Algebraicity of zeta functions associated to matrices

Christian Kassel

Institut de Recherche Mathématique Avancée
CNRS - Université de Strasbourg
Strasbourg, France

Conference "Words, Codes and Algebraic Combinatorics"
Cetraro, Italy
1st of July, 2013

Joint work with C. Reutenauer

•This is a report on the following joint paper

C. Kassel, C. Reutenauer, *Algebraicity of the zeta function associated to a matrix over a free group algebra*, arXiv:1303.3481

• Our paper was inspired by pages 1–3 of the preprint *Noncommutative identities* by M. Kontsevich, arXiv:1109.2469

The general setting

- Let F_N be the free group on N generators $X_1, \ldots, X_N$ and

$$\mathbb{Z}F_N = \mathbb{Z}\langle X_1, X_1^{-1}, \ldots, X_N, X_N^{-1} \rangle$$

be its group ring

- Any element of $\mathbb{Z}F_N$ can be uniquely written as a finite sum

$$a = \sum_{g \in F_N} (a, g)\, g\,,$$

where (a, g) are integers

- Given $a \in \mathbb{Z}F_N$, we are interested in the coefficient of 1:

$$(a, 1) \in \mathbb{Z}$$

The main result

- For a $d \times d$-matrix M with entries in $\mathbb{Z}F_N$ define

$$a_n(M) = (\mathrm{Tr}(M^n), 1) \in \mathbb{Z}\,,$$

where $\mathrm{Tr}(M^n) \in \mathbb{Z}F_N$ is the trace of the n-th power of M

- Consider the "zeta function" of M, which is the formal power series

$$P_M = \exp\left(\sum_{n\geq 1} a_n(M)\,\frac{t^n}{n}\right) \in \mathbb{Q}[[t]]$$

- **Theorem 1**. *For each matrix $M \in M_d(\mathbb{Z}F_N)$, the formal power series P_M has integer coefficients and is algebraic*

"Algebraic" means that $y = P_M$ satisfies an equation of the form

$$y^r + a_1(t)y^{r-1} + \cdots + a_{r-1}(t) = 0$$

where $a_1(t), \ldots, a_{r-1}(t)$ are rational fractions with coefficients in $\mathbb{Q}$

Evidence for Theorem 1

Let us prove Theorem 1 in the very special case where $F_N = \{1\}$

- Recall that for any matrix M with entries in a commutative ring we have Jacobi's formula

$$\exp\left(\sum_{n\geq 1} \mathrm{Tr}(M^n)\,\frac{t^n}{n}\right) = \frac{1}{\det(1-tM)}$$

- Take $M \in M_d(\mathbb{Z}F_N) = M_d(\mathbb{Z})$. Then

$$P_M = \frac{1}{\det(1-tM)} = \frac{1}{(1-\lambda_1 t)\cdots(1-\lambda_d t)}$$

where $\lambda_1, \ldots, \lambda_d$ are the roots of the characteristic polynomial of M

It follows that P_M is not only algebraic, but a rational function

Remarks on Theorem 1

- The case $d = 1$ was settled by Kontsevich in arXiv:1109.2469

A combinatorial proof in the special case $d = 1$ and $N = 1$ was given by Reutenauer and Robado (FPSAC 2012, Nagoya)

- **Logarithmic derivative**. Define the generating function of M by

$$g_M = \sum_{n \geq 1} a_n(M)\, t^n \,,$$

Then g_M is related to the "zeta function" P_M by

$$g_M = t\, \frac{\mathrm{dlog}(P_M)}{\mathrm{d}t} = t\, \frac{P'_M}{P_M}$$

where P'_M is the derivative of P_M

The proof: Kontsevich's three steps

Let us now outline the proof of Theorem 1 following an idea by Kontsevich

Starting from a matrix $M \in M_d(\mathbb{Z}F_N)$,

• **Step 1**. Prove that P_M has integer coefficients

• **Step 2**. Prove that $g_M = t\,\mathrm{dlog}(P_M)/\,\mathrm{d}t = t\,P_M'/P_M$ is algebraic

To conclude that P_M is algebraic, we need a third step

• **Step 3**. Prove that, if f is a formal power series with integer coefficients and its logarithmic derivative $t\,\mathrm{dlog}\,f/\mathrm{d}t$ is algebraic, then f is algebraic

• **Note**.

