SCIEnce Training School in Symbolic Computation
RISC, Univ.Linz, 29.6.–10.7. 2009

Gröbner Bases — Theory and Applications

Franz Winkler

Research Institute for Symbolic Computation
(RISC-Linz)
Johannes Kepler University
Linz, Austria
Franz.Winkler@jku.at

Contents

1 The notion of a Gröbner basis

The material of this chapter is largely taken from [Winkler 1996], where also proofs of theorems are given.

Before we start with the technical details, let us briefly review the historical development leading to the concept of Gröbner bases. In his seminal paper [Hilbert 1890], D. Hilbert gave a proof of his famous Basis Theorem as well as of the structure and length of the sequence of syzygy modules of a polynomial system. Implicitly he also showed that the Hauptproblem, i.e. the problem whether $f \in I$ for a given polynomial f and polynomial ideal I, can be solved effectively. Hilbert's solution of the Hauptproblem (and similar problems) was reinvestigated by G. Hermann in [Hermann 1926]. She counted the field operations required in this effective procedure and arrived at a double exponential upper bound in the number of variables. In fact, Hermann's, or for that matter Hilbert's, algorithm always actually achieves this worst case double exponential complexity. The next important step came when B. Buchberger, in his doctoral thesis [Buchberger 1965] advised by W. Gröbner, introduced the notion of a Gröbner basis (he did not call it that at this time) and also gave an algorithm for computing it. Gröbner bases are very special and useful bases for polynomial ideals. In subsequent publications, e.g. [Buchberger 1970,1985], Buchberger exhibited important additional applications of his Gröbner bases method, e.g. to the solution of systems of polynomial equations. In the worst case, Buchberger's Gröbner bases algorithm is also double exponential in the number of variables, but in practice there are many interesting examples which can be solved in reasonable time. But still, in the worst case, the double exponential behaviour is not avoided. And, in fact, it cannot be avoided by any algorithm capable of solving the Hauptproblem, as was shown by E.W. Mayr and A.R. Meyer in [Mayr,Meyer 1982].

When we are solving systems of polynomial (algebraic) equations, the important parameters are the number of variables n and the degree of the polynomials d. The Buchberger algorithm for constructing Gröbner bases is at the same time a generalization of Euclid's algorithm for computing the greatest common divisor (GCD) of univariate polynomials (the case $n = 1$) and of Gauss' triangularization algorithm for linear systems (the case $d = 1$). Both these algorithms are concerned with solving systems of polynomial equations, and they determine a canonical basis (either the GCD of the inputs or a triangularized form of the system) for the given polynomial system. Buchberger's algorithm can be seen as a generalization to the case of arbitrary n and d.

Let K be a computable field and $K[X] = K[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates over K. If F is any subset of $K[X]$ we write $\langle F \rangle$ or ideal(F) for the ideal generated by F in $K[X]$. By $[X]$ we denote the monoid (under multiplication) of *power products* $x_1^{i_1} \cdots x_n^{i_n}$ in $x_1, \ldots, x_n$. $1 = x_1^0 \ldots x_n^0$ is the unit element in the monoid $[X]$. lcm(s, t) denotes the least common multiple of the power products s, t.

Commutative rings with 1 in which the *basis condition* holds, i.e. in which every ideal has a finite basis, are usually called *Noetherian rings*. This notation is motivated by the following lemma.

Lemma 1.1. *In a Noetherian ring there are no infinitely ascending chains of ideals.* □

Theorem 1.2. (Hilbert's Basis Theorem) *If R is a Noetherian ring then also the univariate polynomial ring $R[x]$ is Noetherian.*

Hilbert's Basis Theorem implies that the multivariate polynomial ring $K[X]$ is Noetherian, if K is a field. So every ideal I in $K[X]$ has a finite basis, and if we are able to effectively compute with finite bases then we are dealing with all the ideals in $K[X]$.

We will define a Gröbner basis of a polynomial ideal via a certain reduction relation for polynomials. A Gröbner basis will be a basis with respect to which the corresponding reduction relation is confluent. Before we can define the reduction relation on the polynomial ring, we have to introduce an ordering of the power products with respect to which the reduction relation should be decreasing.

Definition 1.1. Let $<$ be an ordering on $[X]$ that is compatible with the monoid structure, i.e.

(i) $1 = x_1^0 \dots x_n^0 < t$ for all $t \in [X] \setminus \{1\}$, and

(ii) $s < t \Longrightarrow su < tu$ for all $s, t, u \in [X]$.

We call such an ordering $<$ on $[X]$ an *admissible ordering*. □

Example 1.1. We give some examples of frequently used admissible orderings on $[X]$.

(a) The *lexicographic ordering* with $x_{\pi(1)} > x_{\pi(2)} > \dots > x_{\pi(n)}$, π a permutation of $\{1, \dots, n\}$:

$x_1^{i_1} \dots x_n^{i_n} <_{lex,\pi} x_1^{j_1} \dots x_n^{j_n}$ iff there exists a $k \in \{1, \dots, n\}$ such that for all $l < k$ $i_{\pi(l)} = j_{\pi(l)}$ and $i_{\pi(k)} < j_{\pi(k)}$.

If $\pi = \mathrm{id}$, we get the usual lexicographic ordering $<_{lex}$.

(b) The *graduated lexicographic ordering* w.r.t. the permutation π and the weight function $w : \{1, \dots, n\} \to \mathbb{R}^+$:

for $s = x_1^{i_1} \dots x_n^{i_n}, t = x_1^{j_1} \dots x_n^{j_n}$ we define $s <_{glex,\pi,w} t$ iff

$$\Big(\sum_{k=1}^{n} w(k) i_k < \sum_{k=1}^{n} w(k) j_k\Big) \quad \text{or} \quad \Big(\sum_{k=1}^{n} w(k) i_k = \sum_{k=1}^{n} w(k) j_k \ \text{ and } \ s <_{lex,\pi} t\Big).$$

We get the usual graduated lexicographic ordering $<_{glex}$ by setting $\pi = \mathrm{id}$ and $w = 1_{const}$.

(c) The *graduated reverse lexicographic ordering*:

we define $s <_{grlex} t$ iff

$$\deg(s) < \deg(t) \quad \text{or} \quad (\deg(s) = \deg(t) \text{ and } t <_{lex,\pi} s, \text{ where } \pi(j) = n - j + 1).$$

(d) The *product ordering* w.r.t. $i \in \{1, \ldots, n-1\}$ and the admissible orderings $<_1$ on $X_1 = [x_1, \ldots, x_i]$ and $<_2$ on $X_2 = [x_{i+1}, \ldots, x_n]$:

for $s = s_1 s_2, t = t_1 t_2$, where $s_1, t_1 \in X_1, s_2, t_2 \in X_2$, we define $s <_{prod,i,<_1,<_2} t$ iff

$$s_1 <_1 t_1 \quad \text{or} \quad (s_1 = t_1 \text{ and } s_2 <_2 t_2). \qquad \square$$

A complete classification of admissible orderings is given in [Robbiano 1985].

