Gröbner Basis

Every ideal has many generating sets

$$F = \{x^6-1,\ x^{10}-1,\ x^{15}-1\}$$

generate $I = \langle x-1 \rangle$

$$x-1 = \gcd(x^6-1, x^{10}-1, x^{15}-1)$$

is computed with the Euclidian Algorithm

Using the extended Euclidean Alg.

$$x^5(x^6-1) - (x^5+x)(x^{10}-1) + 1\cdot(x^{15}-1) = x-1$$

$$\Rightarrow \quad x-1 \in \langle F \rangle$$

we can show $\langle F \rangle \subseteq \langle x-1 \rangle$ by factoring

When $n \geq 2$ ideal membership is more difficult

n = # variables in $k[x_1, \dots, x_n]$

$x=1$ is the only solution

to $x^6-1 = x^{10}-1 = x^{15}-1 = 0$.

Gaussian Elimination gives a method to study ideals gen. by linear poly.

Ex) Work $\mathbb{Q}[x,y,z]$

$$\langle 2x+3y+5z+7,\ 11x+13y+17z+19,\ 23x+29y+31z+37 \rangle$$

$$= \langle 7x-16,\ 7y+12,\ 7z+9 \rangle$$

This system has one solution $\left(\frac{16}{7}, \frac{-12}{7}, \frac{-9}{7}\right)$

Informally G. B. (Gröbner basis) generalizes these

Monomials

Identify set $\mathbb{N}^n$ = non negative integer vectors with the monomial basis of $K[x_1,\dots,x_n]$

Coordinate wise partial order on $\mathbb{N}^n$

$a = (a_1,\dots,a_n) \le b$ iff $a_i \le b_i \ \forall i$

$$\Updownarrow$$

$x^a \le x^b$ iff $x^a \mid x^b$

$x^a = x_1^{a_1} \cdots x_n^{a_n}$

Def] An ideal $I \subseteq K[x_1,\dots,x_n]$ is a monomial ideal if $\exists$ a subset $A \subseteq \mathbb{N}^n$ s.t.

$$I = \langle x^\alpha \mid \alpha \in A \rangle$$

E.g. $I = \langle x^4y^2, x^3y^4 \rangle$

Lemma*] Let $I = \langle x^\alpha \mid \alpha \in A \rangle$ be a monomial ideal. Then $x^\beta \in I$ iff $x^\alpha \mid x^\beta$ for some $\alpha \in A$.

Proof:

$\Leftarrow$ If $x^\alpha \mid x^\beta \Rightarrow x^\beta = h_\alpha x^\alpha \Rightarrow x^\beta \in I$.

$\Rightarrow$ If $x^\beta \in I \Rightarrow x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$

$$= \sum_{i=1}^{s} \left(\sum_j c_{ij} x^{\gamma(i,j)} \right) x^{\alpha(i)}$$

$$= \sum_{i,j} c_{ij} x^{\gamma(i,j) + \alpha(i)}$$

$\Rightarrow$ every term is divisable by some minimal $\alpha(i)$

Alt. x^β is a monomial $\therefore$ RHS must have only the exponents s.t. $\beta = \gamma(i,j) + \alpha(i)$

$$\Rightarrow \quad x^{\alpha(i)} \mid x^\beta .$$

$\blacksquare$

Lemma Let I be a monomial ideal, $f \in k[x_1, \dots, x_n]$

The the following are equivalent

i) $f \in I$

ii) Every term of f is in I

iii) f is a k-linear combo of monomial in I

Proof Excise

Corollary Two monomials ideals are the same iff they contain the same monomials

Thm (Dickson's Lemma). Let $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq k[x_1, \dots, x_n]$ be a monomial ideal. Then I can be written as

$$I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle \quad \text{where } \alpha(1), \dots, \alpha(s) \in A.$$

Proof By induction on $n =$ # of variables

$n = 1$, take β to be the smallest integer in A

$$\Rightarrow \quad x_1^\beta \mid x_1^\alpha \quad \forall \alpha \in A \Rightarrow I = \langle x_1^\beta \rangle$$

Assume $n > 1$, Dickson's holds for $n-1$

relabel $k[x_1, \dots, x_{n-1}, \underset{}{\overset{=y}{x_n}}] = k[x_1, \dots, x_{n-1}, y]$

