Gröbner bases, commutative case

Consider $k[x_1,\dots,x_n] \supseteq I$ with I an ideal.

Goal: write elements in $k[X]/I$ as polynomials.

Let M be the set of monomials in $k[X]$, then

Def: A monomial order on M such that

a) $1 \leq m \quad \forall\, m \in M$

b) $m_1 \leq m_2$ then $m_1 m_3 \leq m_2 m_3 \quad \forall\, m_1, m_2, m_3 \in M$

Now fix a monomial order on M.

Def: We call the largest monomial among the monomials of a polynomial

$$f = \sum_{i=0}^{s} c_i m_i \quad \text{so} \quad \underbrace{\text{init}(f)}_{\text{initial ideal}} = \bigwedge_{i=0}^{s} m_i$$

Def: . the initial ideal of I is $\text{init}(I) = \langle \text{init}(f) \mid f \in I \rangle$

. A monomial m is called non-standard if $m \in \text{init}(I)$,

o/w it's called standard. (notion is dependent on I)

. A subset $G \subset I$ is called a Gröbner basis if

$$\langle \text{init}(g),\ g \in G \rangle = \text{init}(I)$$

A Gröbner basis is called reduced if

$\forall g_1, g_2 \in G$, $g_1 \neq g_2$, $\operatorname{init}(g_1) \nmid m$ for m a monomial of g_2.

<u>Lemma:</u> Each monomial ideal is finitely generated by monomials.

<u>proof:</u> Define $I_i := \langle m \in M \cap k[x_1, \dots, x_{n-1}] \mid m x_n^i \in I \}$

$I_0 \subset \dots$ chain of inclusion.

we get $\bigcup_{i \geq 0} I_i$ is finitely generated by monomials so

$\bigcup_{i \geq 0} = I_r$ for some r.

So for generators of I we take $m_{ij} x_n^i$ where

$I_i = \langle m_{ij} \mid j \in S \rangle$ and $i = 0, \dots, r$ $\blacksquare$

<u>Cor:</u> Monomial orders are well orders.

<u>Lemma:</u> Every Gröbner basis generates its ideal

<u>Proof:</u> Let $G \subset I$ a Gröbner basis then $\langle G \rangle = I$?

Ass $I \setminus \langle G \rangle \neq \emptyset$ so

$\operatorname{init}(f_0) := \min \{ \operatorname{init}(f) \mid f \in I \setminus \langle G \rangle \}$ exists.

we have $\mathrm{init}(f_0) \in \mathrm{init}(f) = \mathrm{init}(G)$

but then we can construct $f_0 - mg \in I \setminus \{G\}$ with

$\mathrm{init}(f_0 - mg) < \mathrm{init}(f_0)$

$\lightning$

$\blacksquare$

Cor: Hilbert basis theorem

Thm: Standard monomials form a basis for $k[X]/I$

Given a poly P, determine if it has non standard monomials

- if it doesn't we're done and return P.
- if it does, let h be the largest non-standard monomial and find $g \in G$ s.t. $\mathrm{init}(g) \mid h$, say $h = m \cdot \mathrm{init}(g)$

return standard form of $P - mg$

This terminates with a unique result by well-orderedness. $\blacksquare$

$$\left.\begin{aligned} f &= c\,\mathrm{init}(f) + r \\ g &= d\,\mathrm{init}(g) + s \end{aligned}\right\} \Rightarrow m = \mathrm{lcm}(\mathrm{init}(f), \mathrm{init}(g))$$

And we define $S(f,g) = m\left(f(c \cdot \mathrm{init}(f))^{-1} - g(d \cdot \mathrm{init}(g))\right)^{-1}$

Lemma: A generating set $G \subseteq I$ is a Gröbmer basis iff

$\forall g_1, g_2 \in G$ with $g_1 \neq g_2$: $S(g_1, g_2) \in G$.

Buchberger algo. to construct a Gröbmer basis

Take $I = \langle f_1, \dots, f_t \rangle$

Set $G_0 = \{f_1, \dots, f_t\}$

$$G_i = G_{i-1} \cup \left\{ S(g_1, g_2) \;\middle|\; \begin{array}{l} g_1, g_2 \in G_{i-1} \text{ distinct} \\ S(g_1, g_2) \notin G_{i-1} \end{array} \right\}$$

Non commutative Gröbmer bases (associative algebras)

Take $Q = (Q_0, Q_1, s, t)$.

$P = \{$ paths in Q will be our basis.