Lemma 1.3. *Let $<$ be an admissible ordering on $[X]$.*

(i) If $s, t \in [X]$ and s divides t then $s \leq t$.

(ii) $<$ (or actually $>$) is Noetherian, i.e. there are no infinite chains of the form $t_0 > t_1 > t_2 > \ldots$, and consequently every subset of $[X]$ has a smallest element.

Throughout this chapter let R be a commutative ring with 1, K a field, X a set of variables, and $<$ an admissible ordering on $[X]$.

Definition 1.2. Let s be a power product in $[X]$, f a non-zero polynomial in $R[X]$, F a subset of $R[X]$.

By $\mathrm{coeff}(f, s)$ we denote the coefficient of s in f.

$\mathrm{lpp}(f) := \max_<\{t \in [X] \mid \mathrm{coeff}(f, t) \neq 0\}$ (*leading power product* of f),

$\mathrm{lc}(f) := \mathrm{coeff}(f, \mathrm{lpp}(f))$ (*leading coefficient* of f),

$\mathrm{in}(f) := \mathrm{lc}(f)\mathrm{lpp}(f)$ (*initial* of f),

$\mathrm{red}(f) := f - \mathrm{in}(f)$ (*reductum* of f),

$\mathrm{lpp}(F) := \{\mathrm{lpp}(f) \mid f \in F \setminus \{0\}\}$,

$\mathrm{lc}(F) := \{\mathrm{lc}(f) \mid f \in F \setminus \{0\}\}$,

$\mathrm{in}(F) := \{\mathrm{in}(f) \mid f \in F \setminus \{0\}\}$,

$\mathrm{red}(F) := \{\mathrm{red}(f) \mid f \in F \setminus \{0\}\}$. $\square$

If I is an ideal in $R[X]$, then $\mathrm{lc}(I) \cup \{0\}$ is an ideal in R. However, $\mathrm{in}(F) \cup \{0\}$ in general is not an ideal in $R[X]$.

Definition 1.3. Any admissible ordering $<$ on $[X]$ induces a partial ordering $\ll$ on $R[X]$, the *induced ordering*, in the following way:

$f \ll g$ iff $f = 0$ and $g \neq 0$ or
$f \neq 0$, $g \neq 0$ and $\mathrm{lpp}(f) < \mathrm{lpp}(g)$ or
$f \neq 0$, $g \neq 0$, $\mathrm{lpp}(f) = \mathrm{lpp}(g)$ and $\mathrm{red}(f) \ll \mathrm{red}(g)$. □

Lemma 1.4. *$\ll$ (or actually $\gg$) is a Noetherian partial ordering on $R[X]$.* □

One of the central notions of the theory of Gröbner bases is the concept of polynomial reduction.

Definition 1.4. Let $f, g, h \in K[X]$, $F \subseteq K[X]$. We say that g *reduces to h w.r.t. f* ($g \longrightarrow_f h$) iff there are power products $s, t \in [X]$ such that s has a non–vanishing coefficient c in g ($\mathrm{coeff}(g, s) = c \neq 0$), $s = \mathrm{lpp}(f) \cdot t$, and

$$h = g - \frac{c}{\mathrm{lc}(f)} \cdot t \cdot f.$$

If we want to indicate which power product and coefficient are used in the reduction, we write

$$g \longrightarrow_{f,b,t} h, \qquad \text{where } b = \frac{c}{lc(f)}.$$

We say that g *reduces to h w.r.t. F* ($g \longrightarrow_F h$) iff there is $f \in F$ such that $g \longrightarrow_f h$. □

Example 1.2. Let $F = \{\ldots, f = x_1x_3 + x_1x_2 - 2x_3, \ldots\}$ in $\mathbb{Q}[x_1, x_2, x_3]$, and $g = x_3^3 + 2x_1x_2x_3 + 2x_2 - 1$. Let $<$ be the graduated lexicographic ordering with $x_1 < x_2 < x_3$.

Then $g \longrightarrow_F x_3^3 - 2x_1x_2^2 + 4x_2x_3 + 2x_2 - 1 =: h$, and in fact $g \longrightarrow_{f,2,x_2} h$. □

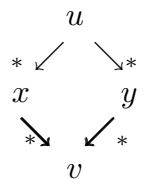
Definition 1.5. Let $\longrightarrow$ be a reduction relation, i.e. a binary relation, on a set X.

- $x \longrightarrow$ means x is *reducible*, i.e. $x \longrightarrow y$ for some y;
- $\underline{x}\!\!\longrightarrow$ means x is *irreducible* or *in normal form* w.r.t. $\longrightarrow$. We omit mentioning the reduction relation if it is clear from the context;
- $x \downarrow y$ means that x and y have a *common successor*, i.e. $x \longrightarrow z \longleftarrow y$ for some z;
- $x \uparrow y$ means that x and y have a *common predecessor*, i.e. $x \longleftarrow z \longrightarrow y$ for some z;
- *x is a $\longrightarrow$–normal form* of y iff $y \longrightarrow^* \underline{x}$. □

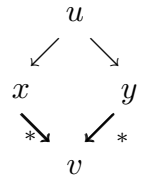
Definition 1.6. (a) $\longrightarrow$ is *Noetherian* or has the *termination property* iff every reduction sequence terminates, i.e. there is no infinite sequence $x_1, x_2, \ldots$ in M such that $x_1 \longrightarrow x_2 \longrightarrow \ldots$.

(b) $\longrightarrow$ is *Church–Rosser* or has the *Church–Rosser property* iff $a \longleftrightarrow^* b$ implies $a \downarrow_* b$.

(c) $\longrightarrow$ is *confluent* iff $x \uparrow^* y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:



(d) $\longrightarrow$ is *locally confluent* iff $x \uparrow y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:



□

As a consequence of the Noetherianity of admissible orderings we get that $\longrightarrow_F$ is Noetherian for any set of polynomials $F \subset K[X]$. So, in contrast to the general theory of rewriting, termination is not a problem for polynomial reductions. But we still have to worry about the Church-Rosser property.

Theorem 1.5. (a) $\longrightarrow$ is Church–Rosser if and only if $\longrightarrow$ is confluent.

(b) (Newman Lemma) Let $\longrightarrow$ be Noetherian. Then $\longrightarrow$ is confluent if and only if $\longrightarrow$ is locally confluent.