- Steps 1–2 use standard techniques of the theory of formal languages
- Step 3 follows from a deep result in arithmetic geometry

Generating and zeta functions

- Let A be a set and A^* the free monoid on the alphabet A
- Let $\mathbb{Z}\langle\langle A\rangle\rangle$ be the ring of non-commutative formal power series on A with integer coefficients. For $S \in \mathbb{Z}\langle\langle A\rangle\rangle$ we have a unique expansion of the form

$$S = \sum_{w \in A^*} (S, w)\, w \qquad \text{with } (S, w) \in \mathbb{Z}$$

- **Definition**. (a) *The generating function of S is*

$$g_S = \sum_{n \geq 1} \left(\sum_{|w|=n} (S, w) \right) t^n \in \mathbb{Z}[[t]]$$

(b) *The zeta function of S is*

$$\zeta_S = \exp \left(\sum_{n \geq 1} \left(\sum_{|w|=n} (S, w) \right) \frac{t^n}{n} \right) \in \mathbb{Q}[[t]]$$

- g_S and ζ_S are related by

$$g_S = t\, \frac{\mathrm{dlog}(\zeta_S)}{dt} = t\, \frac{\zeta_S'}{\zeta_S}$$

Cyclic non-commutative formal power series

- **Definition**. *An element $S \in \mathbb{Z}\langle\langle A\rangle\rangle$ is cyclic if*

  (i) $\forall u, v \in A^*, \ \ (S, uv) = (S, vu)$ *and*

  (ii) $\forall w \in A^* - \{1\}, \forall r \geq 2, \ \ (S, w^r) = (S, w)^r$.

Recall: (a) A word is primitive if it is not the power of a proper subword

(b) Words w and w' are conjugate if $w = uv$ and $w' = vu$ for some u and v

- **Proposition**. *If $S \in \mathbb{Z}\langle\langle A\rangle\rangle$ is cyclic, then we have the factorization*

$$\zeta_S = \prod_{\ell \in L} \frac{1}{1 - (S, \ell)\, t^{|\ell|}}$$

where L is any set of representatives of conjugacy classes of primitive elements of $A^* - \{1\}$ (Lyndon words)

We are mainly interested in the following important consequence

- **Corollary**. *If $S \in \mathbb{Z}\langle\langle A\rangle\rangle$ is cyclic, then ζ_S has integer coefficients*

Algebraic non-commutative formal power series

- A system of proper algebraic non-commutative equations is a finite set of equations

$$\xi_i = p_i(\xi_1, \ldots, \xi_r) \qquad (i = 1, \ldots, r) \tag{1}$$

where each $p_i \in \mathbb{Z}\langle \xi_1, \ldots, \xi_r, A\rangle$ has no constant term and contains no monomial ξ_j

The system (1) has a unique solution $(S_1, \ldots, S_r) \in (\mathbb{Z}\langle\langle A\rangle\rangle)^r$, i.e., a r-tuple such that $S_i = p_i(S_1, \ldots, S_r)$ and has no constant term for all $i = 1, \ldots, r$

Definition. *A series $S \in \mathbb{Z}\langle\langle A\rangle\rangle$ is algebraic if it differs by a constant from such an S_i*

- **Example**. Let $A = \{a, b\}$. The equation $\xi = a\xi^2 + b$ has the solution

$$S = b + abb + aabbb + ababb + \cdots = \sum_{w \in Ł} w$$

where Ł is Łukasiewicz's language

$$Ł = \{w \in A^* \mid |w|_b = |w|_a + 1 \text{ and } |u|_a \geq |u|_b \text{ for all proper prefixes } u \text{ of } w\}$$

More on algebraic power series

We recall results by Schützenberger *et al.*

Proposition.

(a) *Algebraic non-commutative formal power series form a subring of $\mathbb{Z}\langle\langle A \rangle\rangle$, containing all rational series, i.e. those belonging to the smallest subring $\supset \mathbb{Z}\langle A \rangle$ closed under inversion*

(b) *The Hadamard product of a rational series and an algebraic one is algebraic*

(c) *Let $f : A^* \to F$ be a homomorphism to a free group F and $L \subset A^*$ consist of all words $w \in A^*$ such that $f(w) = 1$. Then the characteristic series*

$$\sum_{w \in L} w \in \mathbb{Z}\langle\langle A \rangle\rangle$$

of L is algebraic

(d) *If $S \in \mathbb{Z}\langle\langle A \rangle\rangle$ is algebraic, then its generating series $g_S \in \mathbb{Z}[[t]]$ is algebraic in the usual sense*

Steps 1 and 2 of the proof

Fix a matrix $M \in M_d(\mathbb{Z}F_N)$

• **An alphabet associated to** M. Define A to be the alphabet consisting of all triples $[g, i, j]$ with $1 \leq i, j \leq d$ and $g \in F_N$ such that $(M_{i,j}, g) \neq 0$

• Let $S_M \in \mathbb{Z}\langle\langle A \rangle\rangle$ be the non-commutative formal power series such that, if $w = [g_1, i_1, j_1] \cdots [g_n, i_n, j_n]$ $(n \geq 1)$, then

$$(S_M, w) = (M_{i_1,j_1}, g_1) \cdots (M_{i_n,j_n}, g_n) \in \mathbb{Z}$$

when $g_1 \cdots g_n = 1$ in F_N, and $j_n = i_1$ and $j_k = i_{k+1}$ for all $k = 1, \ldots, n-1$. Otherwise, $(S_M, w) = 0$.

