2.4. Solving ideal problems by Gröbner bases

Computation in the vector space of polynomials modulo an ideal

The ring $K[X]_{/I}$ of polynomials modulo the ideal I is a vector space over K. A Gröbner basis G provides a basis for this vector space.

Theorem 2.4.1. *The irreducible power products modulo G, viewed as polynomials with coefficient 1, form a basis for the vector space $K[X]_{/I}$ over K.*

Proof: [Winkler 1996], Theorem 8.4.1. □

Ideal membership

By definition Gröbner bases solve the *ideal membership problem* for polynomial ideals, i.e.

given: $f, f_1, \ldots, f_m \in K[X]$,
decide: $f \in \langle f_1, \ldots, f_m \rangle$.

Let G be a Gröbner basis for $I = \langle f_1, \ldots, f_m \rangle$. Then $f \in I$ if and only if the normal form of f modulo G is 0.

Example 2.4.2. Suppose that we know the polynomial relations (axioms)

$$\begin{aligned} 4z - 4xy^2 - 16x^2 - 1 &= 0, \\ 2y^2z + 4x + 1 &= 0, \\ 2x^2z + 2y^2 + x &= 0 \end{aligned}$$

between the quantities x, y, z, and we want to decide whether the additional relation (hypothesis)

$$g(x, y) = 4xy^4 + 16x^2y^2 + y^2 + 8x + 2 = 0$$

follows from them, i.e. whether we can write g as a linear combination of the axioms or, in other words, whether g is in the ideal I generated by the axioms.

Trying to reduce the hypothesis g w.r.t. the given axioms does not result in a reduction to 0. But we can compute a Gröbner basis for I w.r.t. the lexicographic ordering with $x < y < z$, e.g. $G = \{g_1, g_2, g_3\}$ where

$$\begin{aligned} g_1 &= 32x^7 - 216x^6 + 34x^4 - 12x^3 - x^2 + 30x + 8, \\ g_2 &= 2745y^2 - 112x^6 - 812x^5 + 10592x^4 - 61x^3 - 812x^2 + 988x + 2, \\ g_3 &= 4z - 4xy^2 - 16x^2 - 1. \end{aligned}$$

Now $g \longrightarrow_G^* 0$, i.e. $g(x, y) = 0$ follows from the axioms. □

Radical membership

Sometimes, especially in applications in geometry, we are not so much interested in the ideal membership problem but in the *radical membership problem*, i.e.

given: $f, f_1, \ldots, f_m \in K[X]$,
decide: $f \in \text{radical}(\langle f_1, \ldots, f_m \rangle)$.

The radical of an ideal I is the ideal containing all those polynomials f, some power of which is contained in I. So $f \in \text{radical}(I) \iff f^n \in I$ for some $n \in \mathbb{N}$. Geometrically $f \in \text{radical}(\langle f_1, \ldots, f_m \rangle)$ means that the hypersurface defined by f contains all the points in the variety (algebraic set) defined by $f_1, \ldots, f_m$.

The following extremely important theorem relates the radical of an ideal I to the set of common roots $V(I)$ of the polynomials contained in I.

Theorem 2.4.3. (Hilbert's Nullstellensatz) *Let I be an ideal in $K[X]$, where K is an algebraically closed field. Then* radical(I) *consists of exactly those polynomials in $K[X]$ which vanish on all the common roots of I.*

Proof: Vorlesung Kommutative Algebra und Algebraische Geometrie. □

By an application of Hilbert's Nullstellensatz we get that $f \in \text{radical}(\langle f_1, \ldots, f_m \rangle)$ if and only if f vanishes at every common root of $f_1, \ldots, f_m$ if and only if the system $f_1 = \ldots f_m = z \cdot f - 1 = 0$ has no solution, where z is a new variable. I.e.

$$f \in \text{radical}(\langle f_1, \ldots, f_m \rangle) \iff 1 \in \langle f_1, \ldots, f_m, z \cdot f - 1 \rangle.$$

So the radical membership problem is reduced to the ideal membership problem.

Equality of ideals

We want to decide whether two given ideals are equal, i.e. we want to solve the *ideal equality problem*:

given: $f_1, \ldots, f_m, g_1, \ldots, g_k \in K[X]$,
decide: $\underbrace{\langle f_1, \ldots, f_m \rangle}_{I} = \underbrace{\langle g_1, \ldots, g_k \rangle}_{J}$.

Choose any admissible ordering. Let G_I, G_J be the normed reduced Gröbner bases of I and J, respectively. Then by Theorem 8.3.6 $I = J$ if and only if $G_I = G_J$.

Solution of algebraic equations by Gröbner bases

We consider a system of equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0, \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0, \end{aligned} \tag{2.4.1}$$

where $f_1, \ldots, f_m \in K[X]$. The system (2.4.1) is called a system of polynomial or algebraic equations. First let us decide whether (2.4.1) has any solutions in $\overline{K}^n$, $\overline{K}$ being the algebraic closure of K. Let $I = \langle f_1, \ldots, f_m \rangle$.

Theorem 2.4.4. *Let G be a normed Gröbner basis of I. (2.4.1) is unsolvable in $\overline{K}^n$ if and only if $1 \in G$.*

Proof: [Winkler 1996] Theorem 8.4.3. □

Now suppose that (2.4.1) is solvable. We want to determine whether there are finitely or infinitely many solutions of (2.4.1) or, in other words, whether or not the ideal I is 0–dimensional.

