Zinb, satisfies $\dim \mathsf{Zinb}(n) = n!$.)

Exercise 6.11. The *alternative operad* Alt is generated by one operation $a_1, a_2 \mapsto a_1 \cdot a_2$ which satisfies the relations

$$(a_1, a_2, a_3) = (-1)^\sigma (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}) \text{ for all } \sigma \in S_3,$$

where $(a_1, a_2, a_3) = (a_1 \cdot a_2) \cdot a_3 - a_1 \cdot (a_2 \cdot a_3)$ is the *associator* of this operation.

(i) Show that the Koszul dual operad $\mathsf{Alt}^!$ is generated by one operation $a_1, a_2 \mapsto a_1 \cdot a_2$ which satisfies the relations

$$(a_1a_2)a_3 = a_1(a_2a_3), \tag{6.15}$$

$$(a_1a_2)a_3 + (a_1a_3)a_2 + (a_2a_1)a_3 + (a_2a_3)a_1 + (a_3a_1)a_2 + (a_3a_2)a_1 = 0. \tag{6.16}$$

(ii) Show that over a ground field $\mathbb{F}$ of characteristic 3, the relation (6.16) can be replaced by the relation

$$[[a_1, a_2], a_3] + [[a_1, a_3], a_2] = 0 \tag{6.17}$$

for the commutator $[a_1, a_2] = a_1a_2 - a_2a_1$.

(iii) Use Exercises 5.17 and 5.20 to establish that over a field $\mathbb{F}$ of characteristic 3, we have $\dim \mathsf{Alt}^!(n) = 2^n - n$.

(iv) Dzhumadil'daev and Zusmanovich established in [82], combining the Ginzburg–Kapranov functional equation (Theorem 6.3.4.3) with fairly heavy computations, that over a field of characteristic 0 the operad Alt is not Koszul. Try to use methods of this book to establish a simpler proof of their result.

Exercise 6.12. It is well known to specialists in nonassociative rings [260, Cor. 7.1.2] that in every characteristic different from 3, an alternative algebra which is commutative is also associative. Try to find an operadic proof of that result, and to relate it to the special role of characteristic 3 for dual alternative algebras observed in Exercise 6.11.

Exercise 6.13 ([72])**.**

(i) Show that if an operad $\mathcal{E}$ is obtained from two quadratic operads $\mathcal{A}$ and $\mathcal{B}$ by a distributing rewriting rule, then the Koszul dual operad $\mathcal{E}^!$ is obtained from $\mathcal{B}^!$ and $\mathcal{A}^!$ by a distributing rewriting rule.

(ii) Assume that the operad $\mathcal{E}$ is obtained from the binary quadratic operads $\mathcal{A}$ and $\mathcal{B}$ via a filtered distributive law. Show that if the distributing rewriting rule between $\mathcal{B}^!$ and $\mathcal{A}^!$ that gives the Koszul dual operad $\mathcal{E}^!$ is split, then that rule is in fact a filtered distributive law.

Exercise 6.14. Prove claim (ii) of Proposition 6.4.1.3.

Exercise 6.15. Justify the claim on decomposition from Proposition 6.4.2.3.

Chapter 7

Commutative Gröbner Bases

7.1 Introduction

The final chapters of this book provide an introduction to the well-known theory of commutative Gröbner bases, which has many applications throughout the mathematical sciences. After much discussion, we made the somewhat unexpected decision to put these chapters at the end of the book, for the following reasons. First, as we mentioned previously, there is a natural logical progression from noncommutative Gröbner bases to Gröbner bases for operads, which cannot be extended backward to include commutative Gröbner bases.[1] Second, we are interested in commutative Gröbner bases almost exclusively for their applications to the classification of operads, which obviously requires a detailed development of the theory of operads as a prerequisite.

In addition to a brief exposition of the standard theory of (commutative) Gröbner bases, we also discuss some aspects of the theory that are not usually presented in much detail in textbooks: Robbiano's classification of monomial orders, and upper and lower bounds on the complexity of computing Gröbner bases. See the appropriate sections for bibliographical information.

Commutative Gröbner bases are an essential tool in the study of linear algebra over polynomial rings, which is the topic of the next chapter. The main problem we consider is determining how the rank of a matrix with polynomial entries behaves as a function of the variables. We give various examples of the applications of this problem to the theory of operads in the rest of this book. For further details on (commutative) Gröbner bases, we refer the reader to one of the many excellent modern introductions to computational commutative algebra and its numerous applications; we mention in particular [1, 14, 64, 65, 162, 163].

[1] We realize that this is a controversial statement, but we are prepared to defend it!

7.2 Commutative associative polynomials

7.2.1 One variable

Let us recall briefly the case of univariate polynomials which we already discussed in Section 1.2.2. For the polynomial algebra $\mathbb{F}[x]$ in one variable x over the field $\mathbb{F}$ the monomial basis consists of the nonnegative powers of x in their standard order defined by increasing degree:

$$1 = x^0 \prec x = x^1 \prec x^2 \prec x^3 \prec \cdots\cdots \prec x^n \prec x^{n+1} \prec \cdots\cdots$$

In other words, $x^m \prec x^n$ if and only if $m < n$ in the natural order on nonnegative integers. A number of important properties are satisfied by this order; we mention only two:

- It is compatible with multiplication: If u, v, w are monomials and $u \prec v$ then $uw \prec vw$. (If i, j, k are integers and $i < j$ then $i + k < j + k$.)
- For every monomial v the set $\{ u \mid u \prec v \}$, of monomials u preceding v, is finite. This allows us to use induction to prove statements about polynomials. It is essentially the well-ordering principle: every non-empty set of nonnegative integers has a least element; if j is a nonnegative integer then there are only finitely many nonnegative integers $i < j$.

7.2.2 The general case

Let us discuss general multivariate polynomials.

Definition 7.2.2.1 (Commutative monomials)**.** In the general case, the set $X = \{ x_1, \ldots, x_k \}$ of variables consists of $k \geq 1$ symbols. Consider the set $\mathsf{C}(X)$ of all *commutative monomials* in the indeterminates X which we identify with exponent sequences of length k of nonnegative integers:

$$\begin{aligned}\mathsf{C}(X) &= \{ x_1^{e_1} \cdots x_i^{e_i} \cdots x_k^{e_k} \mid e_1, \ldots, e_i, \ldots, e_k \in \mathbb{N} \} \\ &= \{ [e_1, \ldots, e_i, \ldots, e_k] \mid e_1, \ldots, e_i, \ldots, e_k \in \mathbb{N} \}.\end{aligned}$$

The (*total*) *degree*[2] of a monomial is the sum of its exponents:

$$\deg(x_1^{e_1} \cdots x_i^{e_i} \cdots x_k^{e_k}) = \sum_{i=1}^{k} e_i \in \mathbb{N}.$$

The unique monomial of degree 0 is called the *constant monomial*, and is denoted 1. The exponent $e_i \geq 0$ is called the *degree in the variable* x_i.

[2] A thorough reader would notice that in all other cases where we discuss monomials we call this number the weight, however, in the commutative case the word "degree" is too standard to be avoided.

We define a commutative associative multiplication on $\mathsf{C}(X)$ as usual by

$$\bigl(x_1^{e_1} \cdots x_i^{e_i} \cdots x_k^{e_k}\bigr)\bigl(x_1^{e'_1} \cdots x_i^{e'_i} \cdots x_k^{e'_k}\bigr) = x_1^{e_1+e'_1} \cdots x_i^{e_i+e'_i} \cdots x_k^{e_k+e'_k},$$

which corresponds to the addition of exponent sequences:

$$[e_1, \dots, e_i, \dots, e_k][e'_1, \dots, e'_i, \dots, e'_k] = [e_1 + e'_1, \dots, e_i + e'_i, \dots, e_k + e'_k].$$

(Compare the equation $\log xy = \log x + \log y$: the degree is a logarithm.)

Definition 7.2.2.2 (Commutative polynomial)**.** A *(commutative) polynomial* in the variables X over the field $\mathbb{F}$ is a (finite) linear combination of monomials in $\mathsf{C}(X)$ with coefficients from $\mathbb{F}$; two such combinations are equal if their respective coefficients are equal. Multiplication of monomials extends bilinearly to polynomials. The vector space of all such polynomials will be denoted by

$$\mathbb{F}[X] = \mathbb{F}[x_1, \dots, x_k].$$

Throughout this chapter, all monomials and polynomials are assumed commutative.

Definition 7.2.2.3 (Polynomial algebra)**.** The graded algebra $\mathbb{F}[X]$ is called the *polynomial algebra* in the variables X with coefficients in $\mathbb{F}$, or the *free commutative associative algebra* generated by X over $\mathbb{F}$.

Proposition 7.2.2.4. *The polynomial algebra $\mathbb{F}[X]$ is infinite dimensional as a vector space over $\mathbb{F}$. It is the direct sum over all nonnegative integers $n \geq 0$ of the finite dimensional homogeneous spaces $\mathbb{F}[X]_n$ spanned by the monomials of total degree n. Moreover, $\mathbb{F}[X]$ is a graded algebra in the sense that $\mathbb{F}[X]_m\mathbb{F}[X]_n \subseteq \mathbb{F}[X]_{m+n}$ for all $m, n \geq 0$.*

Proof. Exercise 7.1. □

Let $\mathsf{C}(X)_n$ be the subset of $\mathsf{C}(X)$ consisting of the monomials of total degree $n \geq 0$; this subset forms a basis of $\mathbb{F}[X]_n$. The size of $\mathsf{C}(X)_n$ is the number of solutions in nonnegative integers of the equation $e_1 + \cdots + e_k = n$.

Lemma 7.2.2.5. *Let k, n be nonnegative integers. The number of distinct monomials of total degree n in k variables is the binomial coefficient*

$$|\mathsf{C}(X)_n| = \binom{n+k-1}{k-1}$$

Proof. Let us explain two different proofs, both of which may be useful both in this context and for other topics discussed in this book.

A combinatorial argument conventionally known as “stars-and-bars” goes as follows. We want to determine the number of ordered k-tuples $(e_1, \dots, e_k)$ of nonnegative integers satisfying $e_1 + \cdots + e_k = n$. Let us encode such a k-tuple by a sequence of n stars separated into k groups by $k-1$ bars, the number of stars in the i-th group being e_i for each $i \leq k$; such a sequence uniquely determines the corresponding k-tuple. The number of such sequences is equal to the binomial coefficient $\binom{n+k-1}{k-1}$, since in the $n+k-1$ slots occupied by n stars and $k-1$ bars, we must choose the positions of $k-1$ bars in order to determine the sequence.

A more algebraic argument goes as follows. Note that we have an isomorphism of vector spaces

$$\mathbb{F}[x_1, \ldots, x_k] = \mathbb{F}[x_1] \otimes \cdots \otimes \mathbb{F}[x_k],$$

and hence the Hilbert series of $\mathbb{F}[x_1, \ldots, x_k]$ (the generating function for dimensions of graded components of this algebra) is equal to the product of the Hilbert series of the tensor factors, each of which is $\frac{1}{1-t}$ because for polynomials in one variable each graded component is one-dimensional. Therefore, we are interested in the coefficient of t^n of the formal power series $\frac{1}{(1-t)^k}$, which is equal to

$$(-1)^n \binom{-k}{n} = \binom{n+k-1}{n} = \binom{n+k-1}{k-1}.$$

□

7.2.3 Monomial orders

In the commutative case, monomial orders (sometimes called term orders) behave quite differently from the case of associative algebras (where monomials are noncommutative words) and the case of operads (where monomials are trees whose vertices are decorated by generating operations). In particular, it is only in the commutative case that it is reasonable to expect a complete classification of monomial orders; this has been achieved by Robbiano [218, 219] and Weispfenning [257]. For now, we shall fix the basic definitions needed for Gröbner bases, however later in this chapter we shall explain the classification result.

Definition 7.2.3.1 (Monomial order)**.** A *monomial order* is a total well-order on $\mathsf{C}(X)$ which is *multiplicative*: for all monomials m, m', m'', if $m' \prec m''$ then $mm' \prec mm''$.

It can be shown (Exercise 7.3) that the well-order condition is equivalent to the statement that every strictly decreasing sequence is finite. This is an essential fact since it allows inductive proofs of termination of algorithms.

Example 7.2.3.2. Let's first consider the standard dictionary order on "words" (monomials) in the $k = 2$ letters a and b, assuming that $a \prec b$. This is *not* a well-order, since the subset $\{\, a^e b \mid e \in \mathbb{N} \,\}$ has no least element:

$$\cdots \prec a^e b \prec \cdots \prec a^2 b \prec ab \prec b.$$

This is perhaps clearer if we avoid exponents:

$$\cdots \prec \underbrace{a \cdots a}_{e} b \prec \cdots \prec aab \prec ab \prec b.$$

It is a good exercise to give a precise definition of the dictionary order on any finite set of letters; see Exercise 7.5.

If we apply dictionary order to sequences of exponents, rather than sequences of variables, then we have much better luck. This leads directly to the three standard monomial orders:

- `plex`: pure lexicographic order (Maple command: plex)
- `dlex`: degree (or graded) lexicographic order (Maple command: grlex)
- `glex`: degree (or graded) reverse lexicographic order (Maple command: tdeg)

Combinations and variations of these provide (in a sense) all other monomial orders, as we will see below.

Definition 7.2.3.3 (Pure lexicographic order)**.** The `plex` (*pure lexicographic*) order on $\mathsf{C}(X)$ is defined as follows: Given $v = [e_1, \dots, e_k]$ and $w = [f_1, \dots, f_k]$ with $v \neq w$, let i be the least index for which $e_i \neq f_i$. Then $v \prec w$ if and only if $e_i < f_i$. Note we can also define i as the greatest index for which $e_1 = f_1, \dots, e_{i-1} = f_{i-1}$: we determine the longest common initial sequence and then compare the next exponents. Also note that if we define $v \prec' w$ if and only if $w \prec v$ then $\prec'$ is not a monomial order (why?).

Example 7.2.3.4. Let $k = 3$ and write a, b, c instead of x_1, x_2, x_3. Consider the monomials $v = [1, 2, 3] = ab^2c^3$ and $w = [3, 2, 1] = a^3b^2c$. Then in `plex` order we have $v \prec w$ since $e_1 = 1$ but $f_1 = 3$ (here $i = 1$). Warning: Even though this order is called pure lexicographic, it is not quite the dictionary order. Writing out the variables, we have $v = abbccc$ and $w = aaabbc$, and clearly w would precede v if these were words in a dictionary.

Recall that x_i corresponds to the i-th standard basis vector e_i for $1 \leq i \leq k$. For the `plex` order this implies the counter-intuitive fact that

$$x_k \prec x_{k-1} \prec \cdots \prec x_2 \prec x_1, \tag{7.1}$$

which provides another difference between `plex` and dictionary order.

In the general definition of a monomial order, there is no reason to distinguish among the variables, but when we deal with a particular problem, the variables may behave quite differently or represent quite different information (for example, some variables may be primary and others secondary, etc.). We may apply an arbitrary permutation to the variables before applying a monomial order. This is the most convenient way of dealing with situations like (7.1).

Definition 7.2.3.5 (Action of permutations on orders)**.** Let $\sigma \in S_k$ be any permutation of $1, \dots, k$ and let $\prec$ be any monomial order. The monomial order $\prec_\sigma$ is defined in terms of the action of S_k permuting the coordinates of vectors in $\mathbb{N}^k$. That is, we first set

$$\sigma \cdot [e_1, \dots, e_i, \dots, e_k] = [e_{\sigma(1)}, \dots, e_{\sigma(i)}, \dots, e_{\sigma(k)}],$$

and then we define $\prec_\sigma$ in terms of $\prec$ by

$$v \;\prec_\sigma\; w \quad\iff\quad \sigma^{-1} \cdot v \;\prec\; \sigma^{-1} \cdot w.$$

(To cancel the σ on $\prec$ we need to apply σ^{-1}.) That is, given $v = [e_1, \dots, e_k]$ and $w = [f_1, \dots, f_k]$ with $v \neq w$, let i be the least index satisfying the inequality $e_{\sigma^{-1}(i)} \neq f_{\sigma^{-1}(i)}$. Then $v \prec w$ if and only if $e_{\sigma^{-1}(i)} > f_{\sigma^{-1}(i)}$ (see Exercise 7.6).

The `plex` order does not take into account the total degrees of the monomials. It is often beneficial to consider orders for which monomials of lower degree precede monomials of higher degree. This leads directly to the definitions of the next two monomial orders.

Definition 7.2.3.6 (Degree lexicographic order)**.** The `dlex` (*degree lexicographic*) order on $\mathsf{C}(X)$ is defined as follows. Given $v = [e_1, \dots, e_k]$ and $w = [f_1, \dots, f_k]$ with $v \neq w$, we say that $v \prec w$ if and only if

- either $\deg(v) < \deg(w)$,
- or $\deg(v) = \deg(w)$ and $v \prec w$ in `plex` order.

Our final example of monomial order appears at first sight to be simply the `dlex` order permuted by the reversal permutation ρ of order 2 which transposes x_i and x_{k+1-i} for $i = 1, \dots, \lfloor k/2 \rfloor$. In fact it is not!

Definition 7.2.3.7 (Graded reverse lexicographic order)**.** The `glex` (*graded reverse lexicographic*)[3] order on $\mathsf{C}(X)$ is defined as follows. Given $v = [e_1, \dots, e_k]$ and $w = [f_1, \dots, f_k]$ with $v \neq w$, we say that $v \prec w$ if and only if

- either $\deg(v) < \deg(w)$,
- or $\deg(v) = \deg(w)$ and $e_i > f_i$ where i is the *greatest* index with $e_i \neq f_i$.

"Reverse" refers to two aspects of this definition: first, we look at the *rightmost* position where the exponents differ; and second, $v \prec w$ if and only if $e_i > f_i$.

Let us also recall an order that generalizes both `plex` and `glex`.

[3] Some authors say "grevlex" but that sounds a bit fishy to us.

Definition 7.2.3.8 (Elimination order)**.** Let $k = a_1 + \cdots + a_s$ be a partition, which we may view as a partition of the alphabet X into s groups of consecutive variables. The *elimination order*, or the *multigraded lexicographic order* associated to this partition is defined as follows: Given $v = [e_1, \dots, e_k]$ and $w = [f_1, \dots, f_k]$ with $v \neq w$, we say that $v \prec w$ if and only if

- either
$$\left[\sum_{i=1}^{a_1} e_i, \sum_{i=a_1+1}^{a_2} e_i, \dots, \sum_{i=a_{s-1}+1}^{a_s} e_i \right] \prec \left[\sum_{i=1}^{a_1} f_i, \sum_{i=a_1+1}^{a_2} f_i, \dots, \sum_{i=a_{s-1}+1}^{a_s} f_i \right]$$
for the lexicographic order of sequences,
- or
$$\left[\sum_{i=1}^{a_1} e_i, \sum_{i=a_1+1}^{a_2} e_i, \dots, \sum_{i=a_{s-1}+1}^{a_s} e_i \right] \prec \left[\sum_{i=1}^{a_1} f_i, \sum_{i=a_1+1}^{a_2} f_i, \dots, \sum_{i=a_{s-1}+1}^{a_s} f_i \right]$$
and $v \prec w$ with respect to the `glex` order.

Example 7.2.3.9. Consider the 35 monomials of the form $a^i b^j c^k$ with total degree at most 4. We sort these monomials in six different ways where "reverse" means reversing the usual order of the variables ($abc \longleftrightarrow cba$): `plex`, reverse `plex`, `dlex`, reverse `dlex`, `glex`, reverse `glex`:

$$[1, c, c^2, c^3, c^4, b, bc, bc^2, bc^3, b^2, b^2c, b^2c^2, b^3, b^3c, b^4, a, ac, ac^2, ac^3, ab, \\ abc, abc^2, ab^2, ab^2c, ab^3, a^2, a^2c, a^2c^2, a^2b, a^2bc, a^2b^2, a^3, a^3c, a^3b, a^4]$$

$$[1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, b^2, ab^2, a^2b^2, b^3, ab^3, b^4, c, ac, a^2c, a^3c, bc, \\ abc, a^2bc, b^2c, ab^2c, b^3c, c^2, ac^2, a^2c^2, bc^2, abc^2, b^2c^2, c^3, ac^3, bc^3, c^4]$$

$$[1, c, b, a, c^2, bc, b^2, ac, ab, a^2, c^3, bc^2, b^2c, b^3, ac^2, abc, ab^2, a^2c, a^2b, a^3, c^4, \\ bc^3, b^2c^2, b^3c, b^4, ac^3, abc^2, ab^2c, ab^3, a^2c^2, a^2bc, a^2b^2, a^3c, a^3b, a^4]$$

$$[1, a, b, c, a^2, ab, b^2, ac, bc, c^2, a^3, a^2b, ab^2, b^3, a^2c, abc, b^2c, ac^2, bc^2, c^3, a^4, \\ a^3b, a^2b^2, ab^3, b^4, a^3c, a^2bc, ab^2c, b^3c, a^2c^2, abc^2, b^2c^2, ac^3, bc^3, c^4]$$

$$[1, c, b, a, c^2, bc, ac, b^2, ab, a^2, c^3, bc^2, ac^2, b^2c, abc, a^2c, b^3, ab^2, a^2b, a^3, c^4, \\ bc^3, ac^3, b^2c^2, abc^2, a^2c^2, b^3c, ab^2c, a^2bc, a^3c, b^4, ab^3, a^2b^2, a^3b, a^4]$$

$$[1, a, b, c, a^2, ab, ac, b^2, bc, c^2, a^3, a^2b, a^2c, ab^2, abc, ac^2, b^3, b^2c, bc^2, c^3, a^4, \\ a^3b, a^3c, a^2b^2, a^2bc, a^2c^2, ab^3, ab^2c, abc^2, ac^3, b^4, b^3c, b^2c^2, bc^3, c^4]$$

7.3 Equivalent definitions of commutative Gröbner bases

In this section, instead of developing the theory and algorithms in the usual way, we attempt to provide more conceptual insight by discussing three different but equivalent definitions of Gröbner bases for ideals in polynomial algebras. The technical details can of course be found in any of the standard textbooks already mentioned, but we cannot avoid some basic definitions. Throughout this chapter, we fix some monomial order Ξ of $\mathsf{C}(X)$, and use all notions of Chapter 1, like the leading monomials, monic polynomials, etc., with respect to that chosen order.

7.3.1 Ideals, generators, and zero sets

Definition 7.3.1.1 (Ideal generated by several polynomials)**.** Let $I \subset \mathbb{F}[X]$ be an ideal, and let $f_1, \dots, f_\ell \in I$ be a set of *generators* for I; this means that

$$g \in I \qquad \Longleftrightarrow \qquad g = \sum_{i=1}^{\ell} h_i f_i \text{ for some } h_1, \dots, h_\ell \in \mathbb{F}[X].$$

In this case we write $I = (\, f_1, \dots, f_\ell \,)$ and we say I is *generated* by $f_1, \dots, f_\ell$.

If the set of generators $\{f_1, \dots, f_\ell\}$ has one (and hence all) of a number of equivalent special properties which are the main topic of this section, then it may be used to solve many fundamental problems in commutative algebra. The most important of these is the solution of systems of polynomial equations, in this case the equations $\{f_1 = 0, \dots, f_\ell = 0\}$ in the variables $x_1, \dots, x_k$. This is equivalent to finding the zero set $V(I)$ of the ideal I.

Definition 7.3.1.2 (Zero set of the ideal)**.** For an ideal $I \subset \mathbb{F}[x_1, \dots, x_k]$, the *zero set* $V(I)$ consists of all k-tuples $[a_1, \dots, a_k] \in \mathbb{F}^k$ such that $g(a_1, \dots, a_k) = 0$ for all $g \in I$. If $I = (\, f_1, \dots, f_\ell \,)$ then $V(I)$ is the set of all k-tuples $[a_1, \dots, a_k] \in \mathbb{F}^k$ for which $f_i(a_1, \dots, a_k) = 0$ for $i = 1, \dots, \ell$.

Remark 7.3.1.3. In the case of one variable, every ideal is principal, and the Euclidean algorithm (Algorithm 1.2.2.2) for computing greatest common divisors answers essentially all of the important questions. In the multivariate case, the polynomial algebra is no longer a principal ideal domain, but it still has unique factorization, so the greatest common divisor of two polynomials still can be defined. However, greatest common divisors cannot be easily computed, and even if they could be, we would not learn much from it, since for example the ideal (f, g) may be proper even though $\textsc{gcd}(f, g) = 1$.

7.3.2 First definition of a Gröbner basis: leading monomials

Definition 7.3.2.1 (First definition of a Gröbner basis)**.** Suppose that the ideal $I \subset \mathbb{F}[X]$ is generated by the finite set $\{f_1, \dots, f_\ell\}$. This set of generators is a *Gröbner basis* for I if and only if

$$\big(\,\textsc{lm}(I)\,\big) = \big(\,\textsc{lm}(f_1), \dots, \textsc{lm}(f_\ell)\,\big). \tag{7.2}$$

That is, the ideal generated by the leading monomials of I coincides with the ideal generated by the leading monomials of $f_1, \dots, f_\ell$.

In one direction, Equation (7.2) is trivial:

$$f_1, \dots, f_\ell \in I \quad\implies\quad \textsc{lm}(f_1), \dots, \textsc{lm}(f_\ell) \in \textsc{lm}(I),$$

and so the right side is contained in the left side. However, the reverse inclusion does not always hold when there is more than one variable, and the converse is a characteristic property of Gröbner bases: every leading monomial of I is a multiple of the leading monomial of one (or more) of the generators $f_1, \dots, f_\ell$.

Example 7.3.2.2. Here is an example for which the left side of (7.2) is not contained in the right side. Let $k = 2$ and write $\mathcal{P} = \mathbb{F}[x, y]$. Let $I = (\,f, g\,)$ where $f = x^2 - 1$ and $g = xy - 1$. We assume that our monomial order sorts first by the degree, so that $\textsc{lm}(f) = x^2$ and $\textsc{lm}(g) = xy$. Consider the following element of I:

$$h = yf - xg = y(x^2 - 1) - x(xy - 1) = x^2y - y - x^2y + x = x - y.$$

Both x and y have degree 1, and so which of them is $\textsc{lm}(h)$ depends on the monomial order. But neither x nor y is a multiple of either x^2 or xy. So f, g do not form a Gröbner basis of the ideal they generate.

7.3.3 Second definition of a Gröbner basis: long division

Let us briefly recall the notion of long division of a polynomial $g \in \mathbb{F}[X]$ by a set of monic polynomials $f_1, \dots, f_\ell$.

Definition 7.3.3.1 (Multivariate long division)**.** The *multivariate long division* of a polynomial g by a set $f_1, \dots, f_\ell \in \mathcal{P}$ is a repetition of simple *reduction steps.* For each of those steps, we search for a term cm in g (where $c \in \mathbb{F} \setminus 0$ and $m \in M$) whose monomial m is a multiple $m = m'm''$ of the leading monomial $m' = \textsc{lm}(f_i)$ for some $i = 1, \dots, \ell$, and then replace g by $g' = g - c(m/m')f_i$. We repeatedly perform these steps, and the algorithm terminates when there are no more such terms in g. The final value of g is the *remainder* of the original value of g modulo $f_1, \dots, f_\ell$.

This algorithm is only well-defined in the case of one variable; in the multivariate case, the algorithm can give different results depending on our choices of which term in g to eliminate at each step.

Example 7.3.3.2. Let us divide $g = x^2y$ by $f_1 = x^2 - 1$ and $f_2 = xy - 1$. Our choice of whether to start with f_1 or f_2 determines the output. If we first use f_1 then we obtain y, but if we first use f_2 then we obtain x:

$$g = x^2y \longrightarrow x^2y - y(x^2 - 1) = y, \qquad g = x^2y \longrightarrow x^2y - x(xy - 1) = x.$$

This lack of uniqueness cannot happen for a Gröbner basis.

Definition 7.3.3.3 (Second definition of a Gröbner basis)**.** Version 1: Suppose that the ideal $I \subset \mathbb{F}[X]$ is generated by the finite set $\{f_1, \dots, f_\ell\}$. This set of generators is a *Gröbner basis* for I if and only if every polynomial g has a unique remainder modulo $f_1, \dots, f_\ell$: no matter what choices we make during long division we always obtain the same result.

Version 2: This version of the definition shows that a Gröbner basis for an ideal I provides an effective membership test for I. The generating set $\{f_1, \dots, f_\ell\}$ for the ideal I is a *Gröbner basis* for I if and only if for all polynomials g the following two conditions are equivalent:

- $g \in I$,
- the remainder of g modulo $f_1, \dots, f_\ell$ is uniquely defined and equals 0.

7.3.4 Third definition of a Gröbner basis: the Church–Rosser property

Definition 7.3.4.1 (One-step reducibility)**.** Consider the reduction step in the division of a polynomial g by a set of polynomials $\{f_1, \dots, f_\ell\}$: for some term cm in g and some f_i for which m is a multiple of $m' = \textsc{lm}(f_i)$ we define $g' = g - c(m/m')f_i$. For fixed $f_1, \dots, f_\ell$, we can regard the set of all such ordered pairs (g, g') as a binary relation $\to$ on $\mathbb{F}[X]$. In other words, we write $g \to g'$ to mean that g is *one-step reducible* to g' using $f_1, \dots, f_\ell$.

Strictly speaking, this binary relation depends in an essential way on $f_1, \dots, f_\ell$, and so we really ought to write

$$g \xrightarrow[f_1, \dots, f_\ell]{} g' \quad \text{instead of} \quad g \to g',$$

but that level of precision is obviously more cumbersome than helpful.

In what follows, we use terminology of abstract rewriting systems from Section 2.6.1. Let $(A, \to)$ be an ARS. We denote by $\leftrightarrow$ the symmetric closure of $\to$, or in other words the union of the relations $\to$ and $\leftarrow$; thus $g \leftrightarrow g'$ if and only if either $g \to g'$ or $g \leftarrow g'$. We write $\overset{*}{\leftrightarrow}$ for the reflexive transitive closure of $\leftrightarrow$, which is also the reflexive, symmetric, transitive closure of $\to$; that is, the smallest equivalence relation containing the original relation $\to$. The diagram representing $\overset{*}{\leftrightarrow}$ is obtained from (2.16) by making each arrow bidirectional:

$$g = g_0 \longleftrightarrow g_1 \longleftrightarrow g_2 \longleftrightarrow \cdots \longleftrightarrow g_{s-1} \longleftrightarrow g_s = g'. \tag{7.3}$$

Definition 7.3.4.2 (Church–Rosser property)**.** An ARS $(A, \to)$ is said to have the *Church–Rosser property* if $\overset{*}{\leftrightarrow}$-equivalence implies joinability. That is, the relation is Church–Rosser if for all $f, g \in A$ we have

$$f \overset{*}{\leftrightarrow} g \quad \Longrightarrow \quad f \downarrow g.$$

(The converse is trivial by definition of the relations.) In other words, if f and g can be connected by a sequence of left-right arrows as in (7.3), then they have a common successor h.

The importance of this property was first pointed out in the work of Church and Rosser [59] on mathematical logic.

Definition 7.3.4.3 (Third definition of a Gröbner basis)**.** Suppose that the ideal $I \subseteq \mathbb{F}[X]$ is generated by the finite set $\{f_1, \ldots, f_\ell\}$. This set of generators is a *Gröbner basis* for I if and only if the one-step reducibility relation $\to$ has the Church–Rosser property.

7.3.5 Equivalence of the three definitions

We now state without proof the theorem guaranteeing that our three definitions of Gröbner bases are equivalent.

Theorem 7.3.5.1. *Let $S = \{f_1, \ldots, f_\ell\} \subset \mathbb{F}[X]$ be a finite set of polynomials with coefficients in $\mathbb{F}$, and let $I = (S)$ be the ideal generated by S. The following conditions on I are equivalent:*

- $\big(\, \textsc{lm}(I) \,\big) = \big(\, \{\, \textsc{lm}(f) \mid f \in S \,\} \,\big)$
- *Every polynomial g has a unique remainder after multivariate division by S, and this remainder is 0 if and only if $g \in I$.*
- *The one-step reducibility relation $g \to h$ on $\mathbb{F}[X]$ has the Church–Rosser property.*

Proof. A proof may be found in any standard textbook on commutative Gröbner bases. □

Corollary 7.3.5.2. *Let I be an ideal in $\mathbb{F}[X]$ and let S be a Gröbner basis for I. Let N be the subspace of $\mathbb{F}[X]$ spanned by the monomials which are not divisible by the leading monomial of any element of S:*

$$N = \operatorname{span}_{\mathbb{F}}\{\, m \in \mathsf{C}(X) \mid m \neq m_1 \, \textsc{lm}(f), \ m_1 \in \mathsf{C}(X), \ f \in S \,\}.$$

There we have the following direct sum of subspaces and linear isomorphism:

$$\mathbb{F}[X] = I \oplus N, \qquad\qquad \mathbb{F}[X]/I \cong N.$$

If we define multiplication on elements of N by letting the product of f and g be the (unique) remainder of fg modulo S, then $\mathbb{F}[X]/I \cong N$ is an isomorphism of algebras.

Proof. For every polynomial g, long division gives $g = q + r$ where $q \in I$ since it is the $\mathbb{F}[X]$-linear combination of the elements of S determined by the reduction steps, and $r \in N$ since no further reduction steps are possible. Hence $\mathcal{P} = I + N$. If $g \in I \cap N$ then since $g \in I$, uniqueness gives $g = q + 0$, and since $g \in N$, uniqueness gives $g = 0 + r$; hence $q = r = 0$ and so $g = 0$. The rest of the proof is left as an exercise for the reader (Exercise 7.11). □

7.3.6 S-polynomials and Buchberger's criterion

Definition 7.3.6.1 (S-polynomial)**.** Let G be a finite set of monic polynomials generating the ideal $I = (G)$. For $f_1, f_2 \in G$ the monomials d, m_1, m_2 are uniquely determined by the following conditions:

$$d = \textsc{gcd}(\,\textsc{lm}(f_1),\, \textsc{lm}(f_2)\,), \qquad \textsc{lm}(f_1) = dm_1, \qquad \textsc{lm}(f_2) = dm_2.$$

Clearly, we have

$$m_1\,\textsc{lm}(f_2) = m_2\,\textsc{lm}(f_1).$$

Hence the leading monomials cancel in the following element of I:

$$g = m_1 f_2 - m_2 f_1.$$

This polynomial g is called the *S-polynomial* of the polynomials f_1 and f_2.

S-polynomials are used for Buchberger's criterion, our final equivalent definition for Gröbner basis, and the only one of the four which leads directly to an algorithm for computing a Gröbner basis of an ideal from an arbitrary set of generators for the ideal.

Theorem 7.3.6.2 (Buchberger's criterion)**.** *Let $G = \{f_1, \dots, f_\ell\}$ be a subset of $\mathbb{F}[x_1, \dots, x_k]$ generating the ideal $I = (G)$. Then G is a Gröbner basis for I if and only if every S-polynomial of two elements $f_i, f_j \in G$ has remainder* 0 *after multivariate long division by G.*

Proof. A proof may be found in any standard textbook on Gröbner bases. □

Note that in Definition 7.3.6.1 we could in principle consider all possible common divisors d, not just the greatest common divisor of two leading monomials. We have already seen that with more general structures there may be several different d for which an S-polynomial is defined (various overlaps of leading monomials), so it is natural to ask for an explanation of why only the greatest common divisors are needed.

Lemma 7.3.6.3. *For commutative polynomials, considering S-polynomials for all common divisors and for greatest common divisors only leads to equivalent versions of Buchberger's criterion.*

Proof. In the notation of Definition 7.3.6.1, suppose that $d = d'd''$ where $d' \neq 1$ and $d'' \neq 1$. Using d' instead of d, we obtain

$$\text{LM}(f_1) = d'(d''m_1), \quad \text{LM}(f_2) = d'(d''m_2), \quad (d''m_1)\,\text{LM}(f_2) = (d''m_2)\,\text{LM}(f_1),$$

so we should replace m_1, m_2 by $d''m_1, d''m_2$, respectively. It follows that the S-polynomial corresponding to d' is simply a monomial multiple of the S-polynomial for d:

$$g' = (d''m_1)f_2 - (d''m_2)f_1 = d'(m_1f_2 - m_2f_1) = d'g.$$

Thus, if g has the remainder 0 then g' has the remainder 0. □

A useful informal exercise is to identify exactly where commutativity is necessary in the last proof!

Remark 7.3.6.4. It is also true that S-polynomials corresponding to $d = 1$ are redundant for purposes of Buchberger's criterion. We leave it to the reader to either find a proof of that or read the proof in a textbook of their choice.

Buchberger's criterion leads directly to the celebrated Buchberger's algorithm, which takes as input any set of generators for the ideal I and produces as output a Gröbner basis for I. To present something different from a usual description of that algorithm which can be found in any textbook on commutative Gröbner bases, we discuss a simple Maple code that implements that algorithm from scratch in Appendix A.

7.4 Classification of commutative monomial orders

7.4.1 The classification theorem

Robbiano [218] has classified all possible monomial orders in k variables $x_1, \ldots, x_k$; see also [219] for his general theory of graded structures on commutative rings. Robbiano's proof was simplified soon afterward in a short note by Weispfenning [257]. For further information about the classification of monomial orders, see Kreuzer and Robbiano [162], especially section 1.4 and tutorials 9, 10. Becker and Weispfenning [14] present this material in the context of abstract reduction relations; see especially chapter 4 and section 5.1. The rest of this section is devoted to an exposition of Robbiano's results; we closely follow his original paper.

Definition 7.4.1.1. We fix a positive integer n and write $\mathbb{T}$ for the semigroup (in fact monoid) of monomials in the variables $x_1, \ldots, x_n$ under multiplication as defined previously. We write $\mathbb{N}$ for the semigroup of nonnegative integers under addition, and $\mathbb{N}^n$ for the semigroup of n-tuples under component-wise addition. Clearly the map $\phi\colon \mathbb{T} \to \mathbb{N}^n$ is an isomorphism of semigroups, and is in fact the multidegree function

$$\phi(m) = (\,\deg_{x_1}(m),\, \dots,\, \deg_{x_n}(m)\,).$$

Thus a monomial order $\prec$ on $\mathbb{F}[x_1, \dots, x_n]$ is equivalent to a total order $\prec$ on $\mathbb{N}^n$ which makes $\mathbb{N}^n$ into a totally ordered positive semigroup, where positive means that $(0, \dots, 0) \prec (d_1, \dots, d_n)$ for all $(d_1, \dots, d_n) \neq (0, \dots, 0)$.

A commutative semigroup can be embedded into a group if and only if the semigroup is cancellative; the proof is analogous to the construction of the field of fractions of an integral domain [60]. Since $\mathbb{N}^n$ is a free commutative semigroup, its minimal embedding is into the free abelian group $\mathbb{Z}^n$. Thus a monomial order $\prec$ on $\mathbb{F}[x_1, \dots, x_n]$ is equivalent to a total order $\prec$ on $\mathbb{Z}^n$ for which the subsemigroup $\mathbb{N}^n$ is positive. For any group G, a total order is determined by the positive elements G^+, since $v \prec w$ if and only if $0 \prec w - v$.

Lemma 7.4.1.2. *Every total order on $\mathbb{Z}^n$ extends uniquely to $\mathbb{Q}^n$.*

Proof. For any $w = (q_1, \dots, q_n) \in \mathbb{Q}^n$ we write uniquely

$$w = \left(\frac{r_1}{s_1}, \cdots, \frac{r_n}{s_n} \right), \qquad \textsc{gcd}(r_i, s_i) = 1 \quad (i = 1, \dots, n).$$

Define $d = \textsc{lcm}(s_1, \dots, s_n)$ so that $dw \in \mathbb{Z}^n$ and $d \in \mathbb{Z}$ is positive and as small as possible. Using the semigroup operation, $dw = w + \cdots + w$ (d summands), and hence we may define $0 \prec w$ in $\mathbb{Q}^n$ if and only if $0 \prec dw$ in $\mathbb{Z}^n$. □

For any subset $G \subseteq \mathbb{Q}^n$ we write as usual G^+ and G^- for the positive and negative elements of G with respect to the total order:

$$G^+ = \{\, w \in G \mid 0 \prec w \,\}, \qquad G^- = \{\, w \in G \mid w \prec 0 \,\}.$$

We now embed $\mathbb{Q}^n$ into $\mathbb{R}^n$ so that we can take advantage of the Euclidean geometry of $\mathbb{R}^n$ induced by the usual scalar product which we denote by $v \cdot w$.

Definition 7.4.1.3. If $G \subseteq \mathbb{Q}^n$ is a subspace with $\dim_{\mathbb{Q}}(G) = r$ then we write $G_{\mathbb{R}} = G \otimes_{\mathbb{Q}} \mathbb{R}$ for the subspace of $\mathbb{R}^n$ spanned by G; we have $\dim_{\mathbb{R}}(G_{\mathbb{R}}) = r$.

Definition 7.4.1.4. For any subspace $G \subseteq \mathbb{Q}^n$ we define the subset $I_G \subseteq G_{\mathbb{R}}$:

$$I_G = \{\, p \in G_{\mathbb{R}} \mid B_\epsilon(p) \cap G^+ \neq \emptyset,\, B_\epsilon(p) \cap G^- \neq \emptyset, \text{ for all } \epsilon > 0 \,\},$$

where $B_\epsilon(p)$ is the open ball in $\mathbb{R}^n$ centered at p with radius $\epsilon > 0$. That is, I_G consists of those $p \in G_{\mathbb{R}}$ for which every open neighborhood of p contains both positive and negative elements from G.

Lemma 7.4.1.5. *If $\dim_{\mathbb{Q}}(G) = r$ then I_G is a subspace of $G_{\mathbb{R}}$ and $\dim_{\mathbb{R}}(I_G) = r - 1$.*

Proof. To show that I_G is a subspace, suppose that $p_1, p_2 \in I_G$. Then for any $\epsilon > 0$ there exist $q_1, q_2 \succ 0$ with

$$|q_1 - p_1| < \epsilon/2, \qquad |q_2 - p_2| < \epsilon/2.$$

Then $q_1 + q_2 \succ 0$ and the triangle inequality gives

$$|(q_1 + q_2) - (p_1 + p_2)| < \epsilon.$$

Hence the ball of radius ϵ centered at $p_1 + p_2$ contains a positive element, and the argument for negative elements is similar. The proof for scalar multiplication is left to the reader as Exercise 7.13.

Define the function $\sigma\colon G_{\mathbb{R}} \setminus I_G \to \{\pm 1\}$ as follows: for $p \in G_{\mathbb{R}} \setminus I_G$,

$$\sigma(p) = \begin{cases} +1 & \text{if } B_\epsilon(p) \cap G \subset G^+ \text{ for some } \epsilon > 0 \\ -1 & \text{if } B_\epsilon(p) \cap G \subset G^- \text{ for some } \epsilon > 0 \end{cases} \tag{7.4}$$

That is, $\sigma(p) = +1$ (resp. -1) if every rational point sufficiently close to p is positive (resp. negative) in the semigroup order on $\mathbb{Q}^n$. Since σ is a surjective and continuous map (Exercise 7.14), and $\{\pm 1\}$ has the discrete topology, it follows that $G_{\mathbb{R}} \setminus I_G$ must be disconnected, and since I_G is a subspace we cannot have $\dim_{\mathbb{R}}(I_G) < r - 1$. Thus $\dim_{\mathbb{R}}(I_G) \geq r - 1$.

Since $G \subset \mathbb{Q}^n$ is a totally ordered group and has dimension r as a rational vector space, we may choose positive elements $e_1, \dots, e_r \in G^+$ which form a basis for G over $\mathbb{Q}$. But then the set of all rational linear combinations of these basis elements with positive rational coefficients is a subset of G^+, hence properly contained in G, and so $\dim_{\mathbb{R}}(I_G) \leq r - 1$. □

As before, $G \subseteq \mathbb{Q}^n$ is a subspace with $\dim_{\mathbb{Q}}(G) = r$, and $\mathbb{Q}^n$ also has the compatible structure of a totally ordered abelian group. We have seen that I_G is a hyperplane (subspace of codimension 1) in $G_{\mathbb{R}}$.

Definition 7.4.1.6. We write $U(G)$ for the line (1-dimensional subspace) of $G_{\mathbb{R}}$ orthogonal to I_G with respect to the restriction of the usual scalar product on $\mathbb{R}^n$ to $G_{\mathbb{R}}$. We write $U(G)^+ = U(G) \cap \sigma^{-1}(1)$ where σ is defined by (7.4); this is the *positive half* of $U(G)$.

Definition 7.4.1.7. We write $\mathbb{R}_{\mathbb{Q}}$ for the 1-dimensional real vector space $\mathbb{R}$ regarded as an infinite-dimensional vector space over $\mathbb{Q}$. For any vector $v \in \mathbb{R}^n$ we write $d(v)$ for the dimension (over $\mathbb{Q}$) of the subspace of $\mathbb{R}_{\mathbb{Q}}$ spanned by the components of v; we call $d(v)$ the *rational dimension* of v. Since $d(v)$ is constant on the set of nonzero real multiples of v, it is uniquely determined on $U(G)^+$.

Example 7.4.1.8. We can modify Definition 7.4.1.7 in the obvious way to deal with vectors $v \in \mathbb{C}^n$ (although in this case we certainly cannot talk about total orders). For each $n \geq 1$, let $\omega_n \in \mathbb{C}$ be a primitive n-th root of unity, and let $v_n = [1, \omega_n, \dots, \omega_n^{n-1}]$. Write $\alpha = \frac{1}{2}(-1 + \sqrt{-3})$ so that

$$v_1 = [1], \qquad v_2 = [1, -1], \qquad v_3 = [1, \alpha, \overline{\alpha}], \qquad v_4 = [1, i, -1, -i].$$

Then clearly $d(v_n) = 1, 1, 2, 2$ for $n = 1, 2, 3, 4$. For $n = 5$ the last 4 components of v_5 are as follows where $\epsilon, \eta \in \{\pm 1\}$ are independent signs:

$$\frac{1}{4}\left(-1 + \epsilon\sqrt{5} + \eta\sqrt{-2}\sqrt{5 + \epsilon\sqrt{5}} \right)$$

Hence $d(\omega_5) = 4$. See Exercise 7.15.

