Gröbner Bases: Computational Algebraic Geometry and its Complexity

Johannes Mittmann

Technische Universität München

May 9, 2007

Abstract

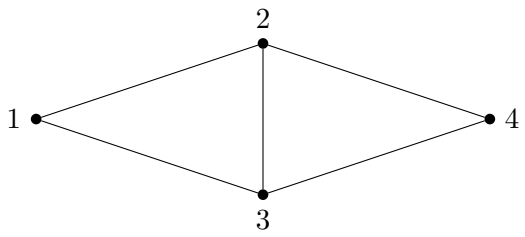
This paper gives an introduction to computational commutative algebra. Besides classical algebraic geometry and Gröbner basis theory, we will discuss the computational complexity of some decision problems involved.

Contents

1 Introduction

Problems from many different areas lead to a system of multivariate polynomial equations. Among them are robotics, term rewriting or automatic theorem proving in geometry. We give a simple example from graph theory.

Example. We want to find a 3-colouring of the following graph $G = (V, E)$:



If we take as colours the three cubic roots of unity $1, e^{(2/3)\pi i}, e^{(4/3)\pi i}$, the 3-colourings of G are exactly the tuples $(\xi_1, \ldots, \xi_4) \in \mathbb{C}^4$ satisfying

$$\begin{aligned} X_i^3 - 1 &= 0, && \text{for all vertices } i \in V, \\ X_i^2 + X_i X_j + X_j^2 &= 0, && \text{for all edges } (i,j) \in E. \end{aligned}$$

2 Algebraic Geometry

Classical algebraic geometry studies zero sets of systems of polynomial equations. This section follows parts of a lecture on commutative algebra given by Prof. Gregor Kemper at the Technische Universität München in 2006. Further references are [CLO97] and [La05].

In this paper, R is always a commutative ring with unity, and K is always a field. By $\mathbb{N}$ we denote the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$.

2.1 Ideals

Our main algebraic object of interest will be the ideal in a ring.

Definition 1. A subset $I \subseteq R$ is called an *ideal* in R, written $I \trianglelefteq R$, if

(i) $0 \in I$,

(ii) $a + b \in I$ for all $a, b \in I$, and

(iii) $r \cdot a \in I$ for all $r \in R$ and $a \in I$.

Ideals are exactly the kernels of ring homomorphisms. In ring theory, they play a similar role as for example normal subgroups in group theory. The following property of ideals is immediate.

Proposition 2. *Let $\mathcal{M}$ be a nonempty set of ideals in R. Then*

$$\bigcap_{I \in \mathcal{M}} I$$

is an ideal in R.

Ideals can be described by means of generating sets.

Definition 3. Let $A \subseteq R$ be a subset. Then

$$\langle A \rangle = \bigcap_{I \trianglelefteq R,\ A \subseteq I} I$$

is called the *ideal generated* by A.

Hence, $\langle A \rangle$ is the smallest ideal containing A. For algorithmic purposes, finite generating sets are of particular interest. In this case, every element of the ideal can be written as an R-linear combination of the generators.

Definition 4. An ideal $I \trianglelefteq R$ is called *finitely generated* if there exist $a_1, \ldots, a_s \in R$ such that

$$I = \langle a_1, \ldots, a_s \rangle.$$

Proposition 5. *Let $a_1, \ldots, a_s \in R$. Then*

$$\langle a_1, \ldots, a_s \rangle = \left\{ \textstyle\sum_{i=1}^{s} r_i a_i \mid r_1, \ldots, r_s \in R \right\}.$$

The basic operations that can be performed with ideals are the following.

Definition 6. Let $I, J \trianglelefteq R$ be ideals.

(1) The *sum* of I and J is defined by

$$I + J = \left\{ a + b \mid a \in I \text{ and } b \in J \right\} \trianglelefteq R.$$

(2) The *product* of I and J is defined by

$$I \cdot J = \left\{ \textstyle\sum_{i=1}^{s} a_i b_i \mid a_i \in I,\ b_i \in J \text{ and } s \in \mathbb{N}_{>0} \right\} \trianglelefteq R.$$

$I + J$ is the smallest ideal containing both I and J. Given the generators of finitely generated ideals it is easy to find generators for the sum and product. For the intersection this is not evident a priori.

Proposition 7. *Let $I = \langle a_1, \ldots, a_s \rangle \trianglelefteq R$ and $J = \langle b_1, \ldots, b_t \rangle \trianglelefteq R$ be ideals. Then:*

(1) $I + J = \langle a_1, \ldots, a_s, b_1, \ldots, b_t \rangle$.

(2) $I \cdot J = \langle a_i b_j \mid 1 \leq i \leq s \text{ and } 1 \leq j \leq t \rangle$.

Rings in which every ideal is finitely generated are called Noetherian and can be characterized as follows.

Definition 8. A ring R is called *Noetherian* if it satisfies the *ascending chain condition (ACC)*: Let $I_1, I_2, I_3, \ldots \trianglelefteq R$ be ideals with

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots,$$

then there exits an $N \in \mathbb{N}_{>0}$ such that $I_N = I_{N+1} = I_{N+2} = \ldots$.

Proposition 9. *Let R be a ring. Then the following are equivalent:*

(1) R is Noetherian.

(2) Every ideal $I \trianglelefteq R$ is finitely generated.

(3) Every nonempty set $\mathcal{M}$ of ideals in R has a maximal element.

Proof. (2) $\Rightarrow$ (1): Let $I_1, I_2, I_3, \ldots \trianglelefteq R$ be ideals with

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots.$$

Then $I := \bigcup_{i \in \mathbb{N}_{>0}} I_i$ is an ideal in R. By (2), there are $a_1, \ldots, a_s \in R$ such that $I = \langle a_1, \ldots, a_s \rangle$. Hence, there is an $N \in \mathbb{N}_{>0}$ with $a_1, \ldots, a_s \in I_N$ and therefore $I_N = I_{N+1} = \ldots$.

(1) $\Rightarrow$ (3): Assume by way of contradiction that there exists a nonempty set $\mathcal{M}$ of ideals in R that has no maximal member. We will use this to construct inductively an infinite proper ascending chain of ideals. Since $\mathcal{M} \neq 0$, we can choose $I_1 \in \mathcal{M}$. Suppose we have

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_i$$

with $I_1, \ldots, I_i \in \mathcal{M}$ for some $i \geq 1$. Since I_i is not maximal in $\mathcal{M}$, there exists an ideal $I_{i+1} \in \mathcal{M}$ with $I_i \subsetneq I_{i+1}$. Continuing this process yields a chain as desired contradicting (1).

(3) $\Rightarrow$ (2): Let $I \trianglelefteq R$. Define

$$\mathcal{M} = \left\{ J \trianglelefteq R \,|\, J \text{ finitely generated with } J \subseteq I \right\} \neq 0.$$

By (3), there is a maximal element $I' \in \mathcal{M}$. Suppose that $I' \subsetneq I$. Then there is an $a \in I \setminus I'$. Hence $I' + \langle a \rangle \subseteq I$ is finitely generated contradicting the maximality of I'. Therefore $I = I'$ is finitely generated. $\square$

As a consequence, principal ideal domains like $\mathbb{Z}$ or $K[X]$ and fields K are Noetherian. A famous result due to Hilbert now shows that polynomial rings over Noetherian rings are again Noetherian.