Theorem 2.4.5. *Let G be a Gröbner basis of I. Then (2.4.1) has finitely many solutions (i.e. I is 0–dimensional) if and only if for every i, $1 \leq i \leq n$, there is a polynomial $g_i \in G$ such that $\mathrm{lpp}(g_i)$ is a pure power of x_i. Moreover, if I is 0–dimensional then the number of zeros of I (counted with multiplicity) is equal to $\dim(K[X]_{/I})$.*

Proof: [Winkler 1996] Theorem 8.4.4. □

The rôle of the Gröbner basis algorithm GRÖBNER_B in solving systems of algebraic equations is the same as that of Gaussian elimination in solving systems of linear equations, namely to triangularize the system, or carry out the elimination process. The crucial observation is the elimination property of Gröbner bases. It states that if G is a Gröbner basis of I w.r.t. the lexicographic ordering with $x_1 < \ldots < x_n$, then the i–th elimination ideal of I, i.e. $I \cap K[x_1, \ldots, x_i]$, is generated by those polynomials in G that depend only on the variables $x_1, \ldots, x_i$.

Theorem 2.4.6. (Elimination Property of Gröbner Bases) *Let G be a Gröbner basis of I w.r.t. the lexicographic ordering $x_1 < \ldots < x_n$. Then*

$$I \cap K[x_1, \ldots, x_i] = \langle G \cap K[x_1, \ldots, x_i] \rangle,$$

where the ideal on the right hand side is generated over the ring $K[x_1, \ldots, x_i]$.

Proof: [Winkler 1996] Theorem 8.4.5. □

Theorem 2.4.6 can clearly be generalized to product orderings, without changing anything in the proof.

Example 2.4.7. Consider the system of equations $f_1 = f_2 = f_3 = 0$, where

$$\begin{aligned} 4xz - 4xy^2 - 16x^2 - 1 &= 0, \\ 2y^2z + 4x + 1 &= 0, \\ 2x^2z + 2y^2 + x &= 0, \end{aligned}$$

are polynomials in $\mathbb{Q}[x, y, z]$. We are looking for solutions of this system of algebraic equations in $\overline{\mathbb{Q}}^3$, where $\overline{\mathbb{Q}}$ is the field of algebraic numbers.

Let $<$ be the lexicographic ordering with $x < y < z$. The algorithm GRÖBNER_B applied to $F = \{f_1, f_2, f_3\}$ yields (after reducing the result) the reduced Gröbner basis

$G = \{g_1, g_2, g_3\}$, where

$$\begin{aligned} g_1 &= 65z + 64x^4 - 432x^3 + 168x^2 - 354x + 104, \\ g_2 &= 26y^2 - 16x^4 + 108x^3 - 16x^2 + 17x, \\ g_3 &= 32x^5 - 216x^4 + 64x^3 - 42x^2 + 32x + 5. \end{aligned}$$

By Theorem 2.4.4 the system is solvable. Furthermore, by Theorem 2.4.5 the system has finitely many solutions. The Gröbner basis G yields an equivalent triangular system in which the variables are completely separated. So we can get solutions by solving the univariate polynomial g_3 and propagating the partial solutions upwards to solutions of the full system. The univariate polynomial g_3 is irreducible over $\mathbb{Q}$, and the solutions are

$$\left(\alpha,\ \pm\frac{1}{\sqrt{26}}\sqrt{16\alpha^4 - 108\alpha^3 + 16\alpha^2 - 17\alpha},\ -\frac{1}{65}(64\alpha^4 - 432\alpha^3 + 168\alpha^2 - 354\alpha + 104)\right),$$

where α is a root of g_3. We can also determine a numerical approximation of a solution from G, e.g.

$$(-0.1284722871,\ 0.3211444930,\ -2.356700326). \qquad \square$$

Arithmetic of polynomial ideals

In commutative algebra and algebraic geometry there is a strong correspondence between radical polynomial ideals and algebraic sets, the sets of zeros of such ideals over the algebraic closure of the field of coefficients. For any ideal I in $K[x_1, \ldots, x_n]$ we denote by $V(I)$ the set of all points in $\mathbb{A}^n(\overline{K}) = \overline{K}^n$, the n–dimensional affine space over the algebraic closure of K, which are common zeros of all the polynomials in I. Such sets $V(I)$ are called *algebraic sets*. On the other hand, for any subset V of $\mathbb{A}^n(\overline{K})$ we denote by $I(V)$ the ideal of all polynomials vanishing on V. Then for radical ideals I and algebraic sets V the functions $V(\cdot)$ and $I(\cdot)$ are inverses of each other, i.e.

$$V(I(V)) = V \quad \text{and} \quad I(V(I)) = I.$$

This correspondence for radical ideals is called Hilbert's Nullstellensatz. In terms of operations on ideals and algebraic sets we get the following relations:

ideal	algebraic set
$I + J$	$V(I) \cap V(J)$
$I \cdot J,\ I \cap J$	$V(I) \cup V(J)$
$I : J$	$V(I) - V(J) = \overline{V(I) - V(J)}$ (Zariski closure of the difference)

So we can effectively compute intersection, union, and difference of varieties if we can carry out the corresponding operations on ideals.

Definition 2.4.8. Let I, J be ideals in $K[X]$.
The *sum* $I + J$ of I and J is defined as

$$I + J = \{f + g \mid f \in I, g \in J\}.$$

The *product* $I \cdot J$ of I and J is defined as

$$I \cdot J = \langle \{f \cdot g \mid f \in I, g \in J\} \rangle.$$

The *quotient* $I : J$ of I and J is defined as

$$I : J = \{f \mid f \cdot g \in I \text{ for all } g \in J\}.$$ □

Theorem 2.4.9. *Let $I = \langle f_1, \ldots, f_r\rangle$ and $J = \langle g_1, \ldots, g_s\rangle$ be ideals in $K[X]$.*

(a) $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s\rangle$.

(b) $I \cdot J = \langle f_i g_j \mid 1 \le i \le r, 1 \le j \le s\rangle$.

