Gröbner Bases

Computational Algebraic Geometry and its Complexity

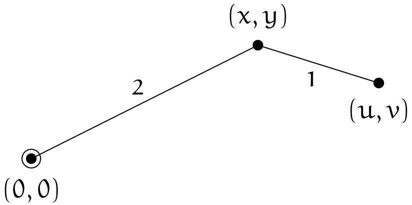
Johannes Mittmann

Technische Universität München (TUM)

5th Joint Advanced Student School (JASS)
St. Petersburg, March 25 – April 4, 2007
Course 1: Polynomials – Their Power and How to Use Them

Outline

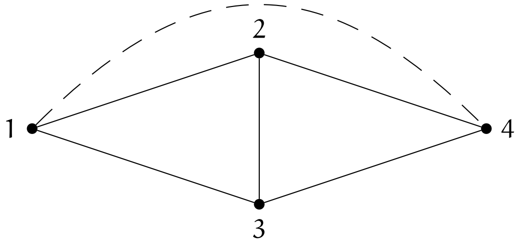
Example 1: A Simple Robot Arm



Positions: $(x, y, u, v) \in \mathbb{R}^4$ satisfying

$$\begin{aligned} x^2 + y^2 - 4 &= 0, \\ (x-u)^2 + (y-v)^2 - 1 &= 0. \end{aligned}$$

Example 2: Graph 3-Colouring



3-Colouring: $(\xi_1, \ldots, \xi_4) \in \mathbb{C}^4$ satisfying

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

Standard Setting

$\mathbb{N}$	natural numbers $0, 1, 2, \ldots$
R, S	commutative rings with unity
K, L	fields

Ideals

Definition

A subset $I \subseteq R$ is called an *ideal* of R, written $I \trianglelefteq R$, if

1. $0 \in I$,
2. $a + b \in I$ for all $a, b \in I$, and
3. $r \cdot a \in I$ for all $r \in R$ and $a \in I$.

Generation of Ideals

Proposition

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

$$\bigcap_{I \in \mathcal{M}} I \quad \textit{is an ideal in } R.$$

Definition

Let $A \subseteq R$ a subset. Then

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

is called the *ideal generated* by A.

Finitely Generated Ideals

Definition

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

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

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

Basic Operations on Ideals

Definition

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

1. The *sum* of I and J is defined by

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

2. The *product* of I and J is defined by

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

Proposition

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

$$I + J = \langle a_1, \dots, a_s, b_1, \dots, b_t \rangle \qquad \text{and}$$
$$I \cdot J = \langle a_i b_j \mid 1 \leqslant i \leqslant s \text{ and } 1 \leqslant j \leqslant t \rangle.$$

Noetherian Rings

Definition

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

$$I_N = I_{N+1} = I_{N+2} = \ldots .$$

Characterization of Noetherian Rings

Proposition

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.*

The Hilbert Basis Theorem

Theorem (Hilbert)

Let R be a Noetherian ring. Then

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

Corollary

Every ideal

$$I \trianglelefteq K[X_1, \ldots, X_n]$$

is finitely generated.

Affine Varieties

Definition

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

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

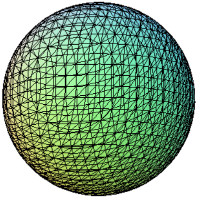
is called the *affine variety* defined by I.

Proposition

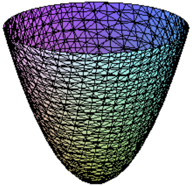
Let $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$. *Then*

$$\mathrm{Var}(f_1, \ldots, f_s) = \mathrm{Var}(\langle f_1, \ldots, f_s \rangle).$$

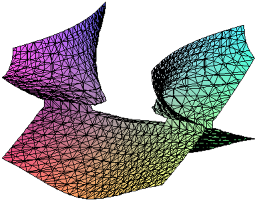
Varieties in $\mathbb{R}^3$



$\mathrm{Var}\left(X^2 + Y^2 + Z^2 - 1\right)$



$\mathrm{Var}\left(Z - X^2 - Y^2\right)$



$\mathrm{Var}\left(X^2 - Y^2 Z^2 + Z^3\right)$

Vanishing Ideals

Definition

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

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

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

Proposition

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

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

The Zariski Topology

Proposition

1. *Let* K *be a field. Then*

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

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.

The Zariski Closure

Proposition

Let $V \subseteq K^n$ be a subset. Then the Zariski closure of V is given by

$$\overline{V} = \mathrm{Var}\big(\mathrm{Id}(V)\big).$$

The Fundamental Theorem of Algebra

Theorem

Every nonconstant polynomial $f \in \mathbb{C}[X]$ *has a root* $\xi \in \mathbb{C}$*:*

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

Lemma

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*.*

The Maximal Ideal Theorem

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 ($\Longleftarrow$).