Theorem 10 (The Hilbert Basis Theorem)**.** *Let R be a Noetherian ring. Then*

$$R[X] \text{ is Noetherian.}$$

Proof. Let $I \trianglelefteq R[X]$. We want to show that I is finitely generated. For $i = 1, 2, \ldots$ define

$$I_i = \big\{\mathrm{LC}(f) \mid f \in I \text{ with } \deg(f) = i\big\} \cup \big\{0\big\} \subseteq R.$$

It is easy to see that $I_1, I_2, \ldots \trianglelefteq R$ and $I_1 \subseteq I_2 \subseteq \cdots$. Since R is Noetherian, there is an $N \in \mathbb{N}_{>0}$ such that $I_N = I_{N+1} = \ldots$. Moreover, there is an $s \in \mathbb{N}_{>0}$ and $a_{i1}, \ldots, a_{is} \in I_i$ such that

$$I_i = \langle a_{i1}, \ldots, a_{is} \rangle$$

for all $i = 1, \ldots, N$. By the definition of the I_i, we can choose polynomials $f_{ij} \in I$ with $\deg(f_{ij}) = i$ or $\deg(f_{ij}) = -\infty$ such that $a_{ij} = \mathrm{LC}(f_{ij})$ for all $i = 1, \ldots, N$ and $j = 1, \ldots, s$. Define

$$I' := \langle f_{ij} \mid i = 1, \ldots, N \text{ and } j = 1, \ldots, s \rangle \subseteq I.$$

To finish the proof it suffices to show $I \subseteq I'$. Let $f \in I$. We argue by induction on $i := \deg(f)$ that $f \in I'$. The statement is clear for $f = 0$. If $i \geq 0$, denote $k = \min\{i, N\}$ and $\ell = \max\{i, N\}$. We can write $\mathrm{LC}(f) = \sum_{j=1}^{s} r_j a_{kj}$ for some $r_1, \ldots, r_s \in R$. Define

$$f' := \sum_{j=1}^{s} r_j f_{kj} X^{\ell - N} \in I'.$$

Then $\deg(f') = i = \deg(f)$ and $\mathrm{LC}(f') = \mathrm{LC}(f)$. Therefore $\deg(f - f') < i$ and by induction it follows that $f - f' \in I'$, hence $f \in I'$. □

Using induction, it follows that every ideal in a multivariate polynomial ring over a field is finitely generated.

Corollary 11. *Every ideal $I \trianglelefteq K[X_1, \ldots, X_n]$ is finitely generated. Moreover, for any $A \subseteq K[X_1, \ldots, X_n]$ there is a finite subset $B \subseteq A$ such that*

$$\langle A \rangle = \langle B \rangle.$$

2.2 Affine Varieties

Affine varieties are the common zero set of a system of polynomials and will be considered as an geometric object in the affine space K^n.

Definition 12. Let $I \subseteq K[X_1, \ldots, X_n]$ be a subset. Then the set

$$\mathrm{Var}(I) = \big\{(\xi_1, \ldots, \xi_n) \in K^n \mid f(\xi_1, \ldots, \xi_n) = 0 \text{ for all } f \in I\big\}$$

is called the *affine variety* defined by I.

By the following proposition, we can always assume our system of polynomials to be an ideal.

Proposition 13. *Let $f_1, \dots, f_s \in K[X_1, \dots, X_n]$. Then*

$$\operatorname{Var}(f_1, \dots, f_s) = \operatorname{Var}\big(\langle f_1, \dots, f_s \rangle\big).$$

On the other hand, given a set of zeros in affine space, we can consider all polynomials that vanish on all zeros simultaneously.

Definition 14. Let $V \subseteq K^n$ be a subset. Then the set

$$\operatorname{Id}(V) = \big\{ f \in K[X_1, \dots, X_n] \mid f(\xi_1, \dots, \xi_n) = 0 \text{ for all } (\xi_1, \dots, \xi_n) \in V \big\}$$

is called the *(vanishing) ideal* of V.

It is easy to verify that $\operatorname{Id}(V)$ is indeed an ideal.

Proposition 15. *Let $V \subseteq K^n$ be a subset. Then*

$$\operatorname{Id}(V) \trianglelefteq K[X_1, \dots, X_n].$$

The following proposition shows how operations on varieties correspond to operations on ideals.

Proposition 16.

(1) We have $\varnothing = \operatorname{Var}\big(K[X_1, \dots, X_n]\big)$ and $K^n = \operatorname{Var}\big(\langle 0 \rangle\big)$.

(2) Let $I, J \trianglelefteq K[X_1, \dots, X_n]$ be ideals. Then

$$\operatorname{Var}(I) \cup \operatorname{Var}(J) = \operatorname{Var}(I \cdot J) = \operatorname{Var}(I \cap J).$$

(3) Let $\mathcal{M}$ be a nonempty set of ideals in $K[X_1, \dots, X_n]$. Then

$$\bigcap_{I \in \mathcal{M}} \operatorname{Var}(I) = \operatorname{Var}\big(\textstyle\bigcup_{I \in \mathcal{M}} I\big).$$

In particular, affine varieties form the closed sets of a topology, which is called the Zariski topology *on K^n.*

2.3 Hilbert's Nullstellensatz

In this section we derive a relationship between Var and Id. The result will be a generalization of the Fundamental Theorem of Algebra.

Theorem 17 (The Fundamental Theorem of Algebra)**.** *Every nonconstant polynomial $f \in \mathbb{C}[X]$ has a root $\xi \in \mathbb{C}$:*

$$f(\xi) = 0.$$

Fields with this property are called algebraically closed. So let K be an algebraically closed field and $I \trianglelefteq K[X_1, \ldots, X_n]$ an ideal. Obviously $\mathrm{Var}(I) \neq 0$ can only hold if $1 \notin I$ or equivalently $I \subsetneq K[X_1, \ldots, X_n]$ is a proper ideal. It turns out that this condition is already sufficient.

Lemma 18. *Let K be a field and let L/K be a field extension which is finitely generated as a K-algebra. Then L is algebraic over K.*

Proof. See for example [La05]. □

Theorem 19 (The Maximal Ideal Theorem)**.** *Let K be algebraically closed. Then an ideal $\mathfrak{m} \trianglelefteq K[X_1, \ldots, X_n]$ is maximal if and only if there exist $\xi_1, \ldots, \xi_n \in K$ such that*

$$\mathfrak{m} = \langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle.$$

Proof. Let $\xi_1, \ldots, \xi_n \in K$ and $\mathfrak{m} = \langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle \trianglelefteq K[X_1, \ldots, X_n]$. The map

$$\varphi : K[X_1, \ldots, X_n] \to K, \qquad f \mapsto f(\xi_1, \ldots, \xi_n)$$

is a ring epimorphism with $\ker \varphi = \mathfrak{m}$. By the first isomorphism theorem

$$K[X_1, \ldots, X_n]/\mathfrak{m} \cong K$$

is a field and therefore $\mathfrak{m}$ is maximal.