(c) $I \cap J = (\langle t\rangle \cdot I + \langle 1 - t\rangle \cdot J) \cap K[X]$, *where t is a new variable.*

(d) $I : J = \bigcap_{j=1}^{s} (I : \langle g_j\rangle)$ *and*
$I : \langle g\rangle = \langle h_1/g, \ldots, h_m/g\rangle$, *where* $I \cap \langle g\rangle = \langle h_1, \ldots, h_m\rangle$.

Proof: [Winkler 1996] Theorem 8.4.9. □

So all these operations can be carried out effectively by operations on the bases of the ideals. In particular the intersection can be computed by the Elimination Property of Gröbner bases (Theorem 2.4.6).

We always have $I \cdot J \subset I \cap J$. However, $I \cap J$ could be strictly larger than $I \cdot J$. For example, if $I = J = \langle x, y\rangle$, then $I \cdot J = \langle x^2, xy, y^2\rangle$ and $I \cap J = I = J = \langle x, y\rangle$. Both $I \cdot J$ and $I \cap J$ correspond to the same variety. Since a basis for $I \cdot J$ is more easily computed, why should we bother with $I \cap J$? The reason is that the intersection behaves much better with respect to the operation of taking radicals (recall that it is really the radical ideals that uniquely correspond to algebraic sets). Whereas the product of radical ideals in general fails to be radical (consider $I \cdot I$), the intersection of radical ideals is always radical.

Theorem 2.4.10. *Let I, J be ideals in $K[X]$. Then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ ($\sqrt{I}$ means the radical of I).*

Proof: [Winkler 1996] Theorem 8.4.10. □

Example 2.4.11. Consider the ideals

$$\begin{aligned} I_1 &= \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4\rangle, \\ I_2 &= \langle x, y^2 - 4\rangle, \\ I_3 &= \langle x, y^2 - 2y\rangle, \\ I_4 &= \langle x, y^2 + 2y\rangle. \end{aligned}$$

The coefficients are all integers, but we consider them as defining algebraic sets in the affine plane over $\mathbb{C}$. In fact, $V(I_1)$ is the tacnode curve (compare Section 1.1), $V(I_2) = \{(0, 2), (0, -2)\}$, $V(I_3) = \{(0, 2), (0, 0)\}$, $V(I_4) = \{(0, 0), (0, -2)\}$.

First, let us compute the ideal I_5 defining the union of the tacnode and the 2 points in $V(I_2)$. I_5 is the intersection of I_1 and I_2, i.e.

$$\begin{aligned} I_5 &= I_1 \cap I_2 \\ &= (\langle z\rangle I_1 + \langle 1 - z\rangle I_2) \cap \mathbb{Q}[x, y] \\ &= \langle -4y^2 + 8y^3 - 3y^4 + 12x^2y - 8x^4 - 2y^5 + y^6 - 3x^2y^3 + 2y^2x^4, \\ &\quad xy^2 - 2xy^3 + xy^4 - 3x^3y + 2x^5\rangle. \end{aligned}$$

Now let us compute the ideal I_6 defining $V(I_5) - V(I_3)$, i.e. the Zariski closure of $V(I_5) \setminus V(I_3)$, i.e. the smallest algebraic set containing $V(I_5) \setminus V(I_3)$.

$$\begin{aligned} I_6 &= I_5 : I_3 \\ &= (I_5 : \langle x \rangle) \cap (I_5 : \langle y^2 - 2y \rangle) \\ &= \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle \cap \\ &\quad \langle y^5 - 3y^3 + 2y^2 - 3x^2y^2 + 2yx^4 - 6x^2y + 4x^4, 2x^5 - 3x^3y + xy^2 - 2xy^3 + xy^4 \rangle \\ &= \langle y^5 - 3y^3 + 2y^2 - 3x^2y^2 + 2yx^4 - 6x^2y + 4x^4, 2x^5 - 3x^3y + xy^2 - 2xy^3 + xy^4 \rangle \end{aligned}$$

$V(I_6)$ is the tacnode plus the point $(0, -2)$.
Finally, let us compute the ideal I_7 defining $V(I_6) - V(I_4)$, i.e. the Zariski closure of $V(I_6) \setminus V(I_4)$.

$$\begin{aligned} I_7 &= I_6 : I_4 \\ &= (I_6 : \langle x \rangle) \cap (I_6 : \langle y^2 + 2y \rangle) \\ &= \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle \ \cap \ \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle \\ &= I_1. \end{aligned}$$

So we get back the ideal I_1 defining the tacnode curve. □

Algebraic curves and surfaces

Algebraic curves and surfaces have been studied intensively in algebraic geometry for decades and even centuries. Thus, there exists a huge amount of theoretical knowledge about these geometric objects. Recently, algebraic curves and surfaces play an important and ever increasing rôle in computer aided geometric design, computer vision, and computer aided manufacturing. Consequently, theoretical results need to be adapted to practical needs. We need efficient algorithms for generating, representing, manipulating, analyzing, rendering algebraic curves and surfaces.

One interesting subproblem is the rational parametrization of curves and surfaces. Consider an affine plane algebraic curve $\mathcal{C}$ in $\mathbb{A}^2(\overline{K})$ in *implicit representation*, defined by the bivariate polynomial $f(x, y) \in K[x, y]$. I.e.

$$\mathcal{C} = \{(a, b) \mid (a, b) \in \mathbb{A}^2(\overline{K}) \text{ and } f(a, b) = 0\}.$$

Definition 2.4.12. A pair of rational functions $\mathcal{P}(t) = (x(t), y(t)) \in \overline{K}(t)$ is a *rational parametrization* of the curve $\mathcal{C}$, if and only if $f(x(t), y(t)) = 0$ and for almost every point $(x_0, y_0) \in \mathcal{C}$ (i.e. up to finitely many exceptions) there is a parameter value $t_0 \in \overline{K}$ such that $(x_0, y_0) = (x(t_0), y(t_0))$.

