Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today we will start to solve the membership problem.

1. Monomials and monomial orders
2. Finite generation of monomial ideals
3. Division with remainder
4. Gröbner basis and Hilbert's basis theorem

Monomials

Definition. A **monomial** in $K[x_1, \ldots, x_n]$ is an element of the form

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$$

where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n = \mathbb{Z}^n_{\geq 0}$ is a multi-exponent. Thus

$$x^\alpha x^\beta = x^{\alpha+\beta}.$$

A **term** in $K[x_1, \ldots, x_n]$ is an element of the form

$$ax^\alpha$$

with $a \in K$. Every element $f \in K[x_1, \ldots, x_n]$ is a finite sum of terms

$$f = \sum f_\alpha x^\alpha$$

where all but finitely many coefficients f_α are zero.

A motivating example

Consider the ideal

$$I = (x^2 + xy, y^2 + xy) \subset K[x, y]$$

in a polynomial ring in two variables. Using division with remainder we can use $x^2 + xy$ to remove from an $f \in K[x, y]$ any multiple of x^2:

$$f = q(x^2 + xy) + r \text{ with } r \in K[x] + yK[x].$$

Likewise, we can use $y^2 + xy$ to remove multiples of y^2. Can we use both to remove multiples of x^2 or y^2 simultaneously?

A motivating example 2

Consider the ideal

$$I = (x^2 + xy, y^2 + xy) \subset K[x, y]$$

Can we use both generators to remove multiples of x^2 or y^2 simultaneously?

Answer: No!

If yes, then $\overline{1}, \overline{x}, \overline{y}, \overline{xy}$ would generate $K[x, y]/I$ as a K-vektor space. But this is an infinite dimensional K-vector space:

$$K[x, y]/I \twoheadrightarrow K[x, y]/(x + y) \cong K[y].$$

What went wrong?

We did not choose the leading terms x^2 and y^2 in a compatible way!

Monomial orders

Definition. A **monomial order** $>$ on $K[x_1, \ldots, x_n] >$ is a complete order of the monomials in $K[x_1, \ldots, x_n]$ satisfying

$$x^\alpha > x^\beta \implies x^\alpha x^\gamma > x^\beta x^\gamma$$

for any triple of monomials. For $f = \sum f_\alpha x^\alpha$ we define the **lead term** with respect to $>$ as

$$\mathrm{Lt}(f) = f_\alpha x^\alpha \text{ where } x^\alpha = \max\{x^\beta \mid f_\beta \neq 0\} \text{ and } \mathrm{Lt}(0) = 0.$$

Example. $\mathrm{Lt}(x^2 + xy) = x^2 \implies x^2 > xy \implies x > y \implies xy > y^2 \implies \mathrm{Lt}(y^2 + xy) = xy$. So our choice above was not compatible with a monomial order.

part 1

Computation rules

Abusing notation we write for non-zero terms

$$ax^\alpha \geq bx^\beta \text{ if } x^\alpha \geq x^\beta \quad (:\Leftrightarrow x^\alpha > x^\beta \text{ or } x^\alpha = x^\beta.)$$

Note that $\geq$ is not an order on the set of non-zero terms since

$$ax^\alpha \geq bx^\beta \text{ and } bx^\beta \geq ax^\alpha \implies x^\alpha = x^\beta$$

but $a \neq b$ is possible.

Proposition. Let $>$ be a monomial order. Then

1. $\operatorname{Lt}(fg) = \operatorname{Lt}(f)\operatorname{Lt}(g)$,
2. $\operatorname{Lt}(f+g) \leq \max(\operatorname{Lt}(f), \operatorname{Lt}(g))$
   and equality holds unless $\operatorname{Lt}(f) + \operatorname{Lt}(g) = 0$.

Global monomial orders

Definition. A **global** monomial order on $K[x_1, \ldots, x_n]$ is a monomial order satisfying

$$x_j > 1 \text{ for } j = 1, \ldots n.$$

In contrast, a **local** monomial order on $K[x_1, \ldots, x_n]$ is a monomial order satisfying

$$x_j < 1 \text{ for } j = 1, \ldots n.$$

The key property of global monomial orders is that there are **no** infinite descending sequences $m_1 > m_2 > \ldots$ of monomials.

In contrast, for a local monomial order

$$1 > x_1 > x_1^2 > \ldots > x_1^k > \ldots$$

is an infinite descending sequence.
Local orders are useful for computations in powerserie rings $K[[x_1, \ldots, x_n]]$. We will consider those only later in the course.