Lemma 7.4.1.9. *For every $v \in G_{\mathbb{R}}$ we have $d(v) \leq r = \dim_{\mathbb{Q}}(G)$.*

Proof. Let $\{v_1, \dots, v_r\}$ be a basis for G over $\mathbb{Q}$; this is also a basis for $G_{\mathbb{R}}$ over $\mathbb{R}$. Thus every $v \in G_{\mathbb{R}}$ has the form $v = a_1 v_1 + \cdots + a_r v_r$ for some $a_1, \dots, a_r \in \mathbb{R}$. Since the components of $v_1, \dots, v_r$ belong to $\mathbb{Q}$, it follows that the rational vector space spanned by the components of v is contained in the span of $a_1, \dots, a_r$ and hence has dimension $\leq r$. □

Definition 7.4.1.10. The *lexicographic* total order $\prec_{\text{lex}}$ on the groups $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$ is determined by defining the positive n-tuples to be those whose first nonzero component is positive. A total order $\prec$ on $\mathbb{G}^n$ (for $\mathbb{G} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$) is said to have *lexicographic type* if there is an order isomorphism (that is, an order-preserving bijection) $f\colon (\mathbb{G}^n, \prec) \longrightarrow (\mathbb{G}^n, \prec_{\text{lex}})$, meaning that $v \prec w \iff f(v) \prec_{\text{lex}} f(w)$.

Theorem 7.4.1.11. *For any total order $\prec$ on $\mathbb{Q}^n$, there exists an integer $s \in \{1, \dots, n\}$, and s orthogonal vectors $u_1, \dots, u_s \in \mathbb{R}^n$, such that*

$$d(u_1) + \cdots + d(u_s) = n,$$

and the map $f\colon (\mathbb{Q}^n, \prec) \longrightarrow (\mathbb{R}^s, \prec_{\text{lex}})$ defined by

$$f(v) = (v \cdot u_1, \dots, v \cdot u_s),$$

is an injective order homomorphism; note that f maps into $\mathbb{R}^s$, not $\mathbb{R}^n$.

Proof. If we take $G = \mathbb{Q}^n$ in Lemma 7.4.1.5 then we see that $I_G \subset \mathbb{R}^n$ is a subspace of dimension $n-1$; we also obtain a vector $u_1 \in U(G)^+$ and we write $d_1 = d(u_1)$. Consider the subspace $G_1 = G \cap I_G$; we have $\dim_{\mathbb{Q}}(G_1) = n - d_1$, and for any $v \in G \setminus G_1$ we have $0 \prec v \iff 0 < v \cdot u_1$. As for G_1, consider $(G_1)_{\mathbb{R}} = G_1 \otimes_{\mathbb{Q}} \mathbb{R}$. Applying Lemma 7.4.1.5 again produces the subspace $I_{G_1} \subset \mathbb{R}^n$ of dimension $n - d_1 - 1$, together with a vector $u_2 \in U(G_1)$ for which $u_1 \cdot u_2 = 0$. We write $d_2 = d(u_2)$; Lemma 7.4.1.9 shows that $d_2 \leq n - d_1$. Clearly this process terminates after a finite number of steps. □

Definition 7.4.1.12 (Type and partition of the order)**.** Given a total order $\prec$ on $\mathbb{Z}^n$, we extend it to $\mathbb{Q}^n$, and consider the map f of Theorem 7.4.1.11. We write:

- $s_\prec$ for the integer s in the description of f, and call this the *type* of the total order; we have $1 \le s_\prec \le n$.
- $d_\prec$ for the s-tuple of positive integers $(d_1, \dots, d_s)$ where $d_i = d(u_i)$; since $d_1 + \cdots + d_s = n$, we call this the *partition* of the total order.

Let $B(d) = \{ v \in \mathbb{R}^n \mid d(v) = d \}$ be the set of all vectors of rational dimension d. For $i = 1, \dots, s$ we set $A(d_i) := B(d_i)/\!\sim$, where $\sim$ is the equivalence relation on $B(d_i)$ defined by $v \sim w$ if and only if $w = av$ for some $a \in \mathbb{R}$, $a > 0$. In other words, $A(d_i)$ is the set of distinct rays (half-lines) starting at 0 in $B(d_i)$.

After all these preliminary results, we have now proved Robbiano's classification theorem for commutative monomial orders.

Theorem 7.4.1.13. *For every monomial order $\prec$ on the polynomial algebra $\mathbb{F}[x_1, \dots, x_n]$, one can uniquely assign the following data:*

- *An integer $s \in \{1, \dots, n\}$.*
- *A partition $d_1, \dots, d_s$ of n with s parts.*
- *An s-tuple $(\overline{u}_1, \dots, \overline{u}_s) \in A(d_1) \times \cdots \times A(d_s)$ satisfying this condition:*
    - *If for $i = 1, \dots, s$ we set $G_{i-1} = \operatorname{span}(u_1, \dots, u_i)^\perp \subseteq \mathbb{Q}^n$ (for $i = 1$ we set $G_0 = \mathbb{Q}^n$) then $u_i \in (G_{i-1})_\mathbb{R}$.*

This data determines the positive elements $v \in \mathbb{N}^n \backslash \{0\}$ with respect to $\prec$ as follows: v is positive if and only if the first nonzero coordinate of $(v \cdot u_1, \dots, v \cdot u_s)$ is positive.

Remark 7.4.1.14. Not any data as above defines a monomial order, as we shall see below.

7.4.2 Examples and non-examples of monomial orders

Example 7.4.2.1. An *Archimedean* total order $\prec$ on a positive semigroup $S = S^+$ is one without infinitesimal elements: for $x, y \in S$ it cannot happen that $nx \prec y$ for all $n \in \mathbb{N}$, where $nx = x + \cdots + x$ (n terms). A monomial order on $\mathbb{F}[x_1, \dots, x_n]$ is Archimedean if and only if the type $s = 1$; hence $d_1 = n$, and so $u_1 \in \mathbb{R}^n$ is any nonzero vector. For example, if $n = 2$ then we may set $u_1 = (1, \sqrt{2})$, noting that $d_1 = 2$ says that the rational dimension of the components must be 2, and then

$$\begin{aligned} x^a y^b \prec x^c y^d &\iff 0 \prec (c-a, d-b) \iff 0 < (c-a, d-b) \cdot (1, \sqrt{2}) \\ &\iff 0 < (c-a) + \sqrt{2}(d-b) \iff a + \sqrt{2}b < c + \sqrt{2}d. \end{aligned}$$

If $n = 3$ then we may set $u_1 = (1, \sqrt[3]{2}, \sqrt[3]{4})$ and obtain

$$x^a y^b z^c \prec x^d y^e z^f \iff 0 < (d-a) + \sqrt[3]{2}(e-b) + \sqrt[3]{4}(f-c).$$

Remark 7.4.2.2. Note that if we set $u_1 = (1, -\sqrt{2})$ in the previous example, this does not lead to a well-order, since this would mean that $x^a y^b \prec x^c y^d$ if and only if $a + \sqrt{2}d < c + \sqrt{2}b$, and in particular $y \prec 1$, implying $\dots y^k \prec y^{k-1} \prec \dots \prec y \prec 1$.

Example 7.4.2.3. A monomial order on $\mathbb{F}[x_1, \dots, x_n]$ is of lexicographic type if and only if the type $s = n$; hence $d_1 = \cdots = d_n = 1$, so all the components are rational, and $u_1, \dots, u_n$ form an orthogonal basis of $\mathbb{Q}^n$. For example, with $n = 2$ we may set $u_1 = (1, 1)$, $u_2 = (1, -1)$; we calculate

$$\big((c-a, d-b) \cdot (1,1),\, (c-a, d-b) \cdot (1,-1) \big) = (\, c-a+d-b,\, c-a-d+b \,)$$

Therefore

$$x^a y^b \prec x^c y^d \iff \begin{cases} c+d < a+b, & \text{or} \\ c+d = a+b & \text{and} \quad b+c < a+d. \end{cases}$$

Under the condition $c + d = a + b$, the condition $b + c < a + d$ becomes simply $b < d$.

Example 7.4.2.4. Suppose that $\prec$ is a monomial order on $\mathbb{F}[x_1, \dots, x_n]$ for which $d_1 = 1$. Then the rational span of the components of u_1 has dimension 1, and so the components are rational multiples of some nonzero $a \in \mathbb{R}$. Dividing u_1 by a makes all the components rational, and in fact we can scale them so that they are all positive integers (see the proof of Theorem 7.4.1.11). It follows that $m \prec m'$ for $m = [e_1, \dots, e_n]$ and $m' = [e'_1, \dots, e'_n]$ if $u_1 \cdot m < u_1 \cdot m'$ which we can write as $\deg(m) < \deg(m')$ where deg now denotes the degree with respect to the weights given by the components of $u_1 = [\deg(x_1), \dots, \deg(x_n)]$. If $u_1 \cdot m = u_1 \cdot m'$ then we consider the scalar products with $u_2, \dots, u_s$. In particular, the standard `glex` order corresponds to the weight vectors in the rows of this $n \times n$ matrix:

$$U = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1-n & 1 & 1 & \cdots & 1 & 1 & 1 \\ 0 & 2-n & 1 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 3-n & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \ddots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & -2 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 1 \end{bmatrix}$$

7.5 Zero-dimensional ideals

In this section, we discuss a fundamental theorem on one of the prettiest topics in commutative algebra: zero-dimensional ideals and how Gröbner bases can be used to study them.

7.5.1 Characterization of zero-dimensional ideals

Definition 7.5.1.1. The ideal $I \subset \mathbb{F}[x_1, \dots, x_k]$ is said to be *zero-dimensional* if the quotient ring $\mathbb{F}[x_1, \dots, x_k]/I$ is finite dimensional (as a vector space over $\mathbb{F}$).

Lemma 7.5.1.2. *If I is zero-dimensional then $I \cap \mathbb{F}[x_i] \neq \{0\}$ for every $i = 1, \dots, k$; in other words, I contains a (nonzero) univariate polynomial for each variable $x_1, \dots, x_k$.*

Proof. For each $i = 1, \dots, k$ consider the cosets of the powers of x_i:

$$1 + I, \qquad x_i + I, \qquad x_i^2 + I, \qquad x_i^3 + I, \qquad \dots, \qquad x_i^n + I, \qquad \dots.$$

Since $\mathbb{F}[x_1, \dots, x_k]/I$ is finite dimensional, these cosets are linearly dependent, and hence some nonzero polynomial f_i must satisfy

$$f_i(x_i) + I = f_i(x_i + I) = 0 + I.$$

Hence $f_i(x_i) \in I$ as required. □

Lemma 7.5.1.3. *If the ideal $I \subset \mathbb{F}[x_1, \dots, x_k]$ contains a (nonzero) univariate polynomial for each variable $x_1, \dots, x_k$ then the zero set $V_{\mathbb{K}}(I)$ is finite for every field extension $\mathbb{F} \subset \mathbb{K}$.*

Proof. It is enough to prove this for $\mathbb{K} = \overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$. By assumption, there exist polynomials $f_i \in \mathbb{F}[x_i] \cap I$ for $i = 1, \dots, n$. Clearly, for each such i, the i-th coordinate of any point of the zero set $V_{\overline{\mathbb{F}}}(I)$ is one of the roots of f_i, so the cardinality of the zero set does not exceed the product of the degrees of the polynomials f_i. □

The following result can be found in any algebraic geometry textbook; for us it is relevant since it marks a path for an application of Gröbner bases.

Theorem 7.5.1.4. *The ideal $I \subset \mathbb{F}[x_1, \dots, x_k]$ is zero-dimensional if and only if the zero set $V_{\mathbb{K}}(I)$ is finite for every field extension $\mathbb{F} \subset \mathbb{K}$.*

Proof. Again, it is enough to prove it for $\mathbb{K} = \overline{\mathbb{F}}$.

The previous two lemmas provide the "only if" part ($\Rightarrow$), so it remains to prove the "if" part ($\Leftarrow$), and this requires one of the fundamental results of algebraic geometry, Hilbert's Nullstellensatz.

Assume that the zero set $V_{\overline{\mathbb{F}}}(I)$ is finite. There are two possibilities:

- either $V_{\overline{\mathbb{F}}}(I) = \emptyset$
- or $V_{\overline{\mathbb{F}}}(I) = \{a_1, \dots, a_\ell\}$ for $a_i = [a_{j1}, \dots, a_{jk}] \in \overline{\mathbb{F}}^k$ for $j = 1, \dots, \ell$.

If $V_{\mathbb{F}}(I) = \emptyset$ then the polynomials in I have no common zeros in $\overline{\mathbb{F}}$, and so by the "weak Nullstellensatz" it follows that $I = (1)$, and in particular, I contains a nonzero univariate polynomial for each x_i, $i = 1, \dots, k$.

On the other hand, if $V_{\overline{\mathbb{F}}}(I) = \{a_1, \ldots, a_\ell\}$ for $a_j = [a_{j1}, \ldots, a_{jk}] \in \overline{\mathbb{F}}^k$ for $j = 1, \ldots, \ell$. Let $M_{ji}(x)$ be the minimal polynomial of a_{ji} over $\mathbb{F}$, and let M_i be the product of all M_{ji} for $j = 1, \ldots, \ell$. Then $M_i(x_i)$ vanishes at all points of $V_{\overline{\mathbb{F}}}(I)$, and hence the Nullstellensatz implies that some power of M_i belongs to I.

We have now proved that there exist polynomials $f_i \in \mathbb{F}[x_i] \cap I$ for $i = 1, \ldots, k$. Thus, multivariate long division by $\{f_1, \ldots, f_k\}$ instantly establishes that the cosets of monomials $m = x_1^{e_1} \cdots x_k^{e_k}$ where $0 \leq e_i < \deg(f_i)$ for each i span the quotient $\mathbb{F}[x_1, \ldots, x_k]/I$. The number of such monomials is $\prod_i \deg(f_i)$, hence $\mathbb{F}[x_1, \ldots, x_k]/I$ is finite dimensional. □

The way to package the theorem we just recalled which is most familiar to experts in commutative Gröbner bases is the following result, commonly known as "shape lemma", since it relates the "shape" of leading terms of Gröbner bases to properties of solution sets.

Theorem 7.5.1.5 (Shape lemma)**.** *Let $f_1, \ldots, f_\ell \in \mathbb{F}[X]$, and fix some monomial order of $\mathsf{C}(X)$. The system of polynomial equations $f_1 = 0, \ldots, f_\ell = 0$ has finitely many solutions in $\overline{\mathbb{F}}$ if and only if every Gröbner basis of the ideal $I = (f_1, \ldots, f_\ell)$ contains, for each i, a polynomial with the leading term $x_i^{n_i}$ for some $n_i \in \mathbb{N}$.*

Proof. In view of Theorem 7.5.1.4, it is enough to prove that $\mathbb{F}[X]/I$ is finite-dimensional if and only if every Gröbner basis of the ideal $I = (f_1, \ldots, f_\ell)$ contains, for each i, a polynomial with the leading term $x_i^{n_i}$ for some $n_i \in \mathbb{N}$. If the latter condition is satisfied for some Gröbner basis, then essentially the same argument as in the end of the proof of Theorem 7.5.1.4 (multivariate long division) shows that $\mathbb{F}[X]/I$ is finite-dimensional. Conversely, for any given Gröbner basis G if $\mathbb{F}[X]/I$ is finite-dimensional, then the cosets of the monomials $1, x_i, x_i^2, \ldots$ are linearly dependent, so not all of these are normal monomials with respect to I, hence one of these monomials is divisible by a leading term of an element of G, which then must be a power of x_i as well. □

7.5.2 Two examples, and a distribution table

We generated 1000 pseudorandom sets of three ideal generators f, g, h in three variables x, y, z using the Maple function `randpoly`; each generator had degree at most 5 with at most three terms and coefficients ±1. We tested each set of three generators using the Maple function `Groebner][IsZeroDimensional]` before computing the `plex` Gröbner basis with $x \succ y \succ z$ and the solution set to the system of equations. In the next two examples we present the set of generators producing the largest Gröbner basis, and the set of generators producing the largest solution set. Following the examples, we display the matrix in Figure 7.1 which gives the distribution of the results: the (i, j) entry is the number of cases out of 1000 which produced a Gröbner basis of j elements having i distinct solutions.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1	43	252	34	11	35	6	11	4	5	1	3	2	1	.	.	.
2	.	4	123	45	19	16	9	11	5	4	2	2	1	1	.	.	.
3	.	1	51	39	18	17	5	5	2	.	1	1	.	.	.	.	.
4	.	.	41	22	8	9	5	8	3	.	.	.	.	.	.	.	.
5	.	.	6	8	6	5	5	1	.	4	2	.	1	.	.	.	1
6	.	.	14	6	3	3	4	2	.	.	.	1	.	.	.	.	.
7	.	.	1	3	4	3	2	1	2	.	.	.	.	1	.	.	.
8	.	.	4	5	1	.	.	1	.	.	.	.	.	.	.	.	.
9	.	.	1	1	1	1	.	.	1	.	.	.	.	.	.	.	.
10	.	.	.	2	.	2	1	.	.	.	.	.	.	.	.	.	.
11	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
12	.	.	.	1	.	.	.	.	.	.	.	.	.	.	.	.	.
13	.	.	.	1	.	.	.	.	.	1	.	.	.	.	.	.	.

FIGURE 7.1: Distribution of zero-dimensional ideals: The (i, j) entry is the number (out of 1000) of pseudorandom zero-dimensional ideals with zero set of i distinct solutions and `plex` Gröbner basis of j polynomials.

Example 7.5.2.1. The original three pseudorandom ideal generators:

$$-x^4 - x^3, \qquad x^2y^2z - xyz^3 - y^2z^3, \qquad x^2y^3 + z^5 + y^4.$$

The `plex` Gröbner basis with pure-power leading monomials boxed:

$\boxed{z^{18}} - 4z^{16} + 6z^{14} + 2z^{13} - 4z^{12} - z^{11} + z^{10}$,

$yz^{10} + z^{17} - 3z^{15} + 3z^{13} + 2z^{12} - z^{11}$,

$y^2z^8 - 2z^{17} + 7z^{15} - 8z^{13} - 4z^{12} + 3z^{11}$,

$y^3z^6 - yz^8 + 3z^{17} - 11z^{15} + 14z^{13} + 6z^{12} - 6z^{11} - z^{10}$,

$y^4z^3 + z^{17} - 7z^{16} - 4z^{15} + 24z^{14} + 6z^{13} - 26z^{12} - 18z^{11} + 10z^{10} + z^8$,

$y^5z+yz^6-2z^{17}+14z^{16}+8z^{15}-48z^{14}-12z^{13}+52z^{12}+36z^{11}-20z^{10}-z^8$,

$\boxed{y^7} + y^6 + y^2z^5 + z^{17} - 7z^{16} - 4z^{15} + 24z^{14} + 6z^{13} - 26z^{12} - 18z^{11} + 10z^{10}$,

$xz^8 - z^{17} - z^{16} + 4z^{15} + 4z^{14} - 6z^{13} - 8z^{12} + 2z^{11} + 5z^{10}$,

$xyz^6 + y^2z^6 - 3z^{17} + z^{16} + 9z^{15} - 4z^{14} - 8z^{13} + 3z^{11} - 7z^{10}$,

$xy^2z^3 + y^4z + y^3z^3 + z^6$,

$xy^4z+xyz^5+xz^6+y^2z^5-z^{17}+7z^{16}+4z^{15}-24z^{14}-6z^{13}+26z^{12}+18z^{11}-10z^{10}$,

$xy^5-y^6+y^3z^5-2y^2z^5-z^{17}+7z^{16}+4z^{15}-24z^{14}-6z^{13}+26z^{12}+18z^{11}-10z^{10}$,

$x^2z^5 + xy^4 + xz^5 - y^5 - yz^5$,

$x^2y^2z - xyz^3 - y^2z^3$,

$x^2y^3 + y^4 + z^5$,
$x^3yz^3 + x^2yz^3 + xyz^5 - y^4z - y^3z^3 + y^2z^5 - z^6$,
$\boxed{x^4} + x^3$.

The solution set clearly contains the following elements:

$$[x, y, z] \;=\; [\,0,\,0,\,0\,],\;\; [\,-1,\,0,\,0\,],\;\; [\,-1,\,-1,\,0\,].$$

Furthermore, if α and β are any roots of the following polynomials,

$$\alpha^2 + \alpha + 1 = 0, \qquad \beta^6 - \beta^5 - 2\beta^4 + \beta^3 + 3\beta^2 - 1 = 0,$$

then the solution set also contains the following elements:

$$[x, y, z] \;=\; [\,-1,\,-\alpha,\,\alpha\,],\;\; [\,-1,\,-\beta^4{+}\beta^3{+}\beta^2{-}1,\,\beta\,].$$

The main step toward establishing this is made by noting that the first element of the Gröbner basis factors as

$$z^{18} - 4z^{16} + 6z^{14} + 2z^{13} - 4z^{12} - z^{11} + z^{10} = \\ z^{10}(z^2 + z - 1)(z^6 - z^5 - 2z^4 + z^3 + 3z^2 - 1),$$

and the second element factors as

$$yz^{10} + z^{17} - 3z^{15} + 3z^{13} + 2z^{12} - z^{11} = z^{10}(y + z^7 - 3z^5 + 3z^3 + 2z^2 - z).$$

Example 7.5.2.2. The original three ideal generators:

$$-x^5 + xz^3, \qquad -yz^3 + y, \qquad y^3 + z^4.$$

The `plex` Gröbner basis consists of four polynomials:

$$\begin{array}{ll} \boxed{x^5} - xz^3 = x(x^4 - z^3), & \boxed{y^3} + z^4 \text{ (irreducible)}, \\ yz^3 - y = y(z-1)(z^2+z+1), & \boxed{z^7} - z^4 = z^4(z-1)(z^2+z+1). \end{array}$$

We leave it as an exercise for the reader (Exercise 7.22) to determine the solution set.

7.6 Complexity of Gröbner bases: a historical survey

The most familiar algorithmic complexity class is that consisting of the NP-complete problems, usually regarded as the canonical class of "very hard" computations: candidate solutions to these problems can be checked quickly (in polynomial time), but finding a solution from scratch is extremely difficult (unless P = NP, see [95]). Very informally, solving a mathematical problem yourself is hard, but having someone explain the solution to you is easy.

7.6.1 A digression on ordinals and computability

Many useful tricks have been developed to circumvent at least partially the intrinsic difficulty of NP-complete problems. For example, the original problem statement may imply that the solutions consist of complex numbers which are algebraic over the rational numbers, and the entire field of algebraic numbers is countable, so in a sense (not a very useful sense) all we have to do is enumerate this countable set and check all possibilities. On the other hand, as we have all known since Abel and Galois (and Cantor), even though the set of algebraic numbers may be countable, labelling them all in a meaningful way, or equivalently constructing a useful bijection between them and the natural numbers, is hardly possible.

The reader who believes that only *uncountable* sets cause serious philosophical problems should investigate the fascinating topic of large *countable* ordinals.

7.6.2 Exponential space complexity

Computing a Gröbner basis for a polynomial ideal using Buchberger's algorithm belongs to the complexity class EXPSPACE, which contains all the decision problems that can be solved by a deterministic Turing machine with a bound of the form $O(2^{f(n)})$ on the amount of space (memory) used, where $f(n)$ is a polynomial function of the problem size n. If we allow a non-deterministic Turing machine instead, we might expect that the complexity would decrease significantly (compare P and NP) but the remarkable theorem of Savitch [226] shows that this is not the case: For any function $s(n) \geq \log_2(n)$, in particular $s(n) = 2^{f(n)}$ for polynomial f, we have $\mathrm{NSPACE}(s(n)) = \mathrm{DSPACE}(s(n)^2)$. Thus using a non-deterministic Turing machine does not reduce the space logarithmically as we might expect, but only by a square root.

Like the notion of NP-complete, a problem G is called EXPSPACE-complete if G belongs to EXPSPACE and every problem H in EXPSPACE can be reduced in polynomial time to G: that is, H can be solved in polynomial time by a procedure that converts input data for H into input data for G and then calls a procedure for G (at no cost of either time or space).

Computing Gröbner bases is in fact EXPSPACE-complete.

We will see an instance of this reduction in Example 7.6.6 when we reduce an instance of the knapsack problem to the computation of a Gröbner basis.

It is known that the class EXPSPACE strictly contains the class PSPACE (problems solvable using polynomial space), which equals NPSPACE by Savitch's theorem, and hence EXPSPACE also strictly contains NP and P (since they are contained in PSPACE):

$$\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} = \mathrm{NPSPACE} \subsetneq \mathrm{EXPSPACE}.$$

So the general case of computing a Gröbner basis is much harder than every NP-complete problem.

7.6.3 Pioneering work by Hermann and Noether

Forty years before Gröbner bases were discovered, the complexity of polynomial computations was the topic of a Ph.D. thesis by Grete Hermann, supervised by Emmy Noether at Göttingen, and defended in 1926; it was published as a 53-page article in *Mathematische Annalen* [128]. The title of the thesis is "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale". An English translation by Michael Abramson was published under the title "The question of finitely many steps in polynomial ideal theory" in 1998 [129]. This paper by Hermann is regarded by many as the foundational document for the discipline of algorithmic and computational algebra.

Hermann's paper established the existence of algorithms, and upper bounds for the number of steps required, for many basic problems in computational commutative algebra; most importantly, the question of deciding whether a given polynomial belongs to the ideal generated by a given set of polynomials (the ideal membership problem). Hermann's definition of her goals sounds remarkably modern; in Abramson's translation:

> The computational methods below are computations in *finitely many steps*. The claim that a computation can be carried out in finitely many steps will mean here that *an upper bound for the number of necessary operations for the computation* can be specified. Thus it is not enough, for example, to suggest a procedure, for which it can be proved theoretically that it can be executed in finitely many operations, if no upper bound for the number of operations is known. In particular, the bounds appearing in the present work will depend only on the number n of variables, the number t of basis elements of the ideal, and the maximum degree q of these basis elements; they are independent of the coefficients of the basis elements. Using these bounds, which indicate up to what degree the variables must be considered, the problems can be reduced to problems of determinant and elementary divisor theory, which can be settled in finitely many steps by known methods.

Of particular interest is Hermann's doubly exponential upper bound for the number of operations required to solve a system of linear equations with coefficients in a polynomial algebra. In view of the importance of this result, we quote it in our own translation; note especially the very last equation:

> **Theorem 2**. Assumption: *Let the f_{ij} be polynomials in $x_1, \dots, x_n$ with coefficients in P, thus quantities in* $\mathsf{P}[x_1, \dots, x_n]$. Conclusion: *For the system of equations*,
>
> $$\begin{gathered} f_{11} z_1 + \cdots + f_{1s} z_s = 0, \\ \vdots \\ f_{t1} z_1 + \cdots + f_{ts} z_s = 0, \end{gathered}$$

a complete system of solutions, which are also quantities belonging to $\mathsf{P}[x_1, \ldots, x_n]$, may be calculated in a finite number of steps. If q is the maximal degree of the f_{ij}, then the degree of the polynomials of the complete system of solutions does not exceed $m(t, q, n)$ where m satisfies the reduction formulas

$$m(t, q, 0) = 0, \qquad m(t, q, n) = qt + m(t^2 q, q, n-1).$$

We also have

$$m(t, q, n) = \sum_{i=1}^{n-1} (qt)^{2^i}.$$

7.6.4 A detour: Seidenberg

Passing over for the moment the essential works of Buchberger from the 1960s, the next major advance in the analysis of complexity was made by Seidenberg [229], a student of Zariski, motivated by some issues with Hermann's work. Samuel has commented rather gently on these issues in the first paragraph of his review of Seidenberg's paper; the translation from the French is our own:

> G. Hermann wrote a historic article on explicit constructions in a polynomial algebra $A = K[X_1, \cdots, X_n]$ over a field K [*Math. Ann.* 95 (1925/26), 736-788]; this article contained some errors, minor but annoying. The author [Seidenberg] here considers the question again in a systematic way. Given two ideals I, J of A, given by systems of generators, the problem is to give explicit procedures allowing one to find, for example, by a finite number of elementary operations, the ideals $I \cap J$ and $I : J$, the primary components of I, its associated prime ideals, its intersection with $K[X_1, \cdots, X_{n-1}]$, etc. One assumes of course that one can calculate explicitly in K.

It is important to point out that Seidenberg's work was published in the mid-1970s, roughly 10 years after the papers by Buchberger that effectively created the independent discipline of computational (or constructive) commutative algebra. Apart from Seidenberg's important but somewhat anomalous contribution, every contribution to this topic after the mid-1960s has used the terminology and conceptual framework of Gröbner bases.

7.6.5 Mayr and Meyer, Bayer and Stillman

A major breakthrough was made in the early 1980s by Mayr and Meyer [194], who were the first to prove that the ideal membership problem is exponential-space hard; that is, the general case inherently requires an amount of computer memory that is exponential in the size of the input. Their focus is primarily on the ideal membership problem for commutative semigroups:

that is, to determine whether the monomial m belongs to the ideal generated by the given relations $m'_i = m''_i$ for $i = 1, \dots, k$. This easily reduces to a special case of the ideal membership problem for polynomial rings: determine whether the monomial m belongs to the ideal generated by the polynomials $m'_i - m''_i$ for $i = 1, \dots, k$. (But note that this reduction only goes one way.) In an appendix to their paper, Mayr and Meyer give a simplified and corrected proof of the theorem of Hermann quoted above.

Six years later, Bayer and Stillman [13] published a self-contained and simplified version of Mayr and Meyer's example of a polynomial ideal exhibiting doubly exponential degrees for the ideal membership problem. We present a very brief introduction to their discussion. Everything takes place in the polynomial ring $\mathsf{P} = \mathbb{F}[x_1, \dots, x_n]$ in n variables over a field $\mathbb{F}$.

Let I be the ideal generated by the polynomials $h_1, \dots, h_s$ which are differences of monomials in the sense that

$$h_i = x^{\alpha_i} - x^{\beta_i}, \quad \alpha_i = [\alpha_{i1}, \dots, \alpha_{in}], \quad x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad i = 1, \dots, s.$$

We also require that the differences $\alpha_i - \beta_i \in \mathbb{Z}^n$ are distinct for $i = 1, \dots, s$.

Corresponding to such an ideal is a directed graph $G(h_1, \dots, h_s)$ whose vertex set consists of all monomials of P, and whose edge set consists of all directed edges (α, β) where $\alpha - \beta = \alpha_i - \beta_i$ for some (unique) $i = 1, \dots, s$.

Definition 7.6.5.1. We choose integers $n \geq 0$ and $d \geq 2$, and set $e_n = d^{2^n}$. For each $r = 0, \dots, n$ we introduce 10 variables which are said to have *level* r:

$$V_r = \{\, s_r,\, f_r,\, b_{r1},\, b_{r2},\, b_{r3},\, b_{r4},\, c_{r1},\, c_{r2},\, c_{r3},\, c_{r4} \,\}.$$

We consider the polynomial ring in the union of these $10(n+1)$ variables:

$$\mathsf{P} = \mathbb{F}\big[\, V_0 \cup \cdots \cup V_n \,\big].$$

We work inductively from one level to the next, and to avoid confusion of subscripts we write upper-case for level r,

$$S, F, B_1, B_2, B_3, B_4, C_1, C_2, C_3, C_4 = s_r, f_r, b_{r1}, b_{r2}, b_{r3}, b_{r4}, c_{r1}, c_{r2}, c_{r3}, c_{r4},$$

and lower case for level $r-1$:

$$s, f, b_1, b_2, b_3, b_4, c_1, c_2, c_3, c_4 = \\ s_{r-1}, f_{r-1}, b_{r-1,1}, b_{r-1,2}, b_{r-1,3}, b_{r-1,4}, c_{r-1,1}, c_{r-1,2}, c_{r-1,3}, c_{r-1,4}.$$

At level $r = 0$, we define the ideal I_0 to be generated by four elements:

$$I_0 = \big(SC_i - FC_iB_i^d \mid i = 1, \dots, 4 \big).$$

Assuming the ideal I_{r-1} at level $r-1$ has been defined, we define the ideal I_r at level r to be generated by I_{r-1} and these new generators at level r:

$$S - sc_1, \qquad sc_4 - F, \qquad sc_3 - fc_4, \qquad sc_3 - sc_2, \qquad fc_1 - sc_2, \\ fc_2b_1 - fc_3b_4, \qquad fc_2C_ib_2 - fc_2C_iB_ib_3 \;\; (1 \leq i \leq 4).$$

Definition 7.6.5.2. We define the map $p_r\colon \mathsf{P} \to \mathsf{P}$ as follows:

- $p_r(v) = v$ for all variables v of level $< r$, and for $v = s_r$ and $v = f_r$;
- $p_r(v) = 1$ for all other variables v.

For $r \geq 1$ we define the *ideal* $J_r = p_r(I_r)$; thus J_r differs from I_r only in that the level r generators $fc_2C_ib_2 - fc_2C_iB_ib_3$ for $i = 1, \dots, 4$ have been replaced by the single generator $fc_2b_2 - fc_2b_3$.

Omitting most of the highly technical and combinatorial details, we arrive at the following lemma:

Lemma 7.6.5.3. *Consider the element $h = S - F$, and let $h_1, \dots, h_s$ be the generators of J_r. For any representation of h as an element of J_r, namely*

$$h = \sum_{i=1}^{s} g_i h_i,$$

at least one of the coefficients g_i has degree no less than

$$\deg(g_i) \geq r - 1 + 2e_0 + \cdots + 2e_{r-1} \quad (e_i = d^{2^i}).$$

This leads directly to the result of Mayr and Meyer from 1982: *Any degree bound for the ideal membership problem must grow doubly exponentially in the maximum of the number of variables and the number of generators.*

Remark 7.6.5.4. For a generalization of these results to polynomials with *integer* coefficients, we refer the reader to the works of Aschenbrenner [6, 7].

7.6.6 An example: the knapsack problem

The knapsack problem is a famous problem in combinatorial optimization; there have been two monographs entirely devoted to variations on this theme: [146], [188]. In its decision form it was one of the first computational problems to be proved NP-complete: [145], [98]. For the first applications of Gröbner basis methods to knapsack problems, see [66].

We will consider only the simplest version. We have a finite set of objects, indexed by the integers $\{1, \dots, n\}$; object i has size a_i which is a positive integer. We also have a knapsack of size b (another positive integer). Our problem is to determine whether there exists a subset of the objects that fit exactly into the knapsack, in the sense that for some $S \subseteq \{1, \dots, n\}$ we have

$$\sum_{i \in S} a_i = b.$$

This is the one-dimensional version of the problem: think of object i as a stick of length a_i cm, and the knapsack as a tube of length b cm; then the problem is to decide whether we can choose a subset of the sticks which exactly fill the tube.

To apply Gröbner bases to this problem, we first have to reformulate it in terms of solving a system of polynomial equations. We introduce variables $x_1, \dots, x_n$ which may only take values in $\{0, 1\}$, and rewrite the last equation as

$$\sum_{i=1}^{n} x_i a_i = b.$$

We set $S = \{\, i \mid x_i = 1 \,\}$: the map $i \mapsto x_i$ is the characteristic function of S. To impose the conditions $x_i \in \{0, 1\}$ we simply include the equations $x_i(x_i - 1) = 0$ for $i = 1, \dots, n$. We now have the following set of $n+1$ generators for the ideal K (for knapsack) in the polynomial ring $P = \mathbb{F}[x_1, \dots, x_n]$:

$$f_0 = a_1 x_1 + \cdots + a_n x_n - b, \qquad f_i = x_i(x_i - 1) \quad (i = 1, \dots, n). \tag{7.5}$$

These generators are very simple: f_0 is linear with $n+1$ terms; f_i is quadratic with two terms.

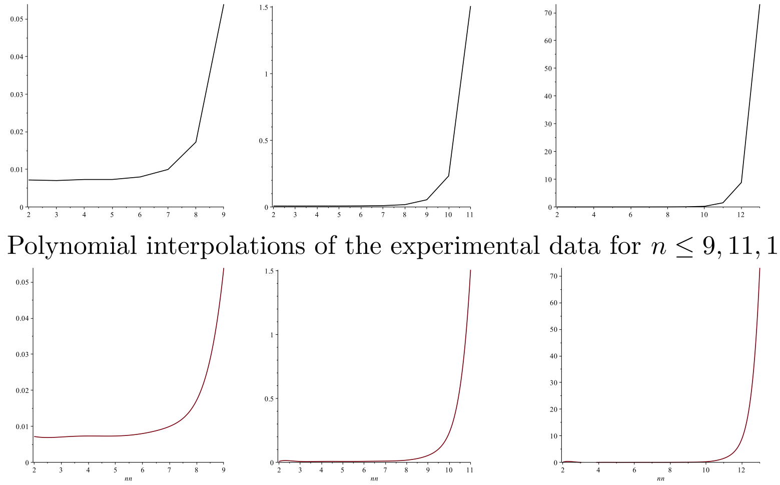
We can use this formulation of the knapsack problem to illustrate the complexity of computing Gröbner bases: the generators (7.5) embed an NP-complete integer programming problem into a system of polynomial equations that can be solved using Gröbner bases. To make this problem precise, we fix a range of values for the number n of variables, choose an upper bound M for the coefficients, and use a pseudorandom number generator to produce integers $a_1, \dots, a_n, b$ in the range $1, \dots, M$. For example, with $n = 10$ and $M = 10^6$, a typical set of generators for the ideal $K \subset \mathbb{F}[x_1, \dots, x_9]$ would be:

$$\begin{array}{l} 74805\, x_1 + 347526\, x_2 + 512608\, x_3 + 608766\, x_4 + 39299\, x_5 \\ \quad +723475\, x_6 + 327134\, x_7 + 377286\, x_8 + 812373\, x_9 + 87438\, x_{10} - 4415, \\ x_1^2 - x_1, \qquad x_2^2 - x_2, \qquad x_3^2 - x_3, \qquad x_4^2 - x_4, \qquad x_5^2 - x_5, \\ \quad x_6^2 - x_6, \qquad x_7^2 - x_7, \qquad x_8^2 - x_8, \qquad x_9^2 - x_9, \qquad x_{10}^2 - x_{10}. \end{array}$$

A moment's inspection of this system of polynomials makes it obvious that the Gröbner basis for K is $[1]$ and its zero set is $Z(K) = \emptyset$. We are interested not in the existence or non-existence of solutions to these systems, but rather in the average time it takes, as a function of the number n of variables, for Buchberger's algorithm to compute the Gröbner basis.

For each $n = 2, \dots, 14$ we performed 100 trials: for each trial, we generated $n+1$ pseudorandom numbers $a_1, \dots, a_n, b$ in the range $1, \dots, 1000000$, recorded the time in seconds for the `Maple 18` command `Groebner[Basis]` on a MacBook Pro to compute the `dlex` Gröbner basis. For each n, we also computed the average time over all 100 trials and obtained the following data:

n	average	n	average	n	average	n	average	n	average
		4	0.00731	7	0.00998	10	0.23285	13	73.11781
2	0.00718	5	0.00731	8	0.01727	11	1.50694	14	445.2669
3	0.00703	6	0.00799	9	0.05395	12	8.8213		



Piecewise linear graphs of the experimental data for $n \le 9, 11, 13$:

Polynomial interpolations of the experimental data for $n \le 9, 11, 13$:

FIGURE 7.2: Average time (seconds) to solve knapsack problem with Gröbner bases as function of number n of objects (6-digit sizes).

The (super-)exponential growth of the time required can be visualized by a piecewise linear graph of the average time as a function of n together with a smooth graph obtained by polynomial interpolation. Figure 7.2 presents these graphs for $n \le 9, 11, 13$.

To close our discussion of the knapsack problem, we mention that it is also an important example in the application of lattice basis reduction to cryptography; see [41, Chapter 7] and the references therein.

7.7 Exercises

Exercise 7.1. Prove Proposition 7.2.2.4.

Exercise 7.2. (i) Suppose one more star (or bar) is added to the left (or right) end of the sequences discussed in the proof of Lemma 7.2.2.5. How does this change the corresponding monomial?

(ii) Suppose the total number of stars and bars is odd, and the middle element (star or bar) is removed. How does this change the corresponding monomial?

(iii) Suppose the total number of stars and bars is even, and a star (or bar) is inserted in the middle. How does this change the corresponding monomial?

Exercise 7.3. Prove that in the definition of monomial order, the well-order condition can be replaced by the condition that every strictly decreasing sequence is finite.

Exercise 7.4. Prove that in the definition of monomial order, the well-order condition can be replaced by the condition that for every monomial $m \neq 1$, we have $1 \prec m$.

Exercise 7.5. Consider two monomials $v = x_1^{e_1} \cdots x_k^{e_k}$ and $w = x_1^{f_1} \cdots x_k^{f_k}$. Give a precise definition of what it means to say that $v \prec w$ in standard dictionary order, assuming that $x_1 \prec \cdots \prec x_k$.

Exercise 7.6. For the permuted `plex` order $\prec_\sigma$ with $\sigma \in S_k$, determine the order of the variables. In particular, for which choice of σ do we obtain $\sigma_i \prec \sigma_j$ if and only if $i < j$?.

Exercise 7.7. For each $k \geq 1$ consider the $k!$ monomials m of degree $n = k(k+1)/2$ in k variables whose exponent sequences are the permutations of $1, \dots, k$:

$$m = x_1^{\sigma(1)} x_2^{\sigma(2)} \cdots x_k^{\sigma(k)} \qquad (\sigma \in S_k).$$

(i) For $k = 4$ sort these monomials by precedence using `dlex` order.

(ii) For $k = 4$ sort these monomials by precedence using `glex` order.

(iii) For $k = 4$ sort these monomials by precedence using ρ-`dlex` order, where ρ is the reversal permutation sending $1, 2, \dots, k$ to $k, k-1, \dots, 1$.

(iv) Repeat (i)–(iii) for $k = 5$; use a computer algebra system.

(v) Repeat (i)–(iii) for $k = 6$; use a computer algebra system.

Exercise 7.8. How many monomials are there of the form $a^i b^j c^k d^\ell$ with total degree at most 4? Sort these monomials in the six different monomial orders of Example 7.2.3.9.

Exercise 7.9. Sort the following monomials in each of the following orders: `plex`, `dlex`, `glex`, elimination ordering for the partition $3 = 2 + 1$, and the same four orders permuted by the reversal *cba*:

abbccc, *bbb*, *abbbccc*, *aaabc*, *aaabbbccc*, *bb*, *aabbb*, *bbc*, *aabccc*, *b*, *aaabb*, *ab*, *bcc*, *bbbc*, *aaabbbcc*, *abbcc*, *abbbcc*, *aacc*, *a*, *aaacc*, *aab*, *aabbc*, *acc*, *aaabbc*, *ac*, *aaabccc*, *aac*, *aabc*, *abb*, *aaab*, *abcc*, *c*, *bc*, *abccc*, *bbccc*, *aabbccc*, *abc*, *aaabbccc*, *bbbcc*, *bbcc*, *aabcc*, *abbbc*, *aaaccc*, *aaabbbc*, *aaccc*, *aa*, *aabbcc*, *abbc*, *ccc*, *aabbbcc*, *accc*, *aaac*, *bbbccc*, *aabb*, *cc*, *aabbbc*, *aaabcc*, *aaabbcc*, *abbb*, *bccc*, *aabbbccc*, *aaa*, *aaabbb*

Exercise 7.10. Prove that the Church–Rosser property of an ARS is equivalent to confluence.

Exercise 7.11. Complete the proof of Corollary 7.3.5.2.

Exercise 7.12. Let $AX = B$ be the matrix form of a linear system over $\mathbb{F}$ with m equations in n variables. Thus $A = [a_{ij}]$ has m rows and n columns, $X = [x_1, \dots, x_n]^t$ is the column vector of unknowns, and $B = [b_1, \dots, b_m]^t$ is the column vector of constant terms. Define m polynomials of degree 1 as follows:

$$f_i(x_1, \dots, x_n) = \left(\sum_{j=1}^{n} a_{ij} x_j \right) - b_i \qquad (1 \leq i \leq m).$$

Let $I \subseteq \mathbb{F}[x_1, \dots, x_n]$ be the ideal generated by $f_1, \dots, f_m$. We assume the `glex` monomial order induced by $x_1 \prec \cdots \prec x_n$.

(i) Prove that the ordered set $\{f_m, \dots, f_1\}$ is a Gröbner basis for I if and only if the augmented matrix $[A|B]$ is in row canonical form (also called reduced row-echelon form).

(ii) What happens if we replace the `glex` order by the `dlex` order?

(iii) What happens if we replace the `glex` order by the `plex` order?

Exercise 7.13. Complete the proof that I_G is a subspace in the proof of Lemma 7.4.1.5. That is, show that if $p \in I_G$ and $a \in \mathbb{R}$ then $ap \in I_G$. Be sure to deal with the possibility that $a < 0$.

Exercise 7.14. Prove that the map σ from the proof of Lemma 7.4.1.5 is surjective and continuous.

Exercise 7.15. Refer to Definition 7.4.1.7 and Example 7.4.1.8. Determine $d(v_n)$ for all $n \geq 1$ where v_n is the vector in $\mathbb{C}^n$ whose components are the n distinct powers of a primitive n-th root of unity.

Exercise 7.16. Let $d(v)$ be the rational dimension of a vector $v \in \mathbb{R}^n$ according to Definition 7.4.1.7. Prove that $d(v) = d(av)$ for any $a \in \mathbb{R}$, $a \neq 0$.

Exercise 7.17. Prove that every Archimedean total order on n variables satisfies $s = 1$ and $d_1 = n$; see Example 7.4.2.1.

Exercise 7.18. Prove that every total order of lexicographic type on n variables satisfies $s = n$ and $d_1 = \cdots = d_n = 1$; see Example 7.4.2.3.