The parametrization $\mathcal{P}$ is *proper* iff almost every point on $\mathcal{C}$ is generated by exactly 1 parameter value. □

Only irreducible curves, i.e. curves whose defining polynomial is absolutely irreducible, can have a rational parametrization. Almost any rational transformation of a rational parametrization is again a rational parametrization, so such parametrizations are not unique.

Implicit representations (by defining polynomial) and parametric representations (by rational parametrization) both have their particular advantages and disadvantages. Given an implicit representation of a curve and a point in the plane, it is easy to check whether the point is on the curve. But it is hard to generate "good" points on the curve, i.e. for instance points with rational coordinates if the defining field is $\mathbb{Q}$. On the other hand, generating good points is easy for a curve given parametrically, but deciding whether a point is on the curve requires the solution of a system of algebraic equations. So it is highly desirable to have efficient algorithms for changing from implicit to parametric representation, and vice versa.

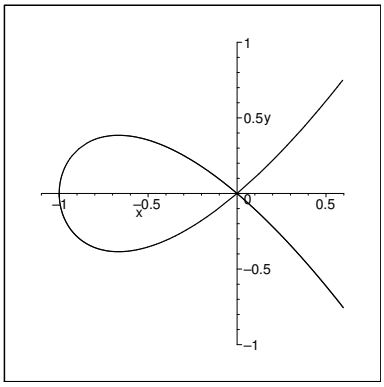

Fig. 2.4.1 parametric cubic

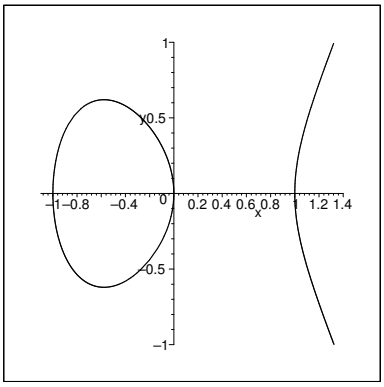

Fig. 2.4.2 elliptic curve

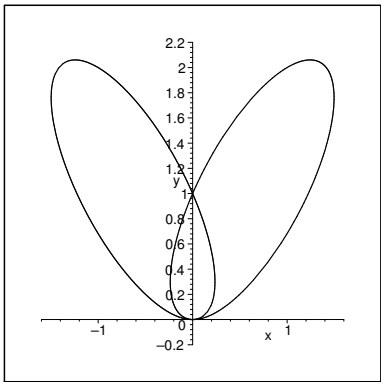

Fig. 2.4.3 tacnode

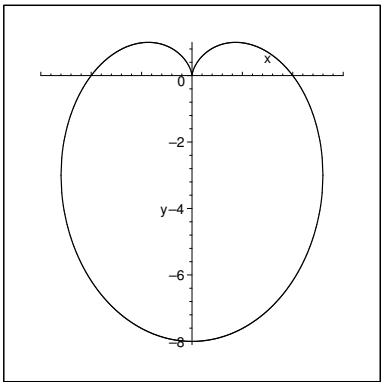

Fig. 2.4.4 cardioid

Example 2.4.13: Let us consider curves in the plane (affine or projective) over $\mathbb{C}$. The curve defined by $f(x,y) = y^2 - x^3 - x^2$ (see Fig. 2.4.1) is rationally parametrizable, and actually a parametrization is $(t^2-1, t(t^2-1))$.

On the other hand, the elliptic curve defined by $f(x,y) = y^2 - x^3 + x$ (see Fig 2.4.2) does not have a rational parametrization.

The tacnode curve (see Fig. 2.4.3) defined by $f(x,y) = 2x^4 - 3x^2y + y^4 - 2y^3 + y^2$ has the parametrization

$$x(t) = \frac{t^3 - 6t^2 + 9t - 2}{2t^4 - 26t^3 + 40t^2 - 32t + 9}, \quad y(t) = \frac{t^2 - 4t + 4}{2t^4 - 26t^3 + 40t^2 - 32t + 9}.$$

The criterion for parametrizability of a curve is its genus. Only curves of genus 0, i.e. curves having as many singularities as their degree permits, have a rational parametrization. □

Computing such a parametrization essentially requires the full analysis of singularities (either by successive blow-ups, or by Puiseux expansion) and the determination of a regular point on the curve. Elimination methods such as Gröbner bases or resultants are the tools for the singularity analysis. If the curve $\mathcal{C}$ is defined over the field K, then the singularitites of $\mathcal{C}$ come in full conjugacy classes over K. Whereas the singularity structure of a curve is fixed, we can control the quality of the resulting parametrization by controlling the field over which we choose the regular point for the parametrization. Thus, finding a regular curve point over a minimal field extension on a curve of genus 0 is one of the central problems in rational parametrization. For a thorough introduction to rational algebraic curves we refer to

J.R. Sendra, F. Winkler, S. Pérez-Díaz,
Rational Algebraic Curves – A Computer Algebra Approach,
Series Algorithms and Computation in Mathematics Vol. 22,
Springer-Verlag Berlin Heidelberg (2008)

Example 2.4.14: Let $\mathcal{C}$ be the cardioid curve in the complex plane defined by

$$f(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) = 0.$$

For a picture of this curve in the real affine plane see Fig. 2.4.4.