Let V be a v.s. and assume it has a preferred basis B

that is well ordered.

we define $\leq$ on $\mathrm{Fin}(B)$ by

$\phi \leq F \in \mathrm{Fin}(B)$ for A_1, A_2 non empty

$$A_1 \leq A_2 \iff (A_1 = \phi) \text{ or } (\wedge A_1 \leq \wedge A_2) \text{ or } (\wedge A_1 = \wedge A_2 \text{ and } A \setminus \wedge A \leq A \setminus \wedge A)$$

it has the property that if you replace an element of $A \in \mathrm{Fin}(B)$ with only small elements (fin. many) then the result is smaller than A.

This order induces a well order on V via

$$\mathrm{supp}: v = \sum \lambda_\beta \beta \longmapsto \{\beta \mid \lambda_\beta \neq 0\}$$

<u>observation</u>: if $v, w \in V$ & $\wedge \mathrm{supp}(w) \in \mathrm{supp}\, v$

then $\exists! \, \lambda \in k^* \mid v - \lambda w < v$ (strict reduction)

$(\iff \wedge \mathrm{supp}(w) \notin \mathrm{supp}(v - \lambda w))$

<u>Def</u> Take $W \subset V$.

$$B_W = \{\beta \in B \mid \wedge \mathrm{supp}(w) \neq \beta \ \forall v \in W\}$$

$= B \setminus \{\wedge \mathrm{supp}$

<u>Lemma:</u> $V = W + \langle B_W \rangle$

<u>proof:</u> $W \cap \langle B_W \rangle = \{0\}$.

To see $W + \langle B_W \rangle = V$. we assume $V \setminus (W + \langle B_W \rangle) \neq \phi$ so

$\exists$ a minimal element u in $V \setminus (W + \langle B_W \rangle)$

We can find a basis in $\mathrm{supp}(u)$ s.t. $\beta = \wedge \mathrm{supp}(w)$. for some $w \in W$.

Then $u - \lambda w < u$ for a suitable λ so $u - \lambda w \in W + \langle B_W \rangle$

$$\rightsquigarrow \begin{tikzcd} 0 \arrow[r] & W \arrow[r] & V \cong W \oplus B_W \arrow[r, "\pi"'] & V/W \cong \langle B_W \rangle \arrow[r] \arrow[l, bend right, "b"'] & 0 \end{tikzcd}$$

Then call $b\pi(v)$ the normal form of v.

<u>Def:</u> A Gröbner generating set for $W \subseteq V$ is a subset $G \subseteq W$ s.t.

$\forall w \in W, \exists g \in G \quad \wedge \mathrm{supp}(w) = \wedge \mathrm{supp}(g)$.

<u>Lemma</u> If G is a Gröbner generating set for W, then every

$v \in V$ reduces to its normal form over G.

<u>Proof:</u> If v not in its normal form, then it can be reduced and $\exists$

finitely many strict reductions.

Cor: If G is a Gröbner generating set for W, then it spans W.

Def: A vector $w \in W$ is called sharp if

$$\operatorname{supp}(w) \cap \{\wedge \operatorname{supp}(u) \mid u \in W\} = \wedge \operatorname{supp}(w).$$

and the coefficients of $\wedge \operatorname{supp}(w)$ is 1.

The set of sharp elements in W will be denoted $W^{\#}$ (

Thm: $W^{\#}$ is a Gröbner generating set for W s.t. no two distinct members reduce over one another.

Proof: $V = kQ$, $B = P = \{\text{paths in } Q\}$

$\exists$ 3 structures we can exploit.

- kQ has an algebraic structure
- P " a well order descending to $\operatorname{Fin}(P)$.
- kQ can be partially ordered by divisibility which respects the previous order.

·The paper emphasises the following properties.

M_1 $P \cup \{0\}$ is closed under multiplication.

M_2 divisibility is reflexive

M_3 each p has finitely many factors.

M_4 Multiplication respects the order on $\mathcal{P}$.

M_5 The order on $\mathcal{P}$ refines the one coming from divisibility.

take $I \subset kQ$ admissible.

Def: A subset $G \subseteq I$ is a Gröbner basis when

$\forall r \in I \setminus \{0\}\ \exists g \in G : \wedge\mathrm{Supp}(g) \mid \wedge\mathrm{Supp}(r)$

Def: A simple reduction of an element $c \in kQ$ is a tuple

$\rho = (\lambda, p, d, q) \in k^* \times \mathcal{P} \times (kQ \setminus \{0\}) \times \mathcal{P}$ s.t.