• **Proposition**.

(a) *We have* $g_{S_M} = g_M$ *and* $\zeta_{S_M} = P_M$

(b) *The non-commutative series* S_M *is cyclic and algebraic*

• **Corollary**. *The "zeta function"* P_M *has integer coefficients and its logarithmic derivative* $g_M = t\, \mathrm{dlog}(P_M)/\,\mathrm{d}t$ *is algebraic*

An algebraicity theorem

To conclude the proof (Step 3) we need the following

• **Theorem 2**. *If $f \in \mathbb{Z}[[t]]$ is a formal power series with integer coefficients and $t \, \mathrm{dlog}\, f/\mathrm{d}t$ is algebraic, then f is algebraic*

• This theorem belongs to a long list of similar results, such as

(Polya) *If $f \in \mathbb{Z}[[t]]$ is a formal power series with integer coefficients and its derivative is rational, then f is a rational function*

But passing from "rational" to "algebraic" is a more challenging problem, having received an answer only in the last 30 years

The Grothendieck-Katz conjecture

• The Grothendieck-Katz conjecture is a very general, mainly unproved, algebraicity criterion:

If $Y' = AY$ is a linear system of differential equations with $A \in M_r(\mathbb{Q}(t))$, then it has a basis of solutions which are algebraic over $\mathbb{Q}(t)$ if and only, for all large enough prime integers p, the reduction modulo p of the system has a basis of solutions that are algebraic over $\mathbb{F}_p(t)$

• Instances of the conjecture have been proved

- by Yves André (1989) following Diophantine approximation techniques of D. V. and G. V. Chudnovsky (1984),
- and by Jean-Benoît Bost (2001) using the language of Arakelov geometry

• These cases cover the system consisting of the single differential equation

$$y' = \frac{g_M}{t}\, y$$

of interest to us, and thus yield Theorem 2

(for an overview, see Bourbaki Seminar by Chambert-Loir, 2001)

Explicit computations by Kontsevich

Kontsevich explicitly computed P_M as an algebraic function for

$$M = X_1 + X_1^{-1} + \cdots + X_N + X_N^{-1} \in \mathbb{Z}F_N = M_1(\mathbb{Z}F_N)$$

- For $M = X_1 + X_1^{-1} + X_2 + X_2^{-1}$,

$$P_M = \frac{2}{3} \cdot \frac{1 + 2\sqrt{1 - 12t^2}}{1 - 6t^2 + \sqrt{1 - 12t^2}}$$

Remark. If X_1 and X_2 were supposed to commute, then P_M would not be algebraic. Indeed, by a computation of Bousquet-Mélou,

$$a_n(M) = (M^n, 1) = \binom{2n}{n}^2 \sim \frac{1}{\pi} \frac{16^n}{n}$$

The generating function g_M, hence P_M, cannot be algebraic due to the presence of $1/n$ in the previous asymptotics

This example shows that we need non-commuting variables for Theorem 1

An explicit computation for a 2×2-matrix

• In our paper Christophe and I computed P_M as an algebraic function for the 2×2-matrix

$$M = \begin{pmatrix} a + a^{-1} & b \\ b^{-1} & d + d^{-1} \end{pmatrix}$$

where a, b, d are non-commuting variables

• **Theorem 3**. *We have*

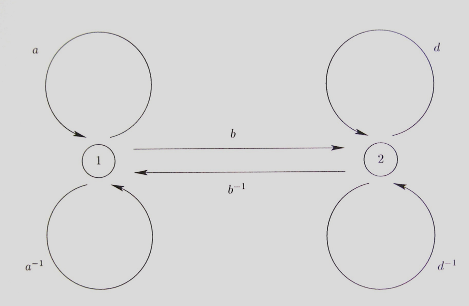
$$P_M = \frac{(1 - 8t^2)^{3/2} - 1 + 12t^2 - 24t^4}{32t^6} .$$

Thus P_M belongs to a quadratic extension of $\mathbb{Q}(t)$

• **Remark**. By Tutte the integers in the expansion of P_M as a formal power series count the planar rooted bicubic maps with an even number of vertices

How we proved Theorem 3

- We represent the matrix M by the following labeled oriented graph



We identify words on $A = \{a, a^{-1}, b, b^{-1}, d, d^{-1}\}$ and paths in this graph

- Let $L \subset A^*$ be the set of non-empty words
  (i) whose corresponding paths are closed loops
  (ii) which represent the identity element in the free group on a, b, d

- Then $a_n(M)$ is the number of words of length n in L

How we proved Theorem 3 (sequel)