The curve $\mathcal{C}$ has the following rational parametrization:

$$\begin{array}{rl} x(t) & = -32 \cdot \frac{-1024i+128t-144it^2-22t^3+it^4}{2304-3072it-736t^2-192it^3+9t^4}, \\ y(t) & = -40 \cdot \frac{1024-256it-80t^2+16it^3+t^4}{2304-3072it-736t^2-192it^3+9t^4}. \end{array}$$

So, as we see in Fig. 2.4.4, $\mathcal{C}$ has infinitely many real points. But generating any one of these real points from the above parametrization is not obvious. Does this real curve $\mathcal{C}$ also have a parametrization over $\mathbb{R}$? Indeed it does, let's see how we can get one.

In the projective plane over $\mathbb{C}$, $\mathcal{C}$ has 3 double points, namely $(0:0:1)$ and $(1:\pm i:0)$. Let $\tilde{\mathcal{H}}$ be the linear system of conics passing through all these double points. The system $\tilde{\mathcal{H}}$ has dimension 2 and is defined by

$$h(x,y,z,s,t) = x^2 + sxz + y^2 + tyz = 0.$$

I.e., for any particular values of s and t we get a conic in $\tilde{\mathcal{H}}$. 3 elements of this linear system define a birational transformation

$$\begin{array}{rl} \mathcal{T} & = (h(x,y,z,0,1) : h(x,y,z,1,0) : h(x,y,z,1,1)) \\ & = (x^2 + y^2 + yz : x^2 + xz + y^2 : x^2 + xz + y^2 + yz) \end{array}$$

which transforms $\mathcal{C}$ to the conic $\mathcal{D}$ defined by

$$15x^2 + 7y^2 + 6xy - 38x - 14y + 23 = 0.$$

For a conic defined over $\mathbb{Q}$ we can decide whether it has a point over $\mathbb{Q}$ or $\mathbb{R}$. In particular, we determine the point $(1, 8/7)$ on $\mathcal{D}$, which, by $\mathcal{T}^{-1}$, corresponds to the regular point

$P = (0, -8)$ on $\mathcal{C}$. Now, by resticting $\tilde{\mathcal{H}}$ to conics through P and intersecting $\tilde{\mathcal{H}}$ with $\mathcal{C}$, we get the parametrization

$$x(t) = \frac{-1024t^3}{256t^4 + 32t^2 + 1}, \quad y(t) = \frac{-2048t^4 + 128t^2}{256t^4 + 32t^2 + 1}.$$

over the reals.

Let us see how some of these computational steps can be executed in Maple 16:

```
> with(Groebner):
> f := (x^2+4*y+y^2)^2 - 16*(x^2+y^2);
```

$$f := (x^2 + 4y + y^2)^2 - 16x^2 - 16y^2$$

```
> h := x^2 + s*x + y^2 + t*y
```

$$h := x^2 + sx + y^2 + ty$$

```
> subs({x=0,y=-8},h);
```

$$64 - 8t$$

```
> hh := subs(t=8,h);
```

$$hh := x^2 + sx + y^2 + 8y$$

```
> Gy := Basis({f,hh},plex(x,y,s));
```

$$Gy := \{16384y^2 + 4096y^3 + 256y^4 - 1024s^2y^2 + 128s^2y^3 + 8s^4y^3 + 32s^2y^4 + s^4y^4, \ldots\}$$

```
> factor(Gy[1]);
```

$$y^2(y + 8)(256y + 32s^2y + s^4y + 2048 - 128s^2)$$

```
> psy := solve(simplify(Gy[1]/(y^2*(y+8))),y);
```

$$psy := \frac{128(s^2 - 16)}{256 + 32s^2 + s^4}$$

```
> Gx := Basis({f,hh},plex(y,x,s));
```

$$Gx := \{256x^3 + 32s^2x^3 + s^4x^3 + 1024x^2s, \ldots\}$$

```
> factor(Gx[1]);
```

$$x^2(256x + 32s^2x + s^4x + 1024s)$$

```
> psx := solve(simplify(Gx[1]/x^2),x);
```

$$psx := -\frac{1024s}{256 + 32s^2 + s^4}$$

```
> simplify(subs({x=psx,y=psy},f));
```

$$0$$

> **ptx := simplify(subs(s=1/t,psx));**

$$ptx := -\frac{1024t^3}{256t^4+32t^2+1}$$

> **pty := simplify(subs(s=1/t,psy));**

$$pty := -\frac{128(-1+16t^2)t^2}{256t^4+32t^2+1}$$

> **simplify(subs({x=ptx,y=pty},f));**

$$0$$

These parametrizations are proper, i.e. they produce every curve point exactly once (with finitely many exceptions). In fact, whenever we transform a proper parametrization by an invertible rational mapping then we get another proper parametrization. □

Many of these ideas which work for curves can actually be generalized to higher dimensional geometric objects.

Example 2.4.15: Let $\mathcal{S}$ be the surface constructed in the following way. Consider a sphere of radius 2 centered at $(0,0,0)$ and a cylinder along the z-axis over the circle of radius 1 centered at $(1,0,0)$ in the $x-y$-plane. These two surfaces intersect in an 8-shaped curve $\mathcal{C}$ on the sphere. Now let a ball of radius r roll along the curve $\mathcal{C}$. The ball starts out with radius $r=0$ at the point $(2,0,0)$, increases in diameter and shrinks again on its way back to $(2,0,0)$, and then traverses the second loop of $\mathcal{C}$ in the same way. The resulting surface $\mathcal{S}$ is a so-called canal surface; compare Fig. 2.4.5.