Conversely, let $\mathfrak{m} \trianglelefteq K[X_1, \ldots, X_n]$ be a maximal ideal. Then $L := K[X_1, \ldots, X_n]/\mathfrak{m}$ is a field extension of K which is generated by

$$X_1 + \mathfrak{m}, \ldots, X_n + \mathfrak{m}$$

as a K-algebra. By Lemma 18, L is algebraic over K, but since K is algebraically closed, there is a ring isomorphism $\varphi : L \to K$. Define $\xi_i := \varphi(X_i + \mathfrak{m})$ for all $i = 1, \ldots, n$. Let $f \in \langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle$, then

$$0 = f(\xi_1, \ldots, \xi_n) = f\big(\varphi(X_1 + \mathfrak{m}), \ldots, \varphi(X_n + \mathfrak{m})\big) = \varphi(f + \mathfrak{m})$$

and so $f \in \mathfrak{m}$. Therefore $\langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle \subseteq \mathfrak{m}$. But by the first part of the proof, $\langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle$ is maximal, and hence equality holds. □

In this situation the variety $\mathrm{Var}(\mathfrak{m}) = \big\{(\xi_1, \ldots, \xi_n)\big\}$ is a point in K^n.

Theorem 20 (The Weak Nullstellensatz)**.** *Let K be algebraically closed and let $I \lhd K[X_1, \ldots X_n]$ be a proper ideal. Then*

$$\mathrm{Var}(I) \neq \varnothing.$$

Proof. Define

$$\mathcal{M} := \big\{ J \lhd K[X_1, \ldots, X_n] \mid J \text{ proper with } I \subseteq J \big\} \neq \varnothing.$$

Since $K[X_1, \ldots X_n]$ is Noetherian, $\mathcal{M}$ contains a maximal element $\mathfrak{m}$ which is also a maximal ideal and satisfies $I \subseteq \mathfrak{m}$. By the Maximal Ideal Theorem there are $\xi_1, \ldots, \xi_n \in K$ such that $\mathfrak{m} = \langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle$.

Let $f \in I$. Then $f \in \mathfrak{m}$ and hence $f(\xi_1, \ldots, \xi_n) = 0$. Therefore

$$(\xi_1, \ldots, \xi_n) \in \mathrm{Var}(I).$$ □

The Weak Nullstellensatz suggests that there is a one-to-one correspondence between varieties and ideals. However, this is not true as one can see from the example $\mathrm{Var}\big(\langle X\rangle\big) = \mathrm{Var}\big(\langle X^2\rangle\big) = \{0\}$. Here, the correspondence fails for the following reason: a power of a polynomial vanishes on the same points as the original polynomial.

Definition 21. Let $I \trianglelefteq R$ be an ideal.

(1) The *radical* of I is defined by

$$\sqrt{I} = \big\{a \in R \,|\, a^e \in I \text{ for some } e \in \mathbb{N}_{>0}\big\} \trianglelefteq R.$$

(2) I is a *radical ideal* if $I = \sqrt{I}$.

Restricting to radical ideals we obtain a strong version of the Nullstellensatz.

Theorem 22 (The Strong Nullstellensatz)**.** *Let K be algebraically closed and let $I \trianglelefteq K[X_1, \dots X_n]$. Then*

$$\mathrm{Id}\big(\mathrm{Var}(I)\big) = \sqrt{I}.$$

Proof. Let $f \in \sqrt{I}$. Then there is an $e \in \mathbb{N}_{>0}$ such that $f^e \in I$. Since $f^e(\xi_1, \dots, \xi_n) = 0$ implies $f(\xi_1, \dots, \xi_n) = 0$ for all $(\xi_1, \dots, \xi_n) \in \mathrm{Var}(I)$, it follows that $f \in \mathrm{Id}\big(\mathrm{Var}(I)\big)$.

Conversely, let $0 \neq f \in \mathrm{Id}\big(\mathrm{Var}(I)\big)$. By the Hilbert Basis Theorem there are $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ such that $I = \langle f_1, \dots, f_s\rangle$. The following construction is known as the *Rabinovich trick*. Define

$$J := \langle f_1, \dots, f_s,\, X_{n+1}f - 1\rangle \trianglelefteq K[X_1, \dots, X_{n+1}].$$

Then $\mathrm{Var}(J) = \varnothing$, because otherwise there is a $(\xi_1, \dots, \xi_{n+1}) \in K^{n+1}$ such that $f_i(\xi_1, \dots, \xi_n) = 0$ for $i = 1, \dots, s$ and $\xi_{n+1} \cdot f(\xi_1, \dots, \xi_n) - 1 = 0$ which contradicts $f \in \mathrm{Var}(I)$. By the Weak Nullstellensatz, $J = K[X_1, \dots, X_{n+1}]$ and hence there are $q_1, \dots, q_s, q \in K[X_1, \dots, X_{n+1}]$ such that

$$1 = q_1 f_1 + \cdots + q_s f_s + q(X_{n+1}f - 1).$$

Applying $K[X_1, \dots, X_{n+1}] \to K(X_1, \dots, X_{n+1})$, $f \mapsto f(X_1, \dots, X_n, \frac{1}{f})$ to both sides we obtain the equation

$$1 = q_1\big(X_1, \dots, X_n, \tfrac{1}{f}\big) f_1 + \cdots + q_s\big(X_1, \dots, X_n, \tfrac{1}{f}\big) f_s$$

in the field of rational functions. Multiplying a suitable power of f at both sides clears all denominators and yields $f \in \sqrt{I}$. □

2.4 Algebra–Geometry Dictionary

From the Strong Nullstellensatz we obtain a one-to-one correspondence between varieties and radical ideals.

Theorem 23. *Let K be algebraically closed. The map*

$$\mathrm{Var} : \{\textit{radical ideals } I \trianglelefteq K[X_1, \ldots, X_n]\} \longrightarrow \{\textit{varieties } V \subseteq K^n\}$$

is a bijection with inverse Id. *Both maps are inclusion-reversing.*

Varieties that cannot be decomposed in smaller subvarieties are called irreducible.

Definition 24. Let $V \subseteq K^n$ be an affine variety. V is called *irreducible* if

$$V = V_1 \cup V_2 \quad \Longrightarrow \quad V = V_1 \text{ or } V = V_2$$

for all varieties $V_1, V_2 \in K^n$.

By the following proposition, irreducible varieties correspond to prime ideals.

Proposition 25. *Let $V \subseteq K^n$ be an affine variety. Then*

$$V \textit{ irreducible} \quad \Longleftrightarrow \quad \mathrm{Id}(V) \textit{ is a prime ideal.}$$

We have shown that there is a strong relationship between algebraic objects in $K[X_1, \ldots, X_n]$ and geometric objects in K^n. We obtain a dictionary between algebra and geometry, provided that K is algebraically closed.

Algebra	Geometry
$K[X_1, \ldots, X_n]$	K^n
radical ideals	affine varieties
prime ideals	irreducible varieties
maximal ideals	points
ascending chain condition	descending chain condition

3 Gröbner Bases

In the last sections a lot of algorithmic questions arised:

- Ideal membership problem: $f \in I$?
- Consistency problem: $1 \in I$?
- Radical membership problem: $f \in \sqrt{I}$?
- Solving systems of polynomial equations

- Computing intersections of ideals
- ...