As an immediate consequence of the previous definitions we get that the reduction relation $\longrightarrow$ is (nearly) compatible with the operations in the polynomial ring. Moreover, the reflexive–transitive–symmetric closure of the reduction relation $\longrightarrow_F$ is equal to the congruence modulo the ideal generated by F.

Lemma 1.6. *Let $a \in K^*$, $s \in [X]$, $F \subseteq K[X]$, $g_1, g_2, h \in K[X]$.*

(a) $\longrightarrow_F \subseteq \gg$,

(b) $\longrightarrow_F$ *is Noetherian,*

(c) if $g_1 \longrightarrow_F g_2$ *then* $a \cdot s \cdot g_1 \longrightarrow_F a \cdot s \cdot g_2$,

(d) if $g_1 \longrightarrow_F g_2$ *then* $g_1 + h \downarrow_F^* g_2 + h$. □

Theorem 1.7. *Let $F \subseteq K[X]$. The ideal congruence modulo $\langle F \rangle$ equals the reflexive–transitive–symmetric closure of $\longrightarrow_F$, i.e. $\equiv_{\langle F \rangle} = \longleftrightarrow_F^*$.* □

So the congruence $\equiv_{\langle F\rangle}$ can be decided if $\longrightarrow_F$ has the Church–Rosser property. Of course, this is not the case for an arbitrary set F. Such distinguished sets (bases for polynomial ideals) are called Gröbner bases.

Definition 1.7. A subset F of $K[X]$ is a *Gröbner basis* (for $\langle F\rangle$) iff $\longrightarrow_F$ is Church–Rosser. □

A Gröbner basis of an ideal I in $K[X]$ is by no means uniquely defined. In fact, whenever F is a Gröbner basis for I and $f \in I$, then also $F \cup \{f\}$ is a Gröbner basis for I.

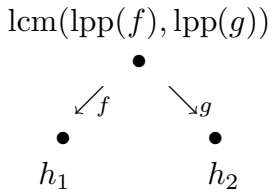
For testing whether a given basis F of an ideal I is a Gröbner basis it suffices to test for local confluence of the reduction relation $\longrightarrow_F$. This, however, does not yield a decision procedure, since there are infinitely many situations $f \uparrow_F g$. However, Buchberger has been able to reduce this test for local confluence to just testing a finite number of sitations $f \uparrow_F g$ [Buchberger 1965]. For that purpose he has introduced the notion of subtraction polynomials, or S–polynomials for short.

Definition 1.8. Let $f, g \in K[X]^*$, $t = \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))$. Then

$$\mathrm{cp}(f,g) = \Big(t - \frac{1}{\mathrm{lc}(f)} \cdot \frac{t}{\mathrm{lpp}(f)} \cdot f,\ t - \frac{1}{\mathrm{lc}(g)} \cdot \frac{t}{\mathrm{lpp}(g)} \cdot g\Big)$$

is the *critical pair* of f and g. The difference of the elements of $\mathrm{cp}(f,g)$ is the *S–polynomial* $\mathrm{spol}(f,g)$ of f and g. □

If $\mathrm{cp}(f,g) = (h_1, h_2)$ then we can depict the situation graphically in the following way:



The critical pairs of elements of F describe exactly the essential branchings of the reduction relation $\longrightarrow_F$.

Theorem 1.8. (Buchberger's Theorem) *Let F be a subset of $K[X]$.*

(a) F is a Gröbner basis if and only if $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2) of elements of F.

(b) F is a Gröbner basis if and only if $\mathrm{spol}(f,g) \longrightarrow_F^* 0$ for all $f, g \in F$.

Buchberger's theorem suggests an algorithm for checking whether a given finite basis is a Gröbner basis: reduce all the S–polynomials to normal forms and check whether they

are all 0. In fact, by a simple extension we get an algorithm for constructing Gröbner bases.

---

algorithm GRÖBNER_B(**in:** F**; out:** G)**;**
[Buchberger algorithm for computing a Gröbner basis. F is a finite subset of $K[X]^*$; G is a finite subset of $K[X]^*$, such that $\langle G\rangle = \langle F\rangle$ and G is a Gröbner basis.]
(1) $G := F$**;**
$C := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$**;**
(2) **while** not all pairs $\{g_1, g_2\} \in C$ are marked **do**
{choose an unmarked pair $\{g_1, g_2\}$**;**
mark $\{g_1, g_2\}$**;**
$h :=$ normal form of $\mathrm{spol}(g_1, g_2)$ w.r.t. $\longrightarrow_G$**;**
if $h \neq 0$
then$\{C := C \cup \{\{g, h\} \mid g \in G\}$**;**
$G := G \cup \{h\}$ **};**
};
return □

Every polynomial h constructed in GRÖBNER_B is in $\langle F\rangle$, so $\langle G\rangle = \langle F\rangle$ throughout GRÖBNER_B. Thus, by Theorem 1.8 GRÖBNER_B yields a correct result if it stops. The termination of GRÖBNER_B is a consequence of Dickson's Lemma which implies that in $[X]$ there is no infinite chain of elements $s_1, s_2, \ldots$ such that $s_i \not| \; s_j$ for all $1 \leq i < j$. The leading power products of the polynomials added to the basis form such a sequence in $[X]$, so this sequence must be finite.

Theorem 1.9. (Dickson's Lemma) *Every $A \subseteq [X]$ contains a finite subset B, such that every $t \in A$ is a multiple of some $s \in B$.*

The termination of GRÖBNER_B also follows from Hilbert's Basis Theorem applied to the initial ideals of the sets G constructed in the course of the algorithm, i.e. $\langle \mathrm{in}(G)\rangle$. See Exercise 8.3.4.

The algorithm GRÖBNER_B provides a constructive proof of the following theorem.

Theorem 1.10. *Every ideal I in $K[X]$ has a Gröbner basis.* □

Example 1.3. Let $F = \{f_1, f_2\}$, with $f_1 = x^2y^2 + y - 1$, $f_2 = x^2y + x$. We compute a Gröbner basis of $\langle F\rangle$ in $\mathbb{Q}[x, y]$ w.r.t. the graduated lexicographic ordering with $x < y$. The following describes one way in which the algorithm GRÖBNER_B could execute (recall that there is a free choice of pairs in the loop):

(1) $\mathrm{spol}(f_1, f_2) = f_1 - yf_2 = -xy + y - 1 =: f_3$ is irreducible, so $G := \{f_1, f_2, f_3\}$.

(2) $\mathrm{spol}(f_2, f_3) = f_2 + xf_3 = xy \longrightarrow_{f_3} y - 1 =: f_4$, so $G := \{f_1, f_2, f_3, f_4\}$.

(3) $\mathrm{spol}(f_3, f_4) = f_3 + xf_4 = y - x - 1 \longrightarrow_{f_4} -x =: f_5$, so $G := \{f_1, \ldots, f_5\}$.