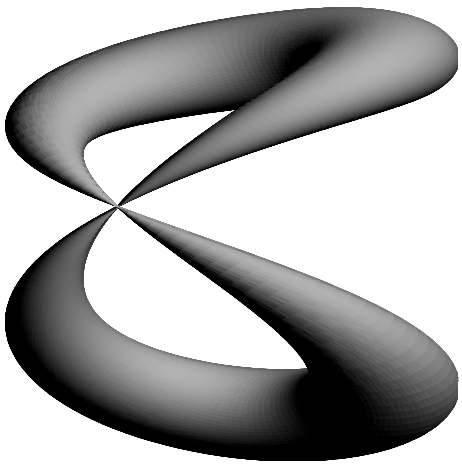

Fig. 2.4.5 canal surface

The surface $\mathcal{S}$ has a rational parametrization. □

Now that we have seen some examples of parametrization treated by symbolic algebraic computation, let us discuss the inverse problem, namely the problem of implicitization. If we are given, for instance, a rational parametrization in $K(t)$ of a plane curve, i.e.

$$x(t)=p(t)/r(t), \quad y(t)=q(t)/r(t),$$

we essentially want to eliminate the parameter t from these relations, and get a relation just between x and y. We also want to make sure that we do not consider components for which the denominator $r(t)$ vanishes. This leads to the system of algebraic equations

$$\begin{aligned} x \cdot r(t) - p(t) &= 0, \\ y \cdot r(t) - q(t) &= 0, \\ r(t) \cdot z - 1 &= 0. \end{aligned}$$

The implicit equation of the curve must be the generator of the ideal

$$I = \langle x \cdot r(t) - p(t), y \cdot r(t) - q(t), r(t) \cdot z - 1 \rangle_{/K[x,y,z,t]} \cap K[x, y].$$

Using the elimination property of Gröbner bases, we can compute this generator by a Gröbner basis computation w.r.t. the lexicographic ordering based on $x < y < z < t$.

Example 2.4.16. Let us do this for the cardioid curve. We start from the parametrization

$$x(t) = \frac{-1024t^3}{256t^4 + 32t^2 + 1}, \quad y(t) = \frac{-2048t^4 + 128t^2}{256t^4 + 32t^2 + 1}.$$

So we have to solve the equations

$$\begin{aligned} x \cdot (256t^4 + 32t^2 + 1) + 1024t^3 &= 0, \\ y \cdot (256t^4 + 32t^2 + 1) + 2048t^4 - 128t^2 &= 0, \\ (256t^4 + 32t^2 + 1) \cdot z - 1 &= 0. \end{aligned}$$

The Gröbner basis of this system w.r.t. the lexicographic ordering based on $x < y < z < t$ is

$$G = \{....., x^4 + y^4 + 8x^2y + 2x^2y^2 + 8y^3 - 16x^2\}.$$

The polynomial in G depending only on x and y is the implicit equation of the curve. □

Syzygies — Linear equations over $K[X]$ — Free resolutions

For given polynomials $f_1, \ldots, f_s, f$ in $K[X]$ we consider the linear equation

$$f_1 z_1 + \ldots + f_s z_s = f, \tag{2.4.2}$$

or the corresponding homogeneous equation

$$f_1 z_1 + \ldots + f_s z_s = 0. \tag{2.4.3}$$

Let F be the vector $(f_1, \ldots, f_s)$. The general solution of (2.4.3) and (2.4.3) is to be sought in $K[X]^s$. The solutions of (2.4.3) form a module over the ring $K[X]$, a submodule of $K[X]^s$ over $K[X]$.

Definition 2.4.17. Any solution of (2.4.3) is called a *syzygy* of the sequence of polynomials $f_1, \ldots, f_s$. The module of all solutions of (2.4.3) is the *module of syzygies* $\mathrm{Syz}(F)$ of $F = (f_1, \ldots, f_s)$. □

It turns out that if the coefficients of this equation are a Gröbner basis, then we can immediately write down a generating set (basis) for the module $\mathrm{Syz}(F)$. The general case will be reduced to this one.

Theorem 2.4.18. *If the elements of $F = (f_1, \ldots, f_s)$ are a Gröbner basis, then S is a basis for $\mathrm{Syz}(F)$, where S is defined as follows.*

For $1 \leq i \leq s$ let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ be the i–th unit vector and for $1 \leq i < j \leq s$ let

$$t = \mathrm{lcm}(\mathrm{lpp}(f_i), \mathrm{lpp}(f_j)),$$
$$p_{ij} = \tfrac{1}{\mathrm{lc}(f_i)} \cdot \tfrac{t}{\mathrm{lpp}(f_i)}, \quad q_{ij} = \tfrac{1}{\mathrm{lc}(f_j)} \cdot \tfrac{t}{\mathrm{lpp}(f_j)},$$

and $k_{ij}^1, \ldots, k_{ij}^s$ be the polynomials extracted from a reduction of $\mathrm{spol}(f_i, f_j)$ to 0, such that

$$\mathrm{spol}(f_i, f_j) = p_{ij} f_i - q_{ij} f_j = \sum_{l=1}^{s} k_{ij}^l f_l.$$

Then

$$S = \{\underbrace{p_{ij} \cdot e_i - q_{ij} \cdot e_j - (k_{ij}^1, \ldots, k_{ij}^s)}_{S_{ij}} \mid 1 \leq i < j \leq s\}.$$

Proof: [Winkler 1996] Theorem 8.4.7.
Obviously every element of S is a syzygy of F, since every S–polynomial reduces to 0.
On the other hand let $z = (z_1, \ldots, z_s) \neq (0, \ldots, 0)$ be an arbitrary non-trivial syzygy of F. Let p be the hightest power product occurring in

$$f_1 z_1 + \ldots + f_s z_s = 0, \qquad (*)$$

i.e.

$$p = \max_{<}\{t \in [X] \mid \mathrm{coeff}(f_i \cdot z_i, t) \neq 0 \text{ for some } i\}$$

and let $i_1 < \ldots < i_m$ be those indices such that $\mathrm{lpp}(f_{i_j} \cdot z_{i_j}) = p$. We have $m \geq 2$. Suppose that $m > 2$. By subtracting a suitable multiple of S_{i_{m-1}, i_m} from z, we can reduce the number of positions in z that contribute to the highest power product p in $(*)$. Iterating this process $m-2$ times, we finally reach a situation, where only two positions i_1, i_2 in the syzygy contribute to the power product p. Now the highest power product in $(*)$ can be decreased by subtracting a suitable multiple of S_{i_1, i_2}. Since $<$ is Noetherian, this process terminates, leading to an expression of z as a linear combination of elements of S. □

Now that we are able to solve homogeneous linear equations in which the coefficients are a Gröbner basis, let us see how we can transform the general case to this one.