Let us first have a look at the ideal membership problem in the univariate case. Let $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq K[X]$ be an ideal and let $f \in K[X]$ be a polynomial. Since $K[X]$ is an Euclidean domain we can write

$$I = \langle f_1, \ldots, f_s \rangle = \langle g \rangle,$$

where $g = \gcd(f_1, \ldots, f_s)$ can be computed by Euclid's Algorithm. Division with remainder yields unique $q, r \in K[X]$ such that

$$f = qg + r, \qquad \deg(r) < \deg(g).$$

By the uniqueness of the remainder it follows that

$$f \in I \quad \iff \quad r = 0.$$

In this section we present a division algorithm in $K[X_1, \ldots, X_n]$ with similar properties, following closely [vzGG03] and [CLO97]. An additional reference is [Eis95].

3.1 Division Algorithm

We identify

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \quad \longleftrightarrow \quad X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in K[X_1, \ldots, X_n]$$

and introduce some notation.

Definition 26. Let $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \in K[X_1, \ldots, X_n]$.

(1) X^α is called *monomial* for all $\alpha \in \mathbb{N}^n$.

(2) The *total degree* of X^α is $|\alpha| := \alpha_1 + \cdots + \alpha_n$.

(3) The *total degree* of f is $\deg(f) = \max\big\{ |\alpha| \;\big|\; \alpha \in \mathbb{N}^n \text{ with } a_\alpha \neq 0 \big\}$.

(4) a_α is called the *coefficient* of X^α.

(5) If $a_\alpha \neq 0$, then $a_\alpha X^\alpha$ is a *term* of f.

As in the univariate case, the division algorithm requires the notion of leading terms. For this, we need an order on the monomials. This order should be total and it should respect the multiplication of monomials. Moreover, for the division algorithm to terminate, it should be a well-order.

Definition 27. A *monomial order* $\prec$ in $K[X_1, \ldots, X_n]$ is a relation on $\mathbb{N}^n$ such that the following hold:

(i) $\prec$ is a total order on $\mathbb{N}^n$,

(ii) $\alpha \prec \beta \implies \alpha + \gamma \prec \beta + \gamma$ for all $\alpha, \beta, \gamma \in \mathbb{N}^n$, and

(iii) $\prec$ is a well-order.

If $\alpha, \beta \in \mathbb{N}^n$ with $\alpha \prec \beta$, we write $X^\alpha \prec X^\beta$.

The three standard examples of monomials orders are the following.

Definition 28. Let $\alpha, \beta \in \mathbb{N}^n$.

(1) The *lexicographic order* $\prec_{\text{lex}}$ on $\mathbb{N}^n$ is defined by

$$\alpha \prec_{\text{lex}} \beta \iff \text{the leftmost nonzero entry in } \alpha - \beta \in \mathbb{Z}^n \text{ is negative.}$$

(2) The *graded lexicographic order* $\prec_{\text{grlex}}$ on $\mathbb{N}^n$ is defined by

$$\alpha \prec_{\text{grlex}} \beta \iff |\alpha| < |\beta| \text{ or } \big(|\alpha| = |\beta| \text{ and } \alpha \prec_{\text{lex}} \beta\big).$$

(3) The *graded reverse lexicographic order* $\prec_{\text{grevlex}}$ on $\mathbb{N}^n$ is defined by

$$\alpha \prec_{\text{grevlex}} \beta \iff |\alpha| < |\beta| \text{ or } \begin{array}{l}\big(|\alpha| = |\beta| \text{ and the rightmost nonzero} \\ \text{entry in } \alpha - \beta \in \mathbb{Z}^n \text{ is positive}\big).\end{array}$$

In analogy to the univariate case we define the following.

Definition 29. Let $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \in K[X_1, \ldots, X_n] \setminus \{0\}$ and let $\prec$ be a monomial order on $\mathbb{N}^n$.

(1) The *multidegree* of f is $\text{multideg}(f) = \max\big\{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\big\}$.

(2) The *leading coefficient* of f is $\text{LC}(f) = a_{\text{multideg}(f)} \in K \setminus \{0\}$.

(3) The *leading monomial* of f is $\text{LM}(f) = X^{\text{multideg}(f)}$.

(4) The *leading term* of f is $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$.

Moreover, $\text{multideg}(0) = -\infty$ and $\text{LC}(0) = \text{LM}(0) = \text{LT}(0) = 0$.

Example. Let $f = X^2Y + XY^2 + Y^2$, $f_1 = XY - 1$ and $f_2 = Y^2 - 1$ be polynomials in $\mathbb{R}[X, Y]$ and let $\prec = \prec_{\text{lex}}$. We perform the straightforward division procedure:

	$XY-1$	Y^2-1	rem
$X^2Y + XY^2 + Y^2$	X		
$-(X^2Y - X)$			
$XY^2 + X + Y^2$	Y		
$-(XY^2 - Y)$			
$X + Y^2 + Y$			X
$-X$			
$Y^2 + Y$		1	
$-(Y^2 - 1)$			
$Y + 1$			

Note that in the second step we could have used f_2 for division as well. In the third step a phenomenon occured that cannot happen in the univariate case. The leading term X is not divisible by any of $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$, whereas there are still terms in $X + Y^2 + Y$ that are divisible by them. Therefore we moved X to the remainder column. From the above table we conclude

$$f = (X + Y) \cdot f_1 + 1 \cdot f_2 + (X + Y + 1).$$

Algorithm 30 (Division Algorithm)**.**
Input: $f, f_1, \ldots, f_s \in K[X_1, \ldots, X_n] \setminus \{0\}$ and a monomial order $\prec$.
Output: $q_1, \ldots, q_s, r \in K[X_1, \ldots, X_n]$ such that $f = q_1 f_1 + \cdots + q_s f_s + r$ and no term in r is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Moreover, $\mathrm{multideg}(f) \succcurlyeq \mathrm{multideg}(q_i f_i)$ for all $i = 1, \ldots, s$.

(1) $p \leftarrow f, \quad r \leftarrow 0, \qquad$ **for** $i = 1, \ldots, s$ **do** $q_i \leftarrow 0$

(2) **while** $p \neq 0$ **do**

- **if** $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$ for a minimal $i \in \{1, \ldots, s\}$ **then**

$$q_i \leftarrow q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}, \qquad p \leftarrow p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i$$

- **else**

$$r \leftarrow r + \mathrm{LT}(p), \qquad p \leftarrow p - \mathrm{LT}(p)$$

(3) **return** $q_1, \ldots, q_s, r$

Proof of correctness. At each entry to the **while**-loop the following invariants hold:

(i) $f = p + q_1 f_1 + \cdots + q_s f_s + r$,

(ii) no term in r is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, and

(iii) $\mathrm{multideg}(f) \succcurlyeq \mathrm{multideg}(q_i f_i)$ for all $i = 1, \ldots, s$.

The algorithm terminates if eventually $p = 0$. If p is redefined to be $p' \neq 0$ during the **while**-loop, then

$$\mathrm{multideg}(p') \prec \mathrm{multideg}(p).$$

Therefore $p = 0$ must finally happen, because otherwise we would get an infinite decreasing sequence of multidegrees contradicting the well-order property of $\prec$. □

The remainder on division of f by the s-tuple $F = (f_1, \ldots, f_s)$ is denoted by

$$\overline{f}^F.$$

The Division Algorithm has a major drawback: the remainder $\overline{f}^F$ need not be unique and depends on the order of $f_1, \ldots, f_s$. In particular it may happen that $f \in \langle f_1, \ldots, f_s \rangle$ and still $\overline{f}^F \neq 0$. Gröbner bases are special generating sets that overcome these problems.

