EE464 More Groebner Bases

example

suppose $I = \mathrm{ideal}\{f_1, f_2\}$, where

$$f_1 = x^2 + z^2 - 1 \qquad f_2 = x^2 + y^2 + z^2 - 2z - 3$$

suppose $p = x^2 + \frac{1}{2}y^2 z - z - 1$; we have $p \in I$ since

$$p = \left(-\frac{1}{2}z + 1\right) f_1 + \left(\frac{1}{2}z\right) f_2$$

but if we divide p by (f_1, f_2) we find

$$p = 1\, f_1 + 0\, f_2 + r \qquad \text{where } r = \frac{1}{2}y^2 z - z^2 - z$$

why wasn't the remainder zero? because the terms of p and r are not divisible by either $\mathrm{lt}(f_1)$ or $\mathrm{lt}(f_2)$

example continued

if for every $p \in I$,

we can remove $\mathrm{lt}(p)$ by division by one of the f_i
i.e., $\mathrm{lt}(f_i)$ divides $\mathrm{lt}(p)$

then we would have remainder $r = 0$ for every $p \in I$

as we'll see, this is the key Groebner basis property

in this case we can easily show $\{f_1, f_2\}$ is not a Groebner basis for I; let

$$p = f_1 - f_2 = -y^2 + 2z - 2$$

then $p \in I$ but neither $\mathrm{lt}(f_i)$ divides y^2

Groebner basis

the set of polynomials $\{g_1, \ldots, g_m\} \subset I$ is a Groebner basis for ideal I if and only if

for all $f \in I$ there is some i such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$

we'll show this is equivalent to our previous definition

example

suppose $I = \mathrm{ideal}\{f_1, f_2\}$ where

$$f_1 = x^3 + 2x^2 - 5x + 2 \qquad f_2 = x^2 + 3x - 4$$

Is $\{f_1, f_2\}$ a Groebner basis for I?

No, because we can construct $p \in I$ whose leading term isn't divisible by either of the $\mathrm{lt}(f_i)$

cancel x^3 terms: $f_3 = xf_2 - f_1 = x^2 + x - 2$ is in I

cancel x^2 terms: $p = f_2 - f_3 = 2x - 2$

equivalence of Groebner basis conditions

suppose $\{g_1, \ldots, g_m\} \subset I$ form a Groebner basis for I, i.e.,

$$\mathrm{ideal}\{\mathrm{lt}(I)\} = \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$$

then

for all $f \in I$ there is some i such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$

because if $f \in I$, then $\mathrm{lt}(f) \in \mathrm{lt}(I)$ so by the assumption

$$\mathrm{lt}(f) \in \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$$

the RHS is a monomial ideal, so membership implies $\mathrm{lt}(f)$ is a multiple of one of the $\mathrm{lt}(g_i)$

equivalence of Groebner basis conditions

suppose $\{g_1, \ldots, g_m\} \subset I$ and

for all $f \in I$ there is some i such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$

then $\{g_1, \ldots, g_m\} \subset I$ form a Groebner basis for I, i.e.,

$$\mathrm{ideal}\{\mathrm{lt}(I)\} = \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$$

let $I_1 = \mathrm{ideal}\{\mathrm{lt}(I)\}$ and $I_2 = \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$

first, we'll show $I_1 \subset I_2$

to see this, suppose $x^\gamma \in I_1$ then $x^\gamma = x^\alpha x^\beta$ for some $x^\beta \in \mathrm{lt}(I)$;

this means $x^\beta = \mathrm{lt}(f)$ for some $f \in I$, so by the hypothesis it is divisible by some $\mathrm{lt}(g_i)$, hence so is x^γ, so $x^\gamma \in I_2$

equivalence of Groebner basis conditions

$I_1 = \mathrm{ideal}\{\mathrm{lt}(I)\}$ and $I_2 = \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$

now we'll show $I_2 \subset I_1$;

suppose $x^\gamma \in I_2$, then $x^\gamma = x^\alpha \, \mathrm{lt}(g_i)$ for some i

since $g_i \in I$, we have $\mathrm{lt}(g_i) \in \mathrm{lt}(I)$ and so $x^\gamma \in I_1$

terminology

- the division algorithm for division of f by $g_1, \ldots, g_m$ is also called *reduction*
- the remainder on division is called the *normal form* of f

cancellation

suppose $I = \mathrm{ideal}\{g_1, \ldots, g_m\}$

this set of polynomials is *not* a Groebner basis for I if there is some $f \in I$ such that

$$\mathrm{lt}(f) \notin \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$$

this can happen if the leading terms in a sum $h_1 g_1 + \cdots + h_m g_m$ cancel

example

in grlex order

$$g_1 = x^3 - 2xy \qquad g_2 = x^2 y - 2y^2 + x$$

we have $-y g_1 + x g_2 = x^2$, so $x^2 \in \mathrm{ideal}\{g_1, \ldots, g_2\}$

but $\mathrm{lt}(x^2) \notin \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$