- The mapping

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

  is a ring epimorphism with $\ker \varphi = \mathfrak{m}$.
- By the First Isomorphism Theorem,

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

Proof ($\Longrightarrow$).

- $L := K[X_1, \dots, X_n]/\mathfrak{m}$ is a field generated by
$$X_1 + \mathfrak{m}, \dots, X_n + \mathfrak{m}$$
as a K-algebra, hence L is algebraic over K.
- Since K is algebraically closed, there is a K-isomorphism $\varphi : L \to K$.
- Define $\xi_i := \varphi(X_i + \mathfrak{m}) \in K$.
- Let $f \in \langle X_1 - \xi_1, \dots, X_n - \xi_n \rangle$, then
$$0 = f(\xi_1, \dots, \xi_n) = f\big(\varphi(X_i + \mathfrak{m}), \dots, \varphi(X_i + \mathfrak{m})\big) = \varphi(f + \mathfrak{m}).$$
- Therefore
$$\langle X_1 - \xi_1, \dots, X_n - \xi_n \rangle \subseteq \mathfrak{m}.$$
□

The Weak Nullstellensatz

Theorem (Hilbert)

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.

- The set

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

  contains a maximal ideal $\mathfrak{m} = \langle X_1 - \xi_1, \ldots, X_n - \xi_n \rangle$ with $I \subseteq \mathfrak{m}$.
- Let $f \in I$. Then $f \in \mathfrak{m}$ and so $f(\xi_1, \ldots, \xi_n) = 0$. Therefore

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

□

Radical Ideals

Definition

Let $I \trianglelefteq R$ be an ideal.

1. The *radical* of I is defined by
$$\sqrt{I} = \{a \in R \mid a^e \in I \text{ for some } e \in \mathbb{N}_{>0}\} \trianglelefteq R.$$
2. I is a *radical ideal* if
$$I = \sqrt{I}.$$

Example

Let $I = \langle X^2 \rangle \trianglelefteq \mathbb{R}[X]$. Then
$$\sqrt{I} = \langle X \rangle.$$

The Strong Nullstellensatz

Theorem (Hilbert)

Let K *be algebraically closed and let* $I \trianglelefteq K[X_1, \ldots X_n]$*. Then*

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

Proof (⊆).

- Let $0 \neq f \in \mathrm{Id}\big(\mathrm{Var}(I)\big)$.
- By the Hilbert Basis Theorem there are $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ such that
$$I = \langle f_1, \ldots, f_s \rangle.$$

The Rabinovich Trick

Proof ($\subseteq$, continued).

- Define
$$J := \langle f_1, \dots, f_s, X_{n+1}f - 1\rangle \trianglelefteq K[X_1, \dots, X_{n+1}].$$
- Then $\mathrm{Var}(J) = \varnothing$, otherwise $\exists(\xi_1, \dots, \xi_{n+1}) \in K^{n+1}$ with
$$f_i(\xi_1, \dots, \xi_n) = 0 \quad \text{and so} \quad \xi_{n+1} \cdot f(\xi_1, \dots, \xi_n) - 1 = -1 \neq 0.$$
- By the Weak Nullstellensatz $\exists q_1, \dots, q_s, q \in K[X_1, \dots, X_{n+1}]$ s. t.
$$1 = q_1 f_1 + \cdots + q_s f_s + q(X_{n+1}f - 1).$$
- Applying $K[X_1, \dots, X_{n+1}] \to K(X_1, \dots, X_{n+1})$, $X_{n+1} \mapsto \frac{1}{f}$, yields
$$1 = q_1\left(X_1, \dots, X_n, \tfrac{1}{f}\right)f_1 + \cdots + q_s\left(X_1, \dots, X_n, \tfrac{1}{f}\right)f_s.$$
□

The Ideal–Variety Correspondence

Theorem

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 and

$$\mathrm{Id} = \mathrm{Var}^{-1} .$$

Both maps are inclusion-reversing.

Irreducible Varieties

Definition

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 $V_1, V_2 \in K^n$.

Proposition

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

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

The Algebra–Geometry Dictionary

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

Algorithmic Questions

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

The Ideal Membership Problem in K[X]

Let $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq K[X]$ an ideal and $f \in K[X]$ a polynomial.

- K[X] is an Euclidean domain:

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

  where $g = \gcd(f_1, \ldots, f_s)$.

- Division with remainder: $q, r \in K[X]$ s. t.