3.2 Existence and Uniqueness

Definition 31. An ideal $I \trianglelefteq K[X_1, \ldots, X_n]$ is called *monomial ideal* if there is a subset $A \subseteq \mathbb{N}^n$ such that

$$I = \langle X^A \rangle := \langle X^\alpha \mid \alpha \in A \rangle.$$

The key property of monomial ideals is the following lemma.

Lemma 32. *Let $A \subseteq \mathbb{N}^n$ be a subset, $I = \langle X^A \rangle \trianglelefteq K[X_1, \ldots, X_n]$ a monomial ideal and $\beta \in \mathbb{N}^n$. Then*

$$X^\beta \in I \quad \Longleftrightarrow \quad \exists \alpha \in A : \; X^\alpha \mid X^\beta.$$

Proof. Let $X^\beta \in I$. Then there are $q_1, \ldots, q_s \in K[X_1, \ldots, X_n]$ and $\alpha_1, \ldots, \alpha_s \in A$ such that $X^\beta = \sum_{i=1}^s q_i X^{\alpha_i}$. Therefore X^β occurs in at least one of the $q_i X^{\alpha_i}$ and hence $X^{\alpha_i} \mid X^\beta$.

The converse implication is obvious. □

Lemma 33 (Dickson)**.** *Let $A \subseteq \mathbb{N}^n$ be a subset and $I = \langle X^A \rangle \trianglelefteq K[X_1, \ldots, X_n]$ a monomial ideal. Then there exists a finite subset $B \subseteq A$ such that*

$$\langle X^A \rangle = \langle X^B \rangle.$$

Proof. This follows immediately from Corollary 11. □

Dickson's Lemma motivates the following definition.

Definition 34. Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let $\prec$ be a monomial order on $\mathbb{N}^n$. A finite set $G \subseteq I$ is a *Gröbner basis* for I with respect to $\prec$ if

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

Theorem 35. *Let $\prec$ be a monomial order on $\mathbb{N}^n$. Then every ideal $I \trianglelefteq K[X_1, \ldots, X_n]$ has a Gröbner basis G w.r.t. $\prec$. Moreover,*

$$I = \langle G \rangle.$$

Proof. The first statement follows directly from Dickson's Lemma. For the second statement let $f \in I$ and $G = \{g_1, \ldots, g_t\}$. The Division Algorithm yields $q_1, \ldots, q_t, r \in K[X_1, \ldots, X_n]$ such that $f = q_1 g_1 + \cdots + q_t g_t + r$ and no term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. But $r = f - q_1 g_1 - \cdots - q_t g_t \in I$ and hence $\mathrm{LT}(r) \in \mathrm{LT}(I) = \langle \mathrm{LT}(G) \rangle$. From Lemma 32 it follows that $r = 0$ and thus $f \in \langle G \rangle$. □

For Gröbner bases, the Division Algorithm yields a unique remainder.

Theorem 36. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let G be a Gröbner basis for I. Let $f \in K[X_1, \ldots, X_n]$. Then there is a unique $r \in K[X_1, \ldots, X_n]$ such that*

(i) $f - r \in I$, *and*

(ii) no term of r *is divisble by any term in* $\operatorname{LT}(G)$.

In particular, $r = \overline{f}^G$ *is the remainder on division of* f *by* G *and is called the* normal form *of* f *with respect to* G.

Proof. The Division Algorithm proves the existence of an r with the desired properties. For the uniqueness, let $g, g' \in I$ and $r, r' \in K[X_1, \ldots, X_n]$ such that $f = g + r = g' + r'$ and both r and r' satisfy (ii). Then $r - r' = g' - g \in I$ and hence $\operatorname{LT}(r - r') \in \langle \operatorname{LT}(I) \rangle = \langle \operatorname{LT}(G) \rangle$. By Lemma 32, there is a $g \in G$ with $\operatorname{LT}(g) \mid \operatorname{LT}(r - r')$. Therefore $r - r' = 0$. □

In general, an ideal can have many different Gröbner bases. By the following observation, there may be elements in a Gröbner basis that can be eliminated.

Lemma 37. *Let* $I \trianglelefteq K[X_1, \ldots, X_n]$ *be an ideal and let* G *be a Gröbner basis for* I. *If* $g \in G$ *such that*

$$\operatorname{LT}(g) \in \big\langle \operatorname{LT}(G \setminus \{g\}) \big\rangle,$$

then $G \setminus \{g\}$ *is also a Gröbner basis for* I.

Definition 38. Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal. A Gröbner basis G for I is called *minimal* if for all $g \in G$

(i) $\operatorname{LC}(g) = 1$, and

(ii) $\operatorname{LT}(g) \notin \big\langle \operatorname{LT}(G \setminus \{g\}) \big\rangle$.

An ideal might still have many different minimal Gröbner bases G. If we replace each $g \in G$ by the reduced element $\overline{g}^{G \setminus \{g\}}$, we obtain a unique basis.

Definition 39. Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let G be a Gröbner basis for I. An element $g \in G$ is called *reduced with respect to* G if no term of g is in

$$\big\langle \operatorname{LT}(G \setminus \{g\}) \big\rangle.$$

G is called *reduced* if G is minimal and every $g \in G$ is reduced with respect to G.

Theorem 40. *Every ideal* $I \trianglelefteq K[X_1, \ldots, X_n]$ *has a unique reduced Gröbner basis.*

3.3 Buchberger's Algorithm

The proof of the existence of Gröbner bases was non-constructive. We are not even able to detect wether a given generating set $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis. One reason why G might fail to be a Gröbner basis could be a linear combination of the g_i whose leading term is not in $\langle \mathrm{LT}(G) \rangle$ due to cancellation of leading terms of the g_i. The S-polynomial of two polynomials f and g is defined in such a way that the leading terms of f and g cancel.

Definition 41. Let $f, g \in K[X_1, \ldots, X_n] \backslash \{0\}$ and let $X^\gamma = \mathrm{lcm}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big)$. Then the *S-polynomial* of f and g is

$$S(f,g) = \frac{X^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{X^\gamma}{\mathrm{LT}(g)} \cdot g.$$

The following theorem shows that every kind of cancellation can be accounted for by S-polynomials.

Theorem 42 (Buchberger 1965)**.** *A finite set $G = \{g_1, \ldots, g_t\} \subseteq K[X_1, \ldots, X_n]$ is a Gröbner basis for the ideal $\langle G \rangle$ if and only if*

$$\overline{S(g_i, g_j)}^{G} = 0 \qquad (*)$$

for all $1 \leq i < j \leq t$.

Proof. If G is a Gröbner basis then $(*)$ is fulfilled because of the uniqueness property in Theorem 36.