Exercise 7.19. Identify where the standard monomial orders (`plex`, `dlex`, `glex`) in n variables appear in Robbiano's classification of monomial orders (Theorem 7.4.1.13). In particular, determine the parameters s, $d_1 + \cdots + d_s = n$, etc., for each of these orders.

Exercise 7.20. Prove all the claims made in Example 7.4.2.4.

Exercise 7.21. Consider the matrix U from Example 7.4.2.4. Choose some integer $i \in \{1, \dots, n-1\}$ and change the first i entries in the first row of U to 0. Show that the resulting matrix $U^{(i)}$ defines a monomial order $\prec_i$ on $\mathbb{F}[x_1, \dots, x_n]$, and that for all $e_1, \dots, e_n \geq 0$ we have

$$x_1^{e_1} \cdots x_i^{e_i} \prec_i x_{i+1}^{e_{i+1}} \cdots x_n^{e_n}.$$

Exercise 7.22. Determine the solution set of the ideal from Example 7.5.2.2.

Chapter 8

Linear Algebra over Polynomial Rings

8.1 Introduction

Over a field $\mathbb{F}$, to determine whether two $m \times n$ matrices A and B belong to the same orbit under the left action of $GL_m(\mathbb{F})$, we compute the row canonical forms (RCFs, also called Gauss–Jordan forms, or reduced row echelon forms) of A and B and check whether they are equal. Similarly, for the left-right action of $GL_m(\mathbb{F}) \times GL_n(\mathbb{F})$, we compute the Smith normal forms Smith(A) and Smith(B) and check whether they are equal.

Over a Euclidean domain, in particular the ring $\mathbb{F}[x]$ of polynomials in one variable x over the field $\mathbb{F}$, a modification of Gaussian elimination gives a similar result. Since the domain is Euclidean, it is also a PID, and this means that we can implement the Euclidean algorithm for GCDs using elementary row operations. Thus during every iteration of row reduction, we use elementary row operations to replace the elements at and below the pivot by a single nonzero element at the pivot, which is the monic GCD of the original elements, together with zeros below the pivot. This analogue of the RCF is called the Hermite normal form (HNF). The same comments apply to column operations, and combining elementary row and column operations produces an algorithm for computing the Smith form of a matrix with entries in a Euclidean domain.

It is not sufficient for the domain to be a PID: there exist PIDs which are not Euclidean, and for a matrix over such a domain, GCDs of elements will exist but in general they may not be computable using row operations.

Once we go beyond PIDs, to domains such as $\mathbb{F}[x_1, \dots, x_k]$ for $k \geq 2$, which remain within the realm of UFDs, these computations suddenly become much more difficult, for two reasons:

- the GCD still exists, but can only be computed by factorization into irreducibles, which is hard even in $\mathbb{Z}$; it cannot be computed by elementary row operations;

- even if the GCD were easily computable, it wouldn't help, since the ideal generated by a finite set of elements is usually not the same as the principal ideal generated by their GCD: once we go beyond PIDs, we can no longer assume that ideals are generated by a single element.

For example, the polynomial ring $\mathbb{F}[x, y]$ in two variables is a UFD, and so GCDs exist for any (finite) set of elements; but the GCD doesn't tell us anything useful from a geometric point of view. The GCD of x and y is 1, and the ideal generated by 1 is the entire ring $\mathbb{F}[x, y]$, which is clearly not the ideal generated by x and y, since that ideal contains only polynomials with zero constant terms. Similar comments apply to any (finite) number of variables.

For matrices A whose entries belong to the ring $\mathbb{F}[x_1, \ldots, x_k]$ for $k \geq 2$, the existence of a canonical form generalizing the RCF or HNF remains an open problem. In the best case, we would like an easily computable normal form $\mathrm{NF}(A)$ such that for any two $m \times n$ matrices A and B with polynomial entries, we have $\mathrm{NF}(A) = \mathrm{NF}(B)$ if and only if A and B belong to the same orbit for the right action of $GL_m(\mathbb{F}[x_1, \ldots, x_k])$. We have to be careful here: we need to use the group generated by the elementary matrices, and for a general commutative unital ring R this may not be the same as the group of all invertible matrices; this is related to K-theory, in particular the group $K_1(R)$.

In spite of these obstacles, we can still obtain useful information about a multivariate polynomial matrix by elementary methods. There are two opposite ways to approach this: first, we can allow division by arbitrary (nonzero) polynomials and compute over the field of rational functions $\mathbb{F}(x_1, \ldots, x_k)$; second, we can exclude division and use only polynomials (such as determinants) and the ideals they generate (such as determinantal ideals).

This chapter is the first one where many large sparse matrices appear. We therefore deem it appropriate to remind the reader of a notational convention mentioned in Introduction: we find it convenient to follow the eastern Arabic custom of writing dot instead of zero ($\cdot$ instead of 0) to make it easier to identify the pattern of nonzero entries in such matrices.

8.2 Rank of a polynomial matrix; determinantal ideals

8.2.1 The rank of the matrix as a function of the variables

To focus the discussion, we will consider the following problem.

Problem 8.2.1.1. Let A be an $m \times n$ matrix with entries in the ring $\mathbb{F}[x_1, \ldots, x_k]$. Determine how the rank of A behaves as a function of the values $a_1, \ldots, a_k \in \mathbb{F}$ assigned to the variables $x_1, \ldots, x_k$.

Computing the rank for each choice of values of variables gives an invariant of a matrix which is more refined than its rank when regarded as a matrix over the field $\mathbb{F}(x_1, \ldots, x_k)$ of rational functions: over a field, we can use Gaussian elimination to compute its RCF, however, crucial information is lost this way, since we are implicitly assuming that none of the denominators that arise during the row reduction process can ever become 0.

8.2.2 Definition of the rank of a polynomial matrix

A more useful (and more complex) definition of the rank is as follows.

Definition 8.2.2.1. Let A be an $m \times n$ matrix over $\mathbb{F}[x_1, \ldots, x_k]$ regarded as a parameterized family of matrices over $\mathbb{F}$. We define the function

$$A| \colon \mathbb{F}^k \to \mathrm{Mat}_{mn}(\mathbb{F}),$$

as follows: for $a_1, \ldots, a_k \in \mathbb{F}$ the matrix $A|(a_1, \ldots, a_k)$ is obtained from A by setting $x_i = a_i$ for $i = 1, \ldots, k$.

Composing $A|$ with the usual rank on $\mathrm{Mat}_{mn}(\mathbb{F})$ gives a function called the *substitution rank*, denoted $\mathrm{subsrank}_A = \mathrm{rank} \circ A|$:

$$\mathrm{subsrank}_A \colon \mathbb{F}^k \to \{\, 0, 1, \ldots, \min(m, n) \,\}.$$

The inverse images of the ranks $0 \leq r \leq \min(m, n)$ under the substitution rank function define the *inverse rank* function, whose range is the power set (set of all subsets) of $\mathbb{F}^k$:

$$\mathrm{invrank}_A(r) = \big\{\, [a_1, \ldots, a_k]^t \in \mathbb{F}^k \mid \mathrm{subsrank}_A(a_1, \ldots, a_k) = r \,\big\}.$$

It is unusual for $\mathrm{subsrank}_A$ to be surjective, so we define the *minimal rank* and *maximal rank* functions

$$r_{\min}, r_{\max} \colon \mathrm{Mat}_{mn}(\mathbb{F}) \to \{\, 0, 1, \ldots, \min(m, n) \,\},$$

in terms of the image of subsrank:

$$r_{\min}(A) = \min(\mathrm{image}(\mathrm{subsrank})),$$
$$r_{\max}(A) = \max(\mathrm{image}(\mathrm{subsrank})).$$

Remark 8.2.2.2. Clearly $0 \leq r_{\min}(A) \leq r_{\max}(A) \leq \min(m, n)$, but

$$r_{\min}(A) < r < r_{\max}(A) \quad \text{does not imply} \quad \mathrm{invrank}_A(r) \neq \emptyset.$$

8.2.3 Determinantal ideals of a polynomial matrix

Definition 8.2.3.1. Let A be an $m \times n$ matrix over $\mathbb{F}[x_1, \ldots, x_k]$, and let r (called the *rank*) belong to $\{0, 1, \ldots, \min(m, n) + 1\}$. The *determinantal ideals* $DI_r(A)$ for $r = 0, \ldots, \min(m, n)$ are defined as follows:

- $DI_0(A) = \emptyset$.

- If $1 \leq r \leq \min(m,n)$ then $DI_r(A)$ is the ideal in $\mathbb{F}[x_1,\dots,x_k]$ generated by all $r \times r$ minors of A, whose number is $\binom{m}{r}\binom{n}{r}$.
- $DI_{\min(m,n)+1}(A) = \mathbb{F}^k$.

The advantage of using determinantal ideals is that they allow us to study the rank of a matrix using only ring operations (addition, subtraction, and multiplication, without division).

The classical theory of determinantal ideals is concerned almost exclusively with the homogeneous case, in which the entries x_{ij} are mn independent indeterminates, and so every minor is a homogeneous polynomial, and every determinantal ideal is homogeneous; see Miró-Roig [200]. Since the entries of the matrices we consider will be general polynomials, the determinantal ideals we study in what follows will be far from homogeneous. We could reformulate our problem in terms of homogeneous polynomials by introducing a new parameter x_0 as in the homogenization process which converts affine geometry to projective geometry. This leads to a theory similar to that of sparse determinantal ideals [38]. However, it will be very useful to us to have as many leading 1s as possible in the matrix; from a computational point of view, this allows us to go further when we do row/column reduction on the matrix.

We continue by recalling a familiar lemma from linear algebra over a field.

Lemma 8.2.3.2. *Let A be an $m \times n$ matrix over the field $\mathbb{F}$. These conditions are equivalent:*

- $\mathrm{rank}(A) = r$
- *Every $(r+1)\times(r+1)$ minor is 0, and at least one $r \times r$ minor is not 0.*

Proposition 8.2.3.3. *Let A be an $m \times n$ matrix over $\mathbb{F}[x_1,\dots,x_k]$. For every $r = 0, 1, \dots, \min(m,n)$ we have*

$$\mathrm{invrank}_A(r) = V(DI_{r+1}) \setminus V(DI_r).$$

Proof. A restatement of the previous lemma using the previous definitions. □

Lemma 8.2.3.4. *Let A be an $m \times n$ matrix over $\mathbb{F}[x_1,\dots,x_k]$. If there exist $a_1,\dots,a_k \in \mathbb{F}$ such that $\mathrm{subsrank}_A(a_1,\dots,a_k) \in \mathrm{Mat}_{mn}(\mathbb{F})$ has full rank $r = \min(m,n)$, then A has full rank regarded as a matrix over the field $\mathbb{F}(x_1,\dots,x_k)$ of rational functions.*

Proof. An immediate consequence of Lemma 8.2.3.2. □

Remark 8.2.3.5. We mention another proof of Lemma 8.2.3.4 which uses an argument by contradiction and illustrates the technique of passing back and forth between a ring and its field of fractions. We consider only the case in which $\mathbb{F}$ is algebraically closed. Suppose that

$$\mathrm{rank}_{\mathbb{F}}(A|(a_1,\dots,a_k)) = \min(m,n), \quad \text{but} \quad \mathrm{rank}_{\mathbb{F}(x_1,\dots,x_k)}(A) < \min(m,n).$$

Since A does not have full rank over $\mathbb{F}(x_1, \dots, x_k)$, it has positive nullity and there is a nonzero vector $V = [v_1, \dots, v_n]^t \in \mathbb{F}(x_1, \dots, x_k)^n$ such that $AV = 0$. For $j = 1, \dots, k$ write $v_i = f_i/g_i$ where $f_i, g_i \in \mathbb{F}[x_1, \dots, x_k]$ have no common factor. Since $\mathbb{F}[x_1, \dots, x_k]$ is a UFD, we can define

$$g = \textsc{lcm}(g_1, \dots, g_k), \quad h = \textsc{gcd}(gv_1, \dots, gv_k), \quad w_j = gv_j/h \;\; (j = 1, \dots, n).$$

The vector $W = [w_1, \dots, w_n]^t = (g/h)V$ is nonzero, satisfies $AW = 0$, and its entries are polynomials with no common factor. If we assume that $\mathbb{F}$ is algebraically closed, then for all $j = 1, \dots, n$ the zero set $V(w_j)$ is a $(k-1)$-dimensional hypersurface in $\mathbb{F}^k$. Since an algebraically closed field is infinite, the union of these n hypersurfaces is not all of $\mathbb{F}^k$. Hence there exists $(a_1, \dots, a_k) \in \mathbb{F}^k$ such that $x_j = w_j(a_1, \dots, a_k) \neq 0$ for all $j = 1, \dots, n$. But then the vector $[x_1, \dots, x_n] \in \mathbb{F}^n$ is a nonzero vector in the nullspace of $A|(a_1, \dots, a_k)$; and this contradiction completes the proof.

8.3 Some elementary examples

8.3.1 Ranks of pseudorandom matrices

Fix a number k of variables and fix a size $n \geq 2$ of square matrices. Let A be an $n \times n$ matrix with entries in $\mathbb{F}[x_1, \dots, x_k]$. In fact, we will take the entries of A from the finite set $\{0, 1, x_1, \dots, x_k\}$, so that we may use a pseudorandom number generator to choose the entries of A uniformly: each of the $k+2$ possible entries is chosen with probability $1/(k+2)$. For each possible rank of A, namely $0 \leq r \leq n$, we want to find all values $a_1, \dots, a_k$ of the variables $x_1, \dots, x_k$ which produce rank exactly r.

Example 8.3.1.1. Consider the matrix

$$A = \begin{bmatrix} x_1 & x_1 & 0 \\ x_2 & x_1 & x_1 \\ x_2 & 1 & x_1 \end{bmatrix}$$

What are the determinantal ideals of A? The first ideal $DI_1(A)$ is generated by the entries of A, and since 1 is an entry of A, we see that [1] is a Gröbner basis. Therefore $DI_1(A) = \mathbb{F}[x_1, x_2]$ and so $V(DI_1(A)) = \emptyset$. It follows that $\det(A) \neq 0$ no matter what values we assign to the variables, and so the inverse image of $r = 0$ is the empty set.

As for $DI_2(A)$, it is generated by the distinct 2×2 minors of A, which are the following polynomials; to avoid trivial repetitions we have scaled each minor to make it monic with respect to the `glex` order with $x_1 \prec x_2$:

$$x_1^2, \qquad x_1^2 - x_1, \qquad x_1x_2 - x_1, \qquad x_1x_2 - x_2, \qquad x_1x_2 - x_1^2.$$

From the first two elements we see that $DI_2(A)$ contains x_1, and then the fourth element shows that $DI_2(A)$ contains x_2. Since none of these elements has a nonzero constant term, we conclude that $[x_1, x_2]$ is a Gröbner basis for $DI_2(A)$. It follows that $DI_2(A) = (x_1, x_2)$ and hence $V(DI_2(A)) = \{(0,0)\}$. This implies that $\mathrm{rank}(A) < 2$ if and only if $x_1 = x_2 = 0$. Since we already know that $\mathrm{rank}(A) \geq 1$, we conclude that the inverse image of $r = 1$ is the single point $\{(0,0)\}$.

For $r = 3$, there is only one determinant to compute: $\det(A) = x_1^3 - x_1^2$, and this polynomial is a Gröbner basis for the (principal) ideal $DI_3(A)$. It follows that $\mathrm{rank}(A) < 3$ if and only if $x_1 \in \{0,1\}$ (and the value of x_2 does not matter). So the inverse image of $r = 2$ consists of two vertical lines in $\mathbb{F}^2$: the line $x_1 = 0$ excluding the point $(0,0)$ which gives rank 1, and the line $x_1 = 1$. We summarize the results of these calculations as follows:

rank r	inverse image in $\mathbb{F}^2$
0	$\emptyset$
1	$\{\,(0,0)\,\}$
2	$\{\,(0,a_2) \mid a_2 \in \mathbb{F},\, a_2 \neq 0\,\} \cup \{\,(1,a_2) \mid a_2 \in \mathbb{F}\,\}$
3	all points $(a_1,a_2) \in \mathbb{F}^2$ with $a_1 \notin \{0,1\}$

Example 8.3.1.2. Consider this matrix involving three variables:

$$A = \begin{bmatrix} x_1 & x_3 & x_3 & 0 \\ x_3 & x_2 & 1 & 1 \\ x_3 & 0 & 0 & x_1 \\ x_3 & x_2 & 1 & x_2 \end{bmatrix}$$

As in the previous example, $DI_1(A) = \mathbb{F}[x_1,x_2,x_3]$ since 1 is a matrix entry, and so $V(DI_1(A)) = \emptyset$. We next compute all 2×2 minors, and obtain the following set of generators for $DI_2(A)$; using `glex` order with $x_1 \prec x_2 \prec x_3$ the elements are monic and increasing:

$$\begin{gathered} x_1, \quad x_2 - 1, \quad x_3, \quad x_1^2, \quad x_2x_1, \quad x_3x_1, \quad x_3(x_1-1), \quad x_2(x_2-1), \\ x_2x_3, \quad x_3(x_2-1), \quad x_3(x_2-x_1), \quad x_3^2, \quad x_3^2 - x_1, \quad x_3^2 - x_2x_1. \end{gathered}$$

From this we directly obtain the Gröbner basis and the zero set:

$$DI_2(A) = \big(\, x_1,\, x_2 - 1,\, x_3 \,\big), \qquad V(DI_2(A)) = \{\,(0,1,0)\,\}.$$

The same procedure for the 3×3 minors produces these generators for $DI_3(A)$:

$$\begin{gathered} x_3(x_2-1), \quad x_3x_1(x_2-1), \quad x_3^2x_1 - x_3^2 - x_1^2, \quad x_3^2x_1 - x_2x_1^2 - x_3^2, \\ x_3x_2(x_2-1), \quad x_3(x_2-1)^2, \quad x_3^2(x_2-1), \quad (x_2-1)(x_3^2-x_1), \\ (x_2-1)(x_3^2-x_2x_1), \quad x_3^2x_2 - x_3^2x_1 + x_1^2, \quad x_3^2x_2 - x_3^2x_1 + x_2x_1^2. \end{gathered}$$

From this we obtain the following `glex` Gröbner basis for $DI_3(A)$:

$$\Big[\quad f = x_1(x_2 - 1), \quad g = x_3(x_2 - 1), \quad h = x_3^2 x_1 - x_3^2 - x_1^2 \quad \Big].$$

If $x_2 \neq 1$ then f and g imply $x_1 = 0$ and $x_3 = 0$, and these values satisfy h, so we have the one-parameter set of solutions,

$$\{ \, (0, a_2, 0) \mid a_2 \in \mathbb{F}, \, a_2 \neq 1 \, \}.$$

If $x_2 = 1$ then f and g vanish, leaving only h, which is quadratic in both x_1 and x_3. Writing h as a polynomial first in x_1 and then in x_3 gives

$$-\big(x_1^2 - x_3^2 x_1 + x_3^2\big) = 0, \qquad (x_1 - 1)x_3^2 - x_1^2 = 0.$$

The second equation is slightly simpler, but it has the non-constant leading coefficient $x_1 - 1$, which means that we would have to treat $x_1 = 1$ as a special case. We therefore solve for x_1 in terms of x_3 using the first equation:

$$x_1 = \frac{1}{2} x_3 \Big(x_3 \pm \sqrt{x_3^2 - 4} \Big).$$

Finally, $DI_4(A)$ is the principal ideal generated by $\det(A) = -x_3^2(x_2 - 1)^2$, and so $\mathrm{rank}(A) < 4$ if and only if either $x_2 = 1$ or $x_3 = 0$.

We now have a complete understanding of how $\mathrm{rank}(A)$ depends on the values a_1, a_2, a_3 assigned to the parameters x_1, x_2, x_3:

rank r	inverse image in $\mathbb{F}^3$
0	$\emptyset$
1	$\{ \, (0, 1, 0) \, \}$
2	$\{ \, (0, a_2, 0) \mid a_2 \in \mathbb{F}, \, a_2 \neq 1 \, \} \cup$ $\{ \, (a_1, 1, a_3) \mid a_3 \in \mathbb{F}, \, a_1 = \frac{1}{2} a_3 (a_3 \pm \sqrt{a_3^2 - 4} \,) \, \}$
3	all points $(a_1, a_2, a_3) \in \mathbb{F}^3$ with $a_2 = 1$ or $a_3 = 0$, excluding the points listed under ranks 0, 1, 2
4	all points $(a_1, a_2, a_3) \in \mathbb{F}^3$ with $a_2 \neq 1$ and $a_3 \neq 0$

8.3.2 Ranks of symmetric matrices

At the opposite end of the spectrum from pseudorandom matrices, we have structured matrices, and in particular symmetric matrices. We consider the sequence of $n \times n$ matrices $A_n = (a_{ij}^{(n)})$ for $n \geq 1$ defined by

$$\begin{aligned} a_{ii} &= 0 \quad (1 \leq i \leq n), \\ a_{i,i+1} = a_{i+1,i} &= 1 \quad (1 \leq i \leq n-1), \\ a_{i,i+k} = a_{i+k,i} &= x_{k-1} \quad (1 \leq i \leq n-k, \; 2 \leq k \leq n-1) \end{aligned}$$

where $x_1, \dots, x_{n-2}$ are variables. The first few cases $A_1, \dots, A_5$ are:

$$\begin{bmatrix} 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & x_1 \\ 1 & 0 & 1 \\ x_1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & x_1 & x_2 \\ 1 & 0 & 1 & x_1 \\ x_1 & 1 & 0 & 1 \\ x_2 & x_1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & x_1 & x_2 & x_3 \\ 1 & 0 & 1 & x_1 & x_2 \\ x_1 & 1 & 0 & 1 & x_1 \\ x_2 & x_1 & 1 & 0 & 1 \\ x_3 & x_2 & x_1 & 1 & 0 \end{bmatrix}$$

We ignore the trivial case $n = 1$ and assume that $n \geq 2$. It is clear that

$$DI_1(A_n) = DI_2(A_n) = \mathbb{F}[x_1, \dots, x_{n-2}] \quad (\text{by convention}\, \mathbb{F}[\emptyset] = \mathbb{F}),$$

since every matrix has 1 as an entry and also as a 2×2 minor (consider any of the diagonal 2×2 blocks). Hence for $n \geq 2$ we have

$$V(DI_1(A_n)) = V(DI_2(A_n)) = \emptyset, \quad \text{which implies} \quad \operatorname{rank}(A_n) \geq 2.$$

For $n = 3$ we have $\det(A_3) = 2x_1$ and so $DI_3(A_3) = (x_1)$, which gives $V(DI_3(A_3)) = \{0\}$. Therefore $\operatorname{rank}(A_3) = 2$ if and only if $x_1 = 0$, and $\operatorname{rank}(A_3) = 3$ otherwise (which can easily be seen by inspection).

For $n = 4$ we find that every 3×3 minor is a scalar multiple of one of the following polynomials:

$$x_1, \quad x_1^2 + x_2 - 1, \quad x_1^2 - x_2 + 1, \quad x_2 x_1, \quad x_1^3 - x_1 x_2 - x_1, \quad x_1^2 x_2 - x_2^2 + x_2.$$

Since this list contains x_1, we can retain x_1 and set $x_1 = 0$ in the others, which leaves us with only $x_2 - 1$ and $x_2(x_2 - 1)$. Hence $[\, x_1,\, x_2 - 1 \,]$ is a Gröbner basis for $DI_3(A_4)$ and so $V(DI_3(A_4)) = \{(0, 1)\}$. We calculate

$$\det(A_4) = \big(x_2 - (x_1 + 1)^2\big)\big(x_2 - (x_1 - 1)^2\big).$$

This polynomial generates the principal ideal $DI_4(A_4)$, and so we have

$$V(DI_4(A_4)) = \big\{ \big(x_1, (x_1{+}1)^2\big) \mid x_1 \in \mathbb{F} \big\} \cup \big\{ \big(x_1, (x_1{-}1)^2\big) \mid x_1 \in \mathbb{F} \big\}.$$

With this information we can write down the inverse image of each rank:

- A_4 never has rank 0 or 1;
- A_4 has rank 2 if and only if $(x_1, x_2) = (0, 1)$;
- A_4 has rank 3 if and only if $x_2 = (x_1 \pm 1)^2$ and $x_1 \neq 0$;
- A_4 has rank 4 if and only if $x_2 \neq (x_1 \pm 1)^2$.

For $n = 5$ we have the following results, which the reader is encouraged to verify (with the help of a computer algebra system):

$$\begin{aligned} V(DI_1(A_5)) &= V(DI_2(A_5)) = \emptyset \\ V(DI_3(A_5)) &= \{(0, 1, 0)\} \\ V(DI_4(A_5)) &= \big\{ \big(x_1, (x_1 + \epsilon)^2, x_1(x_1 + 2\epsilon)^2\big) \mid x_1 \in \mathbb{F},\, \epsilon = \pm 1 \big\} \\ V(DI_5(A_5)) &= \big\{ \big(x_1, x_2, -x_1(x_1^2{-}2x_2{-}2)\big) \mid x_1, x_2 \in \mathbb{F} \big\} \cup \\ &\qquad \big\{ \big(x_1, 1 \pm \sqrt{x_1 x_3}, x_3\big) \mid x_1, x_3 \in \mathbb{F} \big\} \end{aligned}$$

8.3.3 Orthonormal bases in $\mathbb{R}^n$

In this subsection we assume that $\mathbb{F} = \mathbb{R}$ so that we can appeal to the familiar notions and intuitions of n-dimensional Euclidean geometry in $\mathbb{R}^n$, and in particular the *dot product* $x \cdot y = \sum_{i=1}^n x_i y_i$. Recall that a basis $\{x_1, \dots, x_n\}$ of $\mathbb{R}^n$ is called *orthonormal* if and only if its *Gram matrix* (the symmetric $n \times n$ matrix whose (i, j) entry is $x_i \cdot x_j$) is the identity matrix. If we write $x_j = (x_{1j}, \dots, x_{nj})$ for $j = 1, \dots, n$ and form the $n \times n$ matrix $C = (x_{ij})$ in which column j is x_j, then the Gram matrix is $C^t C$, and orthonormality is characterized by the vanishing of the symmetric matrix $\Gamma = C^t C - I$. Since Γ is symmetric, the number of distinct relations is $\frac{1}{2}n(n+1)$. If we regard the coefficients x_{ij} as variables, then the entries of Γ generate an ideal $I = (\Gamma)$ in the polynomial algebra $\mathbb{R}[x_{11}, \dots, x_{nn}]$, whose zero set $V(I)$ is the set of all orthonormal bases of $\mathbb{R}^n$, which we may identify with the real orthogonal Lie group $O(n, \mathbb{R})$. Let's look at some small examples.

For $n = 1$ we have $C = [x_{11}]$ and $\Gamma = [x_{11}^2 - 1]$; the zero set is $\{\pm 1\}$, the two orthonormal bases of $\mathbb{R}$ regarded as a 1-dimensional vector space.

For $n = 2$ we have

$$C = \left[\begin{array}{cc} x_{11} & x_{12} \\ x_{21} & x_{22} \end{array} \right] \qquad \Gamma = \left[\begin{array}{cc} x_{11}^2 + x_{21}^2 - 1 & x_{11}x_{12} + x_{21}x_{22} \\ x_{11}x_{12} + x_{21}x_{22} & x_{12}^2 + x_{22}^2 - 1 \end{array} \right]$$

The distinct entries of Γ are the three polynomials

$$x_{21}^2 + x_{11}^2 - 1, \quad x_{22}x_{21} + x_{12}x_{11}, \quad x_{22}^2 + x_{12}^2 - 1,$$

which generate an ideal whose `glex` Gröbner basis has six elements:

$$\begin{gathered} x_{12}^2 + x_{11}^2 - 1, \\ x_{22}x_{12} + x_{21}x_{11}, \\ x_{21}^2 + x_{11}^2 - 1, \\ x_{22}x_{21} + x_{12}x_{11}, \\ (x_{22} - x_{11})(x_{11} + x_{22}), \\ x_{21}x_{12}x_{11} - x_{22}x_{11}^2 + x_{22}. \end{gathered}$$

These six polynomials vanish whenever the three generators vanish; that is, whenever the x_{ij} are assigned values corresponding to an orthonormal basis. For example, the vanishing of the fifth element of the Gröbner basis means that in every orthonormal basis of $\mathbb{R}^2$ we have either $x_{11} = x_{22}$ or $x_{11} = -x_{22}$. This is not difficult to see: draw a unit circle centered at the origin and two radii at a right angle. Equivalently, note that the two unit vectors orthogonal to $(\cos\theta, \sin\theta)$ are $(-\sin\theta, \cos\theta)$ and $(\sin\theta, -\cos\theta)$. That last calculation provides a tiny example of how Gröbner bases can be used to derive and (possibly) prove new results from old assumptions. This problem belongs to the general topic of automated theorem proving, which has been especially successful in its applications to elementary geometry.

For $n = 3$ the set of generators consists of the six polynomials

$$\begin{gathered}
x_{31}^2 + x_{21}^2 + x_{11}^2 - 1, \\
x_{32}x_{31} + x_{22}x_{21} + x_{12}x_{11}, \\
x_{33}x_{31} + x_{23}x_{21} + x_{13}x_{11}, \\
x_{32}^2 + x_{22}^2 + x_{12}^2 - 1, \\
x_{33}x_{32} + x_{23}x_{22} + x_{13}x_{12}, \\
x_{33}^2 + x_{23}^2 + x_{13}^2 - 1.
\end{gathered}$$

The `glex` Gröbner basis of the ideal generated by these polynomials contains 27 elements, which represent equations holding in spherical trigonometry; see Figure 8.1. The size of the Gröbner basis increases rapidly as a function of n: for $n = 4$ the ten generators of the ideal $I \subset \mathbb{R}[x_{11}, \ldots, x_{44}]$ produce a `glex` Gröbner basis consisting of 141 polynomials.

$$\begin{array}{l}
x_{13}^2 + x_{12}^2 + x_{11}^2 - 1, \qquad x_{23}x_{13} + x_{22}x_{12} + x_{21}x_{11}, \\
x_{23}^2 + x_{22}^2 + x_{21}^2 - 1, \qquad x_{33}x_{13} + x_{32}x_{12} + x_{31}x_{11}, \\
x_{31}^2 + x_{21}^2 + x_{11}^2 - 1, \qquad x_{33}x_{23} + x_{32}x_{22} + x_{31}x_{21}, \\
x_{32}^2 + x_{22}^2 + x_{12}^2 - 1, \qquad x_{33}x_{32} + x_{23}x_{22} + x_{13}x_{12}, \\
x_{32}x_{31} + x_{22}x_{21} + x_{12}x_{11}, \qquad x_{33}x_{31} + x_{23}x_{21} + x_{13}x_{11}, \\
x_{33}^2 - x_{22}^2 - x_{21}^2 - x_{12}^2 - x_{11}^2 + 1, \\
x_{22}x_{13}x_{12} - x_{23}x_{12}^2 + x_{21}x_{13}x_{11} - x_{23}x_{11}^2 + x_{23}, \\
x_{32}x_{13}x_{12} - x_{33}x_{12}^2 + x_{31}x_{13}x_{11} - x_{33}x_{11}^2 + x_{33}, \\
x_{32}x_{23}x_{12} - x_{33}x_{22}x_{12} + x_{31}x_{23}x_{11} - x_{33}x_{21}x_{11}, \\
x_{22}^2x_{13} + x_{21}^2x_{13} - x_{23}x_{22}x_{12} - x_{23}x_{21}x_{11} - x_{13}, \\
x_{32}x_{22}x_{13} + x_{31}x_{21}x_{13} - x_{33}x_{22}x_{12} - x_{33}x_{21}x_{11}, \\
x_{31}x_{22}x_{21} - x_{32}x_{21}^2 + x_{31}x_{12}x_{11} - x_{32}x_{11}^2 + x_{32}, \\
x_{31}x_{23}x_{21} - x_{33}x_{21}^2 + x_{31}x_{13}x_{11} - x_{33}x_{11}^2 + x_{33}, \\
x_{32}x_{23}x_{21} - x_{33}x_{22}x_{21} + x_{32}x_{13}x_{11} - x_{33}x_{12}x_{11}, \\
x_{31}x_{22}^2 - x_{32}x_{22}x_{21} + x_{31}x_{12}^2 - x_{32}x_{12}x_{11} - x_{31}, \\
x_{31}x_{23}x_{22} - x_{33}x_{22}x_{21} + x_{31}x_{13}x_{12} - x_{33}x_{12}x_{11}, \\
x_{32}x_{23}x_{22} - x_{33}x_{22}^2 - x_{31}x_{13}x_{11} + x_{33}x_{11}^2, \\
x_{31}x_{22}x_{13}x_{11} - x_{32}x_{21}x_{13}x_{11} - x_{31}x_{23}x_{12}x_{11} + x_{33}x_{21}x_{12}x_{11} + x_{32}x_{23}x_{11}^2 \\
\qquad -x_{33}x_{22}x_{11}^2 - x_{32}x_{23} + x_{33}x_{22}, \\
x_{21}^2x_{12}^2 - 2x_{22}x_{21}x_{12}x_{11} + x_{22}^2x_{11}^2 - x_{22}^2 - x_{21}^2 - x_{12}^2 - x_{11}^2 + 1, \\
x_{31}x_{21}x_{12}^2 - x_{31}x_{22}x_{12}x_{11} - x_{32}x_{21}x_{12}x_{11} + x_{32}x_{22}x_{11}^2 - x_{32}x_{22} - x_{31}x_{21}, \\
x_{21}^2x_{13}x_{12} - x_{22}x_{21}x_{13}x_{11} - x_{23}x_{21}x_{12}x_{11} + x_{23}x_{22}x_{11}^2 - x_{23}x_{22} - x_{13}x_{12}, \\
x_{31}x_{21}x_{13}x_{12} - x_{32}x_{21}x_{13}x_{11} - x_{31}x_{23}x_{12}x_{11} + x_{32}x_{23}x_{11}^2 - x_{32}x_{23}
\end{array}$$

FIGURE 8.1: Gröbner basis (`glex`) defining orthonormal bases of $\mathbb{R}^3$.

In general, Gröbner bases bring one closer to fulfilling the Descartes' dream of proving geometric theorems using the coordinate method. For further information about automated geometric theorem proving using Gröbner bases, see the following references: [45], [47], [58], [64, §6.4], [93], [144], [164], [213], [214], [258], [259].

8.4 Algorithms for linear algebra over polynomial rings

8.4.1 Introduction: elementary row and column operations

Our naive goal is to construct an algorithm as simple and efficient as Gaussian elimination which would compute an (as yet unspecified) canonical form for matrices over a polynomial ring. This goal is almost certainly not practical, but nonetheless in this section we describe some useful algorithms that can be used in many cases to simplify polynomial matrices very substantially.

To begin, let us recall the valid and permitted elementary row/column operations on matrices with entries in $\mathbb{F}[x_1, \dots, x_k]$:

- Interchange two rows/columns.
- Multiply one row/column by a nonzero scalar $a \in \mathbb{F} \setminus \{0\}$: only these coefficients are allowed since they are the only invertible polynomials.
- Add a multiple (by any polynomial) of one row/column to a different row/column; in this case the coefficients can be arbitrary polynomials since the resulting row/column operation is invertible in all cases.

8.4.2 Partial row/column reduction (partial Smith form)

Like most of the algorithms we will discuss, this one can be described in two different but equivalent ways: top-down (recursively) or bottom-up (inductively). Different readers will prefer different approaches.

The basic idea at each step is to locate any remaining nonzero scalar entry in the matrix, use row/column operations to move it to the pivot and convert them to 1, and then use this 1 to eliminate other entries in the same row and column. The algorithm terminates when there are no more nonzero scalars in the lower right block. That is, the algorithm reduces an arbitrary $m \times n$ matrix with polynomial entries to a block diagonal matrix $\mathrm{diag}(I_r, B_{m-r,n-r})$ where I_r is the $r \times r$ identity matrix and $B_{m-r,n-r}$ is a matrix in which no entry is a nonzero scalar. Over a field, r is the rank of the matrix, $B = 0$ is the zero matrix, and $\mathrm{diag}(I_r, 0_{m-r,n-r})$ is the usual Smith form.

Definition 8.4.2.1 (Equivalence of matrices with polynomial entries)**.** Let A be an $m \times n$ matrix with entries in $\mathbb{F}[x_1, \dots, x_k]$. An $m \times n$ matrix C is said to be *equivalent* to A over $\mathbb{F}[x_1, \dots, x_k]$ if $C = UAV$ where U $(m \times m)$ and V $(n \times n)$ are invertible matrices over $\mathbb{F}[x_1, \dots, x_k]$: that is, $\det(U), \det(V) \in \mathbb{F} \setminus \{0\}$ are nonzero scalars.

Definition 8.4.2.2 (Partial Smith form)**.** The (non-unique) result of the following algorithm is called the *partial Smith form* of the original matrix A.

Algorithm 8.4.2.3 (Partial row/column reduction)**.**

Input: An $m \times n$ matrix A with entries in $\mathbb{F}[x_1, \dots, x_k]$.

Output: The quantities C, r, B where C is an $m \times n$ block diagonal matrix $C = \mathrm{diag}(I_r, B)$ consisting of an identity matrix of size r and a lower right block $B = B_{m-r,n-r}$ in which no entry is a nonzero scalar.

```
• Set $C \leftarrow A$. Set $k \leftarrow 1$.
• While $c_{ij} \in \mathbb{F} \setminus \{0\}$ for some $i, j \geq k$ do:
    – Find the least $i \geq k$ for which $c_{ij} \in \mathbb{F} \setminus \{0\}$ for some $j \geq k$.
    – If $i \neq k$ then interchange rows $i$ and $k$ of $C$.
    – Find the least $j \geq k$ for which $c_{kj} \in \mathbb{F} \setminus \{0\}$.
    – If $j \neq k$ then interchange columns $j$ and $k$ of $C$.
    – If $c_{kk} \neq 1$ then divide row $k$ of $C$ by $c_{kk}$.
    – For $i = k+1, \dots, m$ do: subtract $c_{ik}$ times row $k$ from row $i$.
    – For $j = k+1, \dots, n$ do: subtract $c_{kj}$ times column $k$ from column $j$.
    – Set $k \leftarrow k + 1$.
• Set $r \leftarrow k - 1$.
• Set $B \leftarrow C(r+1, \dots, m; r+1, \dots, n)$.
• Return $C, r, B$.
```

Example 8.4.2.4. Consider the following sparse 8×12 matrix A with entries in $\mathbb{Q}[a, b]$:

$$A = \begin{bmatrix} b & . & 1 & . & . & . & . & . & a & . & . & . \\ . & a & . & . & . & . & . & . & 1 & . & . & b \\ . & . & . & 1 & . & . & . & . & . & b & . & a \\ . & . & . & . & a & 1 & . & . & . & . & b & . \\ . & b & . & . & 1 & . & a & . & . & . & . & . \\ . & . & . & b & . & . & a & 1 & . & . & . & . \\ . & . & 1 & . & . & a & . & b & . & . & . & . \\ 1 & . & . & . & . & . & . & . & . & b & a & . \end{bmatrix}$$

To compute the determinantal ideals of this matrix requires calculating the following numbers of $r \times r$ determinants for $r = 1, \dots, 8$:

$$\binom{8}{r}\binom{12}{r} \;=\; 96,\ 1848,\ 12320,\ 34650,\ 44352,\ 25872,\ 6336,\ 495.$$

Gröbner bases for these determinantal ideals are as follows, $r = 1, \dots, 8$:

$$[1], \quad [1], \quad [1], \quad [1], \quad [1], \quad [1], \quad [1], \quad [b^3 + b^2, ab^2 + ab, a^2b + a^2, a^3 - ab].$$

This computation took 17.371 seconds using Maple 18 on a 2013 MacBook Pro. Computing the partial Smith form took 0.020 seconds, 869 times faster:

$$C = [I_7, B_{1,5}] = \begin{bmatrix} 1 & . & . & . & . & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . & . & . & . & . \\ . & . & . & . & 1 & . & . & . & . & . & . & . \\ . & . & . & . & . & 1 & . & . & . & . & . & . \\ . & . & . & . & . & . & 1 & . & . & . & . & . \\ . & . & . & . & . & . & . & ab^2 + ab & a^3 - ab & b^3 + b^2 & . & a^2b + a^2 \end{bmatrix}$$

In both cases we find the solution $[a, b] \;=\; [0, 0],\ [0, -1],\ [i, -1],\ [-i, -1]$; for these values we have $\operatorname{rank}(A) = 7$, and for all other values the rank is 8.

8.4.3 Canonical forms of row submodules

A submodule R of a free module $\mathbb{F}[x_1, \dots, x_k]^n$ of rank n which is a direct summand is projective (by one of equivalent definitions), and the Quillen–Suslin theorem implies that R is free. But generally submodules of free modules over a polynomial ring $\mathbb{F}[x_1, \dots, x_k]$ are not necessarily free.

Example 8.4.3.1. Let $R = (a, b)$, the row module of the 2×1 matrix $[a, b]^t$. It consists of all polynomials with zero constant term, and as vector spaces we have $R \oplus \mathbb{F} = \mathbb{F}[a, b]$. No submodule of a free $\mathbb{F}[a, b]$-module is 1-dimensional as a vector space. This shows that R is not projective, hence not free.

Let A be an $m \times n$ matrix with entries in $\mathbb{F}[x_1, \cdots, x_k]$. Its row module and null module are defined in the usual way (here A_i is the row i of A):

$$\begin{aligned} \operatorname{row}(A) &= \{\, f_1 A_1 + \cdots + f_m A_m \mid f_1, \dots, f_m \in \mathbb{F}[x_1, \cdots, x_k] \,\} \\ \operatorname{null}(A) &= \{[f_1, \dots, f_n] \mid f_1 A_1 + \cdots + f_m A_m = 0,\ f_1, \dots, f_m \in \mathbb{F}[x_1, \cdots, x_k]\} \end{aligned}$$

These are submodules of the free modules of ranks m and n, respectively. The first natural question to ask is: is either of these submodules also free?

Of course, $\mathbb{F}[x_1, \cdots, x_k]$ itself is a free module, and an ideal is a submodule. The theory of Gröbner bases for submodules of free $\mathbb{F}[x_1, \cdots, x_k]$-modules was generalized in [201] from the free module of rank one to free modules of any finite rank. This is now a standard topic in commutative algebra [65, Chap. 5]. In particular, this theory includes algorithms for computing row canonical forms of matrices over polynomial rings, as we will now demonstrate.

The algorithm for computing a submodule Gröbner basis consists of three components: first, Gaussian elimination using elementary row operations; second, Buchberger's algorithm for Gröbner bases; and third, the occasional addition of a zero row to the matrix as "scratch paper" for computing S-polynomials. We did not find a matrix form of this algorithm in the literature, but we can direct the reader to the original paper [201, §I.4], as well as the somewhat sketchier versions in [1, §3.5] and [65, §5.2]. Algorithm 8.4.3.2 is our own somewhat sketchy matrix version of this algorithm.

Algorithm 8.4.3.2 (Submodule Gröbner basis algorithm (matrix form))**.**

Input: An $m \times n$ matrix A with entries in $\mathbb{F}[x_1, \dots, x_k]$.

Output: The Gröbner basis for row(A), with respect to the given (implicit) order of the columns and some given monomial order.

- Set $i \leftarrow 1$, $j \leftarrow 1$.
- While $i \leq m$ and $j \leq n$ do:
    1. If all entries at and below pivot (i, j) are 0, then set $j \leftarrow j + 1$.
    2. Otherwise:
        - (a) Repeat until convergence: Use row operations to swap the smallest nonzero entry into the pivot and reduce the other entries modulo the pivot.
        - (b) Sort the entries at and below the pivot in increasing order, with 0 being the greatest.
        - (c) For $k = 1, \dots, m - j$ repeat the two previous steps (i and ii) for the entries at and below position $(i + k, j)$ to self-reduce the column.
        - (d) For every pair of indices k, k' such that $i \leq k \neq k' \leq m$ and the entries in positions (i, k) and (i, k') produce an S-polynomial with a nonzero reduced form modulo the entries in rows i through m, do the following:
            - i. Set $m \leftarrow m + 1$; add a new zero row at the bottom.
            - ii. Use row operations to construct the S-polynomial in position $(m{+}1, j)$, and compute its nonzero reduced form modulo the entries in rows i through m.
        - (e) Repeat steps (a)–(d) until the entries at and below the pivot form a reduced Gröbner basis for the ideal they generate.
        - (f) Delete any zero rows and modify m accordingly.
        - (g) Use the Gröbner basis at and below the pivot to reduce the entries above the pivot to their normal forms.
        - (h) Set $i \leftarrow i + 1$, $j \leftarrow j + 1$.

Example 8.4.3.3. Let $\mathbb{F}[a,b]$ equipped with the `plex` order; we view polynomials in a, b as polynomials in b whose coefficients are polynomials in a. We consider the 10×14 matrix A displayed sideways in two parts in Figure 8.2; the significance of this matrix will become clear in the next chapters.

Column 1. The first column has two nonzero entries which generate the principal ideal

$$(ab^2 + ab).$$

We interchange rows 1 and 10, multiply row 1 by -1, and then subtract a times row 1 from row 2. Column 1 is now zero except for the ideal generator in row 1.

Column 2. At this point column 2 has $b^3 + b^2$ in row 1 and zeros in the other rows, so it is already reduced.

Column 3. The entries

$$ba - a^3, \qquad -ba^2 + a^4, \qquad b^2a^2 - ba^4, \qquad b^2a^2 - 2ba^4 + ba^2 + a^6 - a^4$$

in column 3 in row 2 and below generate the principal ideal

$$(ba - a^3).$$

Conveniently, the generator appears in row 8, so we swap it up to row 2 and use row operations to eliminate the entries below it. The entry in row 1 of column 2 is $-ba^3 + a^5$, which is $-a^2$ times the generator; we use one more row operation to make this entry zero too.