Theorem 7.4.19. *Let $F = (f_1, \ldots, f_s)^T$ be a vector of polynomials in $K[X]$ and let the elements of $G = (g_1, \ldots, g_m)^T$ be a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$. We view F and G as column vectors. Let the r rows of the matrix R be a basis for $\mathrm{Syz}(G)$ and let the matrices A, B be such that $G = A \cdot F$ and $F = B \cdot G$. Then the rows of Q are a basis for $\mathrm{Syz}(F)$, where*

$$Q = \begin{pmatrix} I_s - B \cdot A \\ \ldots\ldots\ldots\ldots \\ R \cdot A \end{pmatrix}$$

Proof: [Winkler 1996] Theorem 8.4.8.
Let $b_1, \ldots, b_{s+r}$ be polynomials, $b = (b_1, \ldots, b_{s+r})$.

$$\begin{aligned}
&(b \cdot Q) \cdot F = \\
&((b_1, \ldots, b_s) \cdot (I_s - B \cdot A) + (b_{s+1}, \ldots, b_{s+r}) \cdot R \cdot A) \cdot F = \\
&(b_1, \ldots, b_s) \cdot (F - \underbrace{B \cdot A \cdot F}_{=F}) + (b_{s+1}, \ldots, b_{s+r}) \cdot R \cdot \underbrace{A \cdot F}_{=G} = 0
\end{aligned}$$

So every linear combination of the rows of Q is a syzygy of F.
On the other hand, let $H = (h_1, \ldots, h_s)$ be a syzygy of F. Then $H \cdot B$ is a syzygy of G. So for some H' we can write $H \cdot B = H' \cdot R$, and therefore $H \cdot B \cdot A = H' \cdot R \cdot A$. Thus,

$$H = H \cdot (I_s - B \cdot A) + H' \cdot R \cdot A = (H, H') \cdot Q,$$

i.e. H is a linear combination of the rows of Q. □

What we still need is a particular solution of the inhomogeneous equation (2.4.2). Let $G = (g_1, \ldots, g_m)$ be a Gröbner basis for $\langle F \rangle$ and let A be the transformation matrix such that $G = A \cdot F$ (G and F viewed as column vectors). Then a particular solution of (7.1) exists if and only if $f \in \langle F \rangle = \langle G \rangle$. If the reduction of f to normal form modulo G yields $f' \neq 0$, then (2.4.2) is unsolvable. Otherwise we can extract from this reduction polynomials $h'_1, \ldots, h'_m$ such that

$$g_1 h'_1 + \ldots + g_m h'_m = f.$$

So $H = (h'_1, \ldots, h'_m) \cdot A$ is a particular solution of (2.4.2).

Of course, once we are able to solve single linear equations over $K[X]$, we can also solve systems of linear equations by dealing with the equations recursively. However, it is also possible to extend the concept of Gröbner bases from ideals to modules and solve a whole system of linear equations by a single computation of a Gröbner basis for a submodule of $K[X]^s$.

Example 2.4.20. Consider the linear equation

$$\underbrace{\left(xz - xy^2 - 4x^2 - \frac{1}{4} \quad y^2z + 2x + \frac{1}{2} \quad x^2z + y^2 + \frac{1}{2}x \right)}_{F} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = 0,$$

where the coefficients are in $\mathbb{Q}[x, y, z]$. A basis for the syzygies can be computed as the rows of a matrix Q according to Theorem 2.4.19. Q^T may contain for instance the syzygy

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 2xy^2 + 4x^2y^4 + 2x^3y^2 + 4y^4 - 2x^4 - 8x^3 - 2x^2 - 8x^5 \\ -8x^3y^2 - 4x^5y^2 - 4xy^2 - 3x^2 - 19x^4 - 16x^6 \\ y^2 + 17x^2y^2 + 16x^4y^2 + 4x^3y^4 + 4xy^4 + 8x^4 + 2x^3 + 8x^2 + 2x \end{pmatrix}.$$

In fact, using the concept of Gröbner bases for modules, we get the following basis for $\mathrm{Syz}(F)$:

$$\begin{pmatrix} y^2z + 2x + \frac{1}{2} \\ -xz + xy^2 + 4x^2 + \frac{1}{4} \\ 0 \end{pmatrix}, \quad \begin{pmatrix} x^2z + y^2 + \frac{1}{2}x \\ 0 \\ -xz + xy^2 + 4x^2 + \frac{1}{4} \end{pmatrix}$$

$$\begin{pmatrix} y^4 + \frac{1}{2}xy^2 - 2x^3 - \frac{1}{2}x^2 \\ -x^3y^2 - xy^2 - 4x^4 - \frac{3}{4}x^2 \\ xy^4 + 4x^2y^2 + \frac{1}{4}y^2 + 2x^2 + \frac{1}{2}x \end{pmatrix} \quad , \quad \begin{pmatrix} 0 \\ x^2z + y^2 + \frac{1}{2}x \\ -y^2z - 2x - \frac{1}{2} \end{pmatrix} \qquad \square$$

The computation of syzygies is crucial for free resolution of ideals and modules. Modules are "vector spaces over rings", so the domain of scalars is not (necessarily) a field, but a ring. Every commutative ring R with 1 is a module over itself. The submodules of R are just the ideals in R. For every $n \in \mathbb{N}$ we have that R^n is a module over R; the free module of dimension n over R.