Conversely, suppose that $(*)$ holds. Assume by way of contradiction that G is not a Gröbner basis. Then there is an $f \in I$ with $\mathrm{LT}(f) \notin \langle \mathrm{LT}(G) \rangle$. We choose $q_1, \ldots, q_t \in K[X_1, \ldots, X_n]$ such that

$$f = q_1 g_1 + \cdots + q_t g_t$$

and both

(i) $\delta := \max\big\{\mathrm{multideg}(q_1 g_1), \ldots, \mathrm{multideg}(q_t g_t)\big\}$, and

(ii) $k := \big|\big\{q_i g_i \mid \mathrm{multideg}(q_i g_i) = \delta \text{ and } 1 \leq i \leq t\big\}\big|$

are minimal. This is possible because $\prec$ is a well-order. We may assume w.l.o.g. that $\mathrm{multideg}(q_1 g_1) = \ldots = \mathrm{multideg}(q_k g_k) = \delta$ and $\mathrm{multideg}(q_i g_i) \prec \delta$ for $k < i \leq t$. Since $\mathrm{LT}(f)$ is not divisible by any term in $\mathrm{LT}(G)$, the terms in the $q_i g_i$ that contain the monomial X^δ must cancel, in particular $k \geq 2$. For $i = 1, 2$ we denote $\mathrm{LT}(q_i g_i) = a_i b_i$, where a_i and b_i are terms in q_i and g_i respectively. Since $a_1 b_1 = c \cdot a_2 b_2$ for some $c \in K$, there is a polynomial $r \in K[X_1, \ldots, X_n]$ such that

$$r \cdot \frac{\mathrm{lcm}(b_1, b_2)}{b_1} = a_1.$$

By $(*)$, there are $r_1, \ldots, r_t \in K[X_1, \ldots, X_n]$ such that

$$S(g_1, g_2) = r_1 g_1 + \cdots + r_t g_t$$

and $\operatorname{multideg}\big(S(g_1, g_2)\big) \succcurlyeq \operatorname{multideg}(r_i g_i)$ for $i = 1, \ldots, t$. Expanding the expression

$$\begin{aligned} f &= f - r\big(S(g_1, g_2) - \textstyle\sum_{i=1}^{t} r_i g_i\big) \\ &= q_1' g_1 + \cdots + q_t' g_t \end{aligned}$$

for some $q_1', \ldots, q_t' \in K[X_1, \ldots, X_n]$ yields a representation of f such that $\operatorname{multideg}(q_2' g_2) = \ldots = \operatorname{multideg}(q_k' g_k) = \delta$ and $\operatorname{multideg}(q_i g_i) \prec \delta$ for $i = 1$ and $k < i \leq t$. This contradicts the minimality of k. □

Buchberger's criterion naturally leads to the following algorithm.

Algorithm 43 (Buchberger's Algorithm)**.**
Input: $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ and a monomial order $\prec$.
Output: A Gröbner basis G for the ideal $I = \langle f_1, \ldots, f_s \rangle$ w. r. t. $\prec$ such that $f_1, \ldots, f_s \in G$.

(1) $G \leftarrow \{f_1, \ldots, f_s\}$

(2) **repeat**

  (a) $\mathcal{S} \leftarrow \varnothing$

  (b) **for each** $\{g, g'\} \subseteq G$ with $g \neq g'$ **do**

  - $r \leftarrow \overline{S(g, g')}^{G}$
  - **if** $r \neq 0$ **then** $\mathcal{S} \leftarrow \mathcal{S} \cup \{r\}$

  (c) $G \leftarrow G \cup \mathcal{S}$

  until $\mathcal{S} = \varnothing$

(3) **return** G

Proof of correctness. At each stage of the algorithm $G \subseteq I$ holds, and since $f_1, \ldots, f_s \in G$, we also have $\langle G \rangle = I$. The algorithm terminates if eventually

$$\overline{S(g, g')}^{G} = 0$$

for all $g, g' \in G$ with $g \neq g'$. Then G is a Gröbner basis for I by Theorem 42.

Assume that G is redefined to be G' with $G \subsetneq G'$ during the **repeat-until**-loop. Then there is an $r \in G'$ such that no term in r is divisible by any term in $\operatorname{LT}(G)$. Hence $\operatorname{LT}(r) \notin \langle \operatorname{LT}(G) \rangle$ but $\operatorname{LT}(r) \in \langle \operatorname{LT}(G') \rangle$, and therefore

$$\langle \operatorname{LT}(G) \rangle \subsetneq \langle \operatorname{LT}(G') \rangle.$$

Thus the algorithm must finally terminate, because otherwise we get an infinite proper ascending chain of ideals in contradiction to $K[X_1, \ldots, X_n]$ being Noetherian. □

3.4 Applications

The uniqueness of the remainder on division by a Gröbner basis and the uniqueness of reduced Gröbner bases solves the ideal membership and the consistency problem respectively.

Proposition 44. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let G be a Gröbner basis for I. Let $f \in K[X_1, \ldots, X_n]$, then*

$$f \in I \quad \Longleftrightarrow \quad \overline{f}^G = 0.$$

Proposition 45. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let G be the reduced Gröbner basis for I. Then*

$$1 \in I \quad \Longleftrightarrow \quad G = \{1\}.$$

By applying the Rabinovich trick, we can reduce the radical membership problem to the consistency problem.

Proposition 46. *Let $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let $f \in K[X_1, \ldots, X_n]$. Define*

$$J := \langle f_1, \ldots, f_s,\ X_{n+1} f - 1 \rangle \trianglelefteq K[X_1, \ldots, X_{n+1}].$$

Then

$$f \in \sqrt{I} \quad \Longleftrightarrow \quad 1 \in J.$$

Proof. If $1 \in J$ then we obtain $f \in \sqrt{I}$ like in the proof of the Strong Nullstellensatz.

Conversely, let $f \in \sqrt{I}$. Then there is an $e \in \mathbb{N}_{>0}$ such that $f^e \in I \subseteq J$. Therefore

$$\begin{aligned} 1 &= X_{n+1}^e f^e - (X_{n+1}^e f^e - 1) \\ &= X_{n+1}^e f^e - (X_{n+1}^{e-1} f^{e-1} + \cdots + X_{n+1} f + 1)(X_{n+1} f - 1) \in J. \end{aligned}$$ □

Gröbner bases are also useful for solving systems of polynomial equations because of elimination properties of the $\prec_{\text{lex}}$ order.

Definition 47. Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal. The ℓ-th *elimination ideal* I_ℓ is defined by

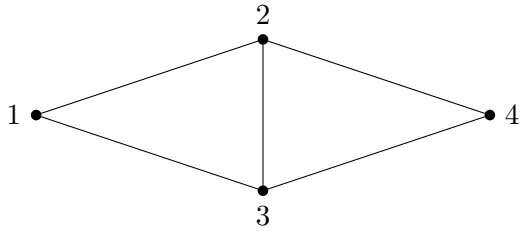
$$I_\ell = I \cap K[X_{\ell+1}, \ldots, X_n].$$

Theorem 48 (Elimination Theorem)**.** *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let G be a Gröbner basis for I with respect to $\prec_{lex}$. Then*

$$G_\ell = G \cap K[X_{\ell+1}, \ldots, X_n]$$

is a Gröbner basis for I_ℓ.