All the other S–polynomials now reduce to 0, so GRÖBNER_B terminates with

$$G = \{x^2y^2 + y - 1, x^2y + x, -xy + y - 1, y - 1, -x\}. \qquad \square$$

In addition to the original definition and the ones given in Theorem 1.8, there are many other characterizations of Gröbner bases. We list only a few of them.

Theorem 1.11. *Let I be an ideal in $K[X]$, $F \subseteq K[X]$, and $\langle F\rangle \subseteq I$. Then the following are equivalent.*

(a) F is a Gröbner basis for I.

(b) $f \longrightarrow_F^* 0$ for every $f \in I$.

(c) $f \longrightarrow_F$ for every $f \in I \setminus \{0\}$.

(d) For all $g \in I, h \in K[X]$: if $g \longrightarrow_F^* \underline{h}$ then $h = 0$.

(e) For all $g, h_1, h_2 \in K[X]$: if $g \longrightarrow_F^* \underline{h_1}$ and $g \longrightarrow_F^* \underline{h_2}$ then $h_1 = h_2$.

(f) $\langle \mathrm{in}(F)\rangle = \langle \mathrm{in}(I)\rangle$.

The Gröbner basis G computed in Example 1.3 is much too complicated. In fact, $\{y - 1, x\}$ is a Gröbner basis for the ideal. There is a general procedure for simplifying Gröbner bases.

Theorem 1.12. *Let G be a Gröbner basis for an ideal I in $K[X]$. Let $g, h \in G$ and $g \neq h$.*

(a) If $\mathrm{lpp}(g) \mid \mathrm{lpp}(h)$ then $G' = G \setminus \{h\}$ is also a Gröbner basis for I.

(b) If $h \longrightarrow_g h'$ then $G' = (G \setminus \{h\}) \cup \{h'\}$ is also a Gröbner basis for I.

Observe that the elimination of basis polynomials described in Theorem 1.12(a) is only possible if G is a Gröbner basis. In particular, we are not allowed to do this during a Gröbner basis computation. Based on Theorem 1.12 we can show that every ideal has a unique Gröbner basis after suitable pruning and normalization.

Definition 1.9. Let G be a Gröbner basis in $K[X]$.

G is *minimal* iff $\mathrm{lpp}(g) \nmid \mathrm{lpp}(h)$ for all $g, h \in G$ with $g \neq h$.

G is *reduced* iff for all $g, h \in G$ with $g \neq h$ we cannot reduce h by g.

G is *normed* iff $\mathrm{lc}(g) = 1$ for all $g \in G$. □

From Theorem 1.12 we obviously get an algorithm for transforming any Gröbner basis for an ideal I into a normed reduced Gröbner basis for I. No matter from which Gröbner basis of I we start and which path we take in this transformation process, we always reach the same uniquely defined normed reduced Gröbner basis of I.

Theorem 1.13. *Every ideal in $K[X]$ has a unique finite normed reduced Gröbner basis.*

Observe that the normed reduced Gröbner basis of an ideal I depends, of course, on the admissible ordering $<$. Different orderings can give rise to different Gröbner bases. However, if we decompose the set of all admissible orderings into sets which induce the same normed reduced Gröbner basis of a fixed ideal I, then this decomposition is finite. This leads to the consideration of universal Gröbner bases. A universal Gröbner basis for I is a basis for I which is a Gröbner basis w.r.t. any admissible ordering of the power products.

If we have a Gröbner basis G for an ideal I, then we can compute in the vector space $K[X]_{/I}$ over K. The irreducible power products (with coefficient 1) modulo G form a basis of $K[X]_{/I}$. We get that $\dim(K[X]_{/I})$ is the number of irreducible power products modulo G. Thus, this number is independent of the particular admissible ordering.

Example 1.4. Let $I = \langle x^3y - 2y^2 - 1, x^2y^2 + x + y\rangle$ in $\mathbb{Q}[x, y]$. Let $<$ be the graduated lexicographic ordering with $x > y$. Then the normed reduced Gröbner basis of I has leading power products x^4, x^3y, x^2y^2, y^3. So there are 9 irreducible power products.

If $<$ is the lexicographic ordering with $x > y$, then the normed reduced Gröbner basis of I has leading power products x and y^9. So again there are 9 irreducible power products.

In fact, $\dim(\mathbb{Q}[x, y]_{/I}) = 9$. □

2 Solving ideal membership 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 2.1. *The irreducible power products modulo G, viewed as polynomials with coefficient 1, form a basis for the vector space $K[X]_{/I}$ over K.*

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 2.1. 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 2.2. (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.*

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 $G_I = G_J$.

3 Solution of algebraic equations by Gröbner bases

We consider a system of equations

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= 0,\\ &\vdots\\ f_m(x_1,\ldots,x_n) &= 0, \end{aligned} \tag{3.1}$$

where $f_1,\ldots,f_m \in K[X]$. The system (3.1) is called a system of polynomial or algebraic equations. First let us decide whether (3.1) has any solutions in $\overline{K}^n$, $\overline{K}$ being the algebraic closure of K. Let $I = \langle f_1,\ldots,f_m\rangle$. The following theorem has first been proved in [Buchberger 1970].

Theorem 3.1. *Let G be a normed Gröbner basis of I. (3.1) is unsolvable in $\overline{K}^n$ if and only if $1 \in G$.*

Now suppose that (3.1) is solvable. We want to determine whether there are finitely or infinitely many solutions of (3.1) or, in other words, whether or not the ideal I is 0–dimensional.

Theorem 3.2. *Let G be a Gröbner basis of I. Then (3.1) has finitely many solutions (i.e. I is 0–dimensional) if and only if for every i, $1 \le i \le n$, 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 $\dim(K[X]_{/I})$.*

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, first stated in [Trinks 1978], 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 3.3. (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 $K[x_1,\ldots,x_i]$.

Theorem 3.3 can clearly be generalized to product orderings, without changing any-

thing in the proof.

Example 3.1. 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 3.1 the system is solvable. Furthermore, by Theorem 3.2, 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

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

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

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

4 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 $\mathbb{A}^n(\overline{K})$, 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 extends to operations on ideals and algebraic sets in the following way:

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 4.1. 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 4.1. *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* $I \cap \langle g \rangle = \langle h_1, \ldots, h_m \rangle$.

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 Theorem 3.3.

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 4.2. *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).*

Example 4.1. 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. □

5 Hilbert functions and computation of dimension

The dimension of an algebraic variety can be defined in several equivalent ways. We will use an algebraic approach, and derive an algorithm for computing the dimension for an ideal (an its corresponding variety) by an application of Gröbner bases. Our treatment of this subject is based on monomial ideals (such as the initial ideal of an ideal) and the concept of the Hilbert function.