Column 4. The entries in column 4 in row 3 and below generate our first non-principal ideal:

$$-ba^2 - a^2, \quad ba^4 + a^4, \quad ba^6 - ba^4 + a^6 - a^4, \quad -b^2a - ba^3 - ba - a^3, \quad -b^2a^4 - ba^4.$$

The `plex` $(a \prec b)$ Gröbner basis for this ideal consists of two elements

$$ba^2 + a^2 \quad \text{and} \quad b^2a + ba.$$

The first of these already appears in the column so we swap it up to row 3 and use row operations to replace each of the lower entries by their remainders after long division by this entry. This makes all the lower entries zero except for $-b^2a - ba$ in row 9; we swap it up to row 4 and change its sign. We now have the Gröbner basis in rows 3 and 4; we use it to reduce the entries in rows 1 and 2. For example, the entry in position 1,4 reduces as follows:

$$(b^2a^3 + b^2a + ba^5 + a^5) - (a^3 + ab - a)(ba^2 + a^2) - (b^2a + ba) \longrightarrow (-ba + a^3).$$

Column 5. The entries in column 5, in row 5 and below, generate the principal ideal

$$(ba^2 + a^2).$$

The negative of the generator is the entry in row 10, so as before we swap it

$$
\left[\begin{array}{ccccccc}
0 & 0 & 0 & -ba^2-a^2 & 0 & ba-a^3 & 0 \\
b^2a^2+ba^2 & b^3a+b^2a & b^2a^2-2ba^4+a^6 & b^2a^4+b^2a^2 & b^3a^3-ba^3 & b^3a-b^2a^3+ba^5+ba^3 & 0 \\
0 & 0 & 0 & 0 & -ba^2-a^2 & 0 & 0 \\
0 & 0 & -ba^2+a^4 & 0 & 0 & -b^2a+ba^3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & ba-a^3 \\
0 & 0 & b^2a^2-2ba^4+ba^2+a^6-a^4 & b^2a^4+ba^4 & b^3a^3+b^2a^3 & b^3a-b^2a^3+b^2a+ba^5 & -b^2a+ba^3 \\
0 & 0 & ba-a^3 & ba^3+a^3 & b^2a^2+ba^2 & 0 & 0 \\
0 & 0 & ba-a^3 & -b^2a-ba & -b^3-b^2 & -ba^2-a^2 & 0 \\
-b^2a-ba & -b^3-b^2 & ba^3-a^5 & -b^2a^3-b^2a & -b^3a^2+ba^2 & -ba^4-ba^2 & 0
\end{array}\right.
$$

$$
\left.\begin{array}{ccccccc}
0 & -b^2a-ba & 0 & 0 & 0 & b^3a+b^2a & b^4+b^3 \\
0 & -b^4a+b^3a^3 & b^4a^2-b^2a^2 & -b^4a-b^3a & b^2a^2-ba^4+ba^2-a^4 & b^5a-b^3a & b^6-b^4 \\
0 & 0 & -b^2a-ba & 0 & ba-a^3 & -b^3-b^2 & 0 \\
0 & b^3a-b^2a^3 & -b^3a^2+ba^2 & b^3a+b^2a & -ba^2-a^2 & -b^4a+b^2a & -b^5+b^3 \\
0 & ba-a^3 & -ba^2-a^2 & 0 & 0 & -b^2a-ba & -b^3-b^2 \\
-ba^2-a^2 & 0 & 0 & -b^2a-ba & 0 & 0 & -b^3-b^2 \\
b^2a^2+ba^2 & -b^4a+b^3a^3-b^3a+b^2a^3 & b^4a^2+b^3a^2 & -b^4a-b^3a & b^2a^2-ba^4 & b^5a+b^4a & b^6+b^5 \\
0 & b^2a^2+ba^2 & b^3a+b^2a & -b^3-b^2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & ba^3+a^3 & 0 & 0
\end{array}\right]
$$

FIGURE 8.2: The 10×14 matrix over $\mathbb{F}[a, b]$ discussed in Example 8.4.3.3.

up to row 5, change its sign, and use row operations to eliminate the entries below it and reduce the entries above it.

The calculations get significantly more complicated at this point, so we record the state of the matrix after the reduction of column 5, at least the reduced part. The upper left 5×5 block is as follows, and the 5×5 block below it is the zero matrix:

$$\begin{bmatrix} b^2a+ba & b^3+b^2 & 0 & -ba+a^3 & -b^3-b^2 \\ 0 & 0 & ba-a^3 & 0 & 0 \\ 0 & 0 & 0 & ba^2+a^2 & 0 \\ 0 & 0 & 0 & b^2a+ba & b^3+b^2 \\ 0 & 0 & 0 & 0 & ba^2+a^2 \end{bmatrix}$$

Column 6. The nonzero entries at or below the current pivot (6,6) are as follows, appearing once each in rows 9, 8, 7, respectively :

$$\begin{aligned} f &= -b^2a + 2ba^3 - a^5, \\ g &= b^3a - 2b^2a^3 + ba^5, \\ h &= b^3a - b^2a^3 + b^2a + 2ba^5 - ba^3 - a^7 + a^5. \end{aligned}$$

Clearly $g = -bf$ so we can use a row operation with f to eliminate g. Negating f and renaming, we are left with these two generators of the column ideal:

$$f = b^2a - 2ba^3 + a^5, \qquad g = b^3a - b^2a^3 + b^2a + 2ba^5 - ba^3 - a^7 + a^5.$$

The normal form of g with respect to f is $3ba^5 + ba^3 - 2a^7$, so our new generators are (renaming again):

$$f = 3ba^5 + ba^3 - 2a^7, \qquad g = b^2a - 2ba^3 + a^5.$$

This is a self-reduced set, so we must consider S-polynomials: there is one, which we will denote by s, corresponding to the overlap ab; we also give its reduced form s' with respect to f and g:

$$s = b^2a^3 + 4ba^7 - 3a^9, \qquad s' = 2ba^3 + 3a^9 + 5a^7.$$

Computing the reduced forms of f and g with respect to s' gives the polynomials f' and g', respectively, where

$$f' = a^{11} + 2a^9 + a^7, \qquad g' = b^2a + 3a^9 + 5a^7 + a^5.$$

We now verify that the ordered set $\{f', s', g'\}$ is the reduced `plex` Gröbner basis for the column ideal in this case.

Let us see how this can be translated into matrix terms. Before computing the S-polynomial, we need to perform these row operations:

- Interchange rows 6 and 9.

- Multiply row 6 by -1.
- Add $-b$ times row 6 to row 8.
- Add $-(a^2+b+1)$ times row 6 to row 7.
- Interchange rows 6 and 7.

At this point rows 6 and 7 contain (the last values of) f and g, respectively. In order to construct the S-polynomial we need either to have a zero row in the matrix, or to temporarily add a new zero row at the bottom of the matrix. Conveniently, it happens that row 8 is zero, and although this is not strictly necessary, we will start by swapping this zero row to the bottom of the matrix so that we can do our calculations there. Recall that the S-polynomial is

$$b(3ba^5+ba^3-2a^7)-3a^4(b^2a-2ba^3+a^5)=b^2a^3+4ba^7-3a^9.$$

To compute the S-polynomial and the Gröbner basis, we need to perform these row operations:

- Interchange rows 8 and 10.
- Add b times row 6 to row 10; add $-3a^4$ times row 7 to row 10.
- Add $-\frac{4}{3}a^2-\frac{2}{9}$ times row 6 to row 10; add $-a^2$ times row 7 to row 10.
- Multiply row 10 by -9.
- Interchange rows 7 and 8, 6 and 7, 10 and 6.
- Add $-\frac{3}{2}a^2-\frac{1}{2}$ times row 6 to row 7; add -1 times row 6 to row 8.
- Multiply row 7 by $-\frac{2}{9}$, and interchange rows 6 and 7.

It remains to reduce the entries above the pivot with respect to the Gröbner basis; these are the entries in the upper right corner of the following array, which is the upper left 8×6 block of the current state of the original matrix. This task is left as an exercise for the reader:

$$\begin{array}{ccccc|c}
b^2a+ba & b^3+b^2 & 0 & -ba+a^3 & -b^3-b^2 & b^2a^2+ba^4-2ba^2-a^6+2a^4-a^2 \\
0 & 0 & ba-a^3 & 0 & 0 & ba^2-a^4 \\
0 & 0 & 0 & ba^2+a^2 & 0 & -ba+a^3 \\
0 & 0 & 0 & b^2a+ba & b^3+b^2 & 2ba^2-a^4+a^2 \\
0 & 0 & 0 & 0 & ba^2+a^2 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & a^{11}+2a^9+a^7 \\
0 & 0 & 0 & 0 & 0 & 2ba^3+3a^9+5a^7 \\
0 & 0 & 0 & 0 & 0 & b^2a+3a^9+5a^7+a^5
\end{array}$$

Column 7. Rows 1–5 and 10 contain 0, row 9 contains $ab-a^3$, and rows 6–8 contain two (one is repeated) somewhat complex polynomials which are a direct result of the S-polynomial calculation from column 6; however, these polynomials

$$-b(4a^4 - 3a^2b + 2a^2 - b)(ab - a^3),$$
$$-b(12a^2 - 9b + 2)(ab - a^3).$$

are multiples of $ab - a^3$ and so the column ideal is principal. These multipliers show us how to use row operations to use the leading entry of row 9 to make every other entry in column 7 equal to 0.

Columns 8–14. Row 10 is not zero, so there is one remaining leading entry to be dealt with. Finishing the reduction of the matrix is left as an exercise for the reader (rather easy with the help of a computer algebra system).

We can obtain simpler (but non-canonical) results by using column operations as well, and always swapping into the current position that column whose Gröbner basis is the smallest (breaking ties using the monomial order). This allows us to show the non-obvious fact that the submodule generated by the rows of the matrix in the previous example (Figure 8.2) is free of rank 9.

Example 8.4.3.4. We start again from the matrix in Figure 8.2, except that now we are allowing column transpositions, as well as general row operations. At each step we consider the (sub)columns below and to the right of the pivot, determine which of them generates the simplest ideal, and swap that column into the current position. By simplest we mean either the Gröbner basis has fewer elements, or the Gröbner basis has the same number of elements but precedes in the monomial order, or the Gröbner bases are equal but the original column has fewer nonzero entries.

Column 1. The columns of the original matrix which generate principal ideals are 1, 2, 3, 7, 8, 14, and their generators are, respectively,

$$ab^2 + ab, \quad b^3 + b^2, \quad a^3 - ab, \quad a^3 - ab, \quad a^2b + a^2, \quad b^3 + b^2.$$

The minimal generator is $a^3 - ab$ corresponding to columns 3 and 7 having, respectively, 6 and 2 nonzero elements, so we swap columns 1 and 7. To reduce the new column 1, we swap rows 1 and 6, and add b times row 6 to row 7. Column 1 now has $a^3 - ab$ in row 1 and 0 in the other rows.

Column 2. We notice that column 8 is the only column apart from column 1 which has a nonzero entry in row 1 with zeros below it, so we swap columns 2 and 8. Column 2 now has $-ba^2 - a^2$ in row 1 and 0 in the other rows.

Column 3. This column already has the minimal generator among the principal ideals generated by the entries in rows 2 to 10 of columns 3 to 14 and so no column operation is necessary. After a sequence of row operations, column 3 has $a^3 - ab$ in row 2 and 0 in the other rows.

Column 4. We swap columns 4 and 7, perform a sequence of row operations, and obtain the result in which $b^2a + ba$ is in row 3 and the other entries are 0.

Column 5. We swap columns 5 and 8; no row operations are necessary. Column 5 now has $b^3 + b^2$ in row 4 and 0 in the other positions.

Column 6. We swap columns 6 and 11, perform a few row operations, and we are left with $b^3 + b^2$ in row 4 and the irreducible entry $-b^2a - ba$ in row 1.

Column 7. We swap columns 7 and 11, and after a few row operations, the first eight columns of the matrix are as follows; the vertical line separates the reduced part (left) from the unreduced part (right):

$$
\begin{array}{ccccccc|c}
ba-a^3 & -ba^2-a^2 & 0 & 0 & 0 & -b^2a-ba & 0 & 0 \\
0 & 0 & ba-a^3 & 0 & 0 & 0 & -a^4-a^2 & -b^3-b^2 \\
0 & 0 & 0 & b^2a+ba & b^3+b^2 & 0 & 0 & -b^2a^2-ba^2 \\
0 & 0 & 0 & 0 & 0 & b^3+b^2 & -a^4-a^2 & -b^3-b^2a^2-b^2-ba^2 \\
0 & 0 & 0 & 0 & 0 & 0 & ba-a^3 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -b^3a^3-2b^2a^3-ba^3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -b^3a^3-b^2a^3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & b^2a^3+ba^3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -ba^2-a^2
\end{array}
$$

Columns 8–14. Continuing in a similar manner, we obtain the reduced form of the remaining 8 columns of the matrix; see Figure 8.3 which gives the complete reduced form, and note that row 10 consists entirely of zeros. Verifying the details is left as an exercise for the reader (use of a computer algebra system is highly recommended).

Example 8.4.3.5. We computed the Gröbner bases (using the `plex` monomial order) for the determinantal ideals of the matrix of Figure 8.2 *before* the row-column reduction of Example 8.4.3.4, and then computed them again *after*. For the reduced matrix of Figure 8.3 computing all the determinantal ideals took 301.769 seconds, just over 5 minutes (all computations using Maple 18 on a Lenovo ThinkCenter). For the original matrix of Figure 8.2 computing all the determinantal ideals took 6524.820 seconds, or 108.747 minutes, more than 21.6 times longer. The reduction process eliminated one row from the matrix, which made the subsequent computations significantly simpler.

Remark 8.4.3.6. We provide some further information about the rank distribution for the matrices of Figure 8.2 and 8.3. Since these matrices are row/column equivalent, they have the same determinantal ideals and the same `plex` Gröbner bases; moreover, the ideals have the same radicals and zero sets. Basic data about the Gröbner bases are summarized in Figure 8.4. One of the most complex polynomials in the Gröbner bases is the following:

$$
\begin{aligned}
& a^7b^3(b+1)^3(\, a^{16} + 6a^{14} - 22a^{12}b - 7a^{12} - 64a^{10}b^3 - 38a^{10}b^2 + 6a^{10}b \\
& + 221a^8b^4 + 252a^8b^3 + 46a^8b^2 - 300a^6b^5 - 398a^6b^4 - 104a^6b^3 - 81a^4b^8 \\
& - 324a^4b^7 - 300a^4b^6 - 58a^4b^5 + 118a^2b^{11} + 450a^2b^{10} + 642a^2b^9 + 428a^2b^8 \\
& + 118a^2b^7 - 148b^{18} - 1228b^{17} - 4711b^{16} - 10914b^{15} - 16688b^{14} - 17222b^{13}
\end{aligned}
$$

$$\left[\begin{array}{ccccccccc}
ba - a^3 & -ba^2 - a^2 & 0 & 0 & 0 & -b^2a - ba & 0 & 0 & 0 \\
0 & 0 & ba - a^3 & 0 & 0 & 0 & -a^4 - a^2 & -b^3 - b^2 & 0 \\
0 & 0 & 0 & b^2a + ba & b^3 + b^2 & 0 & 0 & 0 & b^3a + b^2a \\
0 & 0 & 0 & 0 & 0 & b^3 + b^2 & -a^4 - a^2 & -b^3 - b^2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & ba - a^3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & ba^2 + a^2 & b^2a + ba \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & ba^2 + a^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right.$$

$$\left.\begin{array}{ccccc}
0 & 0 & 0 & 0 & -b^3 - b^2 \\
b^3a^2 + b^2a^2 & 0 & -b^2a - ba^3 - ba - a^3 & -b^2a^2 - ba^2 & b^4a + b^3a \\
b^4 - b^3a^2 + b^3 - b^2a^2 & -b^2a - a^3 & b^2a + a^3 & b^2a^2 + ba^2 & -b^4a - b^3a \\
b^4 + b^3a^2 + b^3 + b^2a^2 & -b^2a + ba^3 & -b^2a - 2ba^3 - ba - 2a^3 & -2b^2a^2 - 2ba^2 & b^4a + b^3a \\
b^3a + b^2a & 0 & -ba^2 - a^2 & -b^2a - ba & b^4 + b^3 \\
b^3 + b^2 & -ba + a^3 & 0 & 0 & 0 \\
b^2a + ba & 0 & 0 & -ba + a^3 & b^3 + b^2 \\
b^3a^3 + b^2a^3 & ba^4 + 2ba^2 + a^2 & -ba^4 - a^4 & -b^2a^3 - b^2a & b^4a^2 + b^4 + b^3a^2 + b^3 \\
0 & b^2a^2 - ba^4 - ba^2 - a^2 & -b^2a^2 + ba^4 - ba^2 + a^4 & -b^3a + b^2a^3 & b^5 + b^4 \\
0 & 0 & 0 & 0 & 0
\end{array}\right]$$

FIGURE 8.3: Final reduced upper triangular matrix from Example 8.4.3.4.

	total minors		nonzero minors		`plex` Gröbner basis			
r	$\binom{10}{r}\binom{14}{r}$	$\binom{9}{r}\binom{14}{r}$	original	reduced	size	degs	terms	max cft
1	140	126	37	24	4	3	2	1
2	4095	3276	401	172	6	5,6	3,4	3
3	43680	30576	2333	814	8	7-9	4-9	6
4	210210	126126	10253	2692	11	10-12	5-12	36
5	504504	252252	30354	5766	13	12-15	6-20	130
6	630630	252252	51624	8017	14	14-18	7-26	474
7	411840	123552	44168	6748	15	17-21	8-37	592
8	135135	27027	15111	2909	14	21-24	9-49	9992
9	20020	2002	1203	436	14	29-32	14-59	124383
10	1001	0	1	0				

FIGURE 8.4: Gröbner bases for original/reduced matrices.

$$- 11739b^{12} - 4930b^{11} - 1090b^{10} - 82b^{9} \,).$$

Nonetheless, the radicals are all very simple, and have the following `plex` Gröbner bases, from which the zero sets can be easily derived (Exercise 8.13):

r	`plex` Gröbner basis, r-th determinantal ideal
1	$b(b+1),\ a(b+1),\ a(a^2+1)$
2	$b(b+1),\ a(b+1),\ a(a^2+1)$
3	$b(b+1),\ a(b+1),\ a(a^2+1)$
4	$b(b+1),\ a(b+1),\ a(a^2+1)$
5	$b(b+1),\ a(b+1),\ a(a^2+1)$
6	$a(b+1),\ a(a^2+1)$
7	$ab(b+1),\ a(a-1)(a+1)(b+1)$
8	$ab(b+1)$
9	$ab(b+1)(b^2+b+1),\ ab(b+1)(a^2-b)$

To conclude this section, we would like to mention very briefly how invoking the notion of a syzygy from commutative algebra can sometimes be used to simplify matrices with polynomial entries. We start with a finitely generated submodule M of a free module of rank n over the polynomial ring $\mathbb{F}[x_1, \dots, x_k]$, in other words with the row module of an $m \times n$ matrix A with polynomial entries.

Definition 8.4.3.7. By a *syzygy* of (the rows of) the matrix A we mean a linear dependence relation for the rows, with polynomial coefficients: in other words, a (nonzero) row vector $S \in \mathbb{F}[x_1, \dots, x_k]^m$ for which $SA = 0$.

Since the rows of A generate the module M, every syzygy is a relation among the generators of M. For a matrix over a field, a syzygy is the same thing as a nonzero element of the left nullspace of the matrix, or equivalently the right nullspace of the transpose of the matrix. In this situation, we can easily determine all syzygies by transposing the matrix, computing the RCF, and extracting a basis for the nullspace.

Example 8.4.3.8. Let us see what happens when we replace polynomials by rational functions and apply Gaussian elimination. This is best illustrated by an example, and we have just seen one: in the last example, the last row became a row of zeros when we computed the upper triangular form. Start with the 10×14 block matrix from Figure 8.2, transpose it, and compute its RCF over $\mathbb{F}(x_1, \dots, x_k)$:

$$\begin{bmatrix} 1 & . & . & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . & . & -1/a \\ . & . & 1 & . & . & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . & . & -b/a \\ . & . & . & . & 1 & . & . & . & . & . \\ . & . & . & . & . & 1 & . & . & . & . \\ . & . & . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & . & . & 1 & . \end{bmatrix}$$

The nullspace is 1-dimensional, and a basis is

$$\begin{bmatrix} 0 & \frac{1}{a} & 0 & \frac{b}{a} & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Now something special happens: when we clear the denominators, we are left with a nonzero scalar as one of the coefficients:

$$\frac{1}{a} \begin{bmatrix} 0 & 1 & 0 & b & 0 & 0 & 0 & 0 & 0 & a \end{bmatrix}$$

This tells us that as long as $a \neq 0$, then $R_2 + bR_4 + aR_{10} = 0$, where R_i is row i of the original block B. It is easy to check that the condition $a \neq 0$ is superfluous, and so we see that

$$R_2 = -aR_4 - bR_{10}.$$

In other words, syzygies that have scalar coefficients allow to simplify matrices we work with: if we perform the polynomial row operations “add aR_4 to R_2” and “add bR_{10} to R_2” then we will have eliminated row 2: it will have become a row of zeros.

8.5 Bibliographical comments

The topic of linear algebra over polynomial rings is not as well known as it should be, for a number of reasons. Perhaps the fundamental reason is that this nomenclature for the topic is relatively recent and has been influenced by the rapid development of computer algebra; until the late 1970s research in this area was regarded as the theory of finitely generated submodules of free modules over commutative rings (which makes it hard to identify the most relevant papers during a bibliographical search). A second reason, closely related to the first, is the dichotomy between axiomatic methods and constructive methods: there are many impressive theorems which require Zorn's Lemma in their proofs, but unless an algorithmic version can be given in the finite case, most specialists in computer algebra tend to lose interest rather quickly. A third reason, not related to the first two, is the breadth of connections of the topic of linear algebra over polynomial rings; all of the following areas can be expected to contribute directly to progress in research on this topic:

- Constructive methods in module theory over commutative rings.
- Complexity of Gröbner basis computations.
- Classification of modules over polynomial rings: free, projective, injective, etc.
- The Quillen–Suslin theorem (solution to Serre's problem).
- Group actions on polynomial matrices, and orbit representatives.
- Algebraic K-theory, especially the K_1 group of polynomial rings.

Nonetheless, we somewhat boldly compiled the list [133, 129, 238, 215, 172, 83, 229, 211, 245, 246, 168, 169, 195, 201, 13, 130] of essential papers, in chronological order (it all, unsurprisingly, starts with Hilbert).

8.6 Exercises

Exercise 8.1. For each possible value r of the rank of each of the following matrices A, determine the values of the parameters x_1, x_2 for which $\mathrm{rank}(A) = r$:

$$\begin{bmatrix} x_1 & x_1 & x_2 \\ 1 & x_1 & 0 \\ 0 & x_1 & 0 \end{bmatrix} \qquad \begin{bmatrix} x_2 & x_1 & 0 \\ x_2 & 0 & 1 \\ x_2 & 0 & x_1 \end{bmatrix} \qquad \begin{bmatrix} 1 & x_2 & 1 \\ 0 & 1 & x_1 \\ x_1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & x_1 & 0 & x_1 \\ x_1 & 1 & x_2 & 0 \\ 0 & 1 & x_1 & x_1 \\ 1 & x_2 & 1 & x_2 \end{bmatrix} \qquad \begin{bmatrix} x_2 & x_1 & 0 & 0 \\ 1 & 1 & x_2 & x_2 \\ x_1 & x_2 & 0 & x_2 \\ x_2 & 0 & x_1 & x_2 \end{bmatrix} \qquad \begin{bmatrix} 0 & x_2 & 1 & x_1 \\ x_2 & 1 & 1 & x_1 \\ 1 & 1 & x_1 & x_2 \\ 1 & 0 & 1 & x_1 \end{bmatrix}$$

$$
\begin{bmatrix} x_1 & 0 & x_1 & x_2 & 0 \\ x_2 & x_2 & x_2 & x_1 & x_2 \\ 1 & x_2 & 0 & x_2 & x_2 \\ 1 & 0 & x_2 & x_2 & 0 \\ 0 & 1 & x_1 & x_1 & 1 \end{bmatrix}
\quad
\begin{bmatrix} 1 & x_2 & x_2 & x_2 & x_2 \\ x_1 & 0 & x_2 & 0 & x_2 \\ x_1 & x_1 & 0 & 0 & 0 \\ x_2 & 1 & x_2 & 0 & 0 \\ x_2 & 1 & 1 & x_2 & x_1 \end{bmatrix}
\quad
\begin{bmatrix} x_2 & 0 & x_2 & x_1 & x_1 \\ x_1 & 1 & 1 & 0 & x_1 \\ 0 & 0 & x_2 & x_1 & 1 \\ 0 & x_2 & x_2 & x_1 & x_2 \\ x_2 & 1 & x_1 & x_1 & x_1 \end{bmatrix}
$$

Exercise 8.2. For each possible value r of the rank of each of the following matrices A, determine the values of the parameters x_1, x_2, x_3 for which $\mathrm{rank}(A) = r$:

$$
\begin{bmatrix} x_3 & x_2 & x_1 \\ 1 & x_1 & 0 \\ 0 & x_1 & x_3 \end{bmatrix}
\qquad
\begin{bmatrix} x_2 & x_3 & x_1 \\ x_2 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}
\qquad
\begin{bmatrix} x_3 & 1 & x_3 \\ 1 & x_1 & x_2 \\ x_2 & x_3 & x_1 \end{bmatrix}
$$

$$
\begin{bmatrix} x_1 & x_2 & 0 & x_1 \\ 1 & x_2 & 1 & 1 \\ x_1 & x_2 & 1 & x_2 \\ 1 & x_2 & x_2 & x_3 \end{bmatrix}
\qquad
\begin{bmatrix} x_2 & x_1 & x_1 & x_2 \\ 0 & 0 & x_3 & x_2 \\ 0 & x_2 & 1 & 1 \\ x_1 & 1 & x_2 & 1 \end{bmatrix}
\qquad
\begin{bmatrix} x_3 & x_1 & x_1 & 1 \\ 1 & 0 & x_1 & x_3 \\ x_3 & x_2 & x_1 & 1 \\ 0 & x_1 & x_1 & x_1 \end{bmatrix}
$$

$$
\begin{bmatrix} 0 & x_1 & x_1 & x_1 & x_2 \\ 0 & x_2 & 1 & 0 & x_3 \\ 0 & x_2 & x_3 & x_3 & 0 \\ 0 & x_1 & 1 & 1 & x_1 \\ x_2 & x_1 & x_3 & x_2 & x_1 \end{bmatrix}
\quad
\begin{bmatrix} x_2 & x_3 & x_1 & 0 & x_2 \\ x_2 & 1 & x_1 & 1 & x_1 \\ x_2 & 0 & 0 & x_3 & 0 \\ 1 & x_1 & 0 & x_2 & x_1 \\ x_1 & 0 & 0 & 0 & x_2 \end{bmatrix}
\quad
\begin{bmatrix} 1 & 0 & x_2 & 0 & x_2 \\ 0 & 1 & 0 & 1 & 1 \\ x_3 & 1 & x_3 & x_2 & x_1 \\ 1 & 0 & x_2 & x_1 & x_2 \\ 0 & 1 & 0 & 1 & x_2 \end{bmatrix}
$$

Exercise 8.3. For each possible value r of the rank of each of the following matrices A, determine the values of the parameters x_1, x_2, x_3, x_4 for which $\mathrm{rank}(A) = r$:

$$
\begin{bmatrix} x_1 & 0 & x_4 \\ x_3 & x_4 & x_2 \\ x_1 & x_4 & x_3 \end{bmatrix}
\qquad
\begin{bmatrix} 1 & x_1 & x_2 \\ x_3 & 0 & x_4 \\ x_2 & 0 & 1 \end{bmatrix}
\qquad
\begin{bmatrix} x_3 & 1 & x_1 \\ x_4 & x_4 & 0 \\ x_2 & x_2 & x_4 \end{bmatrix}
$$

$$
\begin{bmatrix} 0 & 0 & x_4 & 0 \\ 1 & x_3 & 1 & x_3 \\ x_2 & x_1 & 0 & x_2 \\ x_2 & 0 & x_4 & x_3 \end{bmatrix}
\qquad
\begin{bmatrix} x_2 & 0 & 1 & x_4 \\ x_2 & x_4 & x_3 & x_2 \\ x_4 & x_2 & x_2 & x_2 \\ x_1 & 0 & x_3 & 0 \end{bmatrix}
\qquad
\begin{bmatrix} x_4 & x_3 & x_2 & x_1 \\ x_2 & x_3 & x_1 & 0 \\ x_4 & x_2 & x_4 & x_2 \\ 1 & x_1 & 1 & x_1 \end{bmatrix}
$$

$$
\begin{bmatrix} x_3 & 1 & x_1 & x_4 & 0 \\ x_1 & 1 & 0 & x_2 & 0 \\ x_4 & x_2 & 0 & 1 & 0 \\ 1 & 1 & x_3 & 1 & x_3 \\ x_2 & x_4 & x_4 & x_1 & 1 \end{bmatrix}
\quad
\begin{bmatrix} x_2 & 0 & 0 & 0 & 0 \\ 1 & x_3 & x_4 & x_2 & x_1 \\ x_4 & x_3 & x_3 & x_2 & 0 \\ x_2 & 1 & 1 & x_3 & 1 \\ x_3 & x_3 & x_4 & x_2 & x_1 \end{bmatrix}
\quad
\begin{bmatrix} x_3 & 0 & 0 & x_2 & 0 \\ x_3 & 0 & x_1 & 1 & x_2 \\ x_1 & x_1 & x_1 & x_4 & x_1 \\ 1 & x_3 & 0 & 0 & 0 \\ x_2 & 1 & x_2 & x_3 & x_1 \end{bmatrix}
$$

Exercise 8.4. Write a computer program which takes as input a given number k of parameters $x_1, \dots, x_k$ and a given size n of square matrices, and produces as output a pseudorandom $n \times n$ matrix whose entries are chosen uniformly from the set $\mathcal{E} = \{0, 1, x_1, \dots, x_k\}$. Extend this to a program which takes as input positive integers k, m, n and whose output is a pseudorandom $m \times n$ matrix whose entries are chosen uniformly from $\mathcal{E}$.

Exercise 8.5. Write a computer program which takes as input an $m \times n$ matrix A whose entries belong to the polynomial ring $\mathbb{F}[x_1, \dots, x_k]$ and which produces as output Gröbner bases for the determinantal ideals $DI_r(A)$ where $0 \le r \le \min(m, n)$. Extend this to a program which also computes the zero sets $V(DI_r(A))$ and the inverse image for each possible rank:

inverse image	rank(s)
$V(DI_{r+1}(A) \setminus V(DI_r(A))$	$0 \le r < \min(m, n)$
$\mathbb{F}^k \setminus V(DI_r(A))$	$r = \min(m, n)$

Exercise 8.6. Verify the claims made in subsection 8.3.2 about the ranks of the matrices A_n for $n \le 5$.

Exercise 8.7. Verify the following claims about the matrix A_6 (see subsection 8.3.2 for the definition), and fill in the blanks for ranks 5 and 6:

$$\begin{aligned}
V(DI_1(A_6)) &= V(DI_2(A_6)) = \emptyset \\
V(DI_3(A_6)) &= \{(0, 1, 0, 1)\} \\
V(DI_4(A_6)) &= \big\{ \big(x_1,\, (x_1{+}\epsilon)^2,\, x_1(x_1{+}2\epsilon)^2,\, (x_1^2{+}3\epsilon x_1{+}1)^2 \big) \mid \\
&\qquad\qquad x_1 \in \mathbb{F},\, \epsilon = \pm 1 \big\} \\
V(DI_5(A_6)) &= V(DI_6(A_6)) = \text{exercise}
\end{aligned}$$

For this problem, computing the radicals of the determinantal ideals may be useful. Recall that the radical $\sqrt{I}$ of the ideal $I \subseteq \mathbb{F}[x_1, \dots, x_k]$ consists of all polynomials which vanish on the zero set of I, and hence $V(\sqrt{I}) = V(I)$. Typically, $\sqrt{I}$ is much larger than I and has a much simpler Gröbner basis. For example, here is the deglex Gröbner basis of $DI_4(A_6)$,

$$\begin{aligned}
&x_2^2 - x_3x_1 - 2x_2 + 1, \\
&x_3x_2 - x_4x_1 - x_2x_1 - x_3 + 2x_1, \\
&x_3^2 - x_4x_2 - x_3x_1 + x_4 + x_2 - 1, \\
&x_1\big(x_1^3 - 2x_2x_1 + x_3 - 2x_1\big), \\
&x_1\big(x_2x_1^2 - 2x_3x_1 - x_1^2 + x_4 - 3x_2 + 2\big), \\
&x_3x_1^3 - 2x_4x_1^2 - 2x_2x_1^2 + x_4x_2 - 3x_3x_1 + 4x_1^2 - x_4 - x_2 + 1, \\
&\big(x_4 - 1\big)\big(x_1^3 - 2x_2x_1 + x_3 - 2x_1\big), \\
&\big(x_4 - 1\big)\big(x_2x_1^2 - 2x_3x_1 - x_1^2 + x_4 - 3x_2 + 2\big),
\end{aligned}$$

and here is the deglex Gröbner basis of its radical $\sqrt{DI_4(A_6)}$,

$$x_2^2 - x_3x_1 - 2x_2 + 1,$$

$$
\begin{aligned}
&x_3x_2 - x_4x_1 - x_2x_1 - x_3 + 2x_1,\\
&x_3^2 - x_4x_2 - x_3x_1 + x_4 + x_2 - 1,\\
&x_1^3 - 2x_2x_1 + x_3 - 2x_1,\\
&x_2x_1^2 - 2x_3x_1 - x_1^2 + x_4 - 3x_2 + 2.
\end{aligned}
$$

Computing a Gröbner basis for the radical can be very time-consuming, but it can also make finding the zero set of the ideal much easier.

Exercise 8.8. Consider the sequence of symmetric matrices B_n defined by:

$$b_{ii} = 1 \;\; (1 \le i \le n), \quad b_{i,i+k} = b_{i+k,i} = x_k \;\; (1 \le i \le n-k, \; 1 \le k \le n-1).$$

For $n = 1, 2, 3, 4, \dots$ and continuing as far as you can, determine the inverse image for each possible rank of B_n.

Exercise 8.9. Consider the skew-symmetric matrices C_n defined by:

$$
\begin{aligned}
&c_{ii} = 0 \quad (1 \le i \le n), \qquad c_{i,i+1} = 1, \; c_{i+1,i} = -1 \quad (1 \le i \le n-1),\\
&c_{i,i+k} = x_{k-1}, \; c_{i+k,i} = -x_{k-1} \quad (1 \le i \le n-k, \; 2 \le k \le n-1).
\end{aligned}
$$

where $x_1, \dots, x_{n-2}$ are variables. Here are two examples:

$$
C_4 = \begin{bmatrix} 0 & 1 & x_1 & x_2 \\ 1 & 0 & 1 & x_1 \\ -x_1 & 1 & 0 & 1 \\ -x_2 & -x_1 & 1 & 0 \end{bmatrix}
\quad
C_5 = \begin{bmatrix} 0 & 1 & x_1 & x_2 & x_3 \\ 1 & 0 & 1 & x_1 & x_2 \\ -x_1 & 1 & 0 & 1 & x_1 \\ -x_2 & -x_1 & 1 & 0 & 1 \\ -x_3 & -x_2 & -x_1 & 1 & 0 \end{bmatrix}
$$

For $n = 1, 2, 3, 4, \dots$ and continuing as far as you can, determine the inverse image for each possible rank of C_n.

Exercise 8.10. Consider this sequence of skew-symmetric matrices D_n:

$$d_{ii} = 0 \, (1 \le i \le n), \; d_{i,i+k} = x_k, \; d_{i+k,i} = -x_k \, (1 \le i \le n-k, \; 1 \le k \le n-1).$$

For $n = 1, 2, 3, 4, \dots$ and continuing as far as you can, determine the inverse image for each possible rank of D_n.

Exercise 8.11. Explain how to interpret the polynomials in Figure 8.1 as equations in spherical trigonometry. (If necessary, refer to Todhunter's classic 1886 textbook available for free download at Project Gutenberg (`www.gutenberg.org/ebooks/19770`, and to Wolfram webpage `http://mathworld.wolfram.com/SphericalTrigonometry.html`.)

Exercise 8.12. Compute the 141-element deglex Gröbner basis for the ideal generated by the polynomials in 16 variables defining orthonormal bases of $\mathbb{R}^4$; see subsection 8.3.3 for details. (Also, not quite seriously: after you have computed the Gröbner basis, interpret the elements as equations in 4-dimensional spherical trigonometry.)

Exercise 8.13. Determine the zero sets of the determinantal ideals discussed in Remark 8.4.3.6.

Exercise 8.14. In each case, determine all values of the parameters a, b, c, d for which the 4×4 matrix has rank exactly 2:

$$\left[\begin{array}{cccc} 0 & 1 & 0 & a \\ 0 & 0 & 1 & b \\ 1 & 0 & 0 & 0 \\ 0 & -a & b & 1 \end{array} \right] \left[\begin{array}{cccc} 1 & a & b & 0 \\ 0 & 0 & 0 & 1 \\ a & 1 & 0 & 0 \\ -b & 0 & 1 & 0 \end{array} \right] \left[\begin{array}{cccc} 1 & a & 0 & b \\ 0 & 0 & 1 & c \\ a & 1 & 0 & 0 \\ b & 0 & c & 1 \end{array} \right] \left[\begin{array}{cccc} 1 & 0 & a & b \\ 0 & 1 & c & d \\ -a & c & 0 & 0 \\ b & -d & 0 & 0 \end{array} \right]$$

Exercise 8.15. Consider the set of all $n \times n$ matrices A whose entries belong to the set $\{0, 1, x, y\}$. Clearly this set contains a total of 4^{n^2} distinct matrices.

(a) For $n = 2$, determine by hand how many of these matrices satisfy condition RF: their rows generate a free submodule of $\mathbb{F}[x, y]^n$.

(b) For $n = 3$, use a computer algebra system to determine how many of these matrices satisfy condition RF.

Chapter 9

Case Study of Nonsymmetric Binary Cubic Operads

9.1 Introduction

In this chapter we choose one particular question as a model that demonstrates how methods of this book can be used for purposes of studying operads with the given number of generators and relations. Let us consider the generating operation alphabet $\mathcal{X}$ for which

$$\mathcal{X}(2) = \{f\}, \text{ and } \mathcal{X}(k) = \varnothing \text{ for } k \neq 2.$$

We will consider quotients of the free nonsymmetric operad $\mathcal{T}(\mathcal{X})$ by several relations of weight 3. Similarly to how operads with relations of weight 2 are conventionally referred to as quadratic, operads with relations of weight 3 are called cubic. In a more classical language of identities in nonassociative algebra, we focus on identities of arity 4 that involve one binary operation and are nonsymmetric, so that in nonassociative monomials of each identity all arguments appear in the same order (like in the associativity identity). Our methods in principle apply to any number of operations, of any arities, satisfying relations of any arities, either symmetric or nonsymmetric. However, as we shall see below, sizes of matrices involved in investigating these questions grow very fast, so computational feasibility may be an issue in practice.

To appreciate the power of our methods in full, we encourage the reader to examine the large paper [205] (over 200 pages) where similar goals were attempted without the advantage of computer algebra systems or the theory of algebraic operads. This is also an appropriate place to mention the so-called "Russian book" [260] which concentrates on alternative and Jordan algebras but has much useful information on general (nonassociative) algebras.

Throughout this chapter, we implicitly assume that the ground field is algebraically closed or at least contains roots of all equations we solve; we leave it to the reader to adapt the results appropriately for when it is not the case. Interestingly, results of this chapter provide in particular some examples of "notable" operads whose defining relations have irrational coefficients.

9.2 Toy model: the quadratic case

To motivate our problem we recall the analogue for quadratic operads: those for which every term of every relation involves two operations (the monomials have arity 3). Throughout this section, we shall often represent operations in the free operad generated by f by balanced bracketings, e.g., the operations

$$f \circ_1 f \text{ and } f \circ_2 f$$

that form a basis of $\mathcal{T}(\mathcal{X})(3)$ are represented by

$$((**)*) \text{ and } (*(**)),$$

respectively. Hence the most general quadratic element we may consider has the form

$$R = x_1((**)*) + x_2(*(**)). \tag{9.1}$$

In principle, we already discussed this relation in Example 3.6.1.2, but we shall now examine it in a different way, outlining the general methods that we are going to use later on.

The space of arity 4 consequences of Relation (9.1) is spanned by the cubic relations obtained by pre-composing and post-composing this relation with the generating operation f of the operad:

$$\left.\begin{aligned} R \circ_1 f &= x_1(((**)*)*) + x_2((**)(**)), \\ R \circ_2 f &= x_1((*(**))*) + x_2(*((**)*)), \\ R \circ_3 f &= x_1((**)(**)) + x_2(*(*(**))), \\ f \circ_1 R &= x_1(*((**)*)) + x_2(*(*(**))), \\ f \circ_2 R &= x_1(((**)*)*) + x_2((*(**))*). \end{aligned}\right\} \tag{9.2}$$

These relations include all 5 balanced bracketings in arity 4:

$$(((**)*)*), \qquad ((*(**))*), \qquad ((**)(**)), \qquad (*((**)*)), \qquad (*(*(**))).$$

We construct the 5×5 relation matrix R over the polynomial ring $\mathbb{F}[x_1, x_2]$ whose (i, j) entry is the coefficient of bracketing j in consequence i; the row space of R is the subspace of $\mathcal{T}_\mathcal{X}(4)$ consisting of the consequences (9.2) of the general quadratic relation (9.1):

$$R = \begin{bmatrix} x_1 & 0 & x_2 & 0 & 0 \\ 0 & x_1 & 0 & x_2 & 0 \\ 0 & 0 & x_1 & 0 & x_2 \\ 0 & 0 & 0 & x_1 & x_2 \\ x_1 & x_2 & 0 & 0 & 0 \end{bmatrix}$$

A straightforward calculation shows that the set of $r \times r$ minors, which generates the r-th determinantal ideal, is as follows:

$$r = 1,2,3,4\colon\ \{\, \pm x_1^{r-i} x_2^i \mid 0 \le i \le r \,\}, \qquad r = 5\colon\ \{\, x_2^2 x_1^2 (x_1 + x_2) \,\}.$$

For $r = 1,2,3,4$ the Gröbner basis is obtained by taking only the monomials with positive sign, and in these cases the determinantal ideals have the same radical (x_1, x_2). For $r = 5$ the ideal is principal and the generator $\det(R)$ is a Gröbner basis; the radical is also principal with the exponents “erased”:

$$\sqrt{DI_r(R)} = (x_1, x_2) \quad (r = 1,2,3,4), \qquad \sqrt{DI_5(R)} = (x_1 x_2 (x_1 + x_2)).$$

From this we read off the zero sets:

$$\begin{aligned} V(DI_r(R)) &= \{\, (0,0) \,\} \quad (r = 1,2,3,4), \\ V(\sqrt{DI_5(R)}) &= \{\, (0,x_2),\ (x_1,0),\ (x_1,-x_1) \mid x_1, x_2 \in \mathbb{F} \,\}. \end{aligned}$$

With this information we completely understand the rank of R:

$$\operatorname{rank}(R) = \begin{cases} 0 & \text{for } x_1 = x_2 = 0, \\ 4 & \text{for } x_1 = 0, x_2 \neq 0, \\ 4 & \text{for } x_1 \neq 0, x_2 = 0, \\ 4 & \text{for } x_2 = -x_1 \neq 0, \\ 5 & \text{for all other values of } x_1 \text{ and } x_2. \end{cases}$$

In particular, the rank is never 1, 2, or 3. In the case of rank 4, we make the following conclusion: The only interesting case is rank 4:

- if $[x_1 : x_2] = [0 : 1]$ then $R = (*(**))$,
- if $[x_1 : x_2] = [1 : 0]$ then $R = ((**)*)$,
- if $[x_1 : x_2] = [1 : -1]$ then $R = ((**)*) - (*(**))$, so we obtain the associativity identity.

In all other cases the operad is either free (rank 0, no relations) or nilpotent (rank 5, all products of arity 4 vanish). Notably, these computations have identified associativity, together with two trivial relations.

The calculations we have done are homogeneous: every nonzero coefficient in every relation is an indeterminate; there are no nonzero scalars. We can simplify these calculations by recalling that every nonzero scalar multiple of a relation expresses the same algebraic property, and splitting the problem into several different cases depending on whether the leading coefficient is 0 or 1. For example, the general quadratic relation $x_1((**)*) + x_2(*(**))$ can be represented by the 1×2 coefficient matrix $[x_1, x_2]$, and there are 3 possible canonical forms for this matrix: $[0,0]$ (rank 0); $[0,1]$, $[1,x]$ (rank 1). Substituting these values for x_1 and x_2 into the matrix R we obtain the zero matrix, a matrix of rank 4, and the following matrix over $\mathbb{F}[x]$; we present the last matrix together with its Hermite normal form (HNF):

$$\begin{bmatrix} 1 & 0 & x & 0 & 0 \\ 0 & 1 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & x \\ 0 & 0 & 0 & 1 & x \\ 1 & X & 0 & 0 & 0 \end{bmatrix} \xrightarrow{\text{HNF}} \begin{bmatrix} 1 & 0 & 0 & 0 & -x^2 \\ 0 & 1 & 0 & 0 & -x^2 \\ 0 & 0 & 1 & 0 & x \\ 0 & 0 & 0 & 1 & x \\ 0 & 0 & 0 & 0 & x^2(x+1) \end{bmatrix}$$

The Smith normal form is $\text{diag}[1,1,1,1,x^2(x+1)]$. From this we see immediately (without commutative algebra) that rank 4 occurs if and only if $[x_1 : x_2]$ is one of the pairs $[0 : 1]$, $[1 : 0]$, $[1 : -1]$. This approach allows us to reduce the number of indeterminates by 1, which can make the difference between a computation being possible or impossible. The purpose of the next section is to extend these calculations to cubic relations.