Example. Recall the graph $G = (V, E)$ from the introductory example:



Let

$$I = \left\langle X_i^3 - 1 \mid i \in V \right\rangle + \left\langle X_i^2 + X_i X_j + X_j^2 \mid (i,j) \in E \right\rangle \trianglelefteq \mathbb{C}[X_1, \ldots, X_4].$$

The reduced Gröbner basis for I w. r. t. $\prec_{\text{lex}}$ is $G = \{g_1, \ldots, g_4\}$ with

$$\begin{aligned} g_1 &= X_1 - X_4, \\ g_2 &= X_2 + X_3 + X_4, \\ g_3 &= X_3^2 + X_3 X_4 + X_4^2, \\ g_4 &= X_4^3 - 1. \end{aligned}$$

From the triangular form we find that for instance $\left(1, e^{(2/3)\pi i}, e^{(4/3)\pi i}, 1\right) \in \mathrm{Var}(I)$.

The following proposition together with the Elimination Theorem shows how to compute the intersection of ideals.

Proposition 49. *Let $I, J \trianglelefteq K[X_1, \ldots, X_n]$ be ideals. Then*

$$I \cap J = \left(X_0 \cdot I + (1 - X_0) \cdot J\right) \cap K[X_1, \ldots, X_n].$$

Proof. Let $f \in I \cap J$. Then

$$f = X_0 f + (1 - X_0) f \in \left(X_0 \cdot I + (1 - X_0) \cdot J\right) \cap K[X_1, \ldots, X_n].$$

Conversely, let $f \in \left(X_0 \cdot I + (1 - X_0) \cdot J\right) \cap K[X_1, \ldots, X_n]$. Then there are $f_1 \in I$ and $f_2 \in J$ such that $f = X_0 f_1 + (1 - X_0) f_2 \in K[X_1, \ldots, X_n]$. Setting $X_0 = 1$ and $X_0 = 0$ yields $f = f_1 \in I$ and $f = f_2 \in J$ respectively, hence $f \in I \cap J$. □

4 Computational Complexity

In this section we want to discuss the computational complexity of the three decision problems we encountered so far. A survey on complexity results about polynomial ideals is given in [Ma97].

Definition 50. We define the following decision problems using a suitable coding in sparse representation:

(1) The *ideal membership problem* is defined by

$$\mathrm{IM} = \big\{(f, f_1, \ldots, f_s) \in (\mathbb{Q}[X_1, \ldots, X_n])^{s+1} \mid f \in \langle f_1, \ldots, f_s\rangle\big\}.$$

(2) The *consistency problem* is defined by

$$\textsc{Cons} = \big\{(f_1, \ldots, f_s) \in (\mathbb{Q}[X_1, \ldots, X_n])^{s} \mid 1 \in \langle f_1, \ldots, f_s\rangle\big\}.$$

(3) The *radical membership problem* is defined by

$$\mathrm{RM} = \big\{(f, f_1, \ldots, f_s) \in (\mathbb{Q}[X_1, \ldots, X_n])^{s+1} \mid f \in \sqrt{\langle f_1, \ldots, f_s\rangle}\big\}.$$

Lower bounds of the complexity of those problems yield lower bounds for the complexity of Buchberger's Algorithm. Recall the standard complexity classes

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} \subseteq \mathbf{NEXP} \subseteq \mathbf{EXPSPACE}$$

(for a definition, see e. g. [Pa94]).

4.1 Degree Bounds

An upper bound for IM can be obtained by the following degree bound which is double exponential in the number of variables.

Theorem 51 (Hermann 1926)**.** *Let $I = \langle f_1, \ldots, f_s\rangle \trianglelefteq \mathbb{Q}[X_1, \ldots, X_n]$ be an ideal and let $d = \max\big\{\deg(f_1), \ldots, \deg(f_s)\big\}$.*

If $f \in I$ then there are $q_1, \ldots, q_s \in \mathbb{Q}[X_1, \ldots, X_n]$ such that $f = q_1 f_1 + \cdots + q_s f_s$ and

$$\deg(q_i) \leq \deg(f) + (sd)^{2^n} \qquad \textit{for all } i = 1, \ldots, s.$$

Using this bound it is possible to enumerate all monomials that can appear in the q_i, what leads to a system of linear equations. Therefore IM can be reduced to a rank computation of a matrix of size double exponential in the input size. For the latter problem there exist algorithms on a parallel random access machine (PRAM) with a polynomial number of processors using polylogarithmic time. By the Parallel Computation Thesis (parallel time = sequential space) this yields an algorithm in exponential space. However, the matrix is too large and cannot be written down in exponential space. But in [Ma89] it is shown that the entries of the matrix can be generated on the fly from the polynomial description and that this does not affect the algorithm for the rank computation.

Theorem 52 (Mayr 1989)**.**

$$\mathrm{IM} \in \mathbf{EXPSPACE}.$$

For CONS the upper degree bound can be improved to be single exponential in the number of variables. Again, by the Rabinovich trick, this also yields an upper bound for RM.

Theorem 53 (Brownawell 1987)**.** *Let $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq \mathbb{Q}[X_1, \ldots, X_n]$ be an ideal, $\mu = \min\{s, n\}$ and $d = \max\big\{\deg(f_1), \ldots, \deg(f_s)\big\}$.*

(1) If the f_i have no common zero in $\mathbb{C}^n$, then there are $q_1, \ldots, q_s \in \mathbb{Q}[X_1, \ldots, X_n]$ with $1 = q_1 f_1 + \cdots + q_s f_s$ such that

$$\deg(q_i) \leq \mu n d^{\mu} + \mu d \qquad \text{for } i = 1, \ldots, s.$$

(2) If $f \in \mathbb{Q}[X_1, \ldots, X_n]$ such that $f(\xi) = 0$ for all common zeros ξ of the f_i in $\mathbb{C}^n$, then there are $e \in \mathbb{N}_{>0}$ and $q_1, \ldots, q_s \in \mathbb{Q}[X_1, \ldots, X_n]$ with $f^e = q_1 f_1 + \cdots + q_s f_s$ such that

$$\begin{aligned} e &\leq (\mu+1)(n+2)(d+1)^{\mu+1} \qquad \text{and} \\ \deg(q_i) &\leq (\mu+1)(n+2)(d+1)^{\mu+2} \qquad \text{for } i = 1, \ldots, s. \end{aligned}$$

With similar techniques, these bounds can be used to show the following result.

Corollary 54.

$$\text{CONS} \in \textbf{PSPACE} \qquad \textit{and} \qquad \text{RM} \in \textbf{PSPACE}.$$

Finally, we want to mention a degree bound for the polynomials in the reduced Gröbner basis of an ideal.

