341D: Gröbner bases

э

A curve in (x, y)-plane is given parametrically by

$$x(t) = 2t - 4t^3,$$

 $y(t) = t^2 - 3t^4.$

Let us use Gröbner bases to find a polynomial P(x, y) such that P(x(t), y(t)) = 0.

(日) (同) (E) (E) (E)

To eliminate t from these parametric equations, we consider the lex ordering with t > x > y, and compute a Gröbner basis of the ideal $I = (x - 2t + 4t^3, y - t^2 + 3t^4)$; it is

$$2t^{2} - 3tx + 4y,$$

$$9tx^{2} - 8ty - 2t - 12xy + x,$$

$$24txy - 2tx + 3x^{2} - 32y^{2} - 8y,$$

$$192ty^{2} + 32ty - 4t + 27x^{3} - 120xy + 2x,$$

$$27x^{4} - 144x^{2}y - 4x^{2} + 256y^{3} + 128y^{2} + 16y$$

so we may take $P(x, y) = 27x^4 - 144x^2y - 4x^2 + 256y^3 + 128y^2 + 16y$.

(日) (同) (目) (日) (日) []

To eliminate t from these parametric equations, we consider the lex ordering with t > x > y, and compute a Gröbner basis of the ideal $I = (x - 2t + 4t^3, y - t^2 + 3t^4)$; it is

$$2t^{2} - 3tx + 4y,$$

$$9tx^{2} - 8ty - 2t - 12xy + x,$$

$$24txy - 2tx + 3x^{2} - 32y^{2} - 8y,$$

$$192ty^{2} + 32ty - 4t + 27x^{3} - 120xy + 2x,$$

$$27x^{4} - 144x^{2}y - 4x^{2} + 256y^{3} + 128y^{2} + 16y$$

so we may take $P(x, y) = 27x^4 - 144x^2y - 4x^2 + 256y^3 + 128y^2 + 16y$. Note that the Gröbner basis contains the element $2t^2 - 3tx + 4y$ where the coefficient of the highest power of t is nonzero, so the Extension Theorem guarantees that over an algebraically closed field any common root (x, y) of the elimination ideal $I_1 = (P(x, y))$ extends to a root (t, x, y) of I, so we can guarantee that every complex solution corresponds to some value of t.

Suppose that we look for that curve over the real numbers. Is it true that every point corresponds to some value of the parameter t?

∃ ► < ∃ ►</p>

Suppose that we look for that curve over the real numbers. Is it true that every point corresponds to some value of the parameter t? The second element in the Gröbner basis is $9tx^2 - 8ty - 2t - 12xy + x$, so if some triple (t_0, x_0, y_0) solves our equations, then

$$t_0(9x_0^2-8y_0-2)-12x_0y_0+x_0=0.$$

If $9x_0^2 - 8y_0 - 2 \neq 0$, we have

$$t=\frac{12x_0y_0-x_0}{9x_0^2-8y_0-2},$$

so if x_0 and y_0 are real, t_0 is also real.

(本部) (本語) (本語) (語)

If $9x_0^2 - 8y_0 - 2 = 0$, the equation

$$t_0(9x_0^2 - 8y_0 - 2) - 12x_0y_0 + x_0 = 0$$

also forces $12x_0y_0 - x_0 = 0$, so $x_0 = 0$ or $y_0 = \frac{1}{12}$. Substituting each of these into $9x_0^2 - 8y_0 - 2 = 0$, we get three pairs which we have to examine more carefully: $(0, -\frac{1}{4})$ and $(\pm \frac{2\sqrt{2}}{3\sqrt{3}}, \frac{1}{12})$. For those, we look at the first element of the Gröbner basis, $2t^2 - 3tx + 4y$. Substituting these pairs, we obtain the polynomials

$$2t^{2} - 1,$$

$$2t^{2} + \frac{2\sqrt{2}}{\sqrt{3}}t + \frac{1}{3} = (t\sqrt{2} + \frac{1}{\sqrt{3}})^{2},$$

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

All these polynomials have only real roots, so the corresponding values of t are always real.