9.3 The cubic case

Considering now the cubic case, we recall that in arity 4, there are five bracketings for a binary operation, so the most general cubic relation depends on five scalars $x_1, \dots, x_5 \in \mathbb{F}$:

$$x_1(((**)*)*)+x_2((*(**))*)+x_3((**)(**))+x_4(*((**)*))+x_5(*(*(**))). \quad (9.3)$$

The vector space of all such relations has dimension 5, hence it is not sufficient to study one relation at a time: we must also study sets of 2, 3, or 4 linearly independent relations.

9.3.1 Preliminary analysis

Definition 9.3.1.1 (Relation rank)**.** By the *relation rank* we mean the dimension r of the space of cubic relations in a given cubic quotient of $\mathcal{T}(\mathcal{X})$.

For each rank r the coefficients of the relations form an $r \times 5$ matrix R, and we may assume that R is in row canonical form (RCF). For each rank r there are $\binom{5}{r}$ cases depending on the positions of the pivots; entries of the relation matrix which are not pivots, and are not above, below, or to the left of a pivot, are independent free parameters. Within each rank r the cases are sorted by the lexicographic order on the r-element subsets of $\{1, \dots, 5\}$. For example, here are the five relation matrices of rank 1,

$$\big[1\ x_1\ x_2\ x_3\ x_4\big], \big[0\ 1\ x_1\ x_2\ x_3\big], \big[0\ 0\ 1\ x_1\ x_2\big], \big[0\ 0\ 0\ 1\ x_1\big], \big[0\ 0\ 0\ 0\ 1\big]. \quad (9.4)$$

For ranks 2 and 3 there are ten cases each, which we leave to the reader

(Exercise 9.1); here is the first case for each rank, both have 6 parameters:

$$\begin{bmatrix} 1 & 0 & x_1 & x_2 & x_3 \\ 0 & 1 & x_4 & x_5 & x_6 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & x_1 & x_2 \\ 0 & 1 & 0 & x_3 & x_4 \\ 0 & 0 & 1 & x_5 & x_6 \end{bmatrix}. \tag{9.5}$$

Here are the five relation matrices of rank 4:

$$\begin{bmatrix} 1&0&0&0&x_1 \\ 0&1&0&0&x_2 \\ 0&0&1&0&x_3 \\ 0&0&0&1&x_4 \end{bmatrix}, \begin{bmatrix} 1&0&0&x_1&0 \\ 0&1&0&x_2&0 \\ 0&0&1&x_3&0 \\ 0&0&0&0&1 \end{bmatrix}, \begin{bmatrix} 1&0&x_1&0&0 \\ 0&1&x_2&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{bmatrix}, \begin{bmatrix} 1&x_1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{bmatrix}, \begin{bmatrix} 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{bmatrix} \tag{9.6}$$

We ignore the trivial cases: rank 0 (zero relation matrix, free operad), rank 5 (identity relation matrix, nilpotent operad).

Every cubic relation R in arity 4 produces six arity 5 consequences by pre-composing and post-composing that relation with the generator:

$$\left.\begin{array}{lll} R \circ_1 f, & R \circ_2 f, & R \circ_3 f, \\ R \circ_4 f, & f \circ_1 R, & f \circ_2 R. \end{array}\right\} \tag{9.7}$$

The consequences of every cubic relation are linear combinations of the following ordered set of 14 bracketings in arity 5:

$$\left.\begin{array}{llll} ((((**)*)*)*), & (((*(**))*)*), & (((**)(**))*), & ((*((**)*))*), \\ ((*(*(**)))*), & (((**)*)(**)), & ((*(**))(**)), & ((**)((**)*)), \\ ((**)(*(**))), & (*(((**)*)*)), & (*((*(**))*)), & (*((**)(**))), \\ (*(*((**)*))), & (*(*(*(**)))). & & \end{array}\right\} \tag{9.8}$$

With respect to this basis of $\mathcal{T}(\mathcal{X})(5)$, the coefficient vectors of the consequences of the generic relation (9.3) are the rows of the following 6×14 matrix, whose row space consists of all consequences of (9.3) in arity 5:

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & x_5 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & 0 & x_4 & 0 & x_5 & 0 & 0 \\ 0 & 0 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & 0 & x_4 & 0 & x_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & x_1 & x_2 & 0 & x_3 & 0 & 0 & x_4 & 0 & x_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_1 & x_2 & x_3 & x_4 & x_5 \end{bmatrix} \tag{9.9}$$

Thus each cubic relation matrix of rank r in arity 4 produces a $6r \times 14$ *quartic relation matrix* in arity 5, whose row space consists of all consequences in arity 5 of the original relations in arity 4.

Our main goal in the rest of this chapter is to understand how the rank of the $6r \times 14$ quartic relation matrix in arity 5 matrix depends on the parameters in the original cubic relations in arity 4. In particular, for each cubic relation rank we wish to determine the minimal rank of the corresponding quartic relation matrix, and the values of the parameters which produce that minimal rank. This will provide a generalization of the (much simpler) results obtained in Section 9.2 for quadratic relations.

9.3.2 Relation rank 1

The relation matrices for the five cases corresponding to relation rank 1 have been displayed in (9.4). For case 1, we substitute $1, x_1, x_2, x_3, x_4$ for x_1, x_2, x_3, x_4, x_5 into (9.9) to obtain the matrix C of consequences in arity 5:

$$C = \left[\begin{array}{cccccccccccccc} 1 & x_1 & x_2 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 & 0 \\ 0 & 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{array} \right] \tag{9.10}$$

Computing the partial Smith form using Algorithm 8.4.2.3, we obtain

$$C \longrightarrow \left[\begin{array}{cc} I_5 & O_{5,9} \\ O_{1,5} & B_{1,9} \end{array} \right]$$

where the row vector $B = B_{1,9}$ contains the following nonzero entries, which have been made monic and sorted by `glex` order with $x_1 \prec \cdots \prec x_5$:

$$\left. \begin{array}{l} x_1^2 - x_3, \quad x_2x_1 - x_1^2 - x_4, \quad x_2^2 - x_4, \quad x_2^2 - x_2x_1 + x_3, \\ x_3(x_1^2 - x_2 + x_1), \quad x_3x_2x_1 + x_3x_2 - x_4x_1, \\ x_3^2x_1 - x_4x_2 + x_4x_1, \quad x_4(x_3x_1 + x_2). \end{array} \right\} \tag{9.11}$$

It follows that the rank of C is either 5 or 6, and $\text{rank}(C) = 5$ if and only if the ideal I generated by the polynomials (9.11) vanishes. From (9.11) we obtain the `glex` Gröbner basis for I:

$$\begin{array}{l} x_1^2 - x_3, \quad x_2x_1 - x_4 - x_3, \quad x_2^2 - x_4, \quad x_3x_2 - x_4x_1 - x_3x_1, \\ x_4x_2 + x_3x_1, \quad x_3^2 - x_4x_1, \quad x_4x_3 + x_4x_1 + x_3x_1, \quad x_4^2 - x_3x_1. \end{array}$$

From this we obtain the `glex` basis[1] for $\sqrt{I}$:

$$x_3 - x_2 + x_1, \quad x_4 + x_2, \quad x_1^2 + x_1 - x_2, \quad x_1(x_2 + 1), \quad x_2(x_2 + 1).$$

The zero set of the radical (and the original ideal) contains three points, where ω is a primitive cube root of unity:

$$V(\sqrt{I}) = \{\ (x_1, \dots, x_4) \ = \ (0,0,0,0),\ (\omega, -1, \omega^2, 1)\ \}.$$

For cases 2, 3, 4 of relation rank 1, the same steps produce the matrix $[\, I_6 \mid O_{6,8} \,]$ which has rank 6 independently of the values of the parameters. For case 5, there are no parameters and the same steps produce the matrix of rank 5 which has I_5 in the upper left corner and zeros elsewhere. To summarize, we have proved the following result.

[1] Computer algebra systems are not infallible. The first time we did this computation, the output was $\{x_1, x_3, x_4, x_2^2\}$. This set is indeed a Gröbner basis for the ideal it generates, but that ideal is certainly not a radical ideal, neither does it have the same zero set! The CAS in question will remain anonymous, and those responsible have been informed.

Theorem 9.3.2.1. *For a cubic relation matrix of rank* 1*, the dimension of the space of quartic consequences in arity* 5 *is either* 5 *or* 6*. The minimal dimension* 5 *is achieved if and only if the relation matrix represents one of the following four elements:*

$$R = (((**)*)*),$$
$$R = (((**)*)*) + \omega((*(**))*) - ((**)(**)) + \omega^2(*((**)*)) + (*(*(**))),$$
$$R = (*(*(**))).$$

Here ω is one of the two roots of the polynomial t^2+t+1, that is a primitive cube root of unity.

Theorem 9.3.2.2. *Let $\mathcal{P}$ be any of the four operads of Theorem 9.3.2.1. Then the generating function $f_{\mathcal{P}}(t) := \sum_{n\geq 1} \dim \mathcal{P}(n)t^n$ satisfies the algebraic equation*

$$f_{\mathcal{P}}(t) = t(1 + f_{\mathcal{P}}(t) + f_{\mathcal{P}}(t)^2).$$

In particular, the numbers a_n, dimensions of $\mathcal{P}(n)$, are Motzkin numbers [236, Seq. A001006]:

$$a_1 = 1, \quad a_{n+1} = a_n + \sum_{p+q=n} a_p a_q.$$

Proof. Let us establish this equation for the first of those operads. Denote by a_n the dimension of the arity n component of that operad $\mathcal{P}$. Since we are dealing with the operad whose defining relation is $(((**)*)*) = 0$ each basis element T of arity $n+1 \geq 2$ that is not divisible by $(((**)*)*)$ is either of the form $(*T')$, where T' is a basis element of arity n, or of the form $((*T')T'')$, where T' and T'' are basis elements of some arities p and q with $p+q=n$. We immediately conclude that $a_{n+1} = a_n + \sum_{p+q=n} a_p a_q$. Multiplying this equation by t^{n+1} and taking the sum for all $n \geq 1$, we obtain

$$f_{\mathcal{P}}(t) - t = t f_{\mathcal{P}}(t) + t f_{\mathcal{P}}(t)^2,$$

which is the equation for the generating function of Motzkin numbers. The proof for the last operad is similar, one merely has to consider the "mirror reflections" of all bracketings we just discussed. The case of the second and the third operad is more complicated, and involves operadic Gröbner bases. In fact, it turns out that the reduced Gröbner basis of the corresponding operads for the `gpathlex` order consists of the original relation only (Exercise 9.3). This of course implies that the normal forms for the second and the third operad are exactly the same as for the first operad, and therefore they have the same dimensions of components. □

9.3.3 Relation rank 2

The cubic relation matrix for rank 2, case 1 is displayed in (9.5). In matrix (9.9), we independently replace $x_1, \ldots, x_5$ by the two rows of the cubic relation matrix, namely $1, 0, x_1, x_2, x_3$ and $0, 1, x_4, x_5, x_6$ and then stack the two resulting 6×14 matrices, obtaining the following matrix whose row space contains all consequences in arity 5 of the original cubic relations:

$$C = \left[\begin{array}{cccccccccccccc}
1 & . & x_1 & x_2 & x_3 & . & . & . & . & . & . & . & . & . \\
1 & . & . & . & . & x_1 & . & x_2 & x_3 & . & . & . & . & . \\
. & 1 & . & . & . & . & x_1 & . & . & x_2 & . & x_3 & . & . \\
. & . & 1 & . & . & . & . & x_1 & . & . & x_2 & . & x_3 & . \\
. & . & . & . & . & 1 & . & . & x_1 & . & . & x_2 & . & x_3 \\
. & . & . & . & . & . & . & . & . & 1 & . & x_1 & x_2 & x_3 \\
\hline
. & 1 & x_4 & x_5 & x_6 & . & . & . & . & . & . & . & . & . \\
. & . & 1 & . & . & x_4 & . & x_5 & x_6 & . & . & . & . & . \\
. & . & . & 1 & . & . & x_4 & . & . & x_5 & . & x_6 & . & . \\
. & . & . & . & 1 & . & . & x_4 & . & . & x_5 & . & x_6 & . \\
. & . & . & . & . & . & 1 & . & x_4 & . & . & x_5 & . & x_6 \\
. & . & . & . & . & . & . & . & . & . & 1 & x_4 & x_5 & x_6
\end{array} \right] \tag{9.12}$$

The partial Smith form is a block matrix:

$$C \longrightarrow \left[\begin{array}{cc} I_9 & O_{9,5} \\ O_{3,9} & B_{3,5} \end{array} \right].$$

Hence the minimal rank of C is 9, and the maximal rank is at most 12. In fact, another calculation shows that the lower right block $B = B_{3,5}$ has full rank over the field of rational functions $\mathbb{F}(x_1, \dots, x_6)$, and so the maximal rank of C is 12.

Let us focus on a particular classification question: describe all parameters for which the matrix of consequences has the smallest possible rank. The entries of the block $B = (b_{ij})$ are as follows:

$$\begin{gathered}
b_{1,1} = x_5 - x_1, \quad b_{1,2} = -x_4 x_1 + x_6, \quad b_{1,3} = 0, \\
b_{1,4} = x_5 x_2 - x_3, \quad b_{1,5} = -x_4 x_3 + x_6 x_2, \\
b_{2,1} = -x_4(x_1 + x_6), \quad b_{2,2} = x_4(x_4 x_5 + x_1), \\
b_{2,3} = x_6 x_5 x_4 + x_5^2 x_4 + x_4^2 x_2 + x_5^2 x_1 - x_6 x_5 + x_5 x_1 + x_2 x_1 - x_3, \\
b_{2,4} = x_6 x_5^2 + x_5^2 x_2 + x_5 x_4 x_2 - x_6^2 - x_4 x_3 + x_2^2, \\
b_{2,5} = x_6^2 x_5 + x_6 x_5 x_4 + x_5^2 x_3 + x_6 x_4 x_2 + x_3 x_2 + x_6 x_1, \\
b_{3,1} = x_4 x_3 + x_1^2 + x_2, \quad b_{3,2} = -x_4^2 x_2 - x_1^2 + x_3, \\
b_{3,3} = -x_5 x_4 x_3 - x_5 x_4 x_2 - x_5 x_2 x_1 - x_4 x_2 x_1 + x_6 x_2 - x_2 x_1, \\
b_{3,4} = -x_5^2 x_3 - x_5 x_2^2 - x_5 x_2 x_1 + x_6 x_3 + x_3 x_1, \\
b_{3,5} = -x_6 x_5 x_3 - x_6 x_4 x_2 - x_5 x_3 x_2 - x_6 x_2 x_1 - x_3 x_1.
\end{gathered}$$

The `glex` Gröbner basis of the ideal I generated by these entries is as follows:

$$
\begin{array}{l}
x_5 - x_1, \quad x_2x_1 - x_3, \quad x_1(x_3 + x_1), \\
x_4x_1 - x_6, \quad x_6x_1 + 2x_1^2 - x_3 + x_2, \quad x_2(x_2 + 1), \\
x_3(x_2 + 1), \quad x_4x_2 - x_1^2 + x_3, \quad x_6x_2 + x_1^2 + x_2, \\
(x_3 - x_1)(x_3 + x_1), \quad x_4x_3 + x_1^2 + x_2, \quad x_6x_3 - 2x_1^2 + x_3 - x_2, \\
x_6(x_4 + 1), \quad x_6^2 - 2x_1^2 + x_3 - x_2, \quad x_1^3 + 2x_1^2 + x_2.
\end{array}
$$

From this we obtain the `glex` Gröbner basis of the radical $\sqrt{I}$:

$$
\begin{array}{l}
x_3 + x_1, \quad x_5 - x_1, \quad x_1^2 - x_6 + x_2, \quad x_1(x_2 + 1), \quad x_4x_1 - x_6, \\
x_6x_1 + 2x_6 - x_2 + x_1, \quad x_2(x_2 + 1), \quad x_4x_2 - x_6 + x_2 - x_1, \\
x_6(x_2 + 1), \quad x_6(x_4 + 1), \quad x_6^2 - 2x_6 + x_2 - x_1.
\end{array}
$$

From this we find that the zero set $V(\sqrt{I})$ consists of two points and a line:

x_1	x_2	x_3	x_4	x_5	x_6
-1	-1	1	0	-1	0
$-\phi$	-1	ϕ	-1	$-\phi$	ϕ
0	0	0	X	0	0

$\phi^2 - \phi - 1 = 0$

X free

The corresponding cubic relation matrices are

$$
\begin{bmatrix} 1 & 0 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 & 0 \end{bmatrix}
\quad
\begin{bmatrix} 1 & 0 & -\phi & -1 & \phi \\ 0 & 1 & -1 & -\phi & \phi \end{bmatrix}
\quad
\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & X & 0 & 0 \end{bmatrix}
$$

These correspond to the cubic binary nonsymmetric operads defined by the following three pairs of relations:

$$
\left.
\begin{array}{l}
(((\ast\ast)\ast)\ast) - ((\ast\ast)(\ast\ast)) - (\ast((\ast\ast)\ast)) + (\ast(\ast(\ast\ast))) = 0 \\
((\ast(\ast\ast))\ast) - (\ast((\ast\ast)\ast)) = 0 \\
\hline
(((\ast\ast)\ast)\ast) - \phi((\ast\ast)(\ast\ast)) - (\ast((\ast\ast)\ast)) + \phi(\ast(\ast(\ast\ast))) = 0 \\
((\ast(\ast\ast))\ast) - ((\ast\ast)(\ast\ast)) - \phi(\ast((\ast\ast)\ast)) + \phi(\ast(\ast(\ast\ast))) = 0 \\
\hline
(((\ast\ast)\ast)\ast) = 0 \\
((\ast(\ast\ast))\ast) + X((\ast\ast)(\ast\ast)) = 0 \quad (X \in \mathbb{F})
\end{array}
\right\}
\tag{9.13}
$$

Up to this point, we have been studying only the first determinantal ideal of the 3×5 block B, since this is what we need to determine the minimal rank of C and the corresponding cubic relations. But in order to understand completely the possible ranks of C, we need to investigate the second and third determinantal ideals of B. This is significantly harder, since the degrees of the generators increase, and hence computing Gröbner bases for the ideals and their radicals takes much more time and memory. In particular:

- There are $\binom{3}{2}\binom{5}{2} = 30$ minors of size 2, all of which are nonzero; they have degrees between 4 and 6, numbers of terms between 8 and 50, and coefficients at most 2 in absolute value.

- There are $\binom{3}{3}\binom{5}{3} = 10$ minors of size 3, all of which are nonzero; they have degrees 7 and 8, numbers of terms between 87 and 136, and coefficients at most 3 in absolute value.

Further discussion of these ideals is left to Exercises 9.4 and 9.5.

So far we have only considered case 1, and there are altogether 10 cases for rank 2. Further calculations verify that 9 is the minimal dimension of the space of consequences in arity 5 over all 10 cases. (Recall that the matrix C representing these consequences depends on the case.) The remaining cases have fewer parameters than case 1, and so the computations are simpler. Complete verification of the following result is left to the reader.

Theorem 9.3.3.1. *For all ten cases of cubic relation matrices of rank* 2*, the matrix* C *representing the consequences in arity* 5 *satisfies* $\mathrm{rank}(C) \geq 9$*. The following is a complete list over all ten cases of the sets of two relations which produce the minimal rank* 9 *for* C*:*

- *the relations*

$$
\begin{gathered}
(((**)*)*) - ((**)(**)) - (*((**)*)) + (*(*(**))) = 0, \\
((*(**))*) - (*((**)*)) = 0,
\end{gathered}
$$

- *the relations*

$$
\begin{gathered}
(((**)*)*) = 0, \\
((*(**))*) + X((**)(**)) = 0
\end{gathered}
$$

  for any $X \in \mathbb{F}$*,*

- *the monomial relations*

$$
(((**)*)*) = 0, \qquad ((**)(**)) = 0
$$

  (the "$X = \infty$ *version" of the previous case),*

- *the relations*

$$
\begin{gathered}
((**)(**)) + X(*((**)*)) = 0, \\
(*(*(**))) = 0
\end{gathered}
$$

  for any $X \in \mathbb{F}$*,*

- *the monomial relations*

$$
(*((**)*)) = 0, \qquad (*(*(**))) = 0
$$

  (the "$X = \infty$ *version" of the previous case),*

- *the relations*

$$(((**)*)*) - \phi((**)(**)) - (*((**)*)) + \phi(*(*(**))) = 0,$$
$$((*(**))*) - ((**)(**)) - \phi(*((**)*)) + \phi(*(*(**))) = 0$$

where ϕ is a root of the polynomial $t^2 - t - 1$.

Proof. Exercise 9.7. □

Using operadic Gröbner bases, one can prove the following result on dimensions of components of the operads from the previous theorem.

Theorem 9.3.3.2. *For the relations*

$$(((**)*)*) = 0,$$
$$((*(**))*) + X((**)(**)) = 0$$

and

$$((**)(**)) + X(*((**)*)) = 0,$$
$$(*(*(**))) = 0$$

with $X \in \mathbb{F}^{\times}$, the dimension of the n-th component of the corresponding operad is equal to

$$\begin{cases} 1, n = 2, \\ 2, n = 3, \\ 3, n = 4, \\ 5, n = 5, \\ 6, n \geq 6, \end{cases}$$

and for all other operads listed in Theorem 9.3.3.1, the dimension of its n-th component is equal to the n-th Fibonacci number.

Proof. Exercise 9.8. □

Remark 9.3.3.3. It is the most amusing coincidence that Fibonacci numbers arise as dimensions of components for the operad with relations

$$(((**)*)*) - \phi((**)(**)) - (*((**)*)) + \phi(*(*(**))) = 0,$$
$$((*(**))*) - ((**)(**)) - \phi(*((**)*)) + \phi(*(*(**))) = 0$$

involving the golden ratio.

9.3.4 Relation rank 3

The situation for rank 3 is very similar to that for rank 2, although for rank 3 we begin to obtain values of the parameters for which the matrix of consequences in arity 5 has full rank 14, and hence the corresponding operad is nilpotent of index 4: the space of relations has full rank for all arities $n \geq 5$.

For case 1, the matrix of consequences in arity 5 has size 18 × 14; we have sorted the rows to make the matrix as close to upper-triangular as possible, so the blocks representing the three individual relations are no longer visible:

$$C = \begin{bmatrix}
1 & . & . & x_1 & x_2 & . & . & . & . & . & . & . & . & . \\
1 & . & . & . & . & . & . & x_1 & x_2 & . & . & . & . & . \\
. & 1 & . & x_3 & x_4 & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & x_1 & . & x_2 & . & . \\
. & . & 1 & x_5 & x_6 & . & . & . & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & x_3 & x_4 & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . & . & . & x_1 & . & x_2 & . \\
. & . & . & 1 & . & . & . & . & . & x_3 & . & x_4 & . & . \\
. & . & . & . & 1 & . & . & . & . & . & x_3 & . & x_4 & . \\
. & . & . & . & . & 1 & . & x_5 & x_6 & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . & x_1 & . & x_2 \\
. & . & . & . & . & . & 1 & . & . & x_5 & . & x_6 & . & . \\
. & . & . & . & . & . & 1 & . & . & . & . & x_3 & . & x_4 \\
. & . & . & . & . & . & . & 1 & . & . & x_5 & . & x_6 & . \\
. & . & . & . & . & . & . & . & 1 & . & . & x_5 & . & x_6 \\
. & . & . & . & . & . & . & . & . & 1 & . & . & x_1 & x_2 \\
. & . & . & . & . & . & . & . & . & . & 1 & . & x_3 & x_4 \\
. & . & . & . & . & . & . & . & . & . & . & 1 & x_5 & x_6
\end{bmatrix} \qquad (9.14)$$

Computation of the partial Smith form gives the following result:

$$C \longrightarrow \begin{bmatrix} I_{12} & O_{12,2} \\ O_{6,12} & B_{6,2} \end{bmatrix} \qquad (9.15)$$

To display the relatively complex entries of the 6×2 lower right block $B = B_{6,2}$ we write the two column vectors separately, 5 above 6, in Figure 9.1.

As above, let us focus on determining parameters for which the matrix of consequences has the smallest possible rank.

Let I denote the ideal generated by the entries of B: so I is the first determinantal ideal of B. The `glex` Gröbner basis for I is not displayed: it consists of 30 polynomials with degrees 2 and 3, terms from 3 to 12, and coefficients at most 21 in absolute value. Its first and last elements are:

$$\begin{aligned}
f_1 &= x_5x_2 - x_3x_1 + x_1^2 + x_4, \\
f_{30} &= 4x_4^3 + 4x_1^3 - 3x_4^2 + 10x_4x_3 - 18x_4x_2 - 20x_3x_2 \\
&\qquad + 21x_2^2 - 9x_4x_1 + 4x_3x_1 + 11x_2x_1 + 6x_4 - 10x_2.
\end{aligned}$$

$$
\begin{bmatrix}
x_5(x_6 - x_3 + x_1) \\
-x_5x_4x_3 - x_4x_3^2 - x_3^2x_1 + x_4^2 - x_5x_2 - x_1^2 \\
x_5^2x_2 - x_3^2x_2 - x_5x_4x_1 + x_5x_3x_1 - x_3x_1^2 + x_4x_2 - x_6x_1 \\
-x_6x_3^2 + x_5x_3^2 - x_5x_3x_1 + x_6x_4 - x_6x_3 \\
-x_6x_5^2 - x_5^2x_3 + x_6x_5 - x_5x_1 \\
-x_5^2x_4 - x_6x_3^2 - x_5x_3x_1 + x_6x_4 - x_3x_1 + x_2
\end{bmatrix}
$$

$$
\begin{bmatrix}
x_6^2 - x_6x_3 + x_5x_2 + x_4 \\
-x_6x_4x_3 - x_4^2x_3 - x_3^2x_2 - x_6x_2 - x_2x_1 \\
x_6x_5x_2 - x_4x_3x_2 - x_6x_4x_1 + x_5x_4x_1 - x_3x_2x_1 - x_6x_2 \\
-x_6x_4x_3 + x_5x_4x_3 - x_5x_3x_2 - x_6x_4 \\
-x_6^2x_5 - x_5^2x_4 + x_6^2 - x_6x_1 + x_2 \\
-x_6x_5x_4 - x_6x_4x_3 - x_5x_3x_2 - x_4x_1
\end{bmatrix}
$$

FIGURE 9.1: Rank 3, case 1: the lower right block $B = B_{6,2}$.

The `glex` Gröbner basis for the radical $\sqrt{I}$ consists of 19 polynomials with degrees 2 and 3, terms from 3 to 9, and coefficients at most 5 in absolute value. These polynomials are

$$
\begin{gathered}
x_5x_1 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_6 - x_4 + x_2 + x_1, \\
2x_6x_1 + x_4x_1 - 2x_3x_1 - x_2x_1 + 2x_1^2 + 2x_6 + x_4 - x_2, \\
x_2^2 + x_4x_1 + x_2x_1 + x_1^2 + x_2 + x_1, \\
2x_3x_2 + x_4x_1 + 2x_3x_1 - x_2x_1 - x_4 + x_2 + 2x_1, \\
x_4x_2 + x_4x_1 + x_2, \\
x_5x_2 - x_3x_1 + x_1^2 + x_4, \\
2x_6x_2 + x_4x_1 + 2x_3x_1 + x_2x_1 - x_4 + x_2 + 2x_1, \\
2x_4x_3 - x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2, \\
2x_5x_3 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - 2x_6 - x_4 + x_2 + 2x_1, \\
x_6x_3 + x_4x_1 + x_1^2 + x_6 + x_1, \\
x_4^2 - x_4x_1 - 2x_3x_1 + x_2x_1 + x_1^2 + x_4 - x_1, \\
x_5x_4 + 2x_4x_1 + x_3x_1 - x_2x_1 + x_2 + x_1, \\
2x_6x_4 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2, \\
2x_6x_5 - x_4x_1 - 2x_3x_1 + x_2x_1 + 2x_1^2 + x_4 - x_2, \\
x_6^2 + x_4x_1 + x_3x_1 + x_6 + x_1, \\
x_2x_1^2 + x_1^3 - x_4x_1 - 2x_3x_1 + 2x_1^2 + x_4 - x_2 - x_1, \\
2x_3x_1^2 - 2x_1^3 - x_4x_1 - 2x_3x_1 + 3x_2x_1 + 4x_1^2 - x_4 + x_2 + 2x_1,
\end{gathered}
$$

$$x_4x_1^2 + x_1^3 - x_2x_1 + x_4 - x_2 - x_1,$$
$$2x_3^2x_1 - 2x_1^3 - x_4x_1 + 5x_2x_1 + 4x_1^2 - 3x_4 + 3x_2 + 4x_1.$$

This seems like a good opportunity to demonstrate explicitly some methods for solving systems of polynomial equations. We will determine the set of common zeros of the Gröbner basis for the radical that we found (and hence the zero set of the original ideal), relying on a computer algebra system only for computations of intermediate Gröbner bases.

Lemma 9.3.4.1. *The zero set of the ideal I consists of the union of three lines and five points in $\mathbb{F}^6$:*

$$\begin{aligned}[\,x_1,\dots,x_6\,] \in \big\{\,[\,X,-X-1,X,-X-1,-1,0\,] \mid X\in\mathbb{F}\,\big\} &\cup \\ \big\{\,[\,0,0,X,0,0,0\,] \mid X\in\mathbb{F}\,\big\} &\cup \\ \big\{\,[\,0,0,0,0,X,0\,] \mid X\in\mathbb{F}\,\big\} &\cup \\ \big\{\,[\,-1,0,-1,0,0,-1\,]\,\big\} \;\cup\; S&.\end{aligned}$$

Here the set S contains all points of the form

$$[\omega^2\phi, -\phi, \omega\phi, \omega^2, -\omega^2, -\phi],$$

where ω is a root of the polynomial t^2+t+1 and ϕ is a root of the polynomial t^2-t-1.

Proof of Lemma 9.3.4.1. Note that the sum of the elements

$$2x_6x_4 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2,$$
$$2x_6x_5 - x_4x_1 - 2x_3x_1 + x_2x_1 + 2x_1^2 + x_4 - x_2$$

(elements 13 and 14 of the Gröbner basis above) is $2x_6(x_5+x_4)$, and so we can split the proof into two parts: first, set $x_6=0$; second, set $x_5=-x_4$. In both cases we reduce the number of variables by one.

Case 1: We set $x_6=0$ in the 19 polynomials, and compute the `glex` Gröbner basis of the ideal generated by the resulting polynomials in $x_1,\dots,x_5$. This basis has only 8 elements:

$$\left.\begin{array}{lll} x_4 - x_2, & x_1(x_1+x_2+1), & x_1(x_3-x_1), \\ x_1(x_5+1), & (x_2+x_1+1)(x_2-x_1), & \\ x_1^2 + x_2x_3 + x_1, & x_2(x_5+1), & x_3x_5 + x_1. \end{array}\right\} \tag{9.16}$$

The second, third, and fourth elements have x_1 as a factor, and so we can split again into two cases: either $x_1=0$, or $x_2=-x_1-1$ and $x_3=x_1$ and $x_5=-1$.

Case 1.1: We set $x_1=0$ in the polynomials (9.16) and recompute the Gröbner basis in $x_2,\dots,x_5$ which consists of these five polynomials:

$$x_4 - x_2, \qquad x_2(1+x_2), \qquad x_3x_2, \qquad x_2(x_5+1), \qquad x_5x_3.$$

From this we see that either $x_2 = 0$ or $x_2 = -1$; in the former case, $x_4 = 0$ and either x_3 is free or x_5 is free but not both and the other is zero; in the latter case, $x_3 = 0$, $x_4 = -1$, $x_5 = -1$. This produces three solutions:

$$[x_1, \dots, x_6] = \begin{cases} [0, 0, X, 0, 0, 0] \quad (X \in \mathbb{F}) \\ [0, 0, 0, 0, X, 0] \quad (X \in \mathbb{F}) \\ [0, -1, 0, -1, -1, 0] \end{cases} \tag{9.17}$$

Case 1.2: We set $x_2 = -x_1 - 1$, $x_3 = x_1$, $x_5 = -1$ in (9.16) and recompute the Gröbner basis in x_1, x_4; the ideal is principal with generator $x_4 + x_1 + 1$. We obtain this solution

$$[x_1, \dots, x_6] = [X, -X-1, X, -X-1, -1, 0] \; (X \in \mathbb{F}). \tag{9.18}$$

Note that for $X = 0$ we obtain the previous solution $[0, -1, 0, -1, -1, 0]$.

Case 2: We set $x_5 = -x_4$ in the 19 polynomials, and compute the `glex` Gröbner basis of the ideal generated by the resulting polynomials in $x_1, \dots, x_4, x_6$. This Gröbner basis consists of the following 14 elements:

$$\begin{gathered}
2x_3x_1 - x_2x_1 - 2x_1^2 - x_6 - x_4 + x_2 + x_1, \\
2x_4x_1 - x_2x_1 - x_6 + x_4 + 3x_2 + x_1, \\
4x_6x_1 - 3x_2x_1 + 3x_6 - x_4 - 3x_2 + x_1, \\
2x_2^2 + 3x_2x_1 + 2x_1^2 + x_6 - x_4 - x_2 + x_1, \\
4x_3x_2 + x_2x_1 + 4x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\
2x_4x_2 + x_2x_1 + x_6 - x_4 - x_2 - x_1, \\
4x_6x_2 + 5x_2x_1 + 4x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\
4x_4x_3 - x_2x_1 + x_6 + x_4 + 3x_2 - x_1, \\
2x_6x_3 + x_2x_1 + 2x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\
2x_4^2 - x_2x_1 - 2x_1^2 - 3x_6 + x_4 + 5x_2 + x_1, \\
4x_6x_4 + x_2x_1 + 3x_6 - x_4 - 3x_2 - 3x_1, \\
x_6^2 + x_2x_1 + x_1^2 + 2x_6 - 2x_2, \\
4x_1^3 - 13x_2x_1 - 4x_1^2 + x_6 + 9x_4 - 5x_2 - 9x_1, \\
4x_2x_1^2 + 7x_2x_1 + 4x_1^2 - 7x_6 - 7x_4 + 11x_2 + 11x_1.
\end{gathered}$$

Analyzing this Gröbner basis we see that there are equations where the variables x_4 and x_6 appear among linear terms with some scalar coefficients, and do not appear in other terms. This suggests that we should eliminate these variables from our equations, so that only variables x_1, x_2, and x_3 remain. This can be done as follows: consider the monomial order which assigns the weight 1 to the variables x_1, x_2, and x_3, and the weight 10 to the variables x_4 and x_6. The reduced Gröbner basis for this order consists of the nine polynomials

$$x_6 - x_1x_3 + x_2^2 + 2x_1x_2 + 2x_1^2 - x_2,$$

$$
\begin{gathered}
x_4 - x_2^2 - x_3x_1 - x_2x_1 - x_1, \\
(2x_2 + x_1)(x_3 - x_2 - x_1), \\
2x_1^3 + 4x_2^2 + 5x_3x_1 - 3x_2x_1 - 3x_1^2 - 2x_2, \\
2x_2x_1^2 - 7x_3x_1 + 7x_2x_1 + 9x_1^2 + 2x_2 + 2x_1, \\
x_3x_1^2 + 2x_2^2 + x_3x_1 + x_1^2 + x_1, \\
2x_2^2x_1 - 2x_2^2 + 5x_3x_1 - 5x_2x_1 - 7x_1^2 - 2x_1, \\
x_3^2x_1 + x_2^2 + x_3x_1 + x_1^2 + x_2 + x_1, \\
2x_2^3 + 2x_2^2 - x_3x_1 + x_2x_1 + x_1^2 - 2x_2.
\end{gathered}
$$

Examining the polynomial $(2x_2 + x_1)(x_3 - x_2 - x_1)$, we see that either $x_1 = -2x_2$ or $x_1 = x_3 - x_2$, so we again split into two cases.

Case 2.1: We substitute $x_1 = -2x_2$ in the last six polynomials of the set above and compute the reduced Gröbner basis for the `glex` order, obtaining $\{\, x_2(x_2 - 1),\, x_2(x_3 + 2) \,\}$, for which the zero set is

$$[x_2, x_3] \in \{\, [0, X] \mid X \in \mathbb{F} \,\} \cup \{\, [1, -2] \,\}.$$

Solving backwards for the values of the other variables, we obtain

$$[x_1, \dots, x_6] = [0, 0, X, 0, 0, 0],\ [-2, 1, -2, 1, -1, 0].$$

The first has already appeared in (9.17), and the second is the special case $X = -2$ of (9.18), so there are no new solutions.

Case 2.2: We substitute $x_1 = x_3 - x_2$ in the last six polynomials of the set above and compute the reduced Gröbner basis for the `glex` order, obtaining these four polynomials:

$$
\begin{gathered}
x_2(x_2^2 + x_2 - 1), \\
x_3x_2^2 - x_3^2 + 2x_3x_2 - x_2^2 - x_3, \\
x_3^2x_2 - x_3^2 + 2x_3x_2 - 2x_2^2 - x_3 + x_2, \\
x_3^3 + x_3^2 - x_3x_2 + x_2.
\end{gathered}
$$

The first of these implies that either $x_2 = 0$ or $x_2^2 + x_2 - 1 = 0$.

Case 2.2.1: If $x_2 = 0$, we find that the resulting polynomials generate the principal ideal of multiples of $x_3(x_3 + 1)$. Working backward from $x_3 = 0$ we obtain only the solution $[0, 0, 0, 0, 0, 0]$. Working backward from $x_3 = -1$ we obtain a new solution:

$$[x_1, \dots, x_6] = [-1, 0, -1, 0, 0, -1]. \tag{9.19}$$

Case 2.2.2: If $x_2^2 + x_2 - 1 = 0$, we see that $x_2 = -\phi$, where $\phi = \frac{-1 \pm \sqrt{5}}{2}$ is a root of the polynomial $t^2 - t - 1$. Substituting this value of x_2 in elements above, we obtain the following polynomials:

$$
\begin{aligned}
& -x_3^2 - \phi x_3 + (-\phi - 1), \\
& (-\phi - 1)x_3^2 + (-2\phi - 1)x_3 + (-3\phi - 2), \\
& x_3^3 + x_3^2 + \phi x_3 - \phi.
\end{aligned}
$$

By a direct computation,

$$(-\phi-1)x_3^2+(-2\phi-1)x_3+(-3\phi-2)=(\phi+1)(-x_3^2-\phi x_3+(-\phi-1)),$$
$$x_3^3+x_3^2+\phi x_3-\phi=(-x_3^2-\phi x_3-(\phi+1))(-x_3-1+\phi),$$

so the corresponding ideal is generated by the polynomial

$$F=x_3^2+\phi x_3+(\phi+1).$$

In fact, we can rewrite it as

$$F=x_3^2+\phi x_3+\phi^2,$$

which instantly shows that $\frac{x_3}{\phi}=\omega$ is a root of the polynomial t^2+t+1, a primitive cube root of unity. Furthermore, we recall that throughout Case 2.2 we have $x_1=x_3-x_2$, so

$$x_1=\omega\phi+\phi=\phi(\omega+1)=-\omega^2\phi,$$

Next, we substitute the values that we found in the first two polynomials of the set above, obtaining

$$x_6=-\phi^2\omega^3-\phi^2-2\phi^2\omega^2-2\phi^2\omega^4-\phi=-\phi, \tag{9.20}$$
$$x_4=\phi^2-\phi^2\omega^3+\phi^2\omega^2-\phi\omega^2=(\phi^2-\phi)\omega^2=\omega^2. \tag{9.21}$$

Finally, since throughout Case 2 we have $x_5=-x_4$, we conclude that

$$x_5=-\omega^2.$$

□

Theorem 9.3.4.2. *For the ten cases of cubic relation matrices of rank* 3*, the matrix* C *representing the quartic consequences satisfies* $\operatorname{rank}(C)\geq 12$. *Figure 9.2 gives a complete list of the triples of cubic relations which produce the minimal rank* 12 *for the quartic relations.*

Proof. Case 1, the most difficult case, has been done in Lemma 9.3.4.1. The remaining cases 2–10 are left to the reader; see Exercise 9.10. □

Another classification question which we decided to discuss here is how to hunt for values of parameters that give nilpotent operads. The operad corresponding to the cubic relation matrix becomes nilpotent in arity 5 if and only if the 18×14 matrix C has full rank, which happens if and only if the 6×2 lower right block $B=B_{6,2}$ has full rank; see Figure 9.1. Thus nilpotent operads exist if and only if there exist values of $x_1,\dots,x_6$ for which $\operatorname{rank}(B)=2$. Do such values exist? If so, can we find all such values?

To answer the second question requires studying the second determinantal ideal $DI_2(B)$. The values we want form the complement of $V(DI_2(B))$ in $\mathbb{F}^6$.

$(((**)*)*) + X(*((**)*)) - (X+1)(*(*(**))) = 0$ $((*(**))*) + X(*((**)*)) - (X+1)(*(*(**))) = 0$ $((**)(**)) = (*((**)*))$	case 1
$(((**)*)*) = 0,\ ((**)(**)) = 0,$ $((*(**))*) + X(*((**)*)) = 0$	
$(((**)*)*) = 0,\ ((*(**))*) = 0,$ $((**)(**)) + X(*((**)*)) = 0$	
$(((**)*)*) = ((*(**))*) = (*((**)*)),$ $((**)(**)) = (*(*(**)))$	
$(((**)*)*) + \omega^2\phi\,(*((**)*)) - \phi\,(*(*(**))) = 0$ $((*(**))*) + \omega\phi\,(*((**)*)) + \omega^2\,(*(*(**))) = 0$ $((**)(**)) - \omega^2\,(*((**)*)) - \phi\,(*(*(**))) = 0$	
$(((**)*)*) = 0,\ \ ((*(**))*) = 0,\ \ (*((**)*)) = 0$	case 2
$(((**)*)*) = ((**)(**)),$ $((*(**))*) = (*((**)*)) = (*(*(**)))$	
$(((**)*)*) + X((**)(**)) - (X+1)(*(*(**))) = 0,$ $((*(**))*) = ((**)(**)),\ \ (*((**)*)) = (*(*(**)))$	
$(((**)*)*) = ((*(**))*),$ $((**)(**)) = (*((**)*)) = (*(*(**)))$	case 4
$(((**)*)*) = 0,\ ((**)(**)) = 0,\ (*((**)*)) = 0$	
$(((**)*)*) = ((**)(**)) = (*(*(**))) = 0$	case 5
$((*(**))*) = ((**)(**)) = (*((**)*)) = (*(*(**)))$	case 7
$((*(**))*) = 0,\ ((**)(**)) = 0,\ (*((**)*)) = 0$	
$((*(**))*) + X(*((**)*)) = 0,$ $((**)(**)) = 0,\ (*(*(**))) = 0$	case 8
$((*(**))*) + X((**)(**)) = 0,$ $(*((**)*)) = 0,\ (*(*(**))) = 0$	case 9
$((**)(**)) = 0,\ (*((**)*)) = 0,\ (*(*(**))) = 0$	case 10

FIGURE 9.2: Operads with cubic rank 3 and minimal quartic rank 12.

It is not hard to compute the 2×2 minors: there are $\binom{6}{2} = 15$ of them, and all are nonzero; they have degrees 5 and 6, and terms from 19 to 44; and their coefficients lie in $\{-2, \dots, 2\}$. Here is the greatest in `glex` order:

$$\begin{aligned}
&x_5^2x_4^2x_3x_2 - x_6x_5x_4x_3^2x_2 + x_5x_4^2x_3^2x_2 - x_6x_4x_3^3x_2 + x_5^2x_3^2x_2^2 \\
&- x_3^4x_2^2 - x_5^2x_4^2x_3x_1 - x_5x_4^3x_3x_1 + x_6x_5x_4x_3^2x_1 + x_6x_4^2x_3^2x_1 \\
&- x_6x_5x_3^2x_2x_1 + x_5x_3^3x_2x_1 + 2x_4x_3^3x_2x_1 - x_5x_4x_3^2x_1^2 \\
&- x_4^2x_3^2x_1^2 + x_6x_5x_4^2x_2 + x_6x_5x_4x_3x_2 + x_6x_4^2x_3x_2 + x_6x_4x_3^2x_2 \\
&+ x_5x_4x_3x_2^2 - x_6x_3^2x_2^2 + x_4x_3^2x_2^2 - x_6x_4^3x_1 + x_5x_4^3x_1 \\
&- x_6^2x_4x_3x_1 - x_6x_4^2x_3x_1 - x_5^2x_4x_2x_1 + x_6x_5x_3x_2x_1 \\
&- x_4^2x_3x_2x_1 + x_5^2x_2^2x_1 + x_5x_3x_2^2x_1 - x_3^2x_2^2x_1 - x_6x_5x_2x_1^2 \\
&- x_5x_4x_2x_1^2 - x_6x_3x_2x_1^2 + x_5x_3x_2x_1^2 + x_4x_3x_2x_1^2 + x_6x_4x_1^3 \\
&- x_5x_4x_1^3 - x_6x_4^2x_2 + x_6x_5x_2^2 + x_6x_4x_2^2 - x_6^2x_2x_1 + x_4x_2^2x_1.
\end{aligned}$$

Problems begin when we compute the `glex` Gröbner basis. It contains 332 polynomials of degrees between 5 and 19; each has between 19 and 3441 terms; and the coefficients have up to 98 decimal digits. So it seems to be a hard problem to compute a Gröbner basis for the radical, and to find the zero set; see Exercise 9.9.

To answer the first question is much easier: we use modular methods to understand the distribution of the ranks, and if this indicates that full rank is possible, then we use trial and error with pseudorandom values of the parameters to find examples of nilpotent operads. This is reasonable since the nilpotency condition is that the highest determinantal ideal does not vanish, and so the set of parameter values which imply nilpotency is Zariski open. To justify the use of modular methods to obtain rational results, we appeal to the following fact.