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

- Then

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

The Division Algorithm in K[X]

Example

Let $f = 2X^2 + X + 1 \in \mathbb{R}[X]$ and $g = 2X + 1 \in R[X]$.

$$
\begin{array}{r|c}
 & 2X + 1 \\
\hline
2X^2 + X + 1 & X \\
-(2X^2 + X) & \\
\hline
1 &
\end{array}
$$

Therefore,

$$2X^2 + X + 1 = X \cdot (2X + 1) + 1 \quad \text{and} \quad \deg(1) < \deg(2X + 1).$$

Multivariate Polynomials

Identify

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

Definition

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

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

$$\deg(f) = \max\{|\alpha| \mid \alpha \in \mathbb{N}^n \text{ with } a_\alpha \neq 0\}.$$

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.

Monomial Orders

Definition

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

1. $\prec$ is a total order on $\mathbb{N}^n$,
2. $\alpha \prec \beta \implies \alpha + \gamma \prec \beta + \gamma$ for all $\alpha, \beta, \gamma \in \mathbb{N}^n$, and
3. $\prec$ is a well-order.

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

Standard Monomial Orders

Definition

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

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

Example

Consider the monomials $X^3, Y^{100}, XYZ^2, XY^2Z \in K[X, Y, Z]$.

$\succ_{\text{lex}}$	X^3	XY^2Z	XYZ^2	Y^{100}
$\succ_{\text{grlex}}$	Y^{100}	XY^2Z	XYZ^2	X^3
$\succ_{\text{grevlex}}$	Y^{100}	XYZ^2	XY^2Z	X^3

The Multidegree

Definition

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

$$\text{multideg}(f) = \max\{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\}.$$

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,

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

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 $\prec = \prec_{lex}$.

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

Therefore,

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

The Division Algorithm in $K[X_1, \dots, X_n]$

Algorithm

Input: $f, f_1, \dots, f_s \in K[X_1, \dots, X_n] \setminus \{0\}$ and a monomial order $\prec$.

Output: $q_1, \dots, q_s, r \in K[X_1, \dots, X_n]$ such that $f = q_1 f_1 + \cdots + q_s f_s + r$ and no term in r is divisible by any of $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s)$.

1. $p \leftarrow f, \quad r \leftarrow 0, \qquad$ **for** $i = 1, \dots, s$ **do** $q_i \leftarrow 0$
2. **while** $p \neq 0$ **do**
   - **if** $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$ for a minimal $i \in \{1, \dots, s\}$ **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** $q_1, \dots, q_s, r$

Correctness

Proposition

*At each entry to the **while**-loop in the Division Algorithm the following invariants hold:*

1. $f = p + q_1 f_1 + \cdots + q_s f_s + r$ *and* $\mathrm{multideg}(f) \succcurlyeq \mathrm{multideg}(p)$.
2. *No term in* r *is divisible by any of* $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.
3. *If* $q_i f_i \neq 0$ *for some* $i \in \{1, \ldots, s\}$ *then*

$$\mathrm{multideg}(f) \succcurlyeq \mathrm{multideg}(q_i f_i).$$

Definition

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

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

Monomial Ideals

Definition

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

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

Lemma

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*

$$X^\beta \in I \iff \exists \alpha \in A : X^\alpha \mid X^\beta.$$

Dickson's Lemma

Lemma (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*

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

Gröbner Bases

Definition

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

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,

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

The Normal Form

Theorem

Let $I \trianglelefteq K[X_1, \ldots, X_n]$ *be an ideal and let* G *be an 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*

1. $f - r \in I$, *and*
2. *no term of* r *is divisble by any term in* $\mathrm{LT}(G)$.

In particular,

$$r = \overline{f}^{G},$$

and is called the normal form of f *with respect to* G.

Minimal Gröbner Bases

Lemma

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*

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

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

Definition

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

1. $\mathrm{LC}(g) = 1$, and
2. $\mathrm{LT}(g) \notin \langle \mathrm{LT}(G \setminus \{g\}) \rangle$.

Reduced Gröbner Bases

Definition

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 monomial of g is in

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

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

Theorem

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

The Syzygy Polynomial

Definition

Let $f, g \in K[X_1, \dots, X_n] \setminus \{0\}$. Let $\alpha = \mathrm{multideg}(f)$, $\beta = \mathrm{multideg}(g)$ and

$$\gamma = \big(\max\{\alpha_1, \beta_1\}, \dots, \max\{\alpha_n, \beta_n\}\big).$$

Then the *S-polynomial* of f and g is

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

Buchberger's Criterion

Theorem (Buchberger 1965)