$p(\wedge\mathrm{supp}(d))q \in \mathrm{supp}(c)$

$p(\wedge\mathrm{supp}(d))q \notin \mathrm{supp}(c - \lambda pdq)$

so $c - \lambda pdq < c$

A sequence of simple reductions $(\rho)_{i=0}^{t}$ is called a reduction

If $\forall i$, $d_i \in$ some set S, call it a reduction over S.

Th: If G is a Gröbner basis for I then

every $c \in kQ$ reduces to its normal form mod I over G.

Proof: Same as for vector spaces. $\blacksquare$

Rem: $a|b$ means $\exists c,d$ s.t. $b = cad$

Def: Vectors in $I^\#$ that are minimal w.r.t. divisibility are called minimal sharp and the minimal sharp elements in I are denoted $\text{atom}(I^\#)$.

Th: $\text{atom}(I^\#)$ is a Gröbner basis s.t. no two $\neq$ members reduce over each other

Proof. take $r_1 \in I$, consider $\min\{r_2 \in I \mid \wedge\,\text{supp}(r_2) \mid \wedge\,\text{supp}(r_1)\} := r_m$ w.r.t. divisibility, then we can scale r_m to be minimal sharp.

Pairwise non-reducibility follows from minimality.

$\blacksquare$

Lemma: Let R be a set of relations in kQ and $c \in kQ$ further relation reducing to 0 over R.

Then pcq reduces to 0 over R for $p,q \in \mathcal{P}$

Proof: Take a simple reduction of c

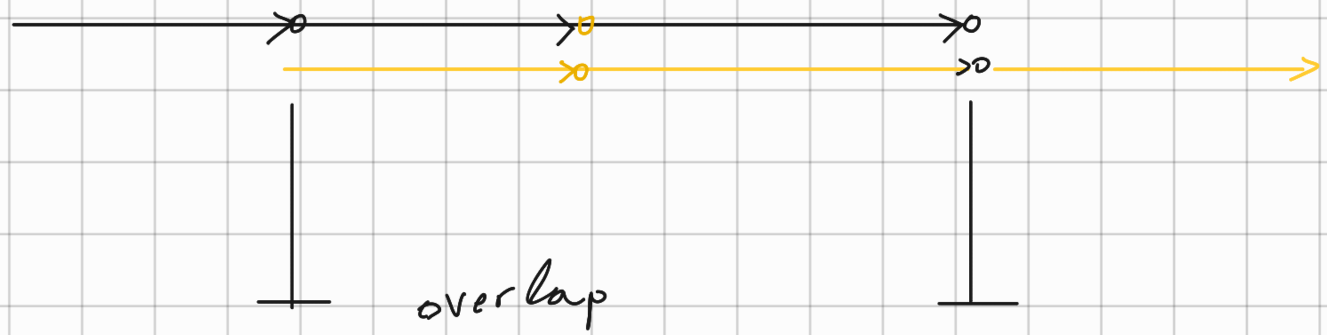
$c - \lambda\, p_1 c_1 q_1$, then you get a reduction of pcq as

$pcq - \lambda_1 p p_1 \lambda q_1 q$ and the statement follows iteratively.

∎

Th: Let G be a set of generators of I such that

- the coeffs of each $\wedge \operatorname{Supp}(g)$ is 1 $(g \in G)$.
- $\forall g_1, g_2 \in G$, $g_1 \neq g_2 \Rightarrow$ they don't reduce over each other.
- $\forall g_1, g_2 \in G$, every overlap difference reduces to 0 over G.



Then $G = \operatorname{atom}(I^{\#})$.

Def: For two monomials, an overlap difference is a pair of factorisations

$$p = bo \qquad\qquad b, a, o \in P$$

$$q = oa \qquad\qquad p \neq b, \; q \neq a.$$

$c_1, c_2 \in kQ$ overlap if $\wedge \operatorname{Supp}(c_1)$ and $\wedge \operatorname{Supp}(c_2)$ do, say like

$\wedge \operatorname{Supp}(c_1) = bo$ | and respective coeffs of $\wedge \operatorname{Supp}(c_1)$ and $\wedge \operatorname{Supp}(c_2)$

$\wedge \operatorname{Supp}(c_2) = a_o$ | are λ_1 and λ_2

then an overlap difference of c_1 and c_2 is

$$\lambda_2 c_1 a - \lambda_1 b c_2.$$