Let $J \subseteq k[x_1,\dots,x_{n-1}]$ be generated by monomials

$$x^\alpha = x_1^{\alpha_1}\cdots x_{n-1}^{\alpha_{n-1}} \in k[x_1,\dots,x_{n-1}] \quad \text{s.t}$$

$$x^\alpha y^m \in I \quad \text{for some } m \geq 0.$$

Since J is a monomial ideal by induction

$$J = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$$

For each $i = 1,\dots,s$ $\quad x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$

Let $m = \max\{m_i \mid i = 1,\dots,s\}$

For $l = 0,\dots,m-1$ let

$$J_l = \langle x^\beta \mid x^\beta y^l \in I \rangle \subseteq k[x_1,\dots,x_{n-1}]$$

By ind.

$$J_l = \langle x^{\alpha_l(1)}, \dots, x^{\alpha_l(s_l)} \rangle$$

Claim: I is generated by the following monomials

$$\left.x^{\alpha(1)}y^m, \dots, x^{\alpha(s)}y^m\right\} \text{ from } J$$

$$\left.x^{\alpha_0(1)}, \dots, x^{\alpha_0(s_0)}\right\} \text{ from } J_0$$

$$\vdots$$

$$\left.x^{\alpha_{m-1}(1)}y^{m-1}, \dots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}\right\} \text{ from } J_{m-1}$$

Proof of claim |

Note every monomial in I is divisible by a listed monomial

Since:

$$\text{If } x^\alpha y^p \in I,\ p \geq m \Rightarrow x^{\alpha(i)} y^m \mid x^\alpha y^p$$

if $p \le m-1$ $\Rightarrow$ $x^{\alpha_p(i)} y^p \mid x^\alpha y^p$

By induction / construction of J_p

$\therefore$ By lemma + corollary

$\Rightarrow$ I is generated by monomials in the list.

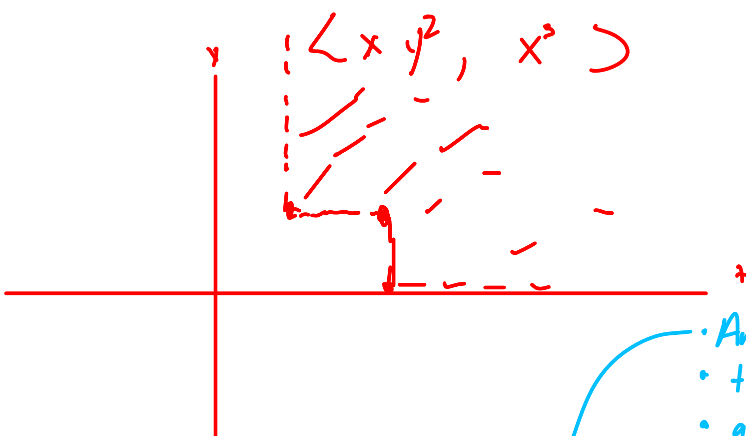
$\therefore$ finitely generated

know $I = \langle x^\alpha \mid \alpha \in A \rangle$ and $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)} \rangle$ for some $x^{\beta(i)} \in I$

by Lemma # $\exists\ \alpha(i) \in A$

s.t. $x^{\alpha(i)} \mid x^{\beta(i)}$ $\forall i$

$\therefore$ $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. ∎



$a \le b$ and $b \le a$ $\Rightarrow a = b$

- Anti-symmetric
- transitive $a \le b$, $b \le c$ $\Rightarrow a \le c$
- $a \le b$ or $b \le a$

Def (Monomial Order) Consider a total ordering $<$ of the set $\mathbb{N}^n$. Write $a \le b$ if $a < b$ or $a = b$.