Lemma 9.3.4.3. *Let A be any $m \times n$ matrix with entries in $\mathbb{Z}$. Let $\mathrm{rank}_0(A)$ be the rank of A over $\mathbb{Q}$, and for any prime p let $\mathrm{rank}_p(A)$ be the rank of A over the field $\mathbb{F}_p$ with p elements. Then*

$$\mathrm{rank}_p(A) \leq \mathrm{rank}_0(A) \text{ for all } p.$$

In particular, if A has full rank over $\mathbb{F}_p$ for some p, then A has full rank over $\mathbb{Q}$.

Proof. Lemma 8.2.3.2 implies that the rank of A over any field $\mathbb{F}$ is the largest integer r satisfying condition $N(r, \mathbb{F})$: at least one $r \times r$ minor is nonzero in $\mathbb{F}$. (To deal with rank 0, we define the unique 0×0 minor to be 1.) Minors are polynomial functions of the matrix entries a_{ij}, and reduction modulo p is a ring homomorphism from polynomials with coefficients in $\mathbb{Z}$ to polynomials with coefficients in $\mathbb{F}_p$. Hence $N(r, \mathbb{F}_p)$ implies $N(r, \mathbb{Q})$ but not conversely. For extensions of this result, see Exercise 9.13. □

It follows that if the relation matrix for a given arity has full rank over $\mathbb{F}_p$ for some prime p then the operad is nilpotent. Figure 9.3 displays the results of

Case 1: parameters 6, block 6 × 2				*Case 2*: parameters 5, block 6 × 2			
rank(B)	rank(C)	number	percent	rank(B)	rank(C)	number	percent
0	12	33	0.001863	0	12	13	0.008072
1	13	3351	0.1892	1	13	488	0.3030
2	14	1768177	99.81	2	14	160550	99.69
Case 3: parameters 4, block 4 × 1				*Case 4*: parameters 4, block 5 × 2			
rank(B)	rank(C)	number	percent	rank(B)	rank(C)	number	percent
		12		0	12	2	0.01366
0	13	11	0.07513	1	13	148	1.011
1	14	14630	99.92	2	14	14491	98.98
Case 5: parameters 3, block 3 × 2				*Case 6*: parameters 2, block 0 × 0			
rank(B)	rank(C)	number	percent	rank(B)	rank(C)	number	percent
0	12	1	0.07513		12		
1	13	39	2.930	0	13	121	100
2	14	1291	96.99		14		
Case 7: parameters 3, block 5 × 1				*Case 8*: parameters 2, block 2 × 1			
rank(B)	rank(C)	number	percent	rank(B)	rank(C)	number	percent
0	12	2	0.1503	0	12	11	9.091
1	13	1329	99.85	1	13	110	90.91
	14				14		
Case 9: parameters 1, block 0 × 0				*Case 10*: parameters 0, block 0 × 0			
rank(B)	rank(C)	number	percent	rank(B)	rank(C)	number	percent
0	12	11	100	0	12	1	100
	13				13		
	14				14		

FIGURE 9.3: Ranks of consequences and nilpotency of operads.

computations for cases 1–10 using $p = 11$. The number of k-tuples $[x_1, \dots, x_k]$ of parameter values in terms of the number k of parameters in each case is

$$p^k = 1,\ 11,\ 121,\ 1331,\ 14641,\ 161051,\ 1771561 \quad (k = 0, \dots, 6).$$

We see that nilpotency, $\text{rank}(C) = 14$, occurs only for cases 1–5, and in those cases a large majority (nearly 100%) of the k-tuples $[x_1, \dots, x_k]$ produce nilpotent operads. This motivates using trial-and-error methods to find examples.

For each case we used a loop over the Cartesian product of k copies of the coefficient set $\mathcal{X} = \{ 0, \pm 1, \dots, \pm 5 \}$ where k is the number of parameters, and obtained the following results, verifying that in cases 1–5 almost all parameter values produce nilpotent operads:

case	parameters	nilpotent	$\lvert\mathcal{X}\rvert^k$	percentage
1	6	1768810	1771561	≈ 99.845
2	5	160662	161051	≈ 99.758
3	4	14636	14641	≈ 99.966
4	4	14570	14641	≈ 99.515
5	3	1310	1331	≈ 98.422

Closer inspection of these results shows that we can obtain nilpotent operads even when only one of the parameters is nonzero. Since this special case has only one parameter, we can make the corresponding substitutions into the quartic relation matrix C, and compute its Smith normal form. In all cases the minimal rank is 12, and so the first 12 diagonal entries of the Smith form are 1; we are only concerned with the last two diagonal entries, which are displayed in the table below. Considering each parameter on its own, we have:

- If $x_1 \neq 0$, others 0, then only case 3 produces a nilpotent operad.
- If $x_2 \neq 0$, others 0, then every case is nilpotent.
- If $x_3 \neq 0$, others 0, then only cases 3, 4, 5 are nilpotent.
- If $x_4 \neq 0$, others 0, then only cases 1, 2, 3 are nilpotent; case 4 is not.
- If $x_5 \neq 0$, others 0, then neither case 1 nor 2 is nilpotent.
- If $x_6 \neq 0$, others 0, then case 1 is not nilpotent.

parameter	case 1		case 2		case 3		case 4		case 5	
x_1	x_1^2	0	x_1^2	0	1	x_1	x_1	0	x_1^2	0
x_2	x_2	x_2	x_2	x_2	1	x_2	x_2	x_2	x_2	x_2
x_3	0	0	x_3^2	0	1	x_3	x_3	x_3	x_3	x_3^2
x_4	x_4	x_4^2	x_4	x_4	1	x_4	x_4	0		
x_5	0	0	x_5^2	0						
x_6	x_6^2	0								

9.3.5 Relation rank 4

Since there are five nonsymmetric cubic monomials, a cubic relation matrix has nullity 1 if and only if it has rank 4. We have the following result.

Theorem 9.3.5.1. *Every nonsymmetric operad defined by a four-dimensional space of cubic relations is nilpotent (in the sense that every quartic composition is zero) except for the three operads defined by the following relation matrices:*

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot & -1 \\ \cdot & 1 & \cdot & \cdot & -1 \\ \cdot & \cdot & 1 & \cdot & -1 \\ \cdot & \cdot & \cdot & 1 & -1 \end{bmatrix} \qquad \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \end{bmatrix} \qquad \begin{bmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

The first matrix says that all five monomials are equal; "cubic associativity":

$$(((\ast\ast)\ast)\ast) = ((\ast(\ast\ast))\ast) = ((\ast\ast)(\ast\ast)) = (\ast((\ast\ast)\ast)) = (\ast(\ast(\ast\ast))).$$

The second matrix says that the first four monomials vanish, and the last is "free":

$$(((\ast\ast)\ast)\ast) = ((\ast(\ast\ast))\ast) = ((\ast\ast)(\ast\ast)) = (\ast((\ast\ast)\ast)) = 0.$$

The third matrix says that the last four monomials vanish, and the first is "free":

$$((\ast(\ast\ast))\ast) = ((\ast\ast)(\ast\ast)) = (\ast((\ast\ast)\ast)) = (\ast(\ast(\ast\ast))) = 0.$$

The operads defined by these three relation matrices have positive dimension in every arity, and are therefore not nilpotent.

Proof. There is a bijection f between the set of 4-dimensional subspaces R of the 5-dimensional space $\mathcal{T}_{\mathcal{X}}(4)$, and the set of 4×5 matrices in row canonical form (RCF). By definition $f(R)$ is the matrix in RCF whose row space is R with respect to the monomial basis. We obtain five cases for $f(R)$ corresponding to the five choices of 4 columns containing leading 1s in the RCF:

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot & x_1 \\ \cdot & 1 & \cdot & \cdot & x_2 \\ \cdot & \cdot & 1 & \cdot & x_3 \\ \cdot & \cdot & \cdot & 1 & x_4 \end{bmatrix} \begin{bmatrix} 1 & \cdot & \cdot & x_1 & \cdot \\ \cdot & 1 & \cdot & x_2 & \cdot \\ \cdot & \cdot & 1 & x_3 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix} \begin{bmatrix} 1 & \cdot & x_1 & \cdot & \cdot \\ \cdot & 1 & x_2 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix} \begin{bmatrix} 1 & x_1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix} \begin{bmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

For each case, the four relations produce 24 consequences, so we obtain a 24×14 matrix C whose (i,j) entry is the coefficient of the j-th monomial in the i-th consequence. The row space of C is the space of relations in arity 5 for the operad defined by the cubic relations represented by the rows of R, and null space of C can be identified with the homogeneous subspace of arity 5 in the quotient operad. In particular, the quotient operad becomes nilpotent in arity 5 (all compositions of arity 5 are 0) if and only if $\mathrm{rank}(C) = 14$.

We will discuss case 1 in more detail than the others. The sorted matrix C of consequences is displayed in Figure 9.4. Using the partial Smith form algorithm, we reduce C to this block diagonal form:

$$\begin{bmatrix} I_{13} & O_{13,1} \\ O_{11,13} & B_{11,1} \end{bmatrix}$$

where I_{13} is the identity matrix, $O_{13,1}$ and $O_{11,13}$ are zero matrices, and the lower right block $B_{11,1}$ is a column vector containing these polynomials:

$$\left.\begin{array}{l} x_4 - x_3, \quad x_3^2 + x_1, \quad x_4x_3 + x_2, \quad x_4^2 + x_1, \quad x_4^2 + x_2, \\ x_1(x_4x_2 + x_3), \quad x_4(x_2^2 + x_1), \quad x_4(x_3x_2 + x_1), \\ x_3x_2(x_4 + 1), \quad x_4x_2(x_4 + 1). \end{array}\right\} \qquad (9.22)$$

One zero entry has been omitted and the others have been made monic and sorted using the `glex` monomial order with $x_1 \prec x_2 \prec x_3 \prec x_4$. It follows that

$$\begin{bmatrix}
1 & \cdot & \cdot & \cdot & x_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_1 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & x_2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_1 & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & x_3 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & x_2 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_1 & \cdot \\
\cdot & \cdot & \cdot & 1 & x_4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_2 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_2 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & x_3 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & x_3 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & x_4 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & x_3 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & x_3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & x_4 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & x_1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & x_4 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & x_2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & x_3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & x_4 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & x_4
\end{bmatrix}$$

FIGURE 9.4: Quartic consequences for cubic relations (rank 4, case 1).

C has rank 13 if and only if the polynomials (9.22) simultaneously vanish; otherwise C has rank 14 and the corresponding operad is nilpotent. The polynomials (9.22) generate the ideal $I \subset \mathbb{F}[x_1, x_2, x_3, x_4]$ which has the following `glex` Gröbner basis:

$$x_2 - x_1, \quad x_4 - x_3, \quad x_1(x_3 - x_1), \quad x_3^2 + x_1, \quad x_1^2(x_1 + 1).$$

A power of each parameter appears as the leading monomial of an element of the Gröbner basis, so I is zero-dimensional: the zero set $V(I)$ is finite. The last element gives $x_1 = 0$ or $x_1 = -1$; if $x_1 = 0$ then element 4 gives $x_3 = 0$, and if $x_1 = -1$ then element 3 gives $x_3 = -1$. Finally, elements 1 and 2 give $x_2 = x_1$ and $x_4 = x_3$. Hence the only solutions are $[0, 0, 0, 0]$ and $[-1, -1, -1, -1]$; they corresponding to the first and second matrices in the statement of the theorem. We remark that I is not a radical ideal; a Gröbner basis for $\sqrt{I}$ is

$$x_2 - x_1, \quad x_3 - x_1, \quad x_4 - x_1, \quad x_1(x_1 + 1),$$

which gives the solutions immediately.

For cases 2–4, the matrix of consequences has full rank for all values of the parameters. For case 5, there are no parameters and the matrix of consequences has rank 13; this corresponds to the third matrix in the statement of the theorem. For the last statement of the theorem, see Exercise 9.14. □

9.4 Exercises

Exercise 9.1. For each rank $r \in \{2, 3\}$, write down the 10 cubic relation matrices for a binary operation, and count the number of parameters in each.

Exercise 9.2. We call a matrix filled with symbols 0, 1, and $*$ a *row canonical pattern* if after replacing symbols $*$ by any elements of the ground field $\mathbb{F}$ we get a matrix in row canonical form. For example, the following matrix is a row canonical pattern:

$$\begin{bmatrix} 1 & * & 0 & 0 & * & 0 & * \\ 0 & 0 & 1 & 0 & * & 0 & * \\ 0 & 0 & 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 0 & * & 1 & * \end{bmatrix}$$

Prove that for $k \leq n$ the set of row canonical patterns of size $k \times n$ which have a 1 in each row (they represent row canonical forms of full rank) is in one-to-one correspondence with Young diagrams contained inside the rectangle $k \times (n-k)$. (For each Young diagram λ of that kind, the set of all row echelon matrices that follow the corresponding row canonical pattern form the so-called Schubert cell X_λ of the Grassmann variety $G(n, k)$ [96].)

Exercise 9.3. Let ω denote a primitive cube root of unity. Show that the element

$$(((**)*)*) + \omega((*(**))*) - ((**)(**)) + \omega^2(*((**)*)) + (*(*(**)))$$

forms the reduced Gröbner basis (with respect to `gpathlex` order) of the ideal it generates.

Exercise 9.4.

(i) Compute a Gröbner basis for the second determinantal ideal $I = DI_2(C)$ of the matrix C of Equation (9.12). The monomial ordering does not have to be `glex` with $x_1 \prec \cdots \prec x_6$; it might be more useful to assume some other ordering of the variables, or to use a `plex` order (with some ordering of the variables).

(ii) Compute a Gröbner basis for the radical $\sqrt{I}$.

(iii) Compute the zero set of I. Use this, together with the results of Section 9.3.3, to determine all values of the parameters for which C has rank 10.

Exercise 9.5. Same as Exercise 9.4 for the third determinantal ideal $I = DI_3(C)$. More precisely:

(i) Compute a Gröbner basis for the second determinantal ideal $I = DI_3(C)$ of the matrix C of Equation (9.12).

(ii) Compute a Gröbner basis for the radical $\sqrt{I}$.

(iii) Compute the zero set of I. Use this, together with the results of Exercise 9.4, to determine all values of the parameters for which C has rank 11.

Exercise 9.6. Referring to Exercises 9.4 and 9.5, what about rank 12?

Exercise 9.7. Extend the computations for case 1 in Section 9.3.3 to cases 2–10. Use these results to complete the proof of Theorem 9.3.3.1.

Exercise 9.8. Prove Theorem 9.3.3.2.

Exercise 9.9. Compute the Gröbner basis (for your choice of monomial order) of the radical of the second determinantal ideal of the 6×2 matrix B (Figure 9.1) arising from case 1 of cubic relation rank 3. Use this to compute the zero set of the ideal.

Exercise 9.10. Extend the computations for case 1 in Section 9.3.4 to cases 2–10. Use these results to complete the proof of Theorem 9.3.4.2.

Exercise 9.11. For operads listed in Theorem 9.3.4.2, compute their Gröbner bases for an ordering of your choice, and determine the dimensions of their homogeneous components.

Exercise 9.12. Explore the case of a cubic relation matrix of rank 3 for which the matrix of quartic consequences has rank 13. Give an example of a non-nilpotent operad presented by relations of that kind. Are there nilpotent operads presented by relations of that kind?

Exercise 9.13. Let $A = (a_{ij})$ be any $m \times n$ matrix with entries in $\mathbb{Z}$. Let $\mathrm{rank}_0(A)$ be the rank of A over $\mathbb{Q}$, and for any prime p let $\mathrm{rank}_p(A)$ be its rank over the field $\mathbb{F}_p$ with p elements. We have $\mathrm{rank}_p(A) \leq \mathrm{rank}_0(A)$ for all primes p by Lemma 9.3.4.3.

(i) Let $\Delta(A)$ be the set of primes p for which we have the strict inequality $\mathrm{rank}_p(A) < \mathrm{rank}_0(A)$. Prove that $\Delta(A)$ is a finite set.

(ii) Let $P(A) = \max \Delta(A)$ be the largest prime for which the ranks are not equal. Find and prove an upper bound (as tight as possible) for P in terms of m, n, and the matrix entries a_{ij}.

(iii) For each prime p, and each number m of rows and n of columns, construct an $m \times n$ matrix A for which $\Delta(A) = \{\, q \mid 2 \leq q \leq p,\ q \text{ prime} \,\}$, or prove that no such matrix exists.

Exercise 9.14. Refer to the operads (cubic rank 4) in the classification of Theorem 9.3.5.1. That result proved only that every other such operad is nilpotent; it remains to show that those three operads are not nilpotent. Prove that all three of those operads have dimension 1 in all arities $n \geq 1$, except in arity $n = 3$ for which the dimension is 2.

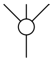
Exercise 9.15. Attempt to extend the classification results of this chapter to the case of several quartic relations.

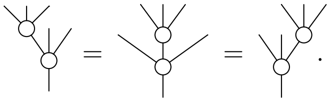
Chapter 10

Case Study of Nonsymmetric Ternary Quadratic Operads

10.1 Introduction

There are not many examples of nonsymmetric operads that arise very naturally in research questions, and most of those that do are generated by binary operations. In this section, we shall discuss some attempts at hunting for interesting examples of operads generated by one ternary operation. Throughout this chapter, we again implicitly assume that the ground field is algebraically closed or at least contains roots of all equations we solve; we leave it to the reader to adapt the results appropriately for when it is not the case. For the extension of these results to one quaternary operation, see [43].

Before we begin a systematic investigation, let us mention some examples of properties of ternary operations that in some way generalize the binary associative law. The simplest possible example of an operad generated by a ternary operation is the totally associative ternary operad. In notation of Chapter 6, it is the operad $\mathsf{tAs}_0^{(3)}$ generated by one ternary generator  subject to the following relations:

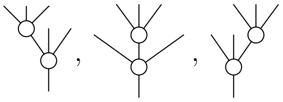


(10.1)

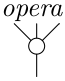
This kind of associativity is exhibited by the so-called triadic groups; see [208] (the first systematic paper in English that established n-ary operations as an independent field of study). The following proposition shows that such algebras are intimately related to usual associative algebras. The first two parts of it are folklore, the third can be traced back to [50], where it is shown that n-ary associativity is intimately related to binary associativity.

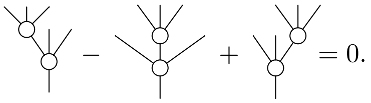
This operad also arises in homology of partially ordered sets, in the spirit of the formalism of [253]. If we consider, for each odd $n = 2k+1$, the partially ordered set of all decompositions of the ordered set $\{1, 2, \ldots, n\}$ into a disjoint union of intervals of odd length, with the partial order induced by merging an odd number of adjacent intervals, the collection of those posets becomes a nonsymmetric cooperad, the bar complex of the operad tAs^3.

Unlike the case of the usual associative algebras, there are several different types of associativity one can talk about in the context of ternary algebras: since there are three different quadratic monomials

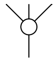


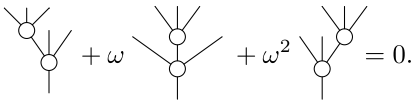
in the free operad, we have a choice between imposing one or two linear dependencies relating these elements. We already gave an example of what happens when considering two dependencies. In the case of one dependency, there are several somewhat natural choices one can make to generalize the associative law.

The *alternating partially associative ternary operad* is the nonsymmetric operad $\mathsf{pAs}^{(3)}_{-1}$ generated by one ternary generator  subject to the relation

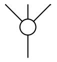


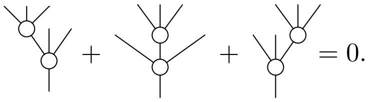
(10.2)

Suppose that $\mathbb{F}$ contains a primitive cube root of unity ω. The *ω-partially associative ternary operad* is the nonsymmetric operad $\omega - \mathsf{pAs}^{(3)}_{0}$ generated by one ternary generator  subject to the relation



(10.3)

The *odd partially associative ternary operad* is the graded nonsymmetric operad $\mathsf{pAs}^{(3)}_{1}$ generated by one ternary generator  *of homological degree* 1 subject to the relation



(10.4)

Each of these relations generalizes the associative law. The first one views the associative law as an alternating sum of partial compositions. The second one views the associative law as a sum of partial compositions with coefficients being powers of a primitive root of unity. The third one utilizes the fact that the associative operad is self-dual for the Koszul duality, and thus examines the Koszul dual of the operad $\mathsf{tAs}_0^{(3)}$. In this chapter, we will investigate general ternary operations satisfying quadratic relations.

10.2 Generalities on nonsymmetric operad with one generator

In this section, we assemble some general results on operads with one generator of some arity n. In the main part of the chapter, we shall focus on the case $n = 3$, but since most basic statements and their proofs do not get more difficult as n grows, we collate those statements here, hoping that the reader will be interested in generalizing some of our classification results for higher arities of generators. Throughout this section, we fix an integer $n \geq 2$, and consider the nonsymmetric collection $\mathcal{X}$ with $\mathcal{X}(n) = \{f\}$ and $\mathcal{X}(k) = \varnothing$ for $k \neq n$, and the corresponding free nonsymmetric operad $\mathcal{T}_{\mathcal{X}}$.

10.2.1 Enumeration and ordering of monomials

The natural basis of the operad $\mathcal{T}_{\mathcal{X}}$ consists of tree monomials. For the collection $\mathcal{X}$ that we consider, the underlying trees of such monomials are "planar rooted complete n-ary trees" [119], meaning that it is a planar rooted tree such that for each vertex v, the set $\mathrm{Parent}^{-1}(v)$ consists of either 0 or n elements. Moreover, since $\mathcal{X}(n)$ is one-dimensional, each tree monomial can be identified with its underlying tree.

Proposition 10.2.1.1 ([119, §7.5])**.** *The number of distinct planar rooted complete n-ary trees of a given weight w is given by the n-ary Catalan number*

$$C^{(n)}(w) = \frac{1}{(n-1)w+1}\binom{nw}{w}$$

Example 10.2.1.2. We compile the values for $n = 2, 3, 4$ and $w = 1, 2, \ldots, 9$:

w	1	2	3	4	5	6	7	8	9
$C^{(2)}(w)$	1	2	5	14	42	132	429	1430	4862
$C^{(3)}(w)$	1	3	12	55	273	1428	7752	43263	246675
$C^{(4)}(w)$	1	4	22	140	969	7084	53820	420732	3362260

Lemma 10.2.1.3. *For a planar rooted complete n-ary tree T, we have the following equation that relates the arity of T to the weight of T:*

$$\mathrm{ar}(T) = 1 + (n-1)\,\mathrm{wt}(T).$$

Proof. Exercise 10.3. □

Corollary 10.2.1.4. *We have the following formula for dimensions of components of $\mathcal{T}_{\mathcal{X}}$:*

$$\dim(\mathcal{T}_{\mathcal{X}}(m)) = \frac{1}{m}\binom{\frac{n}{n-1}(m-1)}{\frac{1}{n-1}(m-1)}.$$

Lemma 10.2.1.5. *The n-ary Catalan numbers satisfy this recurrence relation:*

$$C^{(n)}(0) = 1, \qquad\qquad C^{(n)}(w) = \sum_{w_1,\dots,w_n} \prod_{i=1}^{n} C^{(n)}(w_i),$$

where the sum is over all $\binom{w-1}{n-1}$ compositions (partitions where the order matters) of w into the sum of n positive integers $w_1, \dots, w_n = w$.

Proof. Exercise 10.6. □

We next give a precise definition of the total order on trees which we used in computer algebra computations.

Definition 10.2.1.6. Let $T \neq T'$ be two planar rooted complete n-ary trees of arities m, m', respectively. We say that $T \prec T'$ if and only if

- $m < m'$ or
- $m = m'$ and $T_i \prec T'_i$, where $T_1, \dots, T_n$ are the n subtrees of the root of T in the planar order, and $T'_1, \dots, T'_n$ are the n subtrees of the root of T' in the planar order, and i is the least index for which $T_i \neq T'_i$.

10.2.2 Quadratic relations and their consequences

Recall that an element of $\mathcal{T}_{\mathcal{X}}$ is called quadratic if it is a combination of tree monomials of weight 2. There are n such tree monomials: $f \circ_i f$ for $1, \dots, n$.

Definition 10.2.2.1 (Relation matrix and relation rank)**.** Let U be an r-dimensional subspace of $\mathcal{T}_{\mathcal{X}}^{(2)}$. Such subspaces are parameterized by the Grassmann variety $\mathbf{Gr}(n, r)$ and can be represented bijectively by $r \times n$ matrices in row canonical form (RCF). We call such a matrix the *relation matrix* corresponding to the space of quadratic relations, and we call r the *relation rank.*

The number of distinct ranks for an n-ary operation is $n+1$ since $0 \leq r \leq n$; for rank r there are $\binom{n}{r}$ choices for the columns of the leading 1s in the RCF. Summing these binomial coefficients gives a total of 2^n cases to be considered.

Example 10.2.2.2. Let us list the cases to be considered for $n = 3$. In this case, every space of quadratic relations has dimension $r \in \{0, 1, 2, 3\}$ and is the row space of a unique $r \times 3$ matrix $[R]$ of rank r in row canonical form (RCF). For arbitrary $a, b \in \mathbb{F}$ the possibilities for $[R]$ are as follows:

$$\overbrace{[\text{empty matrix}]}^{r=0} \qquad \overbrace{\begin{bmatrix} 1 & a & b \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & a \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}}^{r=1}$$

$$\overbrace{\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} \quad \begin{bmatrix} 1 & a & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}^{r=2} \qquad \overbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}^{r=3}$$

Further in this chapter, we will study the quotient operads $\mathcal{Q} = \mathcal{T}_{\mathcal{X}}/(R)$ where (R) denotes the ideal generated by the space $R \subseteq \mathcal{T}_{\mathcal{X}}^{(2)}$ of quadratic relations.

To study quotient operads using commutative Gröbner bases, we should form various spaces of consequences of given quadratic relations, and explore dimensions of those.

Definition 10.2.2.3 (Cubic consequences of a quadratic relation)**.** Let R be a quadratic relation for an n-ary operation. There are $2n-1$ compositions $R \circ_i f$ and n compositions $f \circ_j R$, which are cubic relations in f, and which span the subspace $R^{(3)}$ of $\mathcal{T}_{\mathcal{X}}(3n-2)$ called the space of all *cubic consequences* of R. Combining these for several relations, we obtain the space of cubic consequences of arbitrary quadratic relations.

We can inductively repeat this generation of cubic consequences into higher arities to obtain quartic, quintic, etc., consequences of any space of quadratic relations R. We denote the space of weight w consequences by $R^{(w)}$.

Proposition 10.2.2.4. *The number of distinct consequences of weight w of one quadratic relation is equal to $\binom{nw-1}{w-2}$.*

Proof. Exercise 10.7. □

Every consequence of weight w is a linear combination of the $C^{(n)}(w)$ basis elements. Thus the consequences of R in weight w can be represented as the row space of a $\binom{nw-1}{w-2} \times C^{(n)}(w)$ matrix. If the number of rows of this matrix is less than the number of columns, we should expect a generic operad with one relation to have nonzero elements of any weight, and otherwise, we should expect that in “most” operads with one relation all elements of weight w vanish, so that those operads are nilpotent of index at most w. The case of a square matrix is the first interesting instance. Therefore, we identified some natural questions to ask: when is the matrix of consequences square, and more importantly, when is it invertible?

The first question is easy to answer, since for $w \geq 2$ we have

$$\binom{nw-1}{w-2} = \frac{1}{(n-1)w+1}\binom{nw}{w} \qquad \Longleftrightarrow \qquad w = n+1.$$

For this weight, the arity is $a = 1 + w(n-1) = n^2$, which gives the somewhat amusing conclusion that the matrix is square if and only if the arity is n^2. (Note that this solution is only for a single relation; for two or more relations we need to multiply the left side of the equation by the number s of relation, which gives the general solution $w = (n+s)/s$.)

The second question of invertibility is harder to resolve: it corresponds to a zero nullspace and a nilpotent operad.

10.3 Nonsymmetric ternary operads

In this section we consider the simplest case of a non-binary operad: a nonsymmetric operad with one ternary operation satisfying one quadratic relation. We will see that even in this restricted setting there are many interesting features, hard problems, and unanswered questions. However, we are able to obtain some results and state some meaningful conjectures about such operads.

10.3.1 Preliminary analysis

We shall first handle two extreme (and extremely easy) cases of the quotient operad $\mathcal{Q}$: $r = 0$, where there are no relations, and $r = 3$, where every composition is zero.

Lemma 10.3.1.1. *We have the following results for the extreme values of r:*

- *For $r = 0$, we have $\mathcal{Q} = \mathcal{T}_{\mathcal{X}}$.*
- *For $r = 3$, $\mathcal{Q}$ is nilpotent of index 2.*

Proof. Direct inspection. □

There remain two possibilities. For the case of one relation ($r = 1$), we have three cases,

$$\left[\begin{array}{ccc} 1 & a & b \end{array}\right], \qquad \left[\begin{array}{ccc} 0 & 1 & a \end{array}\right], \qquad \left[\begin{array}{ccc} 0 & 0 & 1 \end{array}\right],$$

corresponding, respectively, to the following quadratic relations:

$$f \circ_1 f + a\, f \circ_2 f + b\, f \circ_3 f = 0, \tag{R1.1}$$

$$f \circ_2 f + a\, f \circ_3 f = 0, \tag{R1.2}$$

$$f \circ_3 f = 0. \tag{R1.3}$$

As we discussed in the previous section, each quadratic relation R produces several cubic consequences. For $n = 3$, there are eight *cubic consequences*:

$$R \circ_1 f,\ R \circ_2 f,\ R \circ_3 f,\ R \circ_4 f,\ R \circ_5 f,$$

$$f \circ_1 R,\ f \circ_2 R,\ f \circ_3 R.$$

The number of ternary tree monomials operations of weight w is the ternary Catalan number $\frac{1}{2w+1}\binom{3w}{w}$, and the number of *distinct* consequences of weight w of a single quadratic ternary relation is the binomial coefficient $\binom{3w-1}{w-2}$. This gives the following sizes of matrices representing consequences of one relation in weights $1, \dots, 10$:

w	consequences	monomials
1	0	1
2	1	3
3	8	12
4	55	55
5	364	273
6	2380	1428
7	15504	7752
8	100947	43263
9	657800	246675
10	4292145	430715

For $w \geq 2$, these two quantities are equal if and only if $w = 4$, in which case the common value is 55.

For two relations ($r = 2$) we have three cases,

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix}, \qquad \begin{bmatrix} 1 & a & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

corresponding respectively to the following pairs of quadratic relations:

$$\begin{aligned} f \circ_1 f + a\, f \circ_3 f &= 0, & f \circ_2 f + b\, f \circ_3 f &= 0, \\ f \circ_1 f + a\, f \circ_2 f &= 0, & f \circ_3 f &= 0, \\ f \circ_2 f &= 0, & f \circ_3 f &= 0. \end{aligned}$$

For both $r = 1, 2$, the three cases have, respectively, 2, 1, 0 parameters.

10.3.2 Relation rank 1

10.3.2.1 Cubic consequences

In the case of relation rank 1, we have just one defining relation R, and $\dim \mathcal{Q}(5) = 2$. Let us discuss the three possible row canonical forms individually. We give as many explicit details as possible in this case: for higher arities, the matrices are almost always too large and the entries too complex for us to be able to display the results.

Case 1: In this case, $R = f \circ_1 f + a\, f \circ_2 f + b\, f \circ_3 f$. There are no duplications among the 8 consequences of this relation:

$$(f \circ_1 f) \circ_1 f + a\,(f \circ_2 f) \circ_1 f + b\,(f \circ_3 f) \circ_1 f,$$

$$
\begin{gathered}
(f \circ_1 f) \circ_2 f + a\,(f \circ_2 f) \circ_2 f + b\,(f \circ_3 f) \circ_2 f, \\
(f \circ_1 f) \circ_3 f + a\,(f \circ_2 f) \circ_3 f + b\,(f \circ_3 f) \circ_3 f, \\
(f \circ_1 f) \circ_4 f + a\,(f \circ_2 f) \circ_4 f + b\,(f \circ_3 f) \circ_4 f, \\
(f \circ_1 f) \circ_5 f + a\,(f \circ_2 f) \circ_5 f + b\,(f \circ_3 f) \circ_5 f, \\
f \circ_1 (f \circ_1 f) + a\, f \circ_1 (f \circ_2 f) + b\, f \circ_1 (f \circ_3 f), \\
f \circ_2 (f \circ_1 f) + a\, f \circ_2 (f \circ_2 f) + b\, f \circ_2 (f \circ_3 f), \\
f \circ_3 (f \circ_1 f) + a\, f \circ_3 (f \circ_2 f) + b\, f \circ_3 (f \circ_3 f).
\end{gathered}
$$

Converting these into a matrix, we obtain an 8×12 relation matrix $M(a,b)$ is the first matrix in Figure 10.1. We need to determine the rank of this matrix as a function of the parameters a, b. We consider instead the inverse problem: given an integer $0 \leq r \leq 8$, determine the subset of $\mathbb{F}^2$ consisting of the ordered pairs (a,b) for which $\operatorname{rank} M(a,b) = r$.

We first observe that $M(a,b)$ contains 7 orthogonal 1s for all a, b: every row has a leading 1, and these leading 1s occur in columns 1–6 and 10. We therefore start by computing the partial Smith form (PSF) by using elementary row and column operations to create a block diagonal matrix with the identity matrix I_7 in the upper left corner; we obtain the second matrix in Figure 10.1.

$$
M(a,b) = \left[\begin{array}{cccccccccccc}
1 & a & b & . & . & . & . & . & . & . & . & . \\
1 & . & . & a & b & . & . & . & . & . & . & . \\
. & 1 & . & . & . & a & . & . & b & . & . & . \\
. & . & 1 & . & . & . & a & . & . & b & . & . \\
. & . & . & 1 & . & . & . & a & . & . & b & . \\
. & . & . & . & 1 & . & . & . & a & . & . & b \\
. & . & . & . & . & 1 & a & b & . & . & . & . \\
. & . & . & . & . & . & . & . & . & 1 & a & b
\end{array} \right]
\xrightarrow[\text{PSF}]{\text{partial Smith form}}
$$

$$
\left[\begin{array}{cccccccccccc}
1 & . & . & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & . & . & . & . & . \\
. & . & . & . & . & . & . & a^3 - ab & a^2 b + a^2 & ab^2 + ab & b^3 + b^2 & .
\end{array} \right]
$$

FIGURE 10.1: Rank 1, case 1: original and reduced cubic relation matrices.

From the second matrix we see that $\dim R^{(3)} = 7$ if and only if all the polynomials in the following ordered set vanish:

$$
G \;=\; \left[\quad a^3 - ab, \quad a^2 b + a^2, \quad ab^2 + ab, \quad b^3 + b^2 \quad \right]. \tag{10.5}
$$

In fact G is a `glex` Gröbner basis of the ideal $I(G) \subset \mathbb{F}[a,b]$ that it generates. The first and last elements of G have powers of the parameters as leading monomials, and hence $I(G)$ is zero-dimensional and there are only finitely many ordered pairs (a,b) for which every element of G vanishes. Factoring the elements of G gives

$$I(G) \;=\; \big(\quad a(a^2-b), \quad a^2(b+1), \quad ab(b+1), \quad b^2(b+1) \quad \big). \qquad (10.6)$$

If $b=-1$ then the last 3 elements are 0 and the fourth is $a(a^2+1)$; hence $a \in \{0, \pm i\}$ for $i=\sqrt{-1}$. If $b \neq -1$ then we cancel $b+1$ from the last 3 elements to obtain a^2, ab, b^2; hence a and b must both be 0. Thus the only solutions are the following four:

$$(a,b) \;=\; \big(0,\,0\big), \quad \big(0,\,-1\big), \quad \big(\,\pm i,\,-1\big).$$

The ideal $I(G)$ is not radical; the `glex` Gröbner basis for $\sqrt{I(G)}$ is

$$\big[\quad a(b+1), \quad b(b+1), \quad a(a^2+1) \quad \big].$$

The structure of these ideals becomes clearer if we consider the primary decomposition of $I(G)$ and the prime decomposition of $\sqrt{I(G)}$:

$$\begin{aligned} I(G) \;&=\; (\,a,\,b+1\,) \;\cap\; (\,a+i,\,b+1\,) \;\cap\; (\,a-i,\,b+1\,) \;\cap\; (\,a^2,\,ab,\,b^2\,), \\ \sqrt{I(G)} \;&=\; (\,a,\,b+1\,) \;\cap\; (\,a+i,\,b+1\,) \;\cap\; (\,a-i,\,b+1\,) \;\cap\; (\,a,\,b\,). \end{aligned}$$

All these ideals are maximal except for $(\,a^2,\,ab,\,b^2\,)$ which is primary but not prime.

$$\left[\begin{array}{cccccccccccc}
. & 1 & a & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & a & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & a & . & . & . \\
. & . & . & . & . & . & 1 & a & . & . & . & . \\
. & . & . & . & . & . & 1 & . & . & a & . & . \\
. & . & . & . & . & . & . & 1 & . & . & a & . \\
. & . & . & . & . & . & . & . & 1 & . & . & a \\
. & . & . & . & . & . & . & . & . & . & 1 & a
\end{array}\right]
\xrightarrow{\text{HNF}}
\left[\begin{array}{cccccccccccc}
. & 1 & a & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & a & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . & -a^2 \\
. & . & . & . & . & . & 1 & . & . & . & . & a^3 \\
. & . & . & . & . & . & . & 1 & . & . & . & -a^2 \\
. & . & . & . & . & . & . & . & 1 & . & . & a \\
. & . & . & . & . & . & . & . & . & a & . & -a^3 \\
. & . & . & . & . & . & . & . & . & . & 1 & a
\end{array}\right]$$

FIGURE 10.2: Rank 1, case 2: original and reduced cubic relation matrices.

Case 2: In this case $R = f \circ_2 f + a\, f \circ_3 f$. There are no duplications among the 8 consequences in $\mathcal{O}(7)$: thus $R^{(3)}$ is the row space of the first matrix in Figure 10.2, where we have sorted the rows to make the matrix as upper triangular as possible. Since there is only one parameter, we calculate the Hermite normal form (HNF) of this matrix, and obtain the second matrix in Figure 10.2. From this it is clear that $\dim R^{(3)} = 7$ if and only if $a = 0$; otherwise $\dim R^{(3)} = 8$.

Case 3: In this case $R = f \circ_3 f$. We leave this case as an easy exercise for the reader.

Summarizing, we obtain the following result describing the arity 7 components of quotients by one quadratic relation.

Proposition 10.3.2.1. *Let $\mathcal{Q} = \mathcal{T}_{\mathcal{X}}/(R)$ be the quotient by an ideal generated by one quadratic relation R. Then* $\dim \mathcal{Q}(7) = 4$ *except for the following six relations R for which* $\dim \mathcal{Q}(7) = 5$*:*

$$\begin{array}{ll} f \circ_1 f = 0, & f \circ_1 f - f \circ_3 f = 0 \\ f \circ_2 f = 0, & f \circ_1 f + i\, f \circ_2 f - f \circ_3 f = 0 \\ f \circ_3 f = 0, & f \circ_1 f - i\, f \circ_2 f - f \circ_3 f = 0 \end{array}$$

(here $i = \sqrt{-1}$).

Using operadic Gröbner bases, it is possible to compute dimensions of all components of the six exceptional operads that we found.

Theorem 10.3.2.2. *Let $\mathcal{Q}$ be one of the six operads listed in Proposition 10.3.2.1. Then for each (odd) arity m the dimension of the m-th component of $\mathcal{Q}$ is a Catalan number:*

$$\dim \mathcal{Q}(2m+1) = \frac{1}{m+1}\binom{2m}{m}.$$

Proof. First of all, a direct computation shows that for the `gpathlex` order of tree monomials, each of these operads has a quadratic Gröbner basis of relations. In four of the cases, the leading term of R is $f \circ_1 f$, in one case it is $f \circ_2 f$, and in one case it is $f \circ_3 f$. Thus, normal monomials in each case may be described as all planar rooted ternary trees where we can only use two prescribed slots out of three for each vertex v such that $\mathrm{Parent}^{-1}(v)$ is non-empty. Clearly, the set of such trees is in bijection with the set of all complete binary trees of the same weight, which is the corresponding Catalan number. □

10.3.2.2 Cubic consequences using rational functions

In this section, we show how the results of the previous section could be obtained in a different way, using computations over the field of rational functions. We give as many explicit details as possible in this case, since for higher arities the matrices are almost always too large and the entries too complex to display the results.

Case 1: The relation $f \circ_1 f + a\, f \circ_2 f + b\, f \circ_3 f = 0$.

The matrix whose rows are the coefficient vectors of the consequences in arity 7 of the original relation in arity 5:

$$A = \begin{bmatrix} 1 & a & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & a & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & b & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & b & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & b & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & b \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & b & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & b \end{bmatrix} \qquad (10.7)$$

We compute RCF(A): columns 1–7 are the unique 8×7 matrix of rank 7 in RCF (the diagonal entries are 1 and the others are 0). Columns 8–12 are as follows:

$$\frac{1}{a(a^2-b)} \begin{bmatrix} -a^3(a^2-b) & -a^2b(a^2-b) & \cdot & -a^2b(a^2-b) & -ab^2(a^2-b) \\ a^2(a^2+b^2) & ab(a^2-b) & \cdot & a^3b(b+1) & a^2b^2(b+1) \\ -a^3(b+1) & \cdot & \cdot & -a^2b(a^2+1) & -ab^2(a^2+1) \\ a^2(a^2-b) & \cdot & \cdot & ab(a^2-b) & \cdot \\ \cdot & a^2(a^2-b) & \cdot & \cdot & ab(a^2-b) \\ -a(a^2+b^2) & \cdot & \cdot & -a^2b(b+1) & -ab^2(b+1) \\ a^2(b+1) & \cdot & \cdot & ab(b+1) & b^2(b+1) \\ \cdot & \cdot & a(a^2-b) & a^2(a^2-b) & ab(a^2-b) \end{bmatrix}$$

For future reference, we collect the factors which are irreducible over $\mathbb{Q}$:

$$a, \qquad b, \qquad b+1, \qquad a^2+1, \qquad a^2-b, \qquad a^2+b^2.$$

Since the rows of A are linearly independent, the transform matrix U is uniquely determined. The LCM of the denominators of U is $a(a^2-b)$, and so we write:

$$U = \frac{1}{a(a^2-b)} \begin{bmatrix} \cdot & a(a^2-b) & \cdot & \cdot & -a^2(a^2-b) & -ab(a^2-b) & \cdot & \cdot \\ a^2 & -a^2 & -ab & -a^2b & a^3 & a^2b & a^2b & a^2b^2 \\ -a & a & a^2 & a^3 & -a^2 & -ab & -a^3 & -a^3b \\ \cdot & \cdot & \cdot & \cdot & a(a^2-b) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & a(a^2-b) & \cdot & \cdot \\ -a & a & a^2 & ab & -a^2 & -ab & -ab & -ab^2 \\ 1 & -1 & -a & -b & a & b & a^2 & b^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a(a^2-b) \end{bmatrix}$$

From the irreducible factors of the LCM of the denominators of the entries of U, namely a and $a^2 - b$, we see that there are two special cases, $a = 0$ and $b = a^2$, both of which reduce the problem to a matrix over polynomials in one variable. Except for these two subcases, the matrix A has rank 8. (We obtain the same LCM from the denominators of the matrix R, but this does not hold in general. For example, if we compute the RCF of the 1×1 matrix $[a]$ we obtain $R = [1]$ and $U = [1/a]$.)

Subcase 1.1: $a = 0$.

We set $a = 0$ in the matrix A from Equation (10.7) to obtain a matrix over the Euclidean domain $\mathbb{F}[b]$. We compute the Hermite normal form (HNF) of this matrix and see that its rank is 8, except for the values $b = 0$ and $b = -1$ for which its rank is 7:

$$\begin{bmatrix}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -b^2 \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -b^2 \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & b & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & b \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b^2(b{+}1)
\end{bmatrix}$$

Subcase 1.2: $b = a^2$.

We set $b = a^2$ in the matrix A from Equation (10.7) to obtain a matrix over $\mathbb{F}[a]$. We compute the HNF of this matrix and see that its rank is 8, except for the values $a = 0$ and $b = \pm i$ ($i = \sqrt{-1}$) for which its rank is 7:

$$\begin{bmatrix}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -a^2 & -a^3 & \cdot & -a^3 & -a^4 \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & -a^2 & -a^3 & a^2 & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot & -a^3 & -a^4 \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & a^2 & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & a^2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & a^2 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a^2(a^2{+}1) & \cdot & \cdot & a^3(a^2{+}1) & a^4(a^2{+}1) \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & a^2
\end{bmatrix}$$

Case 2: The relation $f \circ_2 f + a\, f \circ_3 f = 0$.

One variable, standard HNF over $\mathbb{F}[a]$ (without transform matrix), gives rank 8 except for $a = 0$ which gives rank 7:

$$\begin{bmatrix}
\cdot & 1 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & a & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & a & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & a & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & a \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a
\end{bmatrix}
\xrightarrow{\text{HNF}}
\begin{bmatrix}
\cdot & 1 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & -a^2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & a^3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & -a^2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & a \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & -a^3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a
\end{bmatrix}$$

Case 3: The relation $f \circ_3 f = 0$.