In vector spaces we can talk about linear independence of a generating set, which is then called a (vector-space) basis. If 0 can be written as a non-trivial linear combination of generators, then one of the generators can be expressed in terms of the others. Not so in modules; the corresponding scalar might not be invertible. So linear independence poses a special problem in module theory. A free resolution of a module M (or ideal) is a representation of M in terms of generators, the relations between the generators (first syzygies), the relations between the relations of the genarators (second syzygies), etc. In his seminal paper [1] of 1890 David Hilbert has shown that this process terminates for every finitely generated module.

In the following let R be a commutative ring with 1.

Definition 2.4.21. Consider a sequence of R-modules and homomorphisms

$$\cdots \longrightarrow M_{i+1} \longrightarrow^{\varphi_{i+1}} M_i \longrightarrow^{\varphi_i} M_{i-1} \longrightarrow \cdots$$

We say the sequence is *exact at* M_i iff $\mathrm{im}(\varphi_{i+1}) = \ker(\varphi_i)$.
The entire sequence is said to be *exact* iff it is exact at each M_i which is not at the beginning or the end of the sequence. $\square$

Definition 2.4.22. Let M be an R-module. A *free resolution* of M is an exact sequence of the form

$$\cdots \longrightarrow R^{n_2} \longrightarrow^{\varphi_2} R^{n_1} \longrightarrow^{\varphi_1} R^{n_0} \longrightarrow^{\varphi_0} M \longrightarrow 0 \ .$$

Observe that all modules in this sequence except M are free.
If there is an $l \in \mathbb{N}$ s.t. $n_l \neq 0$ but $n_k = 0$ for all $k > l$, then we say that the resolution is *finite*, of *length* l. A finite resolution of length l is usually written as

$$0 \longrightarrow R^{n_l} \longrightarrow R^{n_{l-1}} \longrightarrow \cdots \longrightarrow R^{n_1} \longrightarrow R^{n_0} \longrightarrow M \longrightarrow 0 \ . \qquad \square$$

Let's see how we can construct a free resolution of a finitely generated module $M = \langle m_1, \ldots, m_{n_0} \rangle$. We determine a basis (generating set) $\{s_1, \ldots, s_{n_1}\}$ of $\mathrm{Syz}(m_1, \ldots, m_{n_0})$, the syzygy module of $(m_1, \ldots, m_{n_0})$. Let

$$\begin{array}{rccc} \varphi_0 : & R^{n_0} & \longrightarrow & M \\ & (r_1, \ldots, r_{n_0})^T & \mapsto & \sum r_i m_i \end{array}$$

$$\begin{array}{rccc} \varphi_1 : & R^{n_1} & \longrightarrow & R^{n_0} \\ & (r_1, \ldots, r_{n_1})^T & \mapsto & \sum r_i s_i \end{array}$$

[1] D.Hilbert, *Über die Theorie der algebraischen Formen*, Math.Annalen 36, 473–534 (1890)

Then we have $\mathrm{im}(\varphi_1) = \mathrm{Syz}(m_i) = \ker(\varphi_0)$, so the sequence

$$R^{n_1} \longrightarrow^{\varphi_1} R^{n_0} \longrightarrow^{\varphi_0} M \longrightarrow 0$$

is exact. Continuing this process with $\mathrm{Syz}(m_i)$ instead of M, we finally get a free resolution of M.

Example 2.4. (from [Cox,Little,O'Shea 1998] [2] Chap. 6.1)
Consider the ideal (which is also a module)

$$I = \langle \underbrace{x^2 - x, xy, y^2 - y}_{F} \rangle$$

in $R = K[x, y]$. In geometric terms, I is the ideal of the variety $V = \{(0, 0), (1, 0), (0, 1)\}$ in K^2. Let

$$\begin{array}{rccl} \varphi_0 : & R^3 & \longrightarrow & I \\ & \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} & \mapsto & \underbrace{\left(x^2 - x, xy, y^2 - y\right)}_{A} \cdot \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} \end{array}$$

The mapping φ_0 represents the generation of I from the free module R^3. Next we determine relations between the generators, i.e. (first) syzygies. The columns of the matrix

$$B = \begin{pmatrix} y & 0 \\ -x+1 & y-1 \\ 0 & -x \end{pmatrix}$$

generate the syzygy module $\mathrm{Syz}(F)$. So for

$$\begin{array}{rccl} \varphi_1 : & R^2 & \longrightarrow & R^3 \\ & \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} & \mapsto & B \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \end{array}$$

we get the exact sequence

$$R^2 \longrightarrow^{\varphi_1} R^3 \longrightarrow^{\varphi_0} I \longrightarrow 0 \ .$$

The resolution process terminates right here. If (c_1, c_2) is any syzygy of the columns of B, i.e. a second syzygy of F, then

$$c_1 \begin{pmatrix} y \\ -x+1 \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} 0 \\ y-1 \\ -x \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \ .$$

Looking at the first component we see that $c_1 y = 0$, so $c_1 = 0$. Similarly, from the third component we get $c_2 = 0$. Hence the kernel of φ_1 is the zero module 0. There are no non-trivial relations between the columns of B, so the first syzygy module $\mathrm{Syz}(F)$ is the free module R^2. Finally this leads to the free resolution

$$0 \longrightarrow R^2 \longrightarrow^{\varphi_1} R^3 \longrightarrow^{\varphi_0} I \longrightarrow 0$$

of length 1 of the module (ideal) I in $R = K[x, y]$. □

[2] D.Cox, J.Little, D.O'Shea, *Using Algebraic Geometry*, Springer-Verlag (1998)