Theorem 55 (Dubé 1990)**.** *Let $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let $d = \max\big\{\deg(f_1), \ldots, \deg(f_s)\big\}$.*

Then for any monomial order, the total degree of polynomials in the reduced Gröbner basis for I is bounded above by

$$2\Big(\frac{d^2}{2} + d\Big)^{2^{n-1}}.$$

4.2 Mayr–Meyer Ideals

In [MM82], Mayr and Meyer showed that Hermann's double exponential degree bound is asymptotically tight. We show a slightly modified construction from [BS88]. Let $n \in \mathbb{N}$. For $r \in \mathbb{N}$ we define $e_r := 2^{2^r}$. Then

$$e_r = (e_{r-1})^2 \qquad \text{for all } r \in \mathbb{N}_{>0}.$$

We construct an ideal in the polynomial ring R over $\mathbb{Q}$ with the $10n$ variables

S_r	start
F_r	finish
$B_{r,1}, \ldots, B_{r,4}$	counters
$C_{r,1}, \ldots, C_{r,4}$	catalysts

for each level $r = 0, \ldots, n$. For notational convenience, we will omit subscripts from now on if r is fixed. Upper-case letters denote variables of level r and lower-case letters denote variables of level $r-1$. For $r = 0$ we define $I_0 \trianglelefteq R$ to be generated by

$$SC_i - FC_iB_i^2 \qquad \text{for } i = 1, \ldots, 4.$$

If $r > 0$, then $I_r \trianglelefteq R$ is generated by I_{r-1} and

$$\begin{aligned} &Sc_1 - sc_1, && sc_4 - Fc_4, \\ &fc_1 - sc_2, && sc_3 - fc_4, \\ &fc_2b_1 - fc_3b_4, && sc_3 - sc_2, \\ &fc_2C_ib_2 - fc_2C_iB_ib_3 && \text{for } i = 1, \ldots, 4. \end{aligned}$$

These ideals can be interpreted as quadratic counters. At level r, the ideal I_r counts to $e_r = 2^{2^r}$.

Lemma 56. *For all $r = 0, \ldots, n$ we have*

$$SC_i - FC_iB_i^{e_r} \in I_r \qquad \textit{for } i = 1, \ldots, 4.$$

Proof. Let $i \in \{1, \ldots, 4\}$. We use induction on r. For $r = 0$ the assertion follows from the definition. For $r > 0$ we have

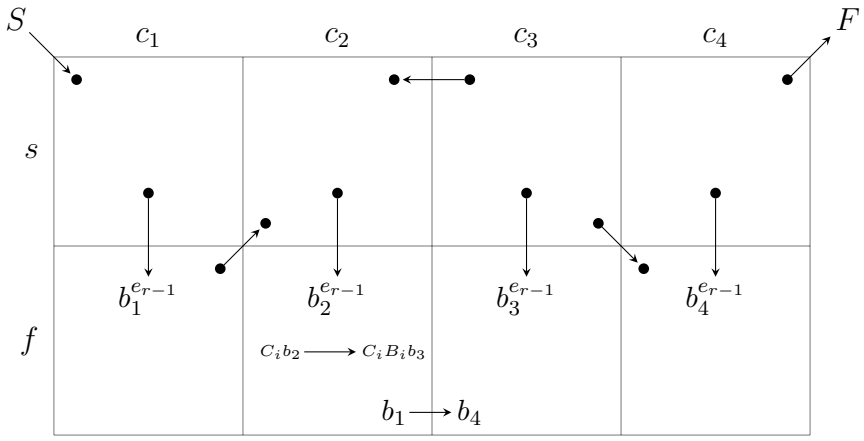


Figure 1: A quadratic counter.

$$
\begin{aligned}
SC_i &= sc_1C_i \\
&= fc_1C_ib_1^{e_{r-1}} && \text{by induction} \\
&= sc_2C_ib_1^{e_{r-1}} \\
&= fc_2C_ib_1^{e_{r-1}}b_2^{e_{r-1}} && \text{by induction} \\
&= \dots \\
&= fc_2C_iB_i^{e_{r-1}}b_1^{e_{r-1}}b_3^{e_{r-1}} \\
&= fc_3C_iB_i^{e_{r-1}}b_1^{e_{r-1}-1}b_3^{e_{r-1}}b_4 \\
&= sc_3C_iB_i^{e_{r-1}}b_1^{e_{r-1}-1}b_4 && \text{by induction} \\
&= sc_2C_iB_i^{e_{r-1}}b_1^{e_{r-1}-1}b_4 \\
&= fc_2C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-1}b_2^{e_{r-1}}b_4 && \text{by induction} \\
&= \dots \\
&= fc_2C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-1}b_3^{e_{r-1}}b_4 \\
&= fc_3C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-2}b_3^{e_{r-1}}b_4^2 \\
&= sc_3C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-2}b_4^2 && \text{by induction} \\
&= \dots && \text{repeating the previous 7 lines} \\
& && e_{r-1}-2 \text{ times} \\
&= sc_3C_iB_i^{e_{r-1}^2}b_4^{e_{r-1}} \\
&= fc_4C_iB_i^{e_{r-1}^2}b_4^{e_{r-1}} \\
&= fc_4C_iB_i^{e_{r-1}^2} && \text{by induction} \\
&= FC_iB_i^{e_r} \pmod{I_r}. && \square
\end{aligned}
$$

A visualization of this proof is given by a path in the graph of Figure 1, where monomials and differences of monomials are depicted by nodes and by directed edges, respectively. Setting $B_1 = \ldots = B_4 = C_1 = \ldots = C_4 = 1$ at level $r = n$, we obtain generators for the *Mayr–Meyer ideal* J_n.

Proposition 57. *Let* $J_n = \langle f_1, \ldots, f_s \rangle \trianglelefteq R$.

1. *We have* $S - F \in J_n$.
2. *If there are* $q_1, \ldots, q_s \in R$ *with* $S - F = q_1f_1 + \cdots + q_sf_s$, *then for some* $i \in \{1, \ldots, s\}$ *we have*

$$\deg(q_i) \geq e_{n-1} = 2^{2^{n-1}}.$$

Using this construction with techniques from complexity theory, Mayr and Meyer could show that IM is **EXPSPACE**-hard. We obtain the following final result.

Theorem 58 (Mayr & Meyer 1982, Mayr 1989)**.**

$$\text{IM} \in \textbf{EXPSPACE}\textit{-complete}.$$

References

[BS88] D. Bayer and M. Stillman. On the complexity of computing syzygies. *J. Symb. Comput.* **6**, 135–147, 1988.

[Bro87] W. D. Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math.* **126**, 577–591, 1987.

[Bu65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Leopold-Franzens-Universität Innsbruck, Austria, 1965.

[CLO97] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer-Verlag, New York, 2nd edition, 1997.

[Du90] T. W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.* **19** (4), 750–775, 1990.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag, New York, 1995.

[vzGG03] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* University Press, Cambridge, 2nd edition, 2003.

[He26] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.* **95**, 736–788, 1926.
English translation: The question of finitely many steps in polynomial ideal theory. *SIGSAM Bull.* **32** (3), 8–30, 1998.

[La05] S. Lang. *Algebra*. Springer-Verlag, New York, 3rd edition, 2005.

[Ma89] E. W. Mayr. Membership in Polynomial Ideals over $\mathbb{Q}$ Is Exponential Space Complete. *Proc. of the 6th Ann. Symp. on Theoretical Aspects of Computer Science STACS '89*, Paderborn, eds. B. Monien and R. Cori, LNCS **349**, Springer Verlag, 400–406, 1989.

[Ma97] E. W. Mayr. Some complexity results for polynomial ideals. *J. of Complexity* **13** (3), 303–325, 1997.

[MM82] E. W. Mayr and A. R. Meyer. The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals. *Advances in Math.* **46**, 305–329, 1982.

[Pa94] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.