A finite set $G \subseteq K[X_1, \ldots, X_n]$ *is a Gröbner basis for the ideal* $\langle G \rangle$ *if and only if*

$$\overline{S(p,q)}^{G} = 0 \qquad \text{for all } p \neq q \in G.$$

Buchberger's Algorithm

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**
   - $\mathcal{S} \leftarrow \varnothing$
   - **for each** $\{p, q\} \subseteq G$ with $p \neq q$ **do**
     - $r \leftarrow \overline{S(p, q)}^G$
     - **if** $r \neq 0$ **then** $\mathcal{S} \leftarrow \mathcal{S} \cup \{r\}$
   - $G \leftarrow G \cup \mathcal{S}$

   until $\mathcal{S} = \varnothing$
3. **return** G

The Ideal Membership Problem

Proposition

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*

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

The Consistency Problem

Proposition

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

$$1 \in I \iff G = \{1\}.$$

The Radical Membership Problem

Proposition

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

$$f \in \sqrt{I} \iff 1 \in J.$$

The Elimination Theorem

Definition

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

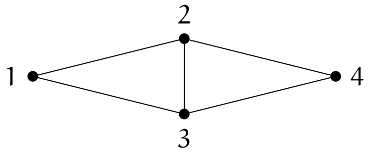
Let $I \trianglelefteq K[X_1, \ldots, X_n]$ *be an ideal and let* G *be a Gröbner basis for* I *with respect to* $\prec_{lex}$. *Then*

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

is a Gröbner basis for I_ℓ.

3-Colouring Revisited

$G = (V, E)$.



Let

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

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

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

Therefore

$$\left(1, e^{2/3\pi i}, e^{4/3\pi i}, 1\right) \in \mathrm{Var}(I).$$

Intersection of Ideals

Theorem

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

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

Decision Problems

Definition

1. The *ideal membership problem* is defined by

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

2. The *consistency problem* is defined by

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

3. The *radical membership problem* is defined by

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

A Degree Bound for Ideal Membership

Theorem (Hermann 1926)

Let $I = \langle f_1, \dots, f_s \rangle \trianglelefteq \mathbb{Q}[X_1, \dots, X_n]$ *be an ideal and let*

$$d = \max\{\deg(f_1), \dots, \deg(f_s)\}.$$

If $f \in I$ *then there are* $q_1, \dots, q_s \in \mathbb{Q}[X_1, \dots, X_n]$ *such that*

$$f = q_1 f_1 + \cdots + q_s f_s$$

and

$$\deg(q_i) \leqslant \deg(f) + (sd)^{2^n} \qquad \text{for all } i = 1, \dots, s.$$

Effective Nullstellensätze

Theorem (Brownawell 1987)

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

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

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

2. *If* $f \in \mathbb{Q}[X_1, \dots, X_n]$ *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* $q_1, \dots, q_s \in \mathbb{Q}[X_1, \dots, X_n]$ *with* $f^e = q_1 f_1 + \cdots + q_s f_s$ *such that*

$$e \leqslant (\mu + 1)(n + 2)(d + 1)^{\mu+1} \qquad \text{and}$$
$$\deg(q_i) \leqslant (\mu + 1)(n + 2)(d + 1)^{\mu+2} \qquad \text{for } i = 1, \dots, s.$$

A Degree Bound for Gröbner Bases

Theorem (Dubé 1990)

Let $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq K[X_1, \ldots, X_n]$ *be an ideal and let*

$$d = \max\{\deg(f_1), \ldots, \deg(f_s)\}.$$

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

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

Upper Bounds

Theorem (Mayr 1989)

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

Corollary

$$\textsc{Cons} \in \mathbf{PSPACE} \qquad \textit{and} \qquad \mathrm{RM} \in \mathbf{PSPACE}.$$

The Mayr–Meyer Construction

For $n \in \mathbb{N}$ define $e_n = 2^{2^n}$. Then

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

Variables:

S	start
F	finish
$B_1, \ldots, B_4$	counters
$C_1, \ldots, C_4$	catalysts

for each level $r = 0, \ldots, n$.

Generators

Level $r = 0$:

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

Level $r > 0$:

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

where $s, f, b_1, \ldots, b_4, c_1, \ldots, c_4$ are variables of level $r - 1$.

An Exponential Space Lower Bound

Theorem (Mayr & Meyer 1982)

IM *is* **EXPSPACE**-*hard.*

For further reading:

- Ernst W. Mayr and Albert R. Meyer:
  The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals.
  Advances in Mathematics **46**, 305-329, 1982.
- David Cox, John Little and Donal O'Shea:
  Ideals, Varieties, and Algorithms.
  Springer-Verlag, New York, 2^{nd} edition, 1997.
- Joachim von zur Gathen and Jürgen Gerhard:
  Modern Computer Algebra.
  University Press, Cambridge, 2^{nd} edition, 2003.