Throughout this chapter we let K be a field of characteristic 0, $\overline{K}$ the algebraic closure of K, and $\mathcal{K}$ a universal domain for K, i.e. $\mathcal{K}$ is an algebraically closed superfield of K with infinite transcendence degree over K. E.g., $\mathbb{C}$ is a universal domain for $\mathbb{Q}$.

An algebraic definition of dimension

The following definition of the dimension of an ideal can be found in [Gröbner 1968/1970], vol. II, p. 38.

Definition 5.1: Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal and $\{i_1, \ldots, i_d\}$ a subset of $\{1, \ldots, n\}$. The set $\{x_{i_1}, \ldots, x_{i_d}\}$ is said to be *independent modulo* I if

$$I \cap K[x_{i_1}, \ldots, x_{i_d}] = \{0\}.$$

We denote the set $\{X \subseteq \{x_1, \ldots, x_n\} \mid X \text{ is independent modulo } I\}$ by $\Delta(I)$. The *dimension* of I, denoted by $\dim(I)$, is the maximal number of elements in any set of variables independent modulo I, i.e.

$$\dim(I) = \max(\{|X| \mid X \in \Delta(I)\}).$$

Furthermore, for a non–empty variety $V \subseteq \overline{K}^n$ we define its dimension as

$$\dim(V) := \dim(\mathbf{I}(V)).$$ □

Observe that for any proper ideal $I \subset K[x_1, \ldots, x_n]$ we have

$$\Delta(I) = \Delta(\sqrt{I}) \quad \text{and therefore} \quad \dim(I) = \dim(\sqrt{I}).$$

Let $\{i_1, \ldots, i_d\} \subseteq \{1, \ldots, n\}$. It follows from the elimination property of Gröbner bases that

$$\{x_{i_1}, \ldots, x_{i_d}\} \in \Delta(I) \quad \text{iff} \quad G \cap K[x_{i_1}, \ldots, x_{i_d}] = \emptyset,$$

where G is the reduced Gröbner basis of I with respect to a lexicographic ordering with $x_{i_1} \prec x_{i_2} \prec \ldots \prec x_{i_d} \prec$ other variables (or, for that matter, a product ordering with

$\{x_{i_1}, \ldots, x_{i_d}\} \prec X \setminus \{x_{i_1}, \ldots, x_{i_d}\}$). From these observations we can immediately derive an algorithm DIMENSION_1 for computing the dimension of an ideal I.

---

algorithm DIMENSION_1(**in:** F**; out:** d, X)**;**
[F is a finite subset of $K[x_1, \ldots, x_n]$, with $I := \langle F \rangle \neq K[x_1, \ldots, x_n]$.
$d = \dim(I)$, and X is a set of independent variables modulo I with $|X| = d$.]
(1) **for** every permutation p of $\{1, \ldots, n\}$ **do**
{ compute the reduced Gröbner basis G_p of I w.r.t. the lexicographic ordering with $x_{p(1)} \prec \ldots \prec x_{p(n)}$**;**
$i_p :=$ the greatest element of $\{0, \ldots, n\}$ such that
$G_p \cap K[x_{p(1)}, \ldots, x_{p(i_p)}] = \emptyset$ **};**
(2) choose a permutation p' such that
$i_{p'} = \max(\{i_p \mid p \text{ a permutation of } \{1, \ldots, n\}\})$**;**
(3) $d := i_{p'}$**;**
$X := \{x_{p'(1)}, \ldots, x_{p'(i_{p'})}\}$**;**
return □

Example 5.1: Let I be the ideal generated by

$$F := \{x_1x_3 + x_1^2 + x_1x_2,\ x_2x_3 + x_1 + 1,\ x_1x_2 + x_1x_2x_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3].$$

We obtain $\Delta(I)$ by computing lexicographic Gröbner bases of F w.r.t. every possible ordering of variables. Here are these six reduced Gröbner bases:

$$\begin{array}{lcc}
x_1 \prec x_2 \prec x_3 & : & \{x_2x_3 + x_1 + 1,\ x_1x_3 + 2x_1^2 + x_1,\ x_1x_2 - x_1^2 - x_1,\ x_1^3 + x_1^2\}, \\
x_2 \prec x_1 \prec x_3 & : & \{x_1x_3 + 2x_1x_2 - x_1,\ x_2x_3 + x_1 + 1,\ x_1^2 - x_1x_2 + x_1,\ x_1x_2^2 - x_1x_2\}, \\
x_1 \prec x_3 \prec x_2 & : & \{x_2x_3 + x_1 + 1,\ x_1x_2 - x_1^2 - x_1,\ x_1x_3 + 2x_1^2 + x_1,\ x_1^3 + x_1^2\}, \\
x_3 \prec x_1 \prec x_2 & : & \{2x_1x_2 + x_1x_3 - x_1,\ x_2x_3 + x_1 + 1,\ 2x_1^2 + x_1x_3 + x_1,\ x_1x_3^2 - x_1\}, \\
x_2 \prec x_3 \prec x_1 & : & \{x_1 + x_2x_3 + 1,\ x_2x_3^2 + 2x_2^2x_3 - x_2x_3 + x_3 + 2x_2 - 1, \\
 & & \quad x_2^3x_3 - x_2^2x_3 + x_2^2 - x_2\}, \\
x_3 \prec x_2 \prec x_1 & : & \{x_1 + x_2x_3 + 1,\ 2x_2^2x_3 + x_2x_3^2 - x_2x_3 + 2x_2 + x_3 - 1, \\
 & & \quad x_2x_3^3 - x_2x_3 + x_3^2 - 1\}.
\end{array}$$

Since every Gröbner basis contains a bivariate polynomial, an independent set of variables can at most contain one variable. Because of the first Gröbner basis, $\{x_1\} \notin \Delta(I)$. But $\{x_2\} \in \Delta(I)$ and $\{x_3\} \in \Delta(I)$, because the second Gröbner basis does not contain an element of $\mathbb{Q}[x_2]$, and the forth Gröbner basis does not contain an element of $\mathbb{Q}[x_3]$. Altogether,

$$\Delta(I) = \{\ \{x_2\},\ \{x_3\}, \emptyset\ \}.$$ □

Obviously this approach suffers from the fact that $n!$ Gröbner bases w.r.t. lexicographic orderings have to be computed. So our goal is to derive a more efficient approach

to the computation of the dimension. The crucial fact for obtaining a faster algorithm is the following theorem, which will be proved later (for graduated orderings), after we have compiled some knowledge about Hilbert functions.