Suppose that we would like to minimize $(a - c)^2 + (b - d)^2$ given that ab = 4 and $c^2 + 4d^2 = 4$. In more geometric terms, we would like to find the minimal distance between the hyperbola xy = 4 and the ellipse $x^2 + 4y^2 = 4$ in \mathbb{R}^2 .

Suppose that we would like to minimize $(a - c)^2 + (b - d)^2$ given that ab = 4 and $c^2 + 4d^2 = 4$. In more geometric terms, we would like to find the minimal distance between the hyperbola xy = 4 and the ellipse $x^2 + 4y^2 = 4$ in \mathbb{R}^2 . The Lagrange multipliers method suggests that we should look at the critical points of the function

$$F(a, b, c, d, \alpha, \beta) = (a - c)^2 + (b - d)^2 - \alpha(ab - 4) - \beta(c^2 + 4d^2 - 4).$$

We have

$$\begin{split} \partial_a F &= 2(a-c) - \alpha b, \\ \partial_b F &= 2(b-d) - \alpha a, \\ \partial_c F &= 2(c-a) - 2\beta c, \\ \partial_d F &= 2(d-b) - 8\beta d, \\ \partial_\alpha F &= ab - 4, \\ \partial_\beta F &= c^2 + 4d^2 - 4. \end{split}$$

Vanishing of these is precisely the system of equations we should solve.

Computing a Gröbner basis for the LEX ordering with $\alpha > \beta > a > b > c > d$ using Singular, we get a Gröbner basis consisting of the elements

Computing a Gröbner basis for the LEX ordering with $\alpha > \beta > a > b > c > d$ using Singular, we get a Gröbner basis consisting of the elements

 $81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} + 13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16,$

(日) (同) (E) (E) (E)

Computing a Gröbner basis for the LEX ordering with $\alpha > \beta > a > b > c > d$ using Singular, we get a Gröbner basis consisting of the elements

 $81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} + 13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16,$

 $\frac{188352c + 4742469d^{15} - 18574191d^{13} + 192181159d^{11} - 323074301d^9 + 769803276d^7 - 459193664d^5 + 97662148d^3 - 7408656d,}{1200}$

(日) (同) (E) (E) (E)

Computing a Gröbner basis for the LEX ordering with $\alpha > \beta > a > b > c > d$ using Singular, we get a Gröbner basis consisting of the elements

 $81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} + 13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16,$

 $\frac{188352c + 4742469d^{15} - 18574191d^{13} + 192181159d^{11} - 323074301d^9 + 769803276d^7 - 459193664d^5 + 97662148d^3 - 7408656d,}{1200}$

 $53680320b - 1638275463d^{15} + 6225285213d^{13} - 65700922861d^{11} + \\ 104081012935d^9 - 255308307124d^7 + 131039721440d^5 - 24029768972d^3 + \\ 1779004976d,$

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Computing a Gröbner basis for the LEX ordering with $\alpha > \beta > a > b > c > d$ using Singular, we get a Gröbner basis consisting of the elements

 $81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} + 13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16,$

 $\frac{188352c + 4742469d^{15} - 18574191d^{13} + 192181159d^{11} - 323074301d^9 + 769803276d^7 - 459193664d^5 + 97662148d^3 - 7408656d,}{1200}$

 $53680320b - 1638275463d^{15} + 6225285213d^{13} - 65700922861d^{11} + \\ 104081012935d^9 - 255308307124d^7 + 131039721440d^5 - 24029768972d^3 + \\ 1779004976d,$

and, on the next slide,

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □ ● ● ● ●

 $71573760a - 490312683d^{15} + 1953288513d^{13} - 20013783641d^{11} +$ $34789074995d^9 - 82428604004d^7 + 53519167360d^5 - 15225418492d^3 +$ 1552217776d.