Examples of global monomial orders

1) The **lexicographic** monomial order is defined by

$$x^\alpha >_{\mathrm{lex}} x^\beta$$

if the first non-zero entry of $\alpha - \beta \in \mathbb{Z}^n$ is positive. Thus

$$x_1 x_3 >_{\mathrm{lex}} x_1 >_{\mathrm{lex}} x_2^k >_{\mathrm{lex}} x_2^2.$$

2) The **reversed lexicographic** order is defined as follows:

$$x^\alpha >_{\mathrm{rlex}} x^\beta$$

if $\deg x^\alpha > \deg x^\beta$ or $\deg x^\alpha = \deg x^\beta$ and the last non-zero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative. Thus

$$x_3^3 >_{\mathrm{rlex}} x_1^2 >_{\mathrm{rlex}} x_2^2 >_{\mathrm{rlex}} x_1 x_3.$$

Degree of a polynomial

Definition. For a monomial x^α the **degree** is defined by

$$\deg x^\alpha = \sum_{j=1}^{n} \alpha_j = |\alpha|.$$

For a non-zero polynomial $f = \sum f_\alpha x^\alpha$ the degee is

$$\deg f = \max\{\deg x^\alpha \mid f_\alpha \neq 0\}$$

3) **Weight orders**. Let $w = (w_1, \ldots, w_n) \in \mathbb{R}^n_{>0}$ be a weight vector and $w(\alpha) = \sum_{j=1}^{n} w_j \alpha_j$. We define

$$x^\alpha >_w x^\beta \text{ if } w(\alpha) > w(\beta) \text{ or } w(\alpha) = w(\beta) \text{ and } x^\alpha >_{\mathrm{tb}} x^\beta$$

where $>_{\mathrm{tb}}$ denotes a tiebreak order, for example $>_{\mathrm{lex}}$. If the weights w_j are $\mathbb{Q}$-linearly independent, then $>_{\mathrm{tb}}$ is superfluous.

Monomial ideals and Dixon's Lemma

Definition. Let J be an arbitrary set of polynomials. The ideal generated by J is

$$I = (J) = \{f \mid \exists r \in \mathbb{N}, f_1, \ldots, j_r \in J \text{ and } g_1, \ldots, g_r \in K[x_1, \ldots, x_n] \\ \text{such that } f = g_1 f_1 + \ldots + g_r f_r \quad \}$$

Definition. A monomial ideal $I \subset K[x_1, \ldots, x_n]$ is an ideal satisfying

$$f = \sum f_\alpha x^\alpha \in I \implies x^\alpha \in I \; \forall \alpha \text{ with } f_\alpha \neq 0$$

In other words I is generated by monomials.

Lemma[Hilbert's basis theorem for monomial ideals]. *Every monomial ideal I is finitely generated,*
i.e. there exists a finite set J of monomials such that $I = (J)$.

Proof of Dixon's Lemma.

Induction on n. Let $I \subset K[x_1, \ldots, x_n]$ be a non-zero monomial ideal, $x^\alpha \in I$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$.
For $j = 1, \ldots, n$ and $\gamma = 0, \ldots, \alpha_j - 1$ consider the monomial ideal $I_{j,\gamma}$ generated

$$\{x^\beta \subset K[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n] | x_j^\gamma x^\beta \in I\}$$

in a polynomial ring with $n - 1$ variables.
By induction hypothesis all $I_{j,\gamma}$ is finitely generated, say by a set of monomials $J_{j,\gamma}$. Then

$$J = \{x^\alpha\} \cup \bigcup_{j,\gamma} \{x_j^\gamma x^\beta \mid x^\beta \in J_{j,\gamma}\}$$

is a finite set of generators of I. $\square$

The descending chain condition

Proposition. *Let* $>$ *be a global monomial order and* $m_1 \geq m_2 \geq \ldots \geq m_k \geq \ldots$ *a descending chain of monomials. Then there exists* $N \in \mathbb{N}$ *such that*

$$m_k = m_{k+1} \, \forall k \geq N.$$

Proof. A global monomial order $>$ refines divisibility in $K[x_1, \ldots, x_n]$:

$$x^\alpha | x^\beta \iff \beta - \alpha \in \mathbb{Z}^n_{\geq 0} \implies x^{\beta-\alpha} > 1 \implies x^\beta > x^\alpha.$$

Consider the ideal $I = (\{m_k \mid k \in \mathbb{N}\})$. By Dixon's Lemma, I is generated by a finite set J of monomials. Set $N = \max\{\ell \mid m_\ell \in J\}$. For $k \geq N$ every monomial m_{k+1} is divisible by a generator $m_\ell \in J$. Thus we have $m_{k+1} \geq m_\ell \geq m_N \geq m_{k+1}$ and equality holds: $m_{k+1} = m_N$. □