No variables, standard RCF over $\mathbb{F}$ (without transform matrix), in fact

7×8 matrix is already in RCF:

$$\begin{bmatrix}
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1
\end{bmatrix}$$

Remark 10.3.2.3. Even though the polynomial ring $\mathbb{F}[a, b]$ is not a Euclidean domain, it is still possible that a matrix with entries in $\mathbb{F}[a, b]$ has a generalized Hermite normal form (GHNF); this happens if the pivot ideal is principal at every step of the row reduction. (By the pivot ideal we mean the ideal generated by the entries at and below the pivot.) In this case, at every step elementary row operations suffice to make the pivot entry equal to the generator of the pivot ideal and to eliminate the entries below the pivot. The matrix A of Equation (10.7) provides a very simple example. We reduce columns 1–6 using their leading 1s, multiply row 7 by -1 so that its leading entry (column 7) becomes monic ($a^3 - ab$), use this leading entry to reduce the other entries in column 7 with respect to the chosen monomial order, and finally use the leading 1 in row 8 (column 10) to eliminate the entries above it. This gives the GHNF; factoring its entries we obtain:

$$\begin{bmatrix}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -a^2 & -ab & \cdot & -ab & -b^2 \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & -a^2 & -ab & b & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot & -ab & -b^2 \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & b & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & a & \cdot & \cdot & b \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & b & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a(a^2{-}b) & a^2(b{+}1) & \cdot & \cdot & ab(b{+}1) & b^2(b{+}1) \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & a & b
\end{bmatrix}$$

The only non-trivial leading entry $a(a^2 - b)$ coincides with the LCM of the denominators of the transform matrix U that we obtained when computing the RCF. Hence this computation of the GHNF has identified the same two special cases, $a = 0$ and $b = a^2$. Furthermore, the nonzero entries of row 7 of the GHNF form a Gröbner basis of the ideal that they generate, and powers of the variables (a^3 and b^3) occur as leading monomials of these generators. It follows that this ideal vanishes only for a finite set of solutions, and these are the ordered pairs (a, b) obtained above.

10.3.2.3 Quartic consequences

We shall only consider here Case 1 of a quadratic relation, leaving Case 2 and Case 3 as (easy) exercises for the reader (Exercise 10.11).

The relation matrix for one quadratic relation in weight 4 (arity 9) is square of size 55. After using row swaps to make this matrix as close to upper-triangular as possible, we obtain the matrix on the left in Figure 10.3, where black, dark gray, light gray represent, respectively, 1, a, and b. After computing the partial Smith form, we obtain the matrix on the right; close inspection of the lower right block reveals the existence of four zero rows.

The upper left identity matrix has size 41, which is the minimal rank of both matrices ($a = b = 0$), and the lower right block has size 14. After removing 4 zero rows, we are left with a 10×14 block B with no nonzero scalar entries and no zero rows or columns; see Figure 8.2 in Chapter 8.

Already at this point we can see that the rank of the original relation matrix over the rational function field $\mathbb{F}(a,b)$ is no more than $41 + 10 = 51$, and so the 55×55 matrix is not invertible. To determine the precise rank over $\mathbb{F}(a,b)$ we need to study the structure of the $\mathbb{F}[a,b]$-module generated by the rows of $[R^{(4)}]$, as in Example 8.4.3.4 of Chapter 8. The calculations in that example imply the following result.

Proposition 10.3.2.4. *The rows of* $[R^{(4)}]$ *generate a free module of rank* 50.

Proof. We give a brief description of the algorithm used in Example 8.4.3.4 from Chapter 8. We consider an $m \times n$ matrix B over $\mathbb{F}[x_1, \dots, x_k]$. Let (i,j) be the current position of the pivot. Suppose that for some $j' \geq j$ the entries in rows $i, \dots, m$ of column j' generate a principal ideal $I = (f) \subseteq \mathbb{F}[x_1, \dots, x_k]$. If no such j' exists, then the algorithm fails; otherwise, we swap columns j and j' so that $I = (b_{ij}, \dots, b_{mj})$. If $f = 0$ then we increment j but not i and continue to the next iteration; otherwise, we make $b_{ij} = f$ and $b_{i'j} = 0$ for $i' = i+1, \dots, m$. For that, we can use an algorithm that is very similar to the standard algorithm applied to all columns during the computation of the Hermite normal form (HNF) of a matrix over a PID. We find the minimal (nonzero) entry among the entries at and below the pivot, and then swap that entry up to the pivot by a row operation. We then use row operations of the add-multiple type to replace the entries below the pivot by their remainders modulo the pivot entry. (We do not care what is happening in the other columns to the right; to the left the affected entries are already zero.) We then repeat the process until it converges: find the minimal entry among those at and below the pivot, swap it into the pivot, and use it to reduce the remaining nonzero entries below the pivot. This algorithm, which is almost identical to the Euclidean algorithm for the GCD of a set of polynomials in one variable, eventually converges with a generator of the principal ideal in the pivot and zeros below the pivot. We then complete this step of the reduction of the matrix with a row operation of scalar-multiple type to make the pivot entry monic.

We then increment i and j and continue to the next iteration. □

The reduced form of the lower right block makes it much easier to compute the determinantal ideals, since so many more entries are zero. We also found

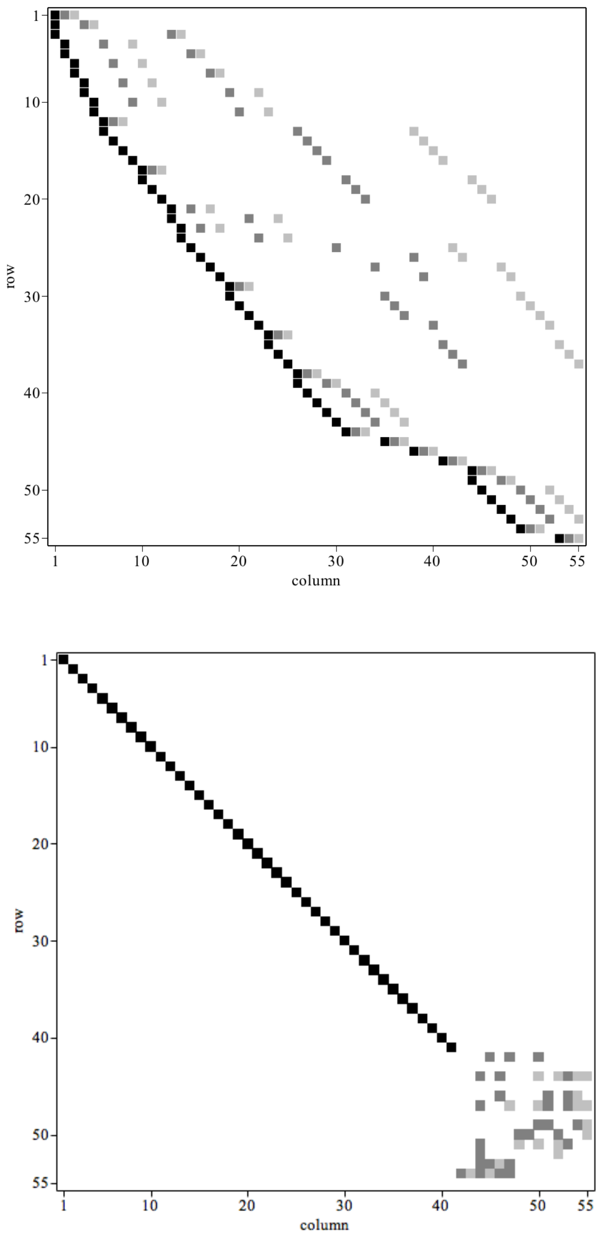


FIGURE 10.3: The relation matrix for one quadratic relation in weight 4 (top), and its partial Smith form (bottom).

to our surprise that these computations illustrate the remarkable effectiveness of the `plex` order in certain cases. We computed Gröbner bases for both the ideal and its radical, and the zero sets in both cases, for all ranks $r \leq 9$, using a Lenovo ThinkCentre. The sets of original generators of the determinantal ideals, namely the $r \times r$ minors, had the following sizes, after removing zero polynomials and making remaining polynomials monic:

$$\text{minors:} \quad 18, \;\; 123, \;\; 560, \;\; 1821, \;\; 4069, \;\; 5951, \;\; 5297, \;\; 2473, \;\; 420.$$

Using the `plex` order, the Gröbner bases of ideal and radical have these sizes:

order	ideal	radical
$a \prec b$	$3, 5, 7, 9, 11, 12, 13, 12, 12$	$3, 2, 2, 2, 2, 2, 2, 1, 2$
$b \prec a$	$4, 6, 8, 11, 13, 14, 15, 14, 14$	$3, 3, 3, 3, 3, 2, 2, 1, 2$

(Using the `glex` order took so much longer that we stopped waiting.)

We summarize the computational results about the radicals of the determinantal ideals, writing r (rank) for the size of the minors under consideration. The following list gives the `plex` order Gröbner bases ($b \prec a$) and zero sets for the radicals of the determinantal ideals of the 9×14 reduced block in arity 9. The horizontal lines separate the different zero sets, which increase (for inclusion) from top to bottom:

r	Gröbner basis of $\sqrt{DI_r(U)}$	Zero set of $\sqrt{DI_r(U)}$
1	$b(b+1), a(b+1), a(a^2+1)$	$(a,b) = (0,0), (0,-1), (\pm i, -1)$
2	$b(b+1), a(b+1), a(a^2+1)$	$(a,b) = (0,0), (0,-1), (\pm i, -1)$
3	$b(b+1), a(b+1), a(a^2+1)$	$(a,b) = (0,0), (0,-1), (\pm i, -1)$
4	$b(b+1), a(b+1), a(a^2+1)$	$(a,b) = (0,0), (0,-1), (\pm i, -1)$
5	$b(b+1), a(b+1), a(a^2+1)$	$(a,b) = (0,0), (0,-1), (\pm i, -1)$
6	$a(b+1), a(a^2+1)$	$(a,b) = (0,b), (0,-1), (\pm i, -1)$
7	$ab(b+1), a(a-1)(a+1)(b+1)$	$(a,b) = (0,b), (a,-1), (\pm 1, 0)$
8	$ab(b+1)$	$(a,b) = (0,b), (a,-1), (a,0)$
9	$ab(b+1)(b^2+b+1)$, $ab(b+1)(a^2-b)$	$(a,b) = (0,b), (a,-1), (a,0)$, (γ, γ^2) for $\gamma^2 \pm \gamma + 1 = 0$

For the solutions in row r the upper triangular block U has rank $\leq r$, and conversely, so the differences between the zero sets imply the following result:

Proposition 10.3.2.5. *The following quadratic relations produce the indicated operadic dimensions in arity 9. All other quadratic relations define operads which have dimension 5 in arity 5. None of these quadratic relations* *defines operads which become nilpotent in arity 9:*

dim $\mathcal{Q}(9)$	quadratic relation
14	$\rho = f \circ_1 f$
14	$\rho = f \circ_1 f - f \circ_3 f$
14	$\rho = f \circ_1 f \pm i f \circ_2 f - f \circ_3 f$
9	$\rho = f \circ_1 f + b\ f \circ_3 f \quad (b \in \mathbb{F} \setminus \{0, -1\})$
8	$\rho = f \circ_1 f + a\ f \circ_2 f - f \circ_3 f \quad (a \in \mathbb{F} \setminus \{0, \pm i\})$
8	$\rho = f \circ_1 f \pm f \circ_2 f$
7	$\rho = f \circ_1 f + a\ f \circ_2 f \quad (a \in \mathbb{F} \setminus \{0, \pm 1\})$
6	$\rho = f \circ_1 f + \gamma\ f \circ_2 f + \gamma^2\ f \circ_3 f \quad (\gamma^2 \pm \gamma + 1 = 0)$
5	all other quadratic relations for a ternary operation

Altogether there are ten individual operads and three one-parameter families (with exceptional points).

The proof is computational; we provide some indication of the complexity of the intermediate results. Let us consider only the last case, rank 9: altogether there are $\binom{14}{9} = 2002$ minors, but only 420 of them are nonzero and distinct up to scalar multiples. These polynomials have degrees between 28 and 35, between 22 and 71 terms, and coefficients between -798 and 777.

Exercise 10.15 suggests an open-ended research problem extending the results of this section.

10.3.2.4 Conjecture on dimension sequences

We shall conclude the discussion of nonsymmetric ternary operads with one quadratic relation with a discussion of how various methods of this book allow one to form a plausible conjecture about the set of all possible Hilbert series of such operads.

The approach we utilized in the previous sections is not feasible for weights higher than 4 (and arities greater than 9): the numbers of rows and columns in the relation matrix become too large, and so it is impractical to reduce the matrix using polynomial arithmetic with rational coefficients. One possibility to go further is to switch to modular arithmetic for the coefficients. Over the field $\mathbb{F}_p$ with p elements, the entire set of operads we consider becomes finite, consisting of p^2 elements. This means that if we are prepared to wait a few hours or perhaps days for the computation to finish, then we can obtain a comprehensive survey of the entire landscape formed by the operads that we wish to classify. We can do the same computations using different primes and compare the results; this allows us to recognize patterns that we can confirm using independent calculations with rational arithmetic.

As long as p is not too large, for each pair a, b we can compute the dimension of the operad in arity $n = 11, 13, 15, \dots$. This gives a sequence of dimensions for each pair a, b and we discover empirically that there is a very small number of distinct dimension sequences.

The first question that arises is: which prime(s) should we use? The smaller the prime, the fewer the cases, the less information, but the faster the computation. Obviously using too small a prime such as 2 or 3 would lead to too much compression of information, but using too large a prime such as 1009 would create a large amount of redundant information and waste a great deal of computer time. One hint is given by considering the symmetrizations of the corresponding operads, for which there is an action of the symmetric group S_n on each homogeneous space $\mathcal{Q}(n)$. The regular representation of S_n over $\mathbb{F}_p$ is semisimple if and only if $p > n$. The largest arity we are interested in is $n = 15$, and the smallest prime bigger than that is $p = 17$. We computed the results for $p = 17, 19, 23, 29, 31$ but we present them only for $p = 17, 19$:

			arity						
	count	%	3	5	7	9	11	13	15
$p = 17,\ p^2 = 289$	196	67.82	1	2	4	5	2	1	0
	30	10.38	1	2	4	5	3	2	1
	14	4.84	1	2	4	5	6	7	8
	14	4.84	1	2	4	7	13	24	44
	16	5.54	1	2	4	8	16	32	64
	15	5.19	1	2	4	9	21	51	127
	4	1.38	1	2	5	14	42	142	429

			arity						
	count	%	3	5	7	9	11	13	15
$p = 19,\ p^2 = 361$	258	71.47	1	2	4	5	2	1	0
	30	8.31	1	2	4	5	3	2	1
	14	3.88	1	2	4	5	6	7	8
	4	1.11	1	2	4	6	7	8	9
	16	4.43	1	2	4	7	13	24	44
	20	5.54	1	2	4	8	16	32	64
	17	4.71	1	2	4	9	21	51	127
	2	0.55	1	2	5	14	42	142	429

For $p = 17$ there are 7 distinct dimension sequences, but for $p = 19$ there are 8: every sequence for $p = 17$ occurs for $p = 19$, but the sequence 1,2,4,6,7,8,9 occurs for $p = 19$ and not for $p = 17$. Note that according to our results in Section 10.3.2.3, the only way to obtain $\dim \mathcal{Q}(9) = 6$ is for the values of parameters (γ, γ^2), where $\gamma^2 \pm \gamma + 1 = 0$. Such elements γ are 6th roots of unity which are not square roots of unity. A field $\mathbb{F}_p$ has sixth roots of unity if and only if $p \equiv 1 \pmod 6$, and this explains why we miss some information for $p = 17$. Our computations show that the results for $p = 23, 29$ resemble those for $p = 17$ but the results for $p = 31$ resemble those for $p = 19$.

Let us consider the operads corresponding to the dimension sequence

1,2,4,5,3,2,1. By a direct inspection, we note that all the corresponding solutions modulo p satisfy one of the two conditions $b = a - 1$ and $b = -a - 1$, and we conjecture that in characteristic zero these are precisely the conditions required to obtain that dimension sequence (excluding the solutions corresponding to $\dim \mathcal{Q}(9) > 5$; see Section 10.3.2.3 for the classification of those). Moreover, computer experiments in characteristic zero suggest that in this case we have $\dim \mathcal{Q}(2k+1) = 1$ for $k \geq 6$. In case $b = -a - 1$, it somewhat easy to furnish an informal justification as to why this should be the case. Since $1 + a + (-a - 1) = 0$, for each element of the operadic ideal generated by our relations, the coefficients must add up to zero. If $\dim \mathcal{Q}(15) = 1$, then the cosets of any two tree monomials of arity 15 are proportional, and the condition that the coefficients of consequences of relations add up to zero imply that all these cosets are equal. This of course implies that all cosets in each subsequent arity are equal.

Considering the other dimension sequences for $p = 19$, starting at the bottom and moving up, we are now able to form an educated guess about all the integer sequences that emerge here:

1. Catalan numbers [236, Seq. A000108]: 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, ...
2. Motzkin numbers [236, Seq. A001006]: 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, ...
3. Powers of two: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, ...
4. Tribonacci numbers [236, Seq. A000073]: 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, ...
5. All natural numbers $\neq 3, 5$: 1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, ...
6. All natural numbers $\neq 3$: 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, ...
7. Dimensions stabilizing at 1: 1, 2, 4, 5, 3, 2, 1, 1, 1, 1, ...
8. Nilpotent: 1, 2, 4, 5, 2, 1, 0, 0, 0, 0, 0, 0, ...

Overall, we we expect that the situation over an algebraically closed field of characteristic 0 will resemble that for $p \equiv 1 \pmod 6$. In particular, a large majority of the operads are nilpotent; in characteristic 0 this suggests that nilpotent operads form a Zariski open subset of the parameter space.

Characteristic 0 reconstruction of the modular results simply by inspection of the pairs of parameter values corresponding to each dimension sequence, paired with numerous characteristic zero experiments, supports the following conjecture.

Conjecture 10.3.2.6. *Over an algebraically closed field $\mathbb{F}$ of characteristic zero, there are eight possible sequences of dimensions of components of* *quadratic nonsymmetric ternary operads defined by a relation of the form*

$$f \circ_1 f + a\, f \circ_2 f + b\, f \circ_3 f = 0;$$

these eight sequences correspond to the following choices of parameters:

1.	*Catalan*	$X_1 = \{(0,0), (0,-1), (\pm i, -1)\}$
2.	*Motzkin*	$X_2 = \{(0,b)\} \setminus X_1$
3.	$2^{\text{weight}-1}$	$X_3 = \{(a,-1)\} \cup \{(\pm 1, 0)\} \setminus X_1$
4.	*Tribonacci*	$X_4 = \{(a,0)\} \setminus (X_1 \cup X_3)$
5.	$\mathbb{N} \setminus \{3,5\}$	$X_5 = \{(a,a^2)\colon a^6 = 1, a \neq \pm 1\}$
6.	$\mathbb{N} \setminus \{3\}$	$X_6 = \{(a,a^2)\} \setminus (X_1 \cup X_5)$
7.	*Stable* dim $= 1$	$X_7 = \{(a,a-1)\} \cup \{(a,-a-1)\} \setminus (X_1 \cup X_3 \cup X_5)$
8.	*Nilpotent*	$\mathbb{F}^2 \setminus (X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5 \cup X_6 \cup X_7)$

Over any field $\mathbb{F}$, nilpotent operads form a Zariski open subset

$$\mathcal{N} = \{ab(b-a^2)(b+1)(b+a+1)(b-a+1) \neq 0\}$$

in the parameter space $\mathbb{F}^2$ for all nonsymmetric ternary quadratic operads with one generator. Each such operad is nilpotent of the same index 7 (*all monomials of weight* 7 *and higher vanish*).

The first three sequences featured in this conjecture and the corresponding values of parameters are discussed in detail in Theorem 10.3.2.2 and Exercises 10.13, 10.14.

10.3.3 Relation rank 2

In this case, we shall see that it is possible to obtain a complete understanding of how the corresponding operads behave: all of them except finitely many are nilpotent, and the finitely many non-nilpotent ones behave in a somewhat similar way.

We have $\dim R = 2$ and $\dim \mathcal{Q}(5) = 1$. Let us discuss the three possible row canonical forms individually.

Case 1: A basis for R consists of these two relations:

$$f \circ_1 f \;\; + \;\; a\, f \circ_3 f, \qquad\qquad f \circ_2 f \;\; + \;\; b\, f \circ_3 f.$$

There are no duplications among the $16 = 2{\cdot}8$ consequences of these; the corresponding 16×12 relation matrix $M(a,b)$ is the first matrix in Figure 10.4. We need to determine the rank of this matrix as a function of the parameters a, b.

We first observe that $M(a,b)$ contains 11 orthogonal 1s for all a, b: every row has a leading 1, and these leading 1s occur in columns 1–11. We therefore start by computing the PSF of $M(a,b)$ by using elementary row and column operations to create a block diagonal matrix with the identity matrix I_{11} in the upper left corner; we obtain the second matrix in Figure 10.4.

$$\left[\begin{array}{cccccccccccc}
1 & . & a & . & . & . & . & . & . & . & . & . \\
1 & . & . & . & a & . & . & . & . & . & . & . \\
. & 1 & b & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & a & . & . & . \\
. & . & 1 & . & . & . & . & . & . & a & . & . \\
. & . & . & 1 & b & . & . & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . & . & . & a & . \\
. & . & . & . & 1 & . & . & . & . & . & . & a \\
. & . & . & . & . & 1 & . & a & . & . & . & . \\
. & . & . & . & . & 1 & . & . & b & . & . & . \\
. & . & . & . & . & . & 1 & b & . & . & . & . \\
. & . & . & . & . & . & 1 & . & . & b & . & . \\
. & . & . & . & . & . & . & 1 & . & . & b & . \\
. & . & . & . & . & . & . & . & 1 & . & . & b \\
. & . & . & . & . & . & . & . & . & 1 & . & a \\
. & . & . & . & . & . & . & . & . & . & 1 & b
\end{array}\right]
\xrightarrow{\text{PSF}}
\left[\begin{array}{cccccccccccc}
1 & . & . & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & . & . & . & . & . \\
. & . & . & . & . & . & . & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & . & . & . \\
. & . & . & . & . & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & . \\
. & . & . & . & . & . & . & . & . & . & . & a^3+a^2 \\
. & . & . & . & . & . & . & . & . & . & . & a^2b+ab \\
. & . & . & . & . & . & . & . & . & . & . & ab^2+b^2 \\
. & . & . & . & . & . & . & . & . & . & . & b^3+ab \\
. & . & . & . & . & . & . & . & . & . & . & .
\end{array}\right]$$

FIGURE 10.4: Rank 2, case 1: original and semi-reduced cubic relation matrices.

Since the weight 3 component of the free operad is 12-dimensional, and the matrix we obtained has 11 pivots, the corresponding operad is nilpotent of index 3 unless all the polynomials in the following ordered set vanish:

$$G \;=\; \big[\quad a^3+a^2, \quad a^2b+ab, \quad ab^2+b^2, \quad b^3+ab \quad\big]. \tag{10.8}$$

In fact G is a Gröbner basis of the ideal $I(G) \subset \mathbb{F}[a,b]$ that it generates with respect to the `glex` order with $a \prec b$. Since two elements of G have powers of the parameters as leading monomials, we know that $I(G)$ is zero-dimensional and so there are only finitely many ordered pairs (a,b) for which every element of G vanishes. Factoring the elements of G gives

$$I(G) \;=\; \big(\quad a^2(a+1), \quad ab(a+1), \quad b^2(a+1), \quad b(b^2+a) \quad\big). \tag{10.9}$$

If $a=-1$ then the first 3 elements are 0 and the fourth is $b(b^2-1)$; hence $b \in \{0,\pm1\}$. If $a \neq -1$ then we cancel $a+1$ from the first 3 elements to obtain a^2, ab, b^2; hence a and b must both be 0. Thus the only solutions are:

$$(a,b) \;=\; \big(-1,\,-1\big), \quad \big(-1,\,0\big), \quad \big(-1,\,1\big), \quad \big(0,\,0\big).$$

The ideal $I(G)$ is not radical; the `glex` Gröbner basis for $\sqrt{I(G)}$ is

$$\sqrt{I(G)} \;=\; \big(\quad a(a+1), \quad b(a+1), \quad b(b-1)(b+1) \quad\big).$$

We record the primary and prime decompositions of $I(G)$ and $\sqrt{I(G)}$:

$$I(G) \;=\; (\,a+1, b+1\,) \;\cap\; (\,a+1, b\,) \;\cap\; (\,a+1, b-1\,) \;\cap\; (\,a^2, ab, b^2\,),$$

$$\sqrt{I(G)} \;=\; (\,a+1, b+1\,) \;\cap\; (\,a+1, b\,) \;\cap\; (\,a+1, b-1\,) \;\cap\; (\,a, b\,).$$

The four ideals in these decompositions correspond in order to the solutions. All these ideals are in fact maximal except for $\langle\, a^2,\, ab,\, b^2\,\rangle$ which is primary but not prime. The two decompositions differ only in the fourth ideal: the first three solutions have multiplicity 1, but $(a, b) = (0, 0)$ has multiplicity 2.

Case 2: A basis for R consists of these two relations:

$$R_1 = f \circ_1 f \;\;+\;\; af \circ_2 f, \qquad\qquad R_2 = f \circ_3 f.$$

There is only one duplication among the 16 consequences: $R_2 \circ_5 f = f \circ_3 R_2$. Thus $R^{(3)}$ is the row space of the first matrix in Figure 10.5, where we have sorted the rows to make the matrix as upper triangular as possible. Since there is only one parameter, we calculate the HNF of this matrix, and obtain the second matrix in Figure 10.5. Since the weight 3 component of the free operad is 12-dimensional, and the matrix we obtained has 11 pivots, the corresponding operad is nilpotent of index 3 unless $a = 0$.

$$\begin{bmatrix}
1 & a & . & . & . & . & . & . & . & . & . & . \\
1 & . & . & a & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & a & . & . & . & . & . & . \\
. & . & 1 & . & . & . & a & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & . & . & . & a & . & . & . & . \\
. & . & . & . & 1 & . & . & . & a & . & . & . \\
. & . & . & . & 1 & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & a & . & . & . & . & . \\
. & . & . & . & . & . & . & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & . & . & . \\
. & . & . & . & . & . & . & . & . & 1 & a & . \\
. & . & . & . & . & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & . \\
. & . & . & . & . & . & . & . & . & . & . & 1
\end{bmatrix}
\xrightarrow{\text{HNF}}
\begin{bmatrix}
1 & . & . & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & a & . & . & . & . & . \\
. & . & . & . & . & . & . & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & . & . & . \\
. & . & . & . & . & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & . \\
. & . & . & . & . & . & . & . & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & .
\end{bmatrix}$$

FIGURE 10.5: Rank 2, case 2: original and reduced cubic relation matrices.

Case 3: A basis for $R(2)$ consists of these two monomial relations:

$$f \circ_2 f, \qquad\qquad f \circ_3 f.$$

Considering this case is left as an exercise for the reader.

Summarizing, we obtain the following result describing the arity 7 components of quotients by two quadratic relations:

Proposition 10.3.3.1. *Let $\mathcal{Q} = \mathcal{T}_{\mathcal{X}}/(R)$ be the quotient by an ideal generated* *by a set* $R = \{R_1, R_2\}$ *of two quadratic relations. Then* $\dim \mathcal{Q}(7) = 0$ *except for the following six pairs of relations* R *for which* $\dim \mathcal{Q}(7) = 1$*:*

$$\begin{aligned}
&R_1 = f \circ_1 f, \qquad R_2 = f \circ_2 f,\\
&R_1 = f \circ_1 f - f \circ_3 f, \qquad R_2 = f \circ_2 f + f \circ_3 f,\\
&R_1 = f \circ_1 f - f \circ_3 f, \qquad R_2 = f \circ_2 f - f \circ_3 f,\\
&R_1 = f \circ_1 f - f \circ_3 f, \qquad R_2 = f \circ_2 f,\\
&R_1 = f \circ_1 f, \qquad R_2 = f \circ_3 f,\\
&R_1 = f \circ_2 f, \qquad R_2 = f \circ_3 f.
\end{aligned}$$

In fact, we can progress much further, and use operadic Gröbner bases to understand the structure of the six exceptional operads we just found.

Theorem 10.3.3.2. *Let* $\mathcal{Q}$ *be one of the six operads of Proposition 10.3.3.1. Then* $\dim \mathcal{Q}(m) = 1$ *for all (odd) arities* m*. If* $\mathcal{Q}$ *is any other ternary quadratic non-symmetric operad for which* $\dim \mathcal{Q}(5) = 1$*, then* $\mathcal{Q}(m) = 0$ *for all (odd) arities* $m \geq 7$*.*

Proof. A direct computation shows that for each of those six operads, the defining relations form a Gröbner basis for the `gpathlex` order. Hence, it suffices to check that for each of these operads there is exactly one normal tree monomial of each weight, which is clear by direct inspection: for the first four operads, $((\cdots(f \circ_3 (f \circ_3 f))\cdots))$ is normal, for the fifth one, $((\cdots(f \circ_2 (f \circ_2 f))\cdots))$ is normal, and for the last operad, $((\cdots(f \circ_1 (f \circ_1 f))\cdots))$ is normal.

The second statement is trivial: we already established that for all other operads $\mathcal{Q}(7) = 0$, and hence all the subsequent components vanish. □

10.4 Further directions

In this section, we outline some further directions of study in case of non-symmetric operads with d generators of given arities $a_1, \ldots, a_d$ and r relations of given weights $w_1, \ldots, w_r$; we hope that the last two chapters of the book would encourage some readers to obtain further results of the same kind.

10.4.1 Hilbert series

The first coarse approximation to classifying operads with the given types of generators and relations is classifying possible Hilbert series of those operads.

Conjecture 10.4.1.1. *For given arities of generators* $a_1, \ldots, a_d$ *and weights* *of relations $w_1, \dots, w_r$, the set of possible Hilbert series of operads with these types of generators and relations is always finite.*

A closely related problem is to determine if there exists the "generic Hilbert series", that is if there exists a Zariski open subset in the parameter space for which all the operads have the same Hilbert series.

For Hilbert series that appear as Hilbert series of a nonsymmetric operad, it is an interesting question to determine a natural class of power series where these series belong. It is known that for nonsymmetric operads with a finite Gröbner basis, the Hilbert series is an algebraic function [148]. Algebraicity of Hilbert series seems, in the case of nonsymmetric operads, to replace rationality of Hilbert series observed in the context of graded associative algebras; for example, according to Theorem 2.5.1.5, a graded algebra with a finite Gröbner basis has a rational Hilbert series. In the case of graded algebras, it is known that the Hilbert series of an algebra with one relation is rational [9]. This suggests the following conjecture.

Conjecture 10.4.1.2. *For each nonsymmetric operad with one relation, its Hilbert series is an algebraic function.*

10.4.2 Nilpotency

One natural question arising when attempting classification results for operads with the given types of generators and relations is to find the set $\mathcal{W}_{a_1,\dots,a_d;w_1,\dots,w_r}$ of all numbers N for which there exists an operad of that type which is nilpotent of index N. Our results and conjectures would imply that $\mathcal{W}_{3;2} = \{7\}$, $\mathcal{W}_{3;2,2} = \{3\}$, $\mathcal{W}_{3;2,2,2} = \{2\}$. Whenever the corresponding set is not empty, for each of its elements N we can further ask for the subset of the parameter space consisting of those parameter values which produce operads which are nilpotent of index N. This is where computational commutative algebra enters the picture, providing another application of commutative Gröbner bases to the classification of operads.

10.5 Exercises

Exercise 10.1.

(i) Suppose that A is an associative algebra with the product

$$a_1, a_2 \mapsto \mu(a_1, a_2) = a_1 a_2.$$

Then the operation $(-,-,-)_\mu \colon A \otimes A \otimes A \to A$, $(a_1, a_2, a_3) := a_1 a_2 a_3$, makes A into a tAs_0^3-algebra.

(ii) Suppose that A is a tAs_0^3-algebra with the structure map

$$(-,-,-)\colon A\otimes A\otimes A\to A,$$

and suppose that it has a "unit element" 1 for which

$$(a,1,1)=(1,a,1)=(1,1,a)=a.$$

Then the operation $a_1 \star a_2 := (a_1,a_2,1)$ is associative, and $(a_1,a_2,a_3)=a_1\star a_2\star a_3$.

(iii) Suppose that A is a tAs_0^3-algebra with the structure map

$$(-,-,-)\colon A\otimes A\otimes A\to A.$$

Consider the vector space $\tilde{A}:=(A\otimes A)/U$, where

$$U=\mathrm{span}((a_1,a_2,a_3)\otimes a_4-a_1\otimes(a_2,a_3,a_4)\colon a_1,a_2,a_3,a_4\in A).$$

Then the vector space $B:=A\oplus\tilde{A}$ has an associative product μ, for which $(A,(-,-,-))$ is a tAs_0^3-subalgebra of $(B,(-,-,-)_\mu)$.

Exercise 10.2. Compute the Gröbner basis for the operad $\mathsf{tAs}_0^{(3)}$ for an ordering of your choice, and use it to prove that this operad is Koszul.

Exercise 10.3. Show that in the case of the free nonsymmetric operad generated by several operations of the same arity n, the arity of each tree monomial is uniquely determined by its weight: $\mathrm{ar}(T)-1=(n-1)\,\mathrm{wt}(T)$. Show that it is not true for a free nonsymmetric operad with generators of different arities.

Exercise 10.4. Show that the order of Definition 10.2.1.6 is a monomial order of the free operad $\mathcal{T}_{\mathcal{X}}$.

Exercise 10.5. Given a positive integer $n\geq 2$, classify all operads $\mathcal{O}$ with one generator of given arity n for which all components $\mathcal{O}(k(n-1)+1)$ are one-dimensional for $k\geq 1$. (Do it by hand for small n, form a conjecture, and prove it.)

Exercise 10.6. Prove Lemma 10.2.1.5. Explain the meaning of this recurrence formula in terms of composition of operations.

Exercise 10.7. Fix $n\geq 2$, and consider the operation alphabet $\mathcal{X}$ with $\mathcal{X}(n)=\{f_1\}$, $\mathcal{X}(2n-1)=\{f_2\}$, and $\mathcal{X}(k)=\varnothing$ otherwise.

(i) Show that $\mathcal{T}_{\mathcal{X}}(k)=0$ unless $k\equiv 1 \pmod{n-1}$.

(ii) The operad $\mathcal{T}_{\mathcal{X}}$ is weight bi-graded: to each tree monomial, we can associate two numbers, the number of occurrences of f_1 and the number of occurrences of f_2. Consider the three-variable generating function $f(s,t,x)$ for which the coefficient of $s^kt^lx^m$ is the number of tree monomials of weight (k,l) and arity m. Show that

$$f(s,t,x)=x+sf(s,t,x)^n+tf(s,t,x)^{2n-1}.$$

(iii) Explain why the two-variable generating function

$$g(s,x) = \frac{\partial}{\partial t} f(s,t,x)\bigg|_{t=0}$$

has, as the coefficient of $s^k x^m$ the number of weight $k+2$ consequences of a quadratic relation R in the free nonsymmetric operad generated by one n-ary operation, and show that this coefficient is equal to the binomial coefficient $\binom{n(k+2)-1}{k}$.

Exercise 10.8. Perform the row/column reduction outlined in Figure 10.1.

Exercise 10.9. Compute the `glex` Gröbner basis for the radical in rank 1, case 1.

Exercise 10.10. Suppose that $\mathcal{Q}$ is a nilpotent operad defined by the following relation:

$$\rho = a\, f \circ_1 f + b\, f \circ_2 f + c\, f \circ_3 f.$$

Prove that $a \neq 0$.

Exercise 10.11. Determine possible sequences of dimensions of components for all operads for rank 1, case 2, and rank 1, case 3.

Exercise 10.12. Let $G_n = GL_n(\mathbb{F}[a,b])$ be the group of invertible $n \times n$ matrices over $\mathbb{F}[a,b]$: the determinant must be invertible in $\mathbb{F}[a,b]$, so it is a nonzero *scalar*. Construct matrices $X \in G_{10}$ and $Y \in G_{14}$ such that $XBY = C$ where B and C are, respectively, the matrices of Figures 8.2 and 8.3. Follow the proof of Proposition 10.3.2.4.

Exercise 10.13. Show that for each $b \neq 0, -1$ the dimensions of components of the operad $\mathcal{Q}$ with one ternary generator f and one relation

$$f \circ_1 f + b\, f \circ_3 f$$

are Motzkin numbers: $\dim \mathcal{Q}(2n+1) = a_n$, where

$$a_1 = 1, \quad a_{n+1} = a_n + \sum_{p+q=n} a_p a_q.$$

Exercise 10.14.

(i) Show that for each $a \neq 0, \pm i$ the dimensions of components of the operad $\mathcal{Q}$ with one ternary generator f and one relation

$$f \circ_1 f + a\, f \circ_2 f - f \circ_3 f$$

are powers of two: $\dim \mathcal{Q}(2n+1) = 2^{n-1}$.

(ii) Show the same for the operads with one relation $f \circ_1 f \pm f \circ_2 f$.

Exercise 10.15. For arity 11 (weight 5), determine the possible ranks and the corresponding parameter values for the 364 × 273 relation matrix $[R^{(5)}]$ where R is a single quadratic relation.

Exercise 10.16. Explore Conjecture 10.3.2.6 further. Attempt to incorporate Gröbner bases for nonsymmetric operads in your investigation.

Exercise 10.17. Compute the Koszul dual of the operad with the defining relations $f \circ_1 f - f \circ_3 f$, $f \circ_2 f + f \circ_3 f$. (This Koszul dual operad appears in representation theory for the celebrated Tamari lattice [54].)

Appendix A

Maple Code for Buchberger's Algorithm

What follows is very basic Maple code designed solely to illustrate Buchberger's algorithm to compute a Gröbner basis using S-polynomials. This code has not been optimized in any way whatsoever, but minimal comments are included (both inside and outside the code) to explain its structure.

The basic idea is to start by generating random polynomials using Maple's `randpoly` function and then convert each polynomial to a list of terms, in which each term in a list of two items, a coefficient and a list of exponents. All remaining computations are done using this list structure to represent polynomials, and only very basic Maple operations are used (for instance, we never call any of the procedures from the `Groebner` package).

A.1 First block: Initialization

The first block of code sets various parameters, and includes the procedures to convert from polynomial to list and from list to polynomial. It also generates the original list `flistlist` of pseudorandom polynomials in list form.

```
# parameters for creating pseudorandom polynomials to test code

VARS  := [x,y,z]: # ordered set of variables
SIZE  := 3:       # number of polynomials to be generated
TERMS := 4:       # number of terms in each polynomial
RANGE := -2..2:   # range of coefficients in each polynomial

# procedure to convert Maple polynomial to list format in which
# each item has form term = [ coefficient, [ exponent list ] ]

polylist := proc( f )
  global VARS: local c, e, g, m, t:
  g := []:
  if f <> 0 then
```

```
    for t in convert(f,list) do
      c := coeffs(t): m := t/c:
      e := [ seq( degree(m,v), v in VARS ) ]:
      g := [ op(g), [ c, e ] ]
    od
  fi:
  return( g )
end:

# procedure to convert polynomial in list format to Maple format

listpoly := proc( f )
  global VARS:
  add( t[1] * mul( VARS[k]^t[2][k], k=1..nops(VARS) ), t in f )
end:

# generate pseudorandom polynomials using Maple's "randpoly"
# and convert pseudorandom polynomials to list format

flistpoly :=
[seq( randpoly(VARS,terms=TERMS,coeffs=rand(RANGE)),i=1..SIZE)]:
flistlist := map( polylist, flistpoly ):
```

A.2 Second block: Monomial orders

The second block of code includes the three procedures for the three standard monomial orders, and chooses one of them, called ORDER, for the rest of the worksheet.

```
# define three standard monomial orders (strict precedence)

pplex := proc( v, w ) # pure lex order
  global VARS: local i, ii:
  ii := 0:
  for i from nops(VARS) to 1 by -1 do
    if v[i] <> w[i] then ii := i fi
  od:
  if ii=0 then return false else return evalb(v[ii]<w[ii]) fi
end:

ddlex := proc( v, w ) # degree lex order
  global VARS: local i, ii, vd, wd:
```

```
  vd := add( v[i], i=1..nops(VARS) ):
  wd := add( w[i], i=1..nops(VARS) ):
  if vd < wd then return true fi:
  if vd > wd then return false fi:
  if vd = wd then
    ii := 0:
    for i from nops(VARS) to 1 by -1 do
      if v[i] <> w[i] then ii := i fi
    od:
    if ii=0 then return false else return evalb(v[ii]<w[ii]) fi
  fi
end:

gglex := proc( v, w ) # degree reverse lex order
  global VARS: local i, ii, vd, wd:
  vd := add( v[i], i=1..nops(VARS) ):
  wd := add( w[i], i=1..nops(VARS) ):
  if vd < wd then return true fi:
  if vd > wd then return false fi:
  if vd = wd then
    ii := 0:
    for i to nops(VARS) do
      if v[i] <> w[i] then ii := i fi
    od:
    if ii=0 then return false else return evalb(v[ii]>w[ii]) fi
  fi
end:

# choose monomial order to be used in this worksheet

ORDER := gglex:
```

A.3 Third block: Sorting polynomials

The third block of code includes the procedures for sorting a polynomial by decreasing order of its monomials, to compare to polynomials using the natural inductive extension of the monomial order, and to sort a list of polynomials by increasing order. It concludes by sorting the original list flistlist of pseudorandom polynomials, obtaining the same polynomials in the new double-sorted form fsortsort,

```
# procedure to sort terms of a polynomial (decreasing)
```

```
polysort := proc( f )
  global ORDER:
  sort( f, proc(x,y) not ORDER( x[2], y[2] ) end )
end:

# procedure to compare two polynomials using monomial order

polyorder := proc( f, g )
  global ORDER: local lcf, lcg, lmf, lmg:
  # consider 0 as basis of recursion, 0 precedes everything
  if f = [] then return true
  else
    if g = [] then return false
    else
      lcf, lmf := op( polysort( f )[ 1 ] ):
      lcg, lmg := op( polysort( g )[ 1 ] ):
      if lmf = lmg then
        return polyorder( f[2..nops(f)], g[2..nops(g)] )
      else
        return ORDER( lmf, lmg )
      fi
    fi
  fi
end:

# procedure to sort list of sorted polynomials (increasing)

polylistsort := proc( flist )
  sort( flist, proc(f,g) polyorder( f, g ) end )
end:

# sort original generators

flistsort := map( polysort, flistlist ):
fsortsort := polylistsort( flistsort ):
```

A.4 Fourth block: Standard forms of polynomials

In order to guarantee that the algorithm works properly, we must make sure that we retain only one representative of each equivalent class of polynomials. Two polynomials in list format are regarded as equivalent if (1) after collecting terms with the same monomial, so that each monomial appears only once, there are no zero coefficients, (2) either the two resulting polynomials are both zero, or they have the same monic form (depending on the choice of monomial order). The two procedures in this block of code implement this equivalence relation. We use the convenient but non-standard term *monicify* to represent this combined process of collecting terms and making monic.

```
# procedure to collect terms of form [ coefficient, monomial ]

compress := proc( f )
  local c, x, i, ff, fff:
  ff := copy( f ): fff := []:
  while ff <> [] do
    x := ff[ 1 ]: c := 0: i := 1:
    while i <= nops( ff ) do
      if ff[ i ][ 2 ] = x[ 2 ] then
        c := c + ff[ i ][ 1 ]:
        ff := [ op( ff[1..i-1] ), op( ff[i+1..-1] ) ]
      else
        i := i + 1
      fi
    od:
    if c <> 0 then fff := [ op( fff ), [ c, x[ 2 ] ] ] fi
  od:
  return fff
end:

# procedure to make a polynomial monic and sort its terms

monicify := proc( f )
  local ff, lc:
  ff := compress( f ):
  if ff <> [] then
    ff := polysort( ff ): lc := ff[1][1]:
    ff := [ seq( [ t[1]/lc, t[2] ], t in ff ) ]
  fi:
  return ff
end:
```

A.5 Fifth block: Reduce and self-reduce

This block contains two procedures:

- First, reduce a polynomial f with respect to a set G of other polynomials, which amounts to eliminating every occurrence of the leading monomials of elements of G as divisors of monomials in f.