< 注 → < 注 → 二 注

 $71573760a - 490312683d^{15} + 1953288513d^{13} - 20013783641d^{11} +$ $34789074995d^9 - 82428604004d^7 + 53519167360d^5 - 15225418492d^3 +$ 1552217776d,

 $214721280\beta + 1638275463d^{14} - 6225285213d^{12} + 65700922861d^{10} - 104081012935d^8 + 255308307124d^6 - 131039721440d^4 + 24029768972d^2 - 1832685296,$

 $71573760a - 490312683d^{15} + 1953288513d^{13} - 20013783641d^{11} +$ $34789074995d^9 - 82428604004d^7 + 53519167360d^5 - 15225418492d^3 +$ 1552217776d,

$$\begin{split} & 214721280\beta + 1638275463d^{14} - 6225285213d^{12} + 65700922861d^{10} - \\ & 104081012935d^8 + 255308307124d^6 - 131039721440d^4 + 24029768972d^2 - \\ & 1832685296, \end{split}$$

 $\frac{107360640\alpha + 1679218371d^{14} - 6538493421d^{12} + 67910186537d^{10} - 112888398095d^8 + 270453063428d^6 - 157077454960d^4 + 32607369964d^2 - 2435055472.$

We note that the first equation

$$81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} +$$

 $13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16 = 0,$

is an equation in d only, and the further equations allow to reconstruct other unknowns uniquely, using d.

프 + + 프 +

We note that the first equation

$$81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} +$$

 $13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16 = 0,$

is an equation in d only, and the further equations allow to reconstruct other unknowns uniquely, using d. First of all, this equation factors as

$$(d^4 - d^2 + 4)(81d^{12} - 243d^{10} + 2743d^8 - 2081d^6 + 600d^4 - 80d^2 + 4) = 0$$

ヨト イヨト

We note that the first equation

$$81d^{16} - 324d^{14} + 3310d^{12} - 5796d^{10} +$$

 $13653d^8 - 9004d^6 + 2484d^4 - 324d^2 + 16 = 0,$

is an equation in d only, and the further equations allow to reconstruct other unknowns uniquely, using d. First of all, this equation factors as

$$(d^4 - d^2 + 4)(81d^{12} - 243d^{10} + 2743d^8 - 2081d^6 + 600d^4 - 80d^2 + 4) = 0$$

The first factor has no real roots, the second has roots (approximately)

-.5814060238, -.3478340245, .3478340245, .5814060238.

This leads to the solutions (a, b, c, d) being

(-2.39097848, -1.67295522, -1.62722710, -.5814060238),(1.722790175, 2.321814961, -1.87511226, -.3478340245),(-1.722790175, -2.321814961, 1.87511226, .3478340245),(2.39097848, 1.67295522, 1.62722710, .5814060238) This leads to the solutions (a, b, c, d) being

 $\begin{array}{l}(-2.39097848,-1.67295522,-1.62722710,-.5814060238),\\(1.722790175,2.321814961,-1.87511226,-.3478340245),\\(-1.722790175,-2.321814961,1.87511226,.3478340245),\\(2.39097848,1.67295522,1.62722710,.5814060238)\end{array}$

and to the values of $(a - c)^2 + (b - d)^2$ being 1.774795818, 20.07192764, 20.07192764, 1.774795818.

イロン 不同と 不足と 不足と 一足

This leads to the solutions (a, b, c, d) being

 $\begin{array}{l} (-2.39097848, -1.67295522, -1.62722710, -.5814060238), \\ (1.722790175, 2.321814961, -1.87511226, -.3478340245), \\ (-1.722790175, -2.321814961, 1.87511226, .3478340245), \\ (2.39097848, 1.67295522, 1.62722710, .5814060238) \end{array}$

and to the values of $(a - c)^2 + (b - d)^2$ being 1.774795818, 20.07192764, 20.07192764, 1.774795818.

At the oral entrance exam to the maths department of the Moscow State University in 1978, some Jewish students were offered the following problem:

Given that
$$ab = 4$$
 and $c^2 + 4d^2 = 4$, show that $(a - c)^2 + (b - d)^2 \ge 1.6$.