Definition 5.2: Let $\prec$ be an admissible ordering on $[x_1, \ldots, x_n]$, I an ideal in $K[x_1, \ldots, x_n]$. The *initial ideal* of I, denoted by $I_\prec$, is the ideal $\langle \mathrm{in}(I) \rangle$, i.e. the ideal generated by the initials or leading terms of I w.r.t. $\prec$. □

Theorem 5.1: *Let $\prec$ be an admissible ordering on $[x_1, \ldots, x_n]$, I a proper ideal in $K[x_1, \ldots, x_n]$. Let X be an element of maximal cardinality in $\Delta(I_\prec)$. Then X is an element of maximal cardinality in $\Delta(I)$ and therefore*

$$\dim(I_\prec) \;=\; |X| \;=\; \dim(I). \qquad \square$$

Hence, the computation of an element of maximal cardinality in $\Delta(I)$ can be reduced to the computation of an element of maximal cardinality in $\Delta(I_\prec)$.

If G is a Gröbner basis of I w.r.t. $\prec$, then $\langle \mathrm{in}(G) \rangle = I_\prec$. In fact, this is equivalent to G being a Gröbner basis w.r.t. $\prec$. So, for every subset $X = \{x_{i_1}, \ldots, x_{i_d}\} \subseteq \{x_1, \ldots, x_n\}$,

$$X \in \Delta(I_\prec) \quad \text{iff} \quad \mathrm{in}(g) \notin K[x_{i_1}, \ldots, x_{i_d}] \text{ for every } g \in G.$$

Therefore, after computing G, we can obtain an element of maximal cardinality in $\Delta(I_\prec)$ by purely combinatorial methods.

This leads immediately to the much more efficient algorithm DIMENSION_2 for computing the dimension of an ideal I.

---

algorithm DIMENSION_2(**in:** F**; out:** d, X)**;**
[F is a finite subset of $K[x_1, \ldots, x_n]$, with $I := \langle F \rangle \neq K[x_1, \ldots, x_n]$.
$d = \dim(I)$, and X is a set of independent variables modulo I with $|X| = d$.]
(1) choose an admissible ordering $\prec$ on $[x_1, \ldots, x_n]$**;**
$G := \mathrm{GB}(F)$ w.r.t. $\prec$**;**
(2) for all subsets $X = \{x_{i_1}, \ldots, x_{i_m}\}$ of $\{x_1, \ldots, x_n\}$ check whether
(*) $X \in \Delta(I_\prec)$, i.e. whether
$\mathrm{in}(g) \notin K[x_{i_1}, \ldots, x_{i_m}]$ for every $g \in G$**;**
(3) $X :=$ a set of maximal cardinality satisfying this condition (*)**;**
$d := |X|$**;**
return □

A proof of Theorem 5.1 can be found in [Kalkbrener,Sturmfels 1995]. In [Kredel,Weispfenning 1991] a different proof for lexicographic orderings is given. We will re-

strict ourselves to another special case: we will prove Theorem 5.1 under the additional assumption that $\prec$ is a *graduated ordering*, i.e.

$$\deg(u) < \deg(v) \Longrightarrow u \prec v \qquad \text{for all } u, v \in [x_1, \ldots, x_n].$$

Our proof is based on the important concept of Hilbert functions.

Example 5.2: Let F be defined as in the previous example and let G be the reduced Gröbner basis of F w.r.t. the lexicographic ordering with $x_1 \prec x_2 \prec x_3$. Then

$$I_\prec = \langle \mathrm{in}(G) \rangle = \langle x_2x_3,\ x_1x_3,\ x_1x_2,\ x_1^3 \rangle.$$

Hence,

$$\Delta(I_\prec) = \{\ \{x_2\},\ \{x_3\},\ \emptyset\ \} \quad \text{and} \quad \dim(I) = \dim(I_\prec) = 1. \qquad \square$$

The initial ideal $I_\prec$ of an ideal I has the special property of being generated by monomials. Such ideals have a structure very similar to homogeneous ideals. Of course, they are particular homogeneous ideals.

Definition 5.3: An ideal I in $K[x_1, \ldots, x_n]$ is a *monomial ideal* iff it has a monomial basis, i.e. a basis B s.t. every $f \in B$ is a monomial $ax_1^{j_1} \cdots x_n^{j_n}$, $a \in K$. $\square$

Theorem 5.2: *Let I be an ideal in $K[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) I is a monomial ideal.

(ii) If $f \in I$ and m is a monomial occurring in f, then $m \in I$.

(iii) I is generated by a finite monomial basis.

The Hilbert function

Let W be a subspace of a finite–dimensional vector space V. Recall that in this case W and the quotient space V/W are also finite–dimensional and

$$\dim(V) = \dim(W) + \dim(V/W). \tag{5.1}$$

Definition 5.4: Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. For a non–negative integer s we let

$$K[x_1, \ldots, x_n]_{\leq s}$$

denote the set of polynomials of total degree $\leq s$ in $K[x_1, \ldots, x_n]$ and we define

$$I_{\leq s} := I \cap K[x_1, \ldots, x_n]_{\leq s}.$$

Note that we can consider $K[x_1, \ldots, x_n]_{\leq s}$ as a finite–dimensional vector space over K and $I_{\leq s}$ as a finite–dimensional subspace. The *(affine) Hilbert function* of I is the function on the non–negative integers s defined by (using (5.1))

$$\begin{aligned} HF_I(s) :&= \dim(K[x_1, \ldots, x_n]_{\leq s}/I_{\leq s}) \\ &= \dim(K[x_1, \ldots, x_n]_{\leq s}) - \dim(I_{\leq s}). \end{aligned}$$

□

Example 5.3: Consider the ideal

$$I = \langle x^2 \rangle \subset \mathbb{Q}[x, y, z].$$

By a simple inspection we see that for $s = 0, 1, 2, 3$ the Hilbert function of I is as follows:

s	$HF_I(s)$
0	1
1	4
2	9
3	16

For $s \geq 2$ we have

$$\begin{aligned} HF_I(s) &= \binom{3+s}{s} - \binom{3+(s-2)}{s-2} \\ &= \frac{(3+s)(2+s)(1+s) - (1+s)s(s-1)}{3!} \\ &= s^2 + 2s + 1. \end{aligned}$$

So we see that for $s \geq 2$ the Hilbert function HF_I agrees with a polynomial function. □

Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal, $\prec$ a graduated ordering on $[x_1, \ldots, x_n]$, and $I_\prec$ the initial ideal of I. We will show that

$$I \text{ and the monomial ideal } I_\prec \text{ have the same Hilbert function.} \tag{5.2}$$

Therefore, we will now study Hilbert functions of monomial ideals. More precisely, we will show that for every monomial ideal J there exists a non–negative integer t and a univariate polynomial $h \in \mathbb{Q}[x]$ such that

$$HF_J(s) = h(s) \text{ for every } s \geq t \quad \text{and} \quad \dim(J) = \deg(h). \tag{5.3}$$

Using (5.2) and (5.3) it will be easy to prove Theorem 5.1 for graduated orderings. For proving (5.3) we introduce the concept of a translate.