- Using this interpretation of $a_n(M)$, we found a quadratic equation for g_M leading to

$$g_M = 3\,\frac{(1-8t^2)^{1/2} - 1 + 6t^2}{1-9t^2}$$

- g_M has the following expansion as a truncated formal power series:

$$g_M = 6\,(t^2 + 5t^4 + 29t^6 + 181t^8 + 1181t^{10} + 7941t^{12}) + O(t^{14})$$

from which we derived the expansion

$$P_M = 1 + 3\,t^2 + 12\,t^4 + 56\,t^6 + 288\,t^8 + 1584\,t^{10} + 4576\,t^{12} + O(t^{14}) \qquad (2)$$

The sequence of integers $(1, 3, 12, 56, 288, 1584, 4576)$ is the beginning of the sequence A000257 in Sloane's OEIS, which counts the "new" intervals in a Tamari lattice, as computed by Chapoton (2006)

- Chapoton gave an algebraic expression for the generating function ν of these "new" intervals. Rescaling ν, we found that $P(t) = (\nu(t^2) - t^4)/t^6$ has up to degree 10 the same expansion as (2).

To complete the proof of Theorem 3, it sufficed to check $t\,P'(t)/P(t) = g_M$.

The algebraic curve behind a matrix

- By the main result, $y = P_M$ satisfies an equation of the form

$$y^r + a_1(t)y^{r-1} + \cdots + a_{r-1}(t) = 0$$

where $a_1(t), \ldots, a_{r-1}(t)$ are rational fractions with coefficients in $\mathbb{Q}$
This equation defines an algebraic curve C_M (over $\mathbb{Z}$)

- For the matrix above

$$M = \begin{pmatrix} a + a^{-1} & b \\ b^{-1} & d + d^{-1} \end{pmatrix}$$

this equation is

$$y^2 + \frac{24t^4 - 12t^2 + 1}{16t^6} y + \frac{9t^2 - 1}{16t^6} = 0$$

- In general what can we say about the algebraic curve C_M?

    What is its geometric meaning?

References for our paper

• F. Chapoton, *Sur le nombre d'intervalles dans les treillis de Tamari*, Séminaire Lotharingien de Combinatoire 55 (2006), B55f; arXiv:math/0602368

• C. Kassel, C. Reutenauer, *Algebraicity of the zeta function associated to a matrix over a free group algebra*, arXiv:1303.3481

• M. Kontsevich, *Noncommutative identities*, talk at *Mathematische Arbeitstagung* 2011, Bonn; arXiv:1109.2469v1

• *The On-Line Encyclopedia of Integer Sequences* (2010), http://oeis.org

• C. Reutenauer, M. Robado, *On an algebraicity theorem of Kontsevich*, FPSAC 2012, Nagoya, Japan

• W. T. Tutte, *A census of planar maps*, Canadian J. Math. 15 (1963), 249-271

Background references: formal languages

- J. Berstel, C. Reutenauer, *Zeta functions of formal languages*, Trans. Amer. Math. Soc. 321 (1990), 533–546

- J. Berstel, C. Reutenauer, *Noncommutative rational series with applications*, Encyclopedia of Mathematics and its Applications, 137, Cambridge University Press, Cambridge, 2011

- M. Bousquet-Mélou, *Algebraic generating functions in enumerative combinatorics, and context-free languages*, V. Diekert and B. Durand (Eds.), STACS 2005, 18–35, Lect. Notes Comput. Sci., 3404, Springer-Verlag, Berlin, Heidelberg, 2005. See Sect. 1, Example 3.

- G. Jacob, *Sur un théorème de Shamir*, Information and Control 27 (1975), 218–261

- M. P. Schützenberger, *On a theorem of R. Jungen*, Proc. Amer. Math. Soc. 13 (1962), 885–890

Background references: algebraicity results

• Y. André, *G-functions and geometry*, Aspects of Mathematics, E13, Friedr. Vieweg & Sohn, Braunschweig, 1989.

• Y. André, *Sur la conjecture des p-courbures de Grothendieck et Katz*, Geometric aspects of Dwork theory, Vol. I, II, 55–112, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

• J.-B. Bost, *Algebraic leaves of algebraic foliations over number fields*, Publ. Math. Inst. Hautes Études Sci. 93 (2001), 161–221.

• A. Chambert-Loir, *Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. & G. Chudnovsky)*, Séminaire Bourbaki, Vol. 2000/2001, Astérisque No. 282 (2002), Exp. No. 886, viii, 175–209.

• D. V. Chudnovsky, G. V. Chudnovsky, *Applications of Padé approximations to the Grothendieck conjecture on linear differential equations*, Number theory (New York, 1983–84), 52–100, Lecture Notes in Math., 1135, Springer, Berlin, 1985.