・ロト ・回ト ・ヨト ・ヨト 三日

Classification of "nonsymmetric operads" leads to looking for common zeros of the following 19 polynomials expressed on 2 pages:

$$\begin{aligned} x_5x_1 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_6 - x_4 + x_2 + x_1, \\ 2x_6x_1 + x_4x_1 - 2x_3x_1 - x_2x_1 + 2x_1^2 + 2x_6 + x_4 - x_2, \\ x_2^2 + x_4x_1 + x_2x_1 + x_1^2 + x_2 + x_1, \\ 2x_3x_2 + x_4x_1 + 2x_3x_1 - x_2x_1 - x_4 + x_2 + 2x_1, \\ x_4x_2 + x_4x_1 + x_2, \\ x_5x_2 - x_3x_1 + x_1^2 + x_4, \\ 2x_6x_2 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2 + 2x_1, \\ 2x_4x_3 - x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2, \\ 2x_5x_3 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - 2x_6 - x_4 + x_2 + 2x_1, \\ x_6x_3 + x_4x_1 + x_1^2 + x_6 + x_1, \\ x_4^2 - x_4x_1 - 2x_3x_1 + x_2x_1 + x_1^2 + x_4 - x_1, \end{aligned}$$

★ E → ★ E →

$$\begin{aligned} x_5x_4 + 2x_4x_1 + x_3x_1 - x_2x_1 + x_2 + x_1, \\ 2x_6x_4 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2, \\ 2x_6x_5 - x_4x_1 - 2x_3x_1 + x_2x_1 + 2x_1^2 + x_4 - x_2, \\ x_6^2 + x_4x_1 + x_3x_1 + x_6 + x_1, \\ x_2x_1^2 + x_1^3 - x_4x_1 - 2x_3x_1 + 2x_1^2 + x_4 - x_2 - x_1, \\ 2x_3x_1^2 - 2x_1^3 - x_4x_1 - 2x_3x_1 + 3x_2x_1 + 4x_1^2 - x_4 + x_2 + 2x_1, \\ x_4x_1^2 + x_1^3 - x_2x_1 + x_4 - x_2 - x_1, \\ 2x_3^2x_1 - 2x_1^3 - x_4x_1 + 5x_2x_1 + 4x_1^2 - 3x_4 + 3x_2 + 4x_1. \end{aligned}$$

$$\begin{split} x_5x_4 + 2x_4x_1 + x_3x_1 - x_2x_1 + x_2 + x_1, \\ 2x_6x_4 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2, \\ 2x_6x_5 - x_4x_1 - 2x_3x_1 + x_2x_1 + 2x_1^2 + x_4 - x_2, \\ x_6^2 + x_4x_1 + x_3x_1 + x_6 + x_1, \\ x_2x_1^2 + x_1^3 - x_4x_1 - 2x_3x_1 + 2x_1^2 + x_4 - x_2 - x_1, \\ 2x_3x_1^2 - 2x_1^3 - x_4x_1 - 2x_3x_1 + 3x_2x_1 + 4x_1^2 - x_4 + x_2 + 2x_1, \\ x_4x_1^2 + x_1^3 - x_2x_1 + x_4 - x_2 - x_1, \\ 2x_3^2x_1 - 2x_1^3 - x_4x_1 + 5x_2x_1 + 4x_1^2 - 3x_4 + 3x_2 + 4x_1. \end{split}$$

This is a Gröbner basis for the glex order with $x_6 > x_5 > x_4 > x_3 > x_2 > x_1$; the lex Gröbner basis is quite disastrous, and consists of polynomials with much larger coefficients.

First, we note that powers of x_1 do not appear as leading terms, so we should expect infinitely many solutions.

E • • E •

First, we note that powers of x_1 do not appear as leading terms, so we should expect infinitely many solutions. Note that the sum of the elements

$$\begin{aligned} & 2x_6x_4 + x_4x_1 + 2x_3x_1 - x_2x_1 - 2x_1^2 - x_4 + x_2, \\ & 2x_6x_5 - x_4x_1 - 2x_3x_1 + x_2x_1 + 2x_1^2 + x_4 - x_2 \end{aligned}$$

(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.