least common multiple

the *least common multiple* of monomials x^α and x^β is x^γ, where

$$\gamma_i = \max\{\alpha_i, \beta_i\} \qquad \text{for all } i = 1, \ldots, n$$

for example, the LCM of x^5yz^2 and x^2y^3z is $x^5y^3z^2$

syzygy polynomials

for $f, g \in \mathbb{K}[x_1, \dots, x_n]$, define the *syzygy polynomial* (S-polynomial)

$$S(f,g) = \frac{x^\gamma}{\mathrm{lt}(f)} f - \frac{x^\gamma}{\mathrm{lt}(g)} g \qquad \text{where } x^\gamma = \mathrm{lcm}\big(\mathrm{lm}(f), \mathrm{lm}(g)\big)$$

example

in grlex order

$$f = x^3y^2 - x^2y^3 + x \qquad g = 3x^4y + y^2$$

$S(f,g)$ is designed to cancel the leading terms of f and g

$$S(f,g) = xf - \tfrac{1}{3}yg$$

$$= -x^3\,y^3 - \tfrac{y^3}{3} + x^2$$

cancellation and syzygy polynomials

suppose $f_1, \ldots, f_m$ each have $\mathrm{multideg}(f_i) = \delta$, and $c_1, \ldots, c_m \in \mathbb{K}$

if the sum $h = \sum_{i=1}^{m} c_i f_i$ has a cancellation, i.e.,

$$\mathrm{multideg}(h) < \max_i \; \mathrm{multideg}(f_i)$$

then h is a linear combination of S-polynomials

$$h = \sum_{j,k} c_{jk} S(f_j, f_k)$$

that is, the only way cancellation can occur is in S-polynomials

one can show this by rearranging the terms in h

example

given polynomials

$$f_1 = x^3y^2 + x \qquad f_2 = 2x^3y^2 + y^2 \qquad f_3 = x^3y^2 - xy + x^2$$

the linear combination has a cancellation

$$f_1 + f_3 - f_2 = x^2 - xy + x - y^2$$

so it is a sum of S-polynomials $s_{ij} = S(f_i, f_j)$

$$= 2s_{12} - s_{13}$$

since

$$s_{12} = x - \tfrac{y^2}{2} \qquad s_{13} = -x^2 + xy + x \qquad s_{23} = -x^2 + xy + \tfrac{y^2}{2}$$

computation of Groebner bases

the polynomials $g_1, \ldots, g_m$ are a Groebner basis if

the remainder of $S(g_i, g_j)$ on division by $(g_1, \ldots, g_m)$ is zero for all i, j

- this gives a *computational test* to check if $g_1, \ldots, g_m$ are a Groebner basis
- to prove this, we'll show that if the above condition implies

  for all $f \in I$ there is some i such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$

proof

we can write any $f \in I$ in terms of the generators

$$f = \sum_i h_i g_i$$

we need to prove that there is some i such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$; this holds if

$$\mathrm{multideg}(f) = \max_i \ \mathrm{multideg}(h_i g_i)$$

proof by contradiction; suppose it does not hold; i.e.,

$$\mathrm{multideg}(f) < \max_i \ \mathrm{multideg}(h_i g_i)$$

for all choices of the h_i such that $f = \sum h_i g_i$

proof, continued

from all choices of h such that $f = \sum h_i g_i$, let δ be the minimum of the max multidegrees

$$\delta = \min_h \max_i \ \mathrm{multideg}(h_i g_i)$$

and let $h_1, \ldots, h_m$ achieve this, so we have

$$f = \sum_i h_i g_i \qquad \text{and} \qquad \max_i \ \mathrm{multideg}(h_i g_i) = \delta$$

for proof by contradiction, assume $\mathrm{multideg}(f) < \delta$

we'll show that this contradicts the choice of δ as minimal; i.e, we can find $\tilde{h}_i$ such that

$$f = \sum_i \tilde{h}_i g_i \qquad \text{and} \qquad \max_i \ \mathrm{multideg}(\tilde{h}_i g_i) < \delta$$

proof, continued

write f as a sum of terms in which cancellation occurs

$$f = \sum_i \mathrm{lt}(h_i) g_i + \text{ terms of lower multidegree}$$

each term in the sum has $\mathrm{multideg}(\mathrm{lt}(h_i)g_i) = \delta$, so from the previous result the sum is a linear combination of S-polynomials

$$f = \sum_{j,k} d_{jk} S\big(\mathrm{lt}(h_j)g_j, \mathrm{lt}(h_k)g_k\big) + \text{ terms of lower multidegree}$$

each S-poly has multideg $< \delta$, and is a multiple of an S-poly of the g_i

$$S\big(\mathrm{lt}(h_j)g_j, \mathrm{lt}(h_k)g_k\big) = p_{jk} S(g_j, g_k)$$

proof, continued

by assumption, each S-poly of the g_i is divisible by the g_i, so

$$S(g_j, g_k) = \sum_i q_{ijk} g_i$$

by the division algorithm, the terms satisfy

$$\operatorname{multideg}(q_{ijk} g_i) \leq \operatorname{multideg} S(g_j, g_k)$$

and since $\operatorname{multideg}(pq) \leq \operatorname{multideg}(p) \operatorname{multideg}(q)$