Definition 5.5: For each monomial ideal I in $K[x_1, \ldots, x_n]$ we let

$$C(I) := \{u \in [x_1, \ldots, x_n] \mid u \notin I\}$$

be the set of power products (power products with coefficient 1) not in I, the *complement* of I.

For $M, N \subseteq [x_1, \ldots, x_n]$ we define their product as

$$M \cdot N := \{uv \mid u \in M, v \in N\}.$$

For every integer $r \in \{1, \ldots, n\}$, every set of variables $\{x_{i_1}, \ldots, x_{i_r}\} \subseteq \{x_1, \ldots, x_n\}$, and every $u \in [x_1, \ldots, x_n]$ we call

$$\{u\} \cdot [x_{i_1}, \ldots, x_{i_r}]$$

a *translate of dimension* r. Furthermore, every singleton $\{u\} \subset [x_1, \ldots, x_n]$ is called a *translate of dimension* 0. □

Example 5.4: Consider the ideal

$$I = \langle x_1^3, x_1 x_2 \rangle \subset \mathbb{Q}[x_1, x_2].$$

Obviously, $C(I) = \{x_1, x_1^2\} \cup [x_2]$. Let s be a non–negative integer and denote the set of those power products in $C(I)$ with total degree $\leq s$ by C_s. It will be shown in the proof of Theorem 2.5 that the set $\{u \mid u \in C_s\}$ (or, more precisely, the equivalence classes with representatives $u \in C_s$) is a basis of the quotient space $\mathbb{Q}[x_1, x_2]_{\leq s}/I_{\leq s}$. Therefore, I has the following Hilbert function:

$$HF_I(0) = 1, \quad HF_I(1) = 3, \quad HF_I(s) = s + 3 \text{ for } s \geq 2.$$

Note that the Hilbert function is a polynomial function for sufficiently large s (in this example s must be at least 2). Furthermore, the degree of this polynomial is equal to the dimension of the ideal. We will show that both results hold for arbitrary ideals. The proof is based on the observation that if I is a monomial ideal, the set of power products not in the ideal can be written as a finite disjoint union of translates. For instance, in this example

$$C(I) = \{x_1\} \cup \{x_1^2\} \cup \{1\} \cdot [x_2].$$ □

Theorem 5.3: *If $I \subset K[x_1, \ldots, x_n]$ is a monomial ideal then $C(I)$ can be written as a finite disjoint union of translates.*

In Example 5.3 we saw that we could write the Hilbert function $HF_I(s)$ as a difference of binomial coefficients depending on the number of variables and s for sufficiently large s. This observation can be generalized and it will lead us to the concept of the Hilbert polynomial.

Lemma 5.4: *The number of power products of degree $\leq s$ in $[x_1, \ldots, x_m]$ is the binomial coefficient*

$$\binom{m+s}{s.}$$

□

Now we can determine the number of power products of degree $\leq s$ in an arbitrary translate.

Lemma 5.5: *Let $u \in [x_1, \ldots, x_n]$ and $t = \deg(u)$.*

(i) *The number of power products of degree $\leq s$ in the translate $\{u\} \cdot [x_1, \ldots, x_m]$ is equal to the binomial coefficient*

$$\binom{m+s-t}{s-t},$$

provided that $s \geq t$.

(ii) *For $s \geq t$, this number of power products is a polynomial function of s of degree m and the coefficient of s^m is $1/m!$.*

Theorem 5.6: *If $I \subset K[x_1, \ldots, x_n]$ is a proper monomial ideal, then for all s sufficiently large, the number of power products not in I of degree $\leq s$ is a polynomial of degree $d = \dim(I)$ in s. Furthermore, the coefficient of s^d in this polynomial is positive.*

Our next goal is to generalize Theorem 5.6 to arbitrary ideals. The following crucial observation is due to Macaulay.

Theorem 5.7: *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and let $\prec$ be a graduated ordering on $[x_1, \ldots, x_n]$. Then the monomial ideal $J = I_\prec$ (the initial ideal) has the same Hilbert function as I.*

Corollary: *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. There exists a polynomial $h(x) \in \mathbb{Q}[x]$, such that for sufficiently large s we have $HF_I(s) = h(s)$.*

Definition 5.6: Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. The polynomial which equals $HF_I(s)$ for sufficiently large s is called the *(affine) Hilbert polynomial* of I, denoted by $HP_I(s)$. □

The smallest integer t such that $HF_I(s) = HP_I(s)$ for all $s \geq t$ is called the *index of regularity* of I. Determining the index of regularity is of considerable interest and importance in many computations with ideals, but we will not pursue this topic here.

Theorem 5.8: *Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal. Then* $\dim(I)$ *equals the degree of the Hilbert polynomial of I.*

Now we have compiled all the necessary prerequisites for proving Theorem 5.1 under the additional assumption, that $\prec$ is a graduated ordering.

Theorem 5.1: *Let $\prec$ be a graduated ordering on $[x_1, \ldots, x_n]$, I a proper ideal in $K[x_1, \ldots, x_n]$. Let X be an element of maximal cardinality in $\Delta(I_\prec)$. Then X is an element of maximal cardinality in $\Delta(I)$ and therefore*

$$\dim(I_\prec) \;=\; |X| \;=\; \dim(I).$$

Proof: Using Theorems 5.6, 5.7, and 5.8, we obtain

$$\begin{aligned} \dim(I_\prec) &= \deg(HP_{I_\prec}) \\ &= \deg(HP_I) \\ &= \dim(I). \end{aligned}$$

We still have to show that any maximal element in $\Delta(I_\prec)$ is also a maximal element in $\Delta(I)$. Clearly, $\Delta(I_\prec) \subseteq \Delta(I)$, since

$$\begin{array}{ccc} X \in \Delta(I_\prec) & & X \in \Delta(I) \\ \Updownarrow & & \Updownarrow \\ I_\prec \cap K[X] = \langle 0 \rangle & \Longrightarrow & I \cap K[X] = \langle 0 \rangle \end{array}$$

Therefore, if X is an element of maximal cardinality in $\Delta(I_\prec)$, then X must also be an element of maximal cardinality in $\Delta(I)$. □

6 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*, i.e. defined by the bivariate polynomial $f(x,y) \in K[x,y]$. I.e.

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

Of course, we could also view this curve in the projective plane $\mathbb{P}^2(\overline{K})$, defined by $F(x,y,z)$, the homogenization of $f(x,y)$.

In this chapter we follow the development in [Sendra,Winkler 1991,1997].