(日) (同) (E) (E) (E)

Case 1: We set $x_6 = 0$ in the 19 polynomials, and compute the Gröbner basis of the ideal generated by the resulting polynomials in x_1, \ldots, x_5 . This basis has only 8 elements:

$$\left.\begin{array}{ccc} x_4 - x_2, & x_1(x_1 + x_2 + 1), & x_1(x_3 - x_1), \\ x_1(x_5 + 1), & (x_2 + x_1 + 1)(x_2 - x_1), \\ x_1^2 + x_2 x_3 + x_1, & x_2(x_5 + 1), & x_3 x_5 + x_1. \end{array}\right\}$$
(1)

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 (1) and recompute the Gröbner basis in x_2, \ldots, x_5 which consists of these five polynomials:

$$x_4 - x_2, \quad x_2(1 + x_2), \quad x_3x_2, \quad x_2(x_5 + 1), \quad x_5x_3.$$

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:

$$[x_1,\ldots,x_6] = \begin{cases} [0,0,X,0,0,0] \quad (X \in \mathbb{F}) \\ [0,0,0,0,X,0] \quad (X \in \mathbb{F}) \\ [0,-1,0,-1,-1,0] \end{cases}$$
(2)

ヘロト 人間 とくほと くほとう

Case 1.1: We set $x_1 = 0$ in the polynomials (1) and recompute the Gröbner basis in x_2, \ldots, x_5 which consists of these five polynomials:

$$x_4 - x_2, \quad x_2(1 + x_2), \quad x_3x_2, \quad x_2(x_5 + 1), \quad x_5x_3.$$

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:

$$[x_1, \dots, x_6] = \begin{cases} [0, 0, X, 0, 0, 0] & (X \in \mathbb{F}) \\ [0, 0, 0, 0, X, 0] & (X \in \mathbb{F}) \\ [0, -1, 0, -1, -1, 0] \end{cases}$$
(2)

Case 1.2: We set $x_2 = -x_1 - 1$, $x_3 = x_1$, $x_5 = -1$ in (1) 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

$$[x_1,\ldots,x_6] = [X,-X-1,X,-X-1,-1,0] \ (X \in \mathbb{F}). \tag{3}$$

Note that for X = 0 we obtain the previous solution $[0, -1, 0, -1, -1, 0]_{1,0,0}$

Case 2: We set $x_5 = -x_4$ in the 19 polynomials, and compute the Gröbner basis of the ideal generated by the resulting polynomials in x_1, \ldots, x_4, x_6 . This Gröbner basis consists of the following 14 elements:

$$\begin{aligned} & 2x_3x_1 - x_2x_1 - 2x_1^2 - x_6 - x_4 + x_2 + x_1, \\ & 2x_4x_1 - x_2x_1 - x_6 + x_4 + 3x_2 + x_1, 4x_6x_1 - 3x_2x_1 + 3x_6 - x_4 - 3x_2 + x_1, \\ & & 2x_2^2 + 3x_2x_1 + 2x_1^2 + x_6 - x_4 - x_2 + x_1, \\ & & 4x_3x_2 + x_2x_1 + 4x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\ & & 2x_4x_2 + x_2x_1 + 4x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\ & & 4x_6x_2 + 5x_2x_1 + 4x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\ & & 4x_4x_3 - x_2x_1 + x_6 + x_4 + 3x_2 - x_1, \\ & & 2x_6x_3 + x_2x_1 + 2x_1^2 + 3x_6 - x_4 - 3x_2 + x_1, \\ & & 2x_4^2 - x_2x_1 - 2x_1^2 - 3x_6 + x_4 + 5x_2 + x_1, \\ & & 4x_6x_4 + x_2x_1 + 3x_6 - x_4 - 3x_2 - 3x_1, \quad x_6^2 + x_2x_1 + x_1^2 + 2x_6 - 2x_2, \\ & & 4x_1^3 - 13x_2x_1 - 4x_1^2 + x_6 + 9x_4 - 5x_2 - 9x_1, \\ & & 4x_2x_1^2 + 7x_2x_1 + 4x_1^2 - 7x_6 - 7x_4 + 11x_2 + 11x_1. \end{aligned}$$