- Second, self-reduce a set of polynomials, which amounts to sorting the set in increasing order, reducing each polynomial with respect to the previous ones, resorting the list, and repeating this process until it stabilizes.

```
# procedure to reduce f using generatorset; do not monicify

reducedformlist := proc( f, generatorset )
  global VARS:
  local ff,ffm,finished,found,g,generators,i,j,k,lmg,s,t,u:
  if f = [] then ff := []
  else
    ff := polysort( f ):
    generators :=
      polylistsort( map(polysort,convert(generatorset,list)) ):
    finished := false:
    while not finished do
      i := 0: found := false:
      while i < nops( ff ) and not found do
        i := i + 1: ffm := ff[i][2]: j := 0:
        while j < nops( generators ) and not found do
          j := j + 1: g := generators[j]:
          lmg := g[1][2]:
          found := true:
          for k to nops(VARS) do
            found := found and evalb( lmg[k] <= ffm[k] )
          od
        od:
        if found then
          s := ff[i][1] / g[1][1]:
          u := [ seq( ffm[k] - lmg[k], k=1..nops(VARS) ) ]:
          ff := [ op(ff), seq(
            [ -s*t[1], [ seq(t[2][k]+u[k],k=1..nops(VARS)) ] ],
            t in g ) ]:
          ff := compress( ff )
        fi
      od:
      finished := not found
    od
  fi:
  return ff
end:
```

```
# procedure to convert set of polynomials to self-reduced form

selfreduce := proc( flistlist )
  local ff, iteration, k, newflistreduced, oldflistreduced:
  iteration := 0:
  oldflistreduced := []:
  newflistreduced := polylistsort( map( polysort, flistlist ) ):
  while oldflistreduced <> newflistreduced do
    iteration := iteration + 1:
    oldflistreduced := copy(newflistreduced):
    newflistreduced := [ monicify( oldflistreduced[1] ) ]:
    for k from 2 to nops(oldflistreduced) do
      ff := reducedformlist(
              oldflistreduced[k], oldflistreduced[1..k-1] ):
      ff := monicify( ff ):
      if ff <> [] and not member( ff, newflistreduced ) then
        newflistreduced := [ op( newflistreduced ), ff ]
      fi
    od:
    newflistreduced :=
      polylistsort( map( polysort, newflistreduced ) ):
  od:
  return newflistreduced
end:
```

A.6 Sixth block: Main loop — Buchberger's algorithm

This block is the main loop of Buchberger's algorithm for computing Gröbner bases: starting with the original generators, we perform the following steps:

1. Self-reduce the generators.
2. Produce all possible S-polynomials, and reduce them with respect to the generators.
3. If every S-polynomial reduces to zero then
   - Terminate: we have a Gröbner basis.
4. Else
   - Add the nonzero S-polynomials to the set of generators, obtaining a new expanded set of generators, and return to item 1 in the loop.

```
# Buchberger's algorithm for computing a Groebner basis

oldgenerators := copy( fsortsort ):
finished := false: iteration := 0:
while not finished do
  iteration := iteration + 1:
  oldgenerators := selfreduce( oldgenerators ):
  spolynomials := table(): spcount := 0:
  for i to nops(oldgenerators) do
    gi := oldgenerators[i]: lcgi := gi[1][1]:
    for j from i to nops(oldgenerators) do
      gj := oldgenerators[j]: lcgj := gj[1][1]:
      mgcd := [ seq( min( gi[1][2][k], gj[1][2][k] ),
                k=1..nops(VARS) ) ]:
      if convert(mgcd,set) <> {0} then
        mi := [ seq( gj[1][2][k]-mgcd[k], k=1..nops(VARS) ) ]:
        mj := [ seq( gi[1][2][k]-mgcd[k], k=1..nops(VARS) ) ]:
        sp := [ seq( [  lcgj*t[1],
                [ seq( t[2][k]+mi[k], k=1..nops(VARS) ) ] ],
                t in gi ),
                seq( [ -lcgi*t[1],
                [ seq( t[2][k]+mj[k], k=1..nops(VARS) ) ] ],
                t in gj ) ]:
        sp := monicify( sp ):
        if sp <> [] then
          sp := reducedformlist( sp, oldgenerators ):
          if sp <> [] and not member( sp, spolynomials ) then
            spcount := spcount + 1:
            spolynomials[ spcount ] := sp
          fi
        fi
      fi
    od
  od:
  if spcount = 0 then finished := true fi:
  oldgenerators := [ op(oldgenerators),
                     seq( spolynomials[s], s=1..spcount ) ]:
od:
```

Bibliography

[1] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] Marcelo Aguiar and Jean-Louis Loday, *Quadri-algebras*, J. Pure Appl. Algebra **191** (2004), no. 3, 205–221.

[3] David. J. Anick, *On the homology of associative algebras*, Trans. Amer. Math. Soc. **296** (1986), no. 2, 641–659.

[4] M. Artin, J. Tate, and M. Van den Bergh, *Some algebras associated to automorphisms of elliptic curves*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 33–85.

[5] Michael Artin and William F. Schelter, *Graded algebras of global dimension* 3, Adv. in Math. **66** (1987), no. 2, 171–216.

[6] Matthias Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), no. 2, 407–441 (electronic).

[7] ______, *Bounds and definability in polynomial rings*, Q. J. Math. **56** (2005), no. 3, 263–300.

[8] Franz Baader and Tobias Nipkow, *Term rewriting and all that*, Cambridge University Press, Cambridge, 1998.

[9] J. Backelin, *La série de Poincaré–Betti d'une algèbre graduée de type fini à une relation est rationnelle*, C. R. Acad. Sci. Paris, Serie A **287** (1978), 843–846.

[10] ______, *A distributiveness property of augmented algebras, and some related homological results*, Ph.D. thesis, Stockholm University, 1983.

[11] Yuri A. Bahturin, Alexander A. Mikhalev, Viktor M. Petrogradsky, and Mikhail V. Zaicev, *Infinite-dimensional Lie superalgebras*, de Gruyter Expositions in Mathematics, vol. 7, Walter de Gruyter & Co., Berlin, 1992.

[12] M. G. Barratt, *Twisted Lie algebras*, Geometric applications of homotopy theory (Proc. Conf., Evanston, Ill., 1977), II, Lecture Notes in Math., vol. 658, Springer, Berlin, 1978, pp. 9–15.

[13] David Bayer and Michael Stillman, *On the complexity of computing syzygies*, J. Symbolic Comput. **6** (1988), no. 2-3, 135–147, Computational aspects of commutative algebra.

[14] Thomas Becker and Volker Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993, A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[15] A. A. Beĭlinson, V. A. Ginsburg, and V. V. Schechtman, *Koszul duality*, J. Geom. Phys. **5** (1988), no. 3, 317–350.

[16] F. A. Berezin, *Introduction to superanalysis*, Mathematical Physics and Applied Mathematics, vol. 9, D. Reidel Publishing Co., Inc., New York, NY, USA, 1987.

[17] Clemens Berger and Ieke Moerdijk, *On the derived category of an algebra over an operad*, Georgian Math. J. **16** (2009), no. 1, 13–28.

[18] Roland Berger, *Weakly confluent quadratic algebras*, Algebr. Represent. Theory **1** (1998), no. 3, 189–213.

[19] ______, *Koszulity for nonquadratic algebras*, J. Algebra **239** (2001), no. 2, 705–734.

[20] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial species and tree-like structures*, Encyclopedia of Mathematics and its Applications, vol. 67, Cambridge University Press, Cambridge, 1998, Translated from the 1994 French original by Margaret Readdy, With a foreword by Gian-Carlo Rota.

[21] George M. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29** (1978), no. 2, 178–218.

[22] I. N. Bernšteĭn, I. M. Gel′fand, and S. I. Gel′fand, *Algebraic vector bundles on* $\mathbf{P}^n$ *and problems of linear algebra*, Funktsional. Anal. i Prilozhen. **12** (1978), no. 3, 66–67.

[23] L. Bokut′ and P. Malcolmson, *Gröbner-Shirshov bases for quantum enveloping algebras*, Israel J. Math. **96** (1996), no. part A, 97–113.

[24] L. A. Bokut′, *Imbeddings into simple associative algebras*, Algebra i Logika **15** (1976), no. 2, 117–142, 245.

[25] L. A. Bokut′, Yu. Chen, and Sh. Den, *Gröbner-Shirshov bases for Rota-Baxter algebras*, Sibirsk. Mat. Zh. **51** (2010), no. 6, 1237–1250.

[26] L. A. Bokut′, Yuĭtsyun′ Chèn′, and Yuĭ Li, *Gröbner-Shirshov bases Vinberg-Koszul-Gerstenhaber for right-symmetric algebras*, Fundam. Prikl. Mat. **14** (2008), no. 8, 55–67.

[27] L. A. Bokut′, Yuqun Chen, and Yongshan Chen, *Gröbner-Shirshov bases for Lie algebras over a commutative algebra*, J. Algebra **337** (2011), 82–102.

[28] L. A. Bokut′, Yuqun Chen, and Jiapeng Huang, *Gröbner-Shirshov bases for L-algebras*, Internat. J. Algebra Comput. **23** (2013), no. 3, 547–571.

[29] L. A. Bokut′, Yuqun Chen, and Cihua Liu, *Gröbner-Shirshov bases for dialgebras*, Internat. J. Algebra Comput. **20** (2010), no. 3, 391–415.

[30] L. A. Bokut′, Yuqun Chen, and Jianjun Qiu, *Gröbner-Shirshov bases for associative algebras with multiple operators and free Rota-Baxter algebras*, J. Pure Appl. Algebra **214** (2010), no. 1, 89–100.

[31] L. A. Bokut′, Y. Fong, and W.-F. Ke, *Composition-diamond lemma for associative conformal algebras*, J. Algebra **272** (2004), no. 2, 739–774.

[32] L. A. Bokut′, Yu. Fong, V.-F. Ke, and P. S. Kolesnikov, *Gröbner and Gröbner-Shirshov bases in algebra, and conformal algebras*, Fundam. Prikl. Mat. **6** (2000), no. 3, 669–706.

[33] L. A. Bokut′ and A. A. Klein, *Serre relations and Gröbner-Shirshov bases for simple Lie algebras. I, II*, Internat. J. Algebra Comput. **6** (1996), no. 4, 389–400, 401–412.

[34] L. A. Bokut′ and P. S. Kolesnikov, *Gröbner-Shirshov bases: from inception to the present time*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **272** (2000), no. Vopr. Teor. Predst. Algebr i Grupp. 7, 26–67, 345.

[35] L. A. Bokut' and L. G. Makar-Limanov, *Basis of a free metabelian associative algebra*, Siberian Math. J. **32** (1991), no. 6, 910–915.

[36] L. A. Bokut′ and I. P. Shestakov, *Some results by A. I. Shirshov and his school*, Second International Conference on Algebra (Barnaul, 1991), Contemp. Math., vol. 184, Amer. Math. Soc., Providence, RI, 1995, pp. 1–12.

[37] L. A. Bokut′ and L.-S. Shiao, *Gröbner-Shirshov bases for Coxeter groups*, Comm. Algebra **29** (2001), no. 9, 4305–4319, Special issue dedicated to Alexei Ivanovich Kostrikin.

[38] Adam Boocher, *Free resolutions and sparse determinantal ideals*, Math. Res. Lett. **19** (2012), no. 4, 805–821.

[39] Armand Borel, *Essays in the history of Lie groups and algebraic groups*, History of Mathematics, vol. 21, American Mathematical Society, Providence, RI; London Mathematical Society, Cambridge, 2001.

[40] Murray R. Bremner, *How to compute the Wedderburn decomposition of a finite-dimensional associative algebra*, Groups Complex. Cryptol. **3** (2011), no. 1, 47–66.

[41] ______, *Lattice basis reduction*, Pure and Applied Mathematics (Boca Raton), vol. 300, CRC Press, Boca Raton, FL, 2012, An introduction to the LLL algorithm and its applications. MR 2829731 (2012h:06001)

[42] Murray R. Bremner and Vladimir Dotsenko, *Classification of regular parametrized one-relation operads*, arXiv:math/1507.06372.

[43] Murray R. Bremner and Juana Sánchez-Ortega, *Quadratic nonsymmetric quaternary operads*, arXiv:math/1512.02880.

[44] B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner-bases*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin-New York, 1979, pp. 3–21.

[45] B. Buchberger, G. E. Collins, and B. Kutzler, *Algebraic methods for geometric reasoning*, Annual review of computer science, vol. 3, Annual Reviews, Palo Alto, CA, 1988, pp. 85–119.

[46] Bruno Buchberger, *History and basic features of the critical-pair/completion procedure*, J. Symbolic Comput. **3** (1987), no. 1-2, 3–38, Rewriting techniques and applications (Dijon, 1985).

[47] ______, *Applications of Gröbner bases in nonlinear computational geometry*, Mathematical aspects of scientific software (Minneapolis, Minn., 1986/87), IMA Vol. Math. Appl., vol. 14, Springer, New York, 1988, pp. 59–87.

[48] ______, *An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symbolic Comput. **41** (2006), no. 3-4, 475–511, Translated from the 1965 German original by Michael P. Abramson.

[49] ______, *Comments on the translation of my PhD thesis: "An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal"*, J. Symbolic Comput. **41** (2006), no. 3-4, 471–474.

[50] Renate Carlsson, *n-ary algebras*, Nagoya Math. J. **78** (1980), 45–56.

[51] P. Cartier, *Remarques sur le théorème de Birkhoff-Witt*, Ann. Scuola Norm. Sup. Pisa (3) **12** (1958), 1–4.

[52] Frédéric Chapoton, *Un théorème de Cartier–Milnor–Moore–Quillen pour les bigèbres dendriformes et les algèbres braces*, J. Pure Appl. Alg. **168** (2002), no. 1, 1–18.

[53] ———, *Free pre-Lie algebras are free as Lie algebras*, Canad. Math. Bull. **53** (2010), no. 3, 425–437.

[54] ———, *Sur une opérade ternaire liée aux treillis de Tamari*, Ann. Fac. Sci. Toulouse Math. (6) **20** (2011), no. 4, 843–869.

[55] Vyjayanthi Chari and Andrew Pressley, *A guide to quantum groups*, Cambridge University Press, Cambridge, 1994.

[56] Yuqun Chen and Bin Wang, *Gröbner-Shirshov bases and Hilbert series of free dendriform algebras*, Southeast Asian Bull. Math. **34** (2010), no. 4, 639–650.

[57] Ivan Cherednik, *Double affine Hecke algebras*, London Mathematical Society Lecture Note Series, vol. 319, Cambridge University Press, Cambridge, 2005.

[58] Shang-Ching Chou, *Mechanical geometry theorem proving*, Mathematics and its Applications, vol. 41, D. Reidel Publishing Co., Dordrecht, 1988, With a foreword by Larry Wos.

[59] Alonzo Church and J. B. Rosser, *Some properties of conversion*, Trans. Amer. Math. Soc. **39** (1936), no. 3, 472–482.

[60] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups. Vol. I*, Mathematical Surveys, No. 7, American Mathematical Society, Providence, R.I., 1961.

[61] D. A. Cohen and E. A. Scott, *Rationality of division orderings*, Inform. Process. Lett. **44** (1992), no. 6, 307–311.

[62] P. M. Cohn, *A remark on the Birkhoff-Witt theorem*, J. London Math. Soc. **38** (1963), 197–203.

[63] ———, *Universal algebra*, Harper & Row, Publishers, New York-London, 1965.

[64] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992, An introduction to computational algebraic geometry and commutative algebra.

[65] ———, *Using algebraic geometry*, Graduate Texts in Mathematics, vol. 185, Springer-Verlag, New York, 1998.

[66] P. Diaconis, R. L. Graham, and B. Sturmfels, *Primitive partition identities*, Combinatorics, Paul Erdős is eighty, Vol. 2 (Keszthely, 1993), Bolyai Soc. Math. Stud., vol. 2, János Bolyai Math. Soc., Budapest, 1996, pp. 173–192.

[67] V. Dotsenko and M. Vejdemo Johansson, *Operadic Gröbner bases: an implementation*, Mathematical Software – ICMS 2010, Third International Congress on Mathematical Software, Kobe, Japan, September 13-17, 2010. Proceedings., Lect. Notes in Comp. Sci., vol. 6327, 2010, pp. 249–252.

[68] ______, *Implementing Gröbner bases for operads*, Operads 2009, Sémin. Congr., vol. 26, 2011, pp. 77–98.

[69] Vladimir Dotsenko, *An operadic approach to deformation quantization of compatible Poisson brackets. I*, J. Gen. Lie Theory Appl. **1** (2007), no. 2, 107–115 (electronic).

[70] ______, *Compatible associative products and trees*, Algebra Number Theory **3** (2009), no. 5, 567–586.

[71] ______, *Dual alternative algebras in characteristic three*, Comm. Algebra **42** (2014), no. 5, 1911–1920.

[72] Vladimir Dotsenko and James Griffin, *Cacti and filtered distributive laws*, Algebr. Geom. Topol. **14** (2014), no. 6, 3185–3225.

[73] Vladimir Dotsenko and Anton Khoroshkin, *Character formulas for the operad of a pair of compatible brackets and for the bi-Hamiltonian operad*, Funktsional. Anal. i Prilozhen. **41** (2007), no. 1, 1–22, 96.

[74] ______, *Gröbner bases for operads*, Duke Math. J. **153** (2010), no. 2, 363–396.

[75] ______, *Quillen homology for operads via Gröbner bases*, Documenta Math. **18** (2013), 707–747.

[76] ______, *Shuffle algebras, homology, and consecutive pattern avoidance*, Algebra Number Theory **7** (2013), no. 3, 673–700.

[77] Vladimir Dotsenko, Martin Markl, and Elisabeth Remm, *Limits of applicability of the Ginzburg–Kapranov criterion for operads*, in preparation.

[78] Vladimir Dotsenko and Bruno Vallette, *Higher Koszul duality for associative algebras*, Glasgow Math. J. **55** (2013), no. A, 55–74.

[79] V. Drensky and R. La Scala, *Gröbner bases of ideals invariant under endomorphisms*, J. Symbolic Comput. **41** (2006), no. 7, 835–846.

[80] Vesselin Drensky and Ralf Holtkamp, *Planar trees, free nonassociative algebras, invariants, and elliptic integrals*, Algebra Discrete Math. (2008), no. 2, 1–41.

[81] G. C. Drummond-Cole and B. Vallette, *The minimal model for the Batalin–Vilkovisky operad*, Selecta Math. (N.S.) **19** (2013), no. 1, 1–47.

[82] A. Dzhumadil'daev and P. Zusmanovich, *The alternative operad is not Koszul*, Exp. Math. **20** (2011), no. 2, 138–144.

[83] J. A. Eagon and D. G. Northcott, *On the Buchsbaum-Eisenbud theory of finite free resolutions*, J. Reine Angew. Math. **262/263** (1973), 205–219, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday.

[84] Samuel Eilenberg, *Extensions of general algebras*, Ann. Soc. Polon. Math. **21** (1948), 125–134.

[85] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[86] David Eisenbud, Irena Peeva, and Bernd Sturmfels, *Non-commutative Gröbner bases for commutative algebras*, Proc. Amer. Math. Soc. **126** (1998), no. 3, 687–691.

[87] Hader A. Elgendy, *Universal associative envelopes of nonassociative triple systems*, Comm. Algebra **42** (2014), no. 4, 1785–1810.

[88] Sergi Elizalde and Marc Noy, *Consecutive patterns in permutations*, Adv. in Appl. Math. **30** (2003), no. 1-2, 110–125, Formal power series and algebraic combinatorics (Scottsdale, AZ, 2001).

[89] P. Etingof, J. Kim, and X. Ma, *On universal Lie nilpotent associative algebras*, J. Algebra **321** (2009), 697–703.

[90] Pavel Etingof and Olivier Schiffmann, *Lectures on quantum groups*, Lectures in Mathematical Physics, International Press, Boston, MA, 1998.

[91] Trevor Evans, *The word problem for abstract algebras*, J. London Math. Soc. **26** (1951), 64–71.

[92] B. Feigin and B. Shoikhet, *On* $[A,A]/[A,[A,A]]$ *and on a* W_n*-action on the consecutive commutators of free associative algebras*, Math. Res. Lett. **14** (2007), no. 5, 781–795.

[93] Alfredo Ferro and Giovanni Gallo, *Automated theorem proving in elementary geometry*, Matematiche (Catania) **43** (1988), no. 1-2, 195–224 (1990).

[94] Dominique Foata and Marcel-P. Schützenberger, *Théorie géométrique des polynômes eulériens*, Lecture Notes in Mathematics, Vol. 138, Springer-Verlag, Berlin-New York, 1970.

[95] Lance Fortnow, *The status of the P versus NP problem*, Commun. ACM **52** (2009), no. 9, 78–86.

[96] William Fulton, *Young tableaux*, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997, With applications to representation theory and geometry.

[97] William Fulton and Joe Harris, *Representation theory: a first course*, Graduate texts in mathematics, vol. 129, Springer-Verlag, 2004.

[98] Michael R. Garey and David S. Johnson, *Computers and intractability*, W. H. Freeman and Co., San Francisco, Calif., 1979, A guide to the theory of NP-completeness, A Series of Books in the Mathematical Sciences.

[99] Lothar Gerritzen, *Tree polynomials and non-associative Gröbner bases*, J. Symbolic Comput. **41** (2006), no. 3-4, 297–316.

[100] Murray Gerstenhaber, *The cohomology structure of an associative ring*, Ann. of Math. (2) **78** (1963), 267–288.

[101] E. Getzler, *Two-dimensional topological gravity and equivariant cohomology*, Comm. Math. Phys. **163** (1994), no. 3, 473–489. MR 1284793 (95h:81100)

[102] ———, *Operads and moduli spaces of genus* 0 *Riemann surfaces*, The moduli space of curves (Texel Island, 1994), Progr. Math., vol. 129, Birkhäuser Boston, Boston, MA, 1995, pp. 199–230. MR 1363058 (96k:18008)

[103] Antonio Giambruno and Mikhail Zaicev, *Polynomial identities and asymptotic methods*, Mathematical Surveys and Monographs, vol. 122, American Mathematical Society, Providence, RI, 2005.

[104] V. Ginzburg, *Calabi–Yau algebras*, arXiv:math/0612139.

[105] Victor Ginzburg and Mikhail Kapranov, *Koszul duality for operads*, Duke Math. J. **76** (1994), no. 1, 203–272.

[106] Victor Ginzburg and Travis Schedler, *Differential operators and BV structures in noncommutative geometry*, Selecta Math. (N.S.) **16** (2010), no. 4, 673–730.

[107] N. M. Gjunter, *A note concerning E. Delassus memoir entitled: Extension of Cauchy's theorem to more general systems of partial differential equations*, Izdanie Inst. Inž. Putej Soobščenija Imp. Al. I. **80** (1910), 1–2.

[108] ———, *On the canonical form of systems of homogeneous equations*, Izdanie Inst. Inž. Putej Soobščenija Imp. Al. I. **84** (1913), 1–22.

[109] ———, *Sur les modules des formes algébriques*, Trav. Inst. Math. Tbilissi [Trudy Tbiliss. Mat. Inst.] **9** (1941), 97–206.

[110] C. M. Glennie, *Some identities valid in special Jordan algebras but not valid in all Jordan algebras*, Pacific J. Math. **16** (1966), 47–59. MR 0186708 (32 #4166)

[111] ———, *Identities in Jordan algebras*, Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967), Pergamon, Oxford, 1970, pp. 307–313. MR 0255629 (41 #289)

[112] Allahtan Victor Gnedbaye, *Les algèbres k-aires et leurs opérades*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 2, 147–152.

[113] ———, *Sur l'homologie des algèbres de Leibniz, opérades des algèbres k-aires*, Prépublication de l'Institut de Recherche Mathématique Avancée [Prepublication of the Institute of Advanced Mathematical Research], 1995/22, Université Louis Pasteur, Département de Mathématique, Institut de Recherche Mathématique Avancée, Strasbourg, 1995, Thèse, Université de Strasbourg I (Louis Pasteur), Strasbourg, 1995.

[114] ———, *Opérades des algèbres $(k+1)$-aires*, Operads: Proceedings of Renaissance Conferences (Hartford, CT/Luminy, 1995), Contemp. Math., vol. 202, Amer. Math. Soc., Providence, RI, 1997, pp. 83–113.

[115] Allahtan Victor Gnedbaye and Marc Wambst, *Jordan triples and operads*, J. Algebra **231** (2000), no. 2, 744–757.

[116] P. Gordan, *Les invariants des formes binaires*, Journal de Mathématiques Pures et Appliquées (1900), no. 6, 141–156.

[117] Iain G. Gordon, *Symplectic reflection algebras*, Trends in representation theory of algebras and related topics, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2008, pp. 285–347.

[118] ———, *Rational Cherednik algebras*, Proceedings of the International Congress of Mathematicians. Volume III, Hindustan Book Agency, New Delhi, 2010, pp. 1209–1225.

[119] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science.

[120] Hans Grauert, *Über die Deformation isolierter Singularitäten analytischer Mengen*, Invent. Math. **15** (1972), 171–198.

[121] Ed Green, Teo Mora, and Victor Ufnarovski, *The non-commutative Gröbner freaks*, Symbolic rewriting techniques (Ascona, 1995), Progr. Comput. Sci. Appl. Logic, vol. 15, Birkhäuser, Basel, 1998, pp. 93–104.

[122] Pierre-Paul Grivel, *Une histoire du théorème de Poincaré-Birkhoff-Witt*, Expo. Math. **22** (2004), no. 2, 145–184.

[123] Wolfgang Gröbner, *Über die algebraischen Eigenschaften der Integrale von linearen Differentialgleichungen mit konstanten Koeffizienten*, Monatsh. Math. Phys. **47** (1939), no. 1, 247–284.

[124] Yves Guiraud, Eric Hoffbeck, and Philippe Malbos, *Linear polygraphs and Koszulity of algebras*, arXiv:math/1406.0815.

[125] Thomas Hawkins, *Emergence of the theory of Lie groups*, Sources and Studies in the History of Mathematics and Physical Sciences, Springer-Verlag, New York, 2000, An essay in the history of mathematics 1869–1926.

[126] Ji-Wei He and Di-Ming Lu, *Higher Koszul algebras and A-infinity algebras*, J. Algebra **293** (2005), no. 2, 335–362.

[127] Lars Hellström, *Rewriting in operads and PROPs*, J. Nonlinear Math. Phys. **13** (2006), no. suppl. 1, 66–75.

[128] Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), no. 1, 736–788.

[129] ______, *The question of finitely many steps in polynomial ideal theory*, SIGSAM Bull. **32** (1998), no. 3, 8–30.

[130] José A. Hermida-Alonso, *On linear algebra over commutative rings*, Handbook of algebra, vol. 3, North-Holland, Amsterdam, 2003, pp. 3–61.

[131] Susan Hermiller and Jon McCammond, *Noncommutative Gröbner bases for the commutator ideal*, Internat. J. Algebra Comput. **16** (2006), no. 1, 187–202.

[132] Susan M. Hermiller, Xenia H. Kramer, and Reinhard C. Laubenbacher, *Monomial orderings, rewriting systems, and Gröbner bases for the commutator ideal of a free algebra*, J. Symbolic Comput. **27** (1999), no. 2, 133–141.

[133] David Hilbert, *Hilbert's invariant theory papers*, Lie Groups: History, Frontiers and Applications, VIII, Math Sci Press, Brookline, Mass., 1978, Translated from the German by Michael Ackerman, With comments by Robert Hermann.

[134] Heisuke Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II*, Ann. of Math. (2) **79** (1964), 109–203; ibid. (2) **79** (1964), 205–326.

[135] Eric Hoffbeck, *A Poincaré-Birkhoff-Witt criterion for Koszul operads*, Manuscripta Math. **131** (2010), no. 1-2, 87–110.

[136] Kenneth Hoffman and Ray Kunze, *Linear algebra*, Second edition, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1971.

[137] Mark Hovey, Brooke Shipley, and Jeff Smith, *Symmetric spectra*, J. Amer. Math. Soc. **13** (2000), no. 1, 149–208.

[138] Gérard Huet, *Confluent reductions: abstract properties and applications to term rewriting systems*, J. Assoc. Comput. Mach. **27** (1980), no. 4, 797–821.

[139] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho, *Splitting full matrix algebras over algebraic number fields*, J. Algebra **354** (2012), 211–223.

[140] Natalia Iyudu and Stanislav Shkarin, *Three dimensional Sklyanin algebras and Gröbner bases*, Preprint IHES M/14/35, 2014.

[141] S. A. Joni, *The multi-indexed partitional*, Discrete Math. **26** (1979), no. 2, 145–163.

[142] André Joyal, *Foncteurs analytiques et espèces de structures*, Combinatoire énumérative (Montreal, Que., 1985/Quebec, Que., 1985), Lecture Notes in Math., vol. 1234, Springer, Berlin, 1986, pp. 126–159.

[143] Alexei Kanel-Belov and Louis Halle Rowen, *Computational aspects of polynomial identities*, Research Notes in Mathematics, vol. 9, A K Peters, Ltd., Wellesley, MA, 2005.

[144] Deepak Kapur, *Using Gröbner bases to reason about geometry problems*, J. Symbolic Comput. **2** (1986), no. 4, 399–408.

[145] Richard M. Karp, *Reducibility among combinatorial problems*, Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, NY, 1972), Plenum, New York, 1972, pp. 85–103.

[146] Hans Kellerer, Ulrich Pferschy, and David Pisinger, *Knapsack problems*, Springer-Verlag, Berlin, 2004.

[147] A. Khoroshkin, *Koszul operads and distributive lattices*, Preprint ITEP-TH-24/06, 2006.

[148] Anton Khoroshkin and Dmitri Piontkovski, *On generating series of finitely presented operads*, J. of Algebra **426** (2015), 377–429.

[149] Sergey Kitaev, *Patterns in permutations and words*, Monographs in Theoretical Computer Science. An EATCS Series, Springer, Heidelberg, 2011, With a foreword by Jeffrey B. Remmel.

[150] Donald E. Knuth and Peter B. Bendix, *Simple word problems in universal algebras*, Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967), Pergamon, Oxford, 1970, pp. 263–297.

[151] Yuji Kobayashi, *Complete rewriting systems and homology of monoid algebras*, J. Pure Appl. Alg. **65** (1990), no. 3, 263–275.

[152] P. Kolesnikov, *Gröbner–Shirshov bases for pre-associative algebras*, arXiv:1509.06860.

[153] C. Kollreider and B. Buchberger, *An improved algorithmic construction of Gröbner-bases for polynomial ideals*, SIGSAM Bull. **12** (1978), no. 2, 27–36.

[154] M. Kontsevich and Yu. Manin, *Gromov-Witten classes, quantum cohomology, and enumerative geometry*, Comm. Math. Phys. **164** (1994), no. 3, 525–562. MR 1291244 (95i:14049)

[155] ———, *Quantum cohomology of a product*, Invent. Math. **124** (1996), no. 1-3, 313–339, With an appendix by R. Kaufmann. MR 1369420 (97e:14064)

[156] ———, *Relations between the correlators of the topological sigma-model coupled to gravity*, Comm. Math. Phys. **196** (1998), no. 2, 385–398. MR 1645019 (99k:14040)

[157] Maxim Kontsevich, *Feynman diagrams and low-dimensional topology*, First European Congress of Mathematics, Vol. II (Paris, 1992), Progr. Math., vol. 120, Birkhäuser, Basel, 1994, pp. 97–121. MR 1341841 (96h:57027)

[158] ———, *Operads and motives in deformation quantization*, Lett. Math. Phys. **48** (1999), no. 1, 35–72, Moshé Flato (1937–1998). MR 1718044 (2000j:53119)

[159] Bertram Kostant, *Graded manifolds, graded Lie theory, and prequantization*, Differential Geometrical Methods in Mathematical Physics, Lecture Notes in Mathematics, vol. 570, Springer, Berlin Heidelberg, 1977, pp. 177–306.

[160] D. Krakowski and A. Regev, *The polynomial identities of the Grassmann algebra*, Trans. Amer. Math. Soc. **181** (1973), 429–438.

[161] Henning Krause, *The artinian conjecture (following Djament, Putman, Sam, and Snowden)*, Proceedings of the 47th Symposium on Ring Theory and Representation Theory, Symp. Ring Theory Represent. Theory Organ. Comm., Okayama, 2015, pp. 104–111. MR 3363953

[162] Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra. 1*, Springer-Verlag, Berlin, 2000.

[163] ———, *Computational commutative algebra. 2*, Springer-Verlag, Berlin, 2005.

[164] B. Kutzler and S. Stifter, *On the application of Buchberger's algorithm to automated geometry theorem proving*, J. Symbolic Comput. **2** (1986), no. 4, 389–397.

[165] Larry A. Lambe, *Resolutions via homological perturbation*, J. Symb. Comp. **12** (1991), no. 1, 71–87.

[166] V. N. Latyshev, *Algebras with identical relations*, Dokl. Akad. Nauk SSSR **146** (1962), 1003–1006.

[167] ———, *Combinatorial ring theory. standard bases.*, Izdatel′stvo MGU, 1988.

[168] Daniel Lazard, *Algèbre linéaire sur* $K[X_1, \cdots, X_n]$*, et élimination*, Bull. Soc. Math. France **105** (1977), no. 2, 165–190.

[169] ———, *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations*, Computer algebra (London, 1983), Lecture Notes in Comput. Sci., vol. 162, Springer, Berlin, 1983, pp. 146–156.

[170] M. Lazard, *Sur les algèbres enveloppantes universelles de certaines algèbres de Lie*, Publ. Sci. Univ. Alger. Sér. A. **1** (1954), 281–294 (1955).

[171] D. A. Leites, *Introduction to the theory of supermanifolds*, Russian Mathematical Surveys **35** (1980), no. 1, 1–64.

[172] David Lissner, *Matrices over polynomial rings*, Trans. Amer. Math. Soc. **98** (1961), 285–305.

[173] Jean-Louis Loday, *Une version non commutative des algèbres de Lie: les algèbres de Leibniz*, Enseign. Math. (2) **39** (1993), no. 3-4, 269–293.

[174] ———, *La renaissance des opérades*, Séminaire Bourbaki **37** (1994-1995), 47–74.

[175] ———, *Dialgebras*, Dialgebras and related operads, Lecture Notes in Math., vol. 1763, Springer, Berlin, 2001, pp. 7–66.

[176] ———, *Completing the operadic butterfly*, Georgian Math. J. **13** (2006), no. 4, 741–749.

[177] ———, *Generalized bialgebras and triples of operads*, Astérisque (2008), no. 320, x+116.

[178] Jean-Louis Loday and María Ronco, *Algèbres de Hopf colibres*, C. R. Math. Acad. Sci. Paris **337** (2003), no. 3, 153–158.

[179] ———, *Trialgebras and families of polytopes*, Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic K-theory, Contemp. Math., vol. 346, Amer. Math. Soc., Providence, RI, 2004, pp. 369–398.

[180] Jean-Louis Loday and Bruno Vallette, *Algebraic operads*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 346, Springer, Heidelberg, 2012.

[181] F. S. MacAulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. **S2-26** (1927), no. 1, 531–555.

[182] Sara Madariaga, *Gröbner-Shirshov bases for the non-symmetric operads of dendriform algebras and quadri-algebras*, J. Symbolic Comput. **60** (2014), 1–14.

[183] Martin Markl, *Distributive laws and Koszulness*, Ann. Inst. Fourier (Grenoble) **46** (1996), no. 2, 307–323.

[184] ———, *Models for operads*, Comm. Algebra **24** (1996), no. 4, 1471–1500.

[185] Martin Markl and Elisabeth Remm, *Algebras with one operation including Poisson and other Lie-admissible algebras*, J. Algebra **299** (2006), no. 1, 171–189.

[186] ———, *(Non-)Koszulness of operads for n-ary algebras, galgalim and other curiosities*, Journal of Homotopy and Related Structures (2014), 1–31 (English).

[187] Martin Markl, Steve Shnider, and Jim Stasheff, *Operads in algebra, topology and physics*, Mathematical Surveys and Monographs, vol. 96, American Mathematical Society, Providence, RI, 2002.

[188] Silvano Martello and Paolo Toth, *Knapsack problems*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Ltd., Chichester, 1990, Algorithms and computer implementations.

[189] Ursula Martin, *On the diversity of orderings on strings*, Fund. Inform. **24** (1995), no. 1-2, 25–46.

[190] Ursula Martin and Elizabeth Scott, *The order types of termination orderings on monadic terms, strings and multisets*, Eighth Annual IEEE Symposium on Logic in Computer Science (Montreal, PQ, 1993), IEEE Comput. Soc. Press, Los Alamitos, CA, 1993, pp. 356–363.

[191] ———, *The order types of termination orderings on monadic terms, strings and multisets*, J. Symbolic Logic **62** (1997), no. 2, 624–635.

[192] J. P. May, *The geometry of iterated loop spaces*, Springer-Verlag, Berlin, 1972, Lectures Notes in Mathematics, Vol. 271.

[193] ———, *Operads, algebras and modules*, Operads: Proceedings of Renaissance Conferences (Hartford, CT/Luminy, 1995), Contemp. Math., vol. 202, Amer. Math. Soc., Providence, RI, 1997, pp. 15–31.

[194] Ernst W. Mayr and Albert R. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals*, Adv. in Math. **46** (1982), no. 3, 305–329.

[195] Bernard R. McDonald, *Linear algebra over commutative rings*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 87, Marcel Dekker, Inc., New York, 1984.

[196] S. A. Merkulov, *Lectures on PROPs, Poisson geometry and deformation quantization*, Poisson Geometry in Mathematics and Physics (International Conference, June 5-9, 2006, Tokyo, Japan), Contemp. Math., vol. 450, Amer. Math. Soc., Providence, RI, 2008, pp. 223–258.

[197] Alexander A. Mikhalev and Andrej A. Zolotykh, *Combinatorial aspects of Lie superalgebras*, CRC Press, Boca Raton, FL, 1995, With 1 IBM-PC floppy disk (3.5 inch; HD).

[198] ———, *Standard Gröbner-Shirshov bases of free algebras over rings. I. Free associative algebras*, Internat. J. Algebra Comput. **8** (1998), no. 6, 689–726.

[199] John W. Milnor and John C. Moore, *On the structure of Hopf algebras*, Ann. of Math. (2) **81** (1965), 211–264.

[200] Rosa M. Miró-Roig, *Determinantal ideals*, Progress in Mathematics, vol. 264, Birkhäuser Verlag, Basel, 2008.

[201] H. Michael Möller and Ferdinando Mora, *New constructive methods in classical ideal theory*, J. Algebra **100** (1986), no. 1, 138–178.

[202] Ian M. Musson, *Lie superalgebras and enveloping algebras*, Graduate Studies in Mathematics, vol. 131, American Mathematical Society, Providence, RI, 2012.

[203] R. Nagpal, Steven V. Sam, and Andrew Snowden, *Noetherianity of some degree two twisted commutative algebras*, arXiv:1501.06925.

[204] M. H. A. Newman, *On theories with a combinatorial definition of "equivalence"*, Ann. of Math. (2) **43** (1942), 223–243.

[205] J. Marshall Osborn, *Varieties of algebras*, Advances in Math. **8** (1972), 163–369 (1972).

[206] Samuel M. H. W. Perlo-Freeman and Péter Pröhle, *Scott's conjecture is true, position sensitive weights*, Proceedings of the 8th International Conference on Rewriting Techniques and Applications, RTA '97, 1997, pp. 217–227.

[207] Alexander Polishchuk and Leonid Positselski, *Quadratic algebras*, University Lecture Series, vol. 37, American Mathematical Society, Providence, RI, 2005.

[208] Emil L. Post, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208–350.

[209] Dag Prawitz, *An improved proof procedure*, Theoria (Lund) **26** (1960), 102–139.

[210] Stewart B. Priddy, *Koszul resolutions*, Trans. Amer. Math. Soc. **152** (1970), 39–60.

[211] Daniel Quillen, *Projective modules over polynomial rings*, Invent. Math. **36** (1976), 167–171.

[212] Saeed Rajaee, *Non-associative Gröbner bases*, J. Symbolic Comput. **41** (2006), no. 8, 887–904.

[213] T. Recio and M. P. Vélez, *Automatic discovery of theorems in elementary geometry,* J. Automat. Reason. **23** (1999), no. 1, 63–82.

[214] Tomas Recio, Hans Sterk, and M. Pilar Vélez, *Automatic geometry theorem proving*, Some tapas of computer algebra, Algorithms Comput. Math., vol. 4, Springer, Berlin, 1999, pp. 276–296.

[215] D. Rees, *A basis theorem for polynomial modules*, Proc. Cambridge Philos. Soc. **52** (1956), 12–16.

[216] Bodo Renschuch, Hartmut Roloff, and Georgij G. Rasputin, *Beiträge zur konstruktiven Theorie der Polynomideale. XXIII. Vergessene Arbeiten des Leningrader Mathematikers N. M. Gjunter zur Theorie der Polynomideale*, Wiss. Z. Pädagog. Hochsch. "Karl Liebknecht" Potsdam **31** (1987), no. 1, 111–126.

[217] B. Renshukh, Kh. Roloff, and G. G. Rasputin, *On forgotten papers of N. M. Günter on the theory of polynomial ideals*, Vestnik Leningrad. Univ. Mat. Mekh. Astronom. (1987), no. vyp. 1, 119–122, 127.

[218] Lorenzo Robbiano, *Term orderings on the polynomial ring*, EUROCAL '85, Vol. 2 (Linz, 1985), Lecture Notes in Comput. Sci., vol. 204, Springer, Berlin, 1985, pp. 513–517.

[219] ______, *On the theory of graded structures*, J. Symbolic Comput. **2** (1986), no. 2, 139–170.

[220] J. A. Robinson, *A machine-oriented logic based on the resolution principle*, J. Assoc. Comput. Mach. **12** (1965), 23–41.

[221] Paolo Salvatore and Roberto Tauraso, *The operad Lie is free*, J. Pure Appl. Algebra **213** (2009), no. 2, 224–230.

[222] Steven V. Sam and Andrew Snowden, *Gröbner methods for representations of combinatorial categories*, arXiv:1409.1670.

[223] ______, *Introduction to twisted commutative algebras*, arXiv:1209.5122.

[224] ______, *Stability patterns in representation theory*, Forum Math. Sigma **3** (2015), e11, 108.

[225] ______, *GL-equivariant modules over polynomial rings in infinitely many variables*, Trans. Amer. Math. Soc. **368** (2016), no. 2, 1097–1158. MR 3430359

[226] Walter J. Savitch, *Relationships between nondeterministic and deterministic tape complexities*, J. Comput. System. Sci. **4** (1970), 177–192.

[227] Mike Schlessinger and Jim Stasheff, *Deformation theory and rational homotopy type*, arXiv:1211.1647.

[228] E. A. Scott, *Weights for total division orderings on strings*, Theoret. Comput. Sci. **135** (1994), no. 2, 345–359.

[229] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.

[230] James B. Shearer, *A graded algebra with a nonrational Hilbert series*, J. Algebra **62** (1980), no. 1, 228–231.

[231] A. I. Shirshov, *On the representation of Lie rings as associative rings*, Uspehi Matem. Nauk (N.S.) **8** (1953), no. 5, 173–175.

[232] ______, *Some algorithm problems for Lie algebras*, Sibirsk. Mat. Ž. **3** (1962), 292–296.

[233] ______, *Selected works of A. I. Shirshov*, Contemporary Mathematicians, Birkhäuser Verlag, Basel, 2009, Translated from the Russian by Murray Bremner and Mikhail V. Kotchetov, Edited by Leonid A. Bokut′, Victor Latyshev, Ivan Shestakov and Efim Zelmanov.

[234] E. K. Sklyanin, *Some algebraic structures connected with the Yang-Baxter equation*, Funktsional. Anal. i Prilozhen. **16** (1982), no. 4, 27–34, 96.

[235] ______, *Some algebraic structures connected with the Yang-Baxter equation. Representations of a quantum algebra*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 4, 34–48.

[236] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, http://oeis.org/.

[237] S. P. Smith, *The four-dimensional Sklyanin algebras*, *K*-Theory **8** (1994), no. 1, 65–80.

[238] Ernst Snapper, *Polynomial matrices in several variables*, Amer. J. Math. **69** (1947), 622–652.

[239] Andrew Snowden, *Syzygies of Segre embeddings and Δ-modules*, Duke Math. J. **162** (2013), no. 2, 225–277.

[240] Wilhelm Specht, *Gesetze in Ringen. I*, Math. Z. **52** (1950), 557–589.

[241] James D. Stasheff, *Homotopy associativity of H-spaces. i, ii*, Trans. Amer. Math. Soc. **108** (1963), no. 2, 275–292, 293–312.

[242] James D. Stasheff, *The pre-history of operads*, Operads: Proceedings of Renaissance Conferences (Hartford, CT/Luminy, 1995), Contemp. Math., vol. 202, Amer. Math. Soc., Providence, RI, 1997, pp. 9–14.

[243] Einar Steingrímsson, *Generalized permutation patterns—a short survey*, Permutation patterns, London Math. Soc. Lecture Note Ser., vol. 376, Cambridge Univ. Press, Cambridge, 2010, pp. 137–152.

[244] M. H. Stone, *On one-parameter unitary groups in Hilbert space*, Ann. of Math. (2) **33** (1932), no. 3, 643–648.

[245] A. A. Suslin, *Projective modules over polynomial rings are free*, Dokl. Akad. Nauk SSSR **229** (1976), no. 5, 1063–1066.

[246] ______, *The structure of the special linear group over rings of polynomials*, Izv. Akad. Nauk SSSR Ser. Mat. **41** (1977), no. 2, 235–252, 477.

[247] Joshua Tobin, *A case study of Gröbner bases and Anick resolution*, Undergraduate honors thesis, Trinity College Dublin, 2011.

[248] Tuong Ton-That and Thai-Duong Tran, *Poincaré's proof of the so-called Birkhoff-Witt theorem*, Rev. Histoire Math. **5** (1999), no. 2, 249–284 (2000).

[249] V. A. Ufnarovskiĭ, *Criterion for the growth of graphs and algebras given by words*, Mat. Zametki **31** (1982), no. 3, 465–472, 476.

[250] ______, *Algebras specified by two quadratic relations*, Mat. Issled. (1984), no. 76, 148–171.

[251] ______, *On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras*, Mat. Sb. **180** (1989), no. 11, 1548–1560, 1584.

[252] ______, *Combinatorial and asymptotic methods in algebra*, Current problems in mathematics. Fundamental directions, Vol. 57 (Russian), Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1990, pp. 5–177.

[253] Bruno Vallette, *Homology of generalized partition posets*, J. Pure Appl. Algebra **208** (2007), no. 2, 699–725.

[254] ______, *A Koszul duality for props*, Trans. of Amer. Math. Soc. **359** (2007), 4865–4993.

[255] È. B. Vinberg, *The theory of homogeneous convex cones*, Trudy Moskov. Mat. Obšč. **12** (1963), 303–358.

[256] J. von Neumann, *Über einen Satz von Herrn M. H. Stone*, Ann. of Math. (2) **33** (1932), no. 3, 567–573.

[257] Volker Weispfenning, *Admissible orders and linear forms*, SIGSAM Bull. **21** (1987), no. 2, 16–18.

[258] Franz Winkler, *A geometrical decision algorithm based on the Gröbner bases algorithm*, Symbolic and algebraic computation (Rome, 1988), Lecture Notes in Comput. Sci., vol. 358, Springer, Berlin, 1989, pp. 356–363.

[259] Wen Tsün Wu, *Mechanical theorem proving in geometries*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1994, Basic principles, Translated from the 1984 Chinese original by Xiao Fan Jin and Dong Ming Wang.

[260] K. A. Zhevlakov, A. M. Slin′ko, I. P. Shestakov, and A. I. Shirshov, *Rings that are nearly associative*, Pure and Applied Mathematics, vol. 104, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1982, Translated from the Russian by Harry F. Smith.

Index