Division with remainder

Theorem. *Let $>$ be a global monomial order on $K[x_1, \ldots, x_n]$, $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ non-zero polynomials. For every $f \in K[x_1, \ldots, x_n]$ there exist uniquely determined $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ and a unique remainder $h \in K[x_1, \ldots, x_n]$ satisfying*

1) $f = g_1 f_1 + \ldots + g_r f_r + h$
2a) *No term of $g_j \operatorname{Lt}(f_j)$ is divisible by a lead term $\operatorname{Lt}(f_i)$ for some $i < j$.*
2b) *No term of h is divisible by a lead term $\operatorname{Lt}(f_j)$.*

Proof of the Division with Theorem

Uniqueness: Taking difference it suffices that

$$0 = g_1 f_1 + \ldots + g_r f_r + h \Rightarrow g_1 = 0, \ldots g_r = 0, h = 0.$$

Since the non-zero lead terms $\mathrm{Lt}(g_j f_j) = \mathrm{Lt}(g_j)\,\mathrm{Lt}(f_j)$ and $\mathrm{Lt}(h)$ belong to different monomials by condition 2), they cannot cancel in the sum. So all are zero, hence all g_j and h are zero.

Existence: The theorem is trivially true for monomial ideals. Thus we can write

$$f = g_1^{(0)}\,\mathrm{Lt}(f_1) + \ldots + g_r^{(0)}\,\mathrm{Lt}(f_r) + h^{(0)}$$

satisfying 2a) and 2b). Consider

$$f^{(1)} = f - (g_1^{(0)} f_1 + \ldots + g_r^{(0)} f_r + h^{(0)}).$$

In the difference on the right hand side, the lead term cancels. Hence either $f^{(1)} = 0$ and we are done, or

$$\mathrm{Lt}(f^{(1)}) < \mathrm{Lt}(f).$$

Proof of the Division with Theorem 2

Continuing with $f^{(1)}$ we obtain a sequences of polynomials

$$f^{(k+1)} = f^{(k)} - (g_1^{(k)} f_1 + \ldots + g_r^{(k)} f_r + h^{(k)})$$

where

$$f^{(k)} = g_1^{(k)} \operatorname{Lt}(f_1) + \ldots + g_r^{(k)} \operatorname{Lt}(f_r) + h^{(k)}$$

whose lead terms form a descending sequence

$$\operatorname{Lt}(f) > \operatorname{Lt}(f^{(1)}) > \operatorname{Lt}(f^{(2)}) > \ldots.$$

So after a finite number of steps we arrive at $f^{(N+1)} = 0$, and

$$\text{the } g_j = \sum_{k=0}^{N} g_j^{(k)} \text{ and } h = \sum_{k=0}^{N} h^{(k)}$$

are the desired coefficients and remainder.

Gröbner basis and Hilbert's basis theorem

Definition. Let $>$ be a global monomial order and $I \subset K[x_1, \ldots, x_n]$ an ideal. The **lead term ideal** of I is the ideal generated by the lead terms of elements of I:

$$\mathrm{Lt}(I) = (\{\mathrm{Lt}(f) \mid f \in I\}).$$

Elements $f_1, \ldots, f_r \in I$ are a **Gröbner basis** of I (with respect to $>$) if

$$\mathrm{Lt}(I) = (\mathrm{Lt}(f_1), \ldots, \mathrm{Lt}(f_r)).$$

Theorm (Hilbert, 1899). *Every ideal in $K[x_1, \ldots, x_n]$ is finitely generated.*

Gordon's proof of Hilbert's basis theorem

Let $I \subset K[x_1, \ldots, x_n]$ be an ideal. Consider the lead term ideal $\mathrm{Lt}(I)$. This is a monomial ideal, hence it is finitely generated by Dixon's Lemma.

Let $f_1, \ldots, f_r \in I$ be elements whose lead terms generate $\mathrm{Lt}(I)$. We claim

$$I = (f_1, \ldots, f_r).$$

$(f_1, \ldots, f_r) \subset I$ is clear since $f_1, \ldots, f_r \in I$. For the other inclusion,

let $f \in I$ be an arbitrary element. Consider the remainder h of f divided by $f_1, \ldots, f_r$,

$$h = f - (g_1 f_1 + \ldots + g_r f_r).$$

Then on one hand we have $h \in I$ and on the other hand no non-zero term of h lies in $\mathrm{Lt}(I) = (\mathrm{Lt}(f_1), \ldots, \mathrm{Lt}(f_r))$ by condition 2b). Thus $\mathrm{Lt}(h) = 0$. Hence $h = 0$ and $f \in (f_1, \ldots, f_r)$. $\square$