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 leads to a system of the nine polynomials

$$\begin{aligned} x_6 - x_1 x_3 + x_2^2 + 2x_1 x_2 + 2x_1^2 - x_2, \\ x_4 - x_2^2 - x_3 x_1 - x_2 x_1 - x_1, \\ (2x_2 + x_1)(x_3 - x_2 - x_1), \end{aligned}$$

$$\begin{aligned} 2x_1^3 + 4x_2^2 + 5x_3 x_1 - 3x_2 x_1 - 3x_1^2 - 2x_2, \\ 2x_2 x_1^2 - 7x_3 x_1 + 7x_2 x_1 + 9x_1^2 + 2x_2 + 2x_1, \\ x_3 x_1^2 + 2x_2^2 + x_3 x_1 + x_1^2 + x_1, \end{aligned}$$

$$\begin{aligned} 2x_2^2 x_1 - 2x_2^2 + 5x_3 x_1 - 5x_2 x_1 - 7x_1^2 - 2x_1, \\ x_3^2 x_1 + x_2^2 + x_3 x_1 + x_1^2 + x_2 + x_1, \\ 2x_2^3 + 2x_2^2 - x_3 x_1 + x_2 x_1 + x_1^2 - 2x_2. \end{aligned}$$

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 $x_1 = x_2 - x_2$.

Case 2.1: We substitute $x_1 = -2x_2$ in the last six polynomials of the set above and compute the reduced Gröbner basis, 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

$$[x_1,\ldots,x_6] = [0,0,X,0,0,0], \ [-2,1,-2,1,-1,0].$$

The first has already appeared in (2), and the second is the special case X = -2 of (3), so there are no new solutions.

◆□▶ ◆□▶ ◆□▶ ◆□▶ ● □ ● ○○○

Case 2.1: We substitute $x_1 = -2x_2$ in the last six polynomials of the set above and compute the reduced Gröbner basis, 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

$$[x_1,\ldots,x_6] = [0,0,X,0,0,0], \ [-2,1,-2,1,-1,0].$$

The first has already appeared in (2), and the second is the special case X = -2 of (3), 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, obtaining these four polynomials:

$$\begin{aligned} & x_2(x_2^2+x_2-1), \\ & x_3x_2^2-x_3^2+2x_3x_2-x_2^2-x_3, \\ & x_3^2x_2-x_3^2+2x_3x_2-2x_2^2-x_3+x_2, \\ & x_3^3+x_3^2-x_3x_2+x_2. \end{aligned}$$

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:

$$[x_1,\ldots,x_6] = [-1,0,-1,0,0,-1]. \tag{4}$$

(日) (同) (E) (E) (E)

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

$$F = x_3^2 + \phi x_3 + (\phi + 1).$$

(日) (同) (E) (E) (E)

In fact, we can rewrite $F = x_3^2 + \phi x_3 + (\phi + 1)$ as

$$\mathbf{T} = x_3^2 + \phi x_3 + \phi^2,$$

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

$$x_{6} = -\phi^{2}\omega^{3} - \phi^{2} - 2\phi^{2}\omega^{2} - 2\phi^{2}\omega^{4} - \phi = -\phi,$$
(5)

$$x_4 = \phi^2 - \phi^2 \omega^3 + \phi^2 \omega^2 - \phi \omega^2 = (\phi^2 - \phi) \omega^2 = \omega^2.$$
 (6)

Finally, since throughout Case 2 we have $x_5 = -x_4$, we conclude that

$$x_5 = -\omega^2.$$

Overall, in this case we end up with the four points

$$[\omega^2\phi, -\phi, \omega\phi, \omega^2, -\omega^2, -\phi],$$

where ω is a root of the polynomial $t^2 + t + 1$ and ϕ is a root of the polynomial $t^2 - t - 1$.

341D: Grobner bases

◆□ ▶ ◆□ ▶ ◆三 ▶ ◆□ ▶ ◆□ ▶