Definition 6.1. 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 the corresponding map is an isomorphism between $\mathbb{A}^1(K)$ and $\mathcal{C}$. □

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. 6.1

Fig. 6.2

Fig. 6.3

Fig. 6.4

Example 6.1: 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. 6.1) 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 6.2) does not have a rational parametrization.

The tacnode curve (see Fig. 6.3) 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, compare [Sendra,Winkler 1997], [Sendra,Winkler 1999].

Example 6.2: Let $\mathcal{C}$ be the 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. 6.4.

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

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

So, as we see in Fig.6.4, $\mathcal{C}$ 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

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

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 $\mathcal{C}$ (for details see [Sendra,Winkler 1997]), 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. □

Many of these ideas which work for curves can actually be generalized to higher dimensional geometric objects. For an algorithmic treatment of the general parametrization problem of algebraic surfaces we refer to [Schicho 1998]. Special algorithmic approaches have been designed for specific classes of algebraic surfaces. For instance, one subproblem in computer aided geometric design is the manipulation of offset curves, offset surfaces, pipe and canal surfaces. These are geometric objects keeping certain distances from a generating object. In [Peternell,Pottmann 1997] it has been proved that pipe and canal surfaces can be rationally parametrized. A symbolic algorithm for actually computing such a parametrization is described in [Landsmann et al. 2000] and [Landsmann et al. 2001].

Now that we have seen some examples of parametrization treated by symbolic algebraic computation, let us just briefly 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 6.3: Let us do this for the curve of Example 6.2. 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. □

7 Syzygies — Linear equations over $K[X]$

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

$$f_1 z_1 + \ldots + f_s z_s = f, \tag{7.1}$$

or the corresponding homogeneous equation

$$f_1 z_1 + \ldots + f_s z_s = 0. \tag{7.2}$$

Let F be the vector $(f_1, \ldots, f_s)$. The general solution of (7.1) and (7.2) is to be sought in $K[X]^s$. The solutions of (7.2) form a module over the ring $K[X]$, a submodule of $K[X]^s$ over $K[X]$.

Definition 7.1. Any solution of (7.2) is called a *syzygy* of the sequence of polynomials $f_1, \ldots, f_s$. The module of all solutions of (7.2) 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 7.1. *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 $1 \le i \le s$ let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ be the i–th unit vector and for $1 \le i < j \le s$ let

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

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

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

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 7.2. *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*

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

What we still need is a particular solution of the inhomogeneous equation (7.1). 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 (7.1) 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 (7.1).

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. An algorithm along these lines is presented in [Winkler 1986]. However, it is also possible to extend the concept of Gröbner bases from ideals to modules (see [Furukawa et al. 1986] and [Mora,Möller 1986]) and solve a whole system of linear equations by a single computation of a Gröbner basis for a submodule of $K[X]^s$.

Example 7.1. 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 8.4.8. 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 $\mathrm{Syz}(F)$:

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

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

References

[Buchberger 1965] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, doctoral thesis, Univ. Innsbruck, Austria (1965)

[Buchberger 1970] B. Buchberger, "Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems", *aequationes math.* 4/3, 374–383 (1970)

[Buchberger 1985] B. Buchberger, "Gröbner–Bases: An Algorithmic Method in Polynomial Ideal Theory", in *Multidimensional Systems Theory*, N.K. Bose (ed.), D.Reidel Publ. Comp. (1985)

[Furukawa et al. 1986] A. Furukawa, T. Sasaki, H. Kobayashi, "Gröbner basis of a module over $K[x_1, \ldots, x_n]$ and polynomial solutions of a system of linear equations", in *Proc. of SYMSAC'86*, 222–224, B.W. Char (ed.), ACM, New York (1986)

[Gröbner 1968/70] W. Gröbner, *Algebraische Geometrie I, II*, B.I. Hochschultaschenbücher (1968/70)

[Hermann 1926] G. Hermann, "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale", *Math. Annalen* 95, 736–788 (1926)

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

[Kalkbrener,Sturmfels 1995] M. Kalkbrener, B. Sturmfels, "Initial complexes of prime ideals", *Advances in Mathematics* **116/2**, 365–376 (1995)

[Kredel,Weispfenning 1991] H. Kredel, V. Weispfenning, "Computing dimension and independent sets for polynomial ideals", *J. Symbolic Computation* **12/6**, 607–631 (1991)

[Landsmann et al. 2000] G. Landsmann, J. Schicho, F. Winkler, E. Hillgarter, "Symbolic Parametrization of Pipe and Canal Surfaces", in *Proc. Internat. Symposium on Symbolic and Algebraic Computation (ISSAC'2000)*, 202–208, C. Traverso (ed.), ACM Press (2000)

[Landsmann et al. 2001] G. Landsmann, J. Schicho, F. Winkler, "The Parametrization of Canal Surfaces and the Decomposition of Polynomials into a Sum of Two Squares", *J. Symbolic Computation* 32/1& 2, 119–132 (2001)

[Mayr,Meyer 1982] E.W. Mayr, A.R. Meyer, "The Complexity of the Word Problem for Commutative Semigroups and Polynomial Ideals", *Adv. in Math.* 46, 305–329 (1982)

[Mora,Möller 1986] F. Mora, H.M. Möller, "New constructive methods in classical ideal theory", *J. of Algebra* 100, 138–178 (1986)

[Peternell,Pottmann 1997] M. Peternell, H. Pottmann, "Computing Rational Parametrizations of Canal Surfaces", *J. Symbolic Computation* 23/2&3, 255–266 (1997)

[Robbiano 1985] L. Robbiano, "Term Orderings on the Polynomial Ring", in *Proc. EUROCAL'85*, B.F. Caviness (ed.), Springer-Verlag, LNCS 204 (1985)

[Schicho 1998] J. Schicho, "Rational Parametrization of Surfaces", *J. Symbolic Computation* 26/1, 1–30 (1998)

[Sendra,Winkler 1991] J.R. Sendra, F. Winkler, "Symbolic Parametrization of Curves", *J. Symbolic Computation* 12/6, 607–631 (1991)

[Sendra,Winkler 1997] J.R. Sendra, F. Winkler, "Parametrization of Algebraic Curves over Optimal Field Extensions", *J. Symbolic Computation* 23/2& 3, 191–207 (1997)

[Sendra,Winkler 1999] J.R. Sendra, F. Winkler, "Algorithms for Rational Real Algebraic Curves", *Fundamenta Informaticae* 39/1-2, 211–228 (1999)

[Trinks 1978] W. Trinks, "Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen", *J. Number Theory* 10/4, 475–488 (1978)

[Winkler 1996] F. Winkler, *Polynomial Algorithms in Computer Algebra*, Springer-Verlag Wien New York (1996)