The ordering $<$ is a monomial order if $\forall a, b, c \in \mathbb{N}^n$

- $(0, \dots, 0) \le a$
- $a \le b \Rightarrow a + c \le b + c$

Common monomial orders are:

- Lexographic (Lex) ordering:

  $a <_{lex} b$ if left most non-zero entry of $b-a$ is positive

  i.e. $b-a = (\underset{=0}{b_1-a_1}, \ldots, \underset{=0}{\ldots}, \underset{\neq 0}{b_\ell - a_\ell}, \ldots, b_n-a_n)$, $b_\ell - a_\ell > 0$ $\Rightarrow a <_{lex} b$

- Degree Lexographic Order OR Graded Lex Order (GLex, Dlex, Deglex)

  $a <_{deglex} b$ if either $\underbrace{|a| = a_1 + \cdots + a_n}_{\deg(x^a)} < |b| = b_1 + \cdots + b_n$

  or $|a| = |b|$ and the left most non zero entry of $b-a$ is positive

- Degree Reverse Lexographic order (drevlex) OR Graded Reverse Lex order (Grevlex)

  $a <_{grevlex} b$ if either $|a| < |b|$

  or the right most non-zero entry of $b-a$ is negative

Note $x_1 > x_2 > \cdots > x_n$ in all orders.

Fix a monomial order $<$

Def Given $f \in k[x_1, \ldots, x_n]$ its initial monomial $in_<(f)$ (leading monomial $LM_<(f)$) is the $<$-largest monomial x^a appearing in f

Ex] $f = x^2 + xz^2 + y^3$ with $x>y>z$

then $in_{<lex}(f) = x^2$

$in_{<deglex}(f) = xz^2$

$in_{grevlex}(f) = y^3$.

For any ideal $I \subseteq k[x_1,\dots,x_n]$ we define the initial ideal (Leading monomial ideal) (Lead term ideal) as

monomial ideal

$$in_<(I) = \langle in_<(f) \mid f \in I \rangle$$

Dickson's Lemma tells us

$$= \langle in_<(f_1), \dots, in_<(f_m) \rangle$$ for some $f_1,\dots,f_m \in I$.

Def/Proposition | (Gröbner basis) Fix a monomial order $<$

Every ideal I in $k[x_1,\dots,x_n]$ has a finite subset $G = \{g_1,\dots,g_r\} \subseteq I$ s.t

$$in_<(I) = \langle in_<(g_1), \dots, in_<(g_r) \rangle$$

This finite set G is called a Gröbner basis of I w.r.t $<$.

Proof (that such a G exists)

we know by Dickson's Lemma that $in_<(I)$ has finite generating set consisting of $\{in_<(f_1), \dots, in_<(f_r)\}$ take

$$G = \{f_1, \dots, f_r\}$$

Want $I = \langle g_1, \dots, g_r \rangle$ for $G = \{g_1, \dots, g_r\}$ our G.B.

Thm If $G = \{g_1, \dots, g_r\}$ is a Gröbner basis for an ideal I in $K[x_1, \dots, x_n]$ then $I = \langle g_1, \dots, g_r \rangle$

Proof: Suppose G does not generate I.

set difference

Among all $f \in I - \langle g_1, \dots, g_r \rangle$

there exists an f s.t. $x^b = in_<(f)$ is minimal w.r.t $<$

Since $x^b \in in_<(I)$ and $in_<(g_1), \dots, in_<(g_r)$ generate $in_<(I)$

$$\Rightarrow \quad x^b = x^c \cdot in_<(g_i) \quad \text{for some } i$$

$$f - x^c g_i \in I \quad (\text{since } f, g \in I)$$

and $f - x^c g_i \notin \langle G \rangle$ by assumption

since if $h = f - x^c g_i \in \langle G \rangle$

$\Rightarrow h + x^c g_i = f \in \langle G \rangle$, not true by assumption.

But $f - x^c g_i$ has strictly smaller initial monomial compared to f, but this contradicts f minimal ∎

Corollary (Hilberts Basis Theorem)

Every ideal I in $K[x_1, \dots, x_n]$ is finitely generated

Proof: Fix any monomial order. By Thm $\exists$ a finite G.B. $\{g_1, \dots, g_r\}$ for I, so $I = \langle g_1, \dots, g_r \rangle$ ∎

G.B. are <u>not</u> unique

I.e. if $G = \{g_1, \dots, g_r\}$ is a G.B. for I w.r.t $<$ then so is every finite subset of I containing G

e.g. $\{f_1, f_2\}$ is a G.B so is $\{f_1, f_2, f_1+f_2, f_1 f_2\}$

To fix this, define

Def Fix I and $<$. A G.B. G is <u>reduced</u> if the following conditions hold:

a) The leading coefficient (= coefficient of initial monomial) of each $g \in G$ is 1.

b) For $g \neq h$, $g, h \in G$ no monomial in g is a multiple of $\text{in}_<(h)$.