$$\begin{aligned} \operatorname{multideg}(p_{jk} q_{ijk} g_i) &\leq \operatorname{multideg}\Big(S\big(\operatorname{lt}(h_j) g_j, \operatorname{lt}(h_k) g_k\big)\Big) \\ &< \delta \end{aligned}$$

proof, continued

now we have a basis expansion for f

$$f = \sum_{i,j,k} d_{jk} p_{jk} q_{ijk} g_i + \text{ terms of lower multidegree}$$
$$= \sum_i \tilde{h}_i g_i + \text{ terms of lower multidegree}$$

and each term has $\mathrm{multideg}(\tilde{h}_i q_i) < \delta$,

as required, this contradicts the assumption that δ was minimal

this proves the result

the Buchberger algorithm

given $f_1, \ldots, f_m$, the following algorithm constructs a Groebner basis for $\mathrm{ideal}\{f_1, \ldots$

$G = \{f_1, \ldots, f_m\}$

repeat

for each pair $f_i, f_j \in G,$ divide $S(f_i, f_j)$ by G

if any remainder $r_{ij} \neq 0$

$G = G \cup \{r_{ij}\}$

until all remainders are zero

example

we'd like to find a Groebner basis for $I = \mathrm{ideal}\{f_1, f_2\}$ using grlex order

$$f_1 = x^3 - 2xy \qquad f_2 = x^2y - 2y^2 + x$$

we find $S(f_1, f_2) = -x^2$;

remainder on division of $S(f_1, f_2)$ by $\{f_1, f_2\}$ is $-x^2$; call this f_3

now we have $G = \{f_1, f_2, f_3\}$ we find $S(f_1, f_3) = -2xy$

remainder on division of $S(f_1, f_3)$ by G is $-2xy$; call this f_4

example, continued

now we have $G = \{f_1, f_2, f_3, f_4\}$ we find $S(f_1, f_4) = -2xy^2$

remainder on division of $S(f_1, f_4)$ by G is 0; ignore it

we find $S(f_2, f_3) = -2y^2 + x$

remainder on division $S(f_2, f_3)$ by G is $-2y^2 + x$; call it f_5

now we have $G = \{f_1, f_2, f_3, f_4, f_5\}$

we find the remainder on division of $S(f_i, f_j)$ by G is zero for all i, j

algorithm terminates

$G = \{f_1, f_2, f_3, f_4, f_5\}$ is a Groebner basis for I

notes on Buchberger algorithm

- at each step, the candidate basis grows
- the final basis may contain redundant polynomials; we'll see how to remove these
- we still need to show that the algorithm always terminates; we'll do this via the *ascending chain condition*

ascending chains

a sequence of ideals $I_1, I_2, I_3, \ldots$ is called an *ascending chain* if

$$I_1 \subset I_2 \subset I_3$$

we say this chain *stabilizes* if for some N

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

the ascending chain condition

every ascending chain of ideals in $\mathbb{K}[x_1, \ldots, x_n]$ stabilizes

this holds because, if we define

$$I = \bigcup_{i=1}^{\infty} I_i$$

then I is an ideal, so it is finitely generated, by say $\{f_1, \ldots, f_m\} \in I$

pick N sufficiently large that $\{f_1, \ldots, f_m\} \subset I_N$, then

$$I_k = I_N \qquad \text{for all } k \geq N$$

termination of the Buchberger algorithm

the algorithm generates an ascending chain

$$\mathrm{ideal}\{\mathrm{lt}(G_1)\} \subset \mathrm{ideal}\{\mathrm{lt}(G_2)\} \subset \mathrm{ideal}\{\mathrm{lt}(G_3)\} \subset \cdots$$

which therefore stabilizes

remains to show that the set of basis functions stops growing

we'll show that if $G_k \neq G_{k+1}$ then $\mathrm{ideal}\{\mathrm{lt}(G_k)\} \neq \mathrm{ideal}\{\mathrm{lt}(G_{k+1})\}$ to see this, suppose r is the non-zero remainder of an S-poly, and

$$G_{k+1} = G_k \cup \{r\}$$

since r is a remainder on division, it is not divisible by any element of $\mathrm{lt}(G_k)$, so

$$\mathrm{lt}(r) \notin \mathrm{ideal}\{\mathrm{lt}(G_k)\}$$

minimal Groebner bases

suppose $G = \{g_1, \ldots, g_m\}$ is a Groebner basis;

we can remove polynomial g_i, leaving $G \backslash \{g_i\}$ a Groebner basis, if

$\mathrm{lt}(g_i)$ is divisible by $\mathrm{lt}(g_j)$ for some $j \neq i$

this holds because removing g_i does not change the monomial ideal

$$\mathrm{ideal}\{\mathrm{lt}(G)\}$$

a Groebner basis where all such redundant polynomials have been removed is called *minimal*

example

the following polynomials are a Groebner basis w.r.t. grlex order

$$f_1 = x^3 - 2xy \qquad f_2 = x^2y - 2y^2 + x \qquad f_3 = -x^2$$
$$f_4 = -2xy \qquad f_5 = -2y^2 + x$$

since $\mathrm{lt}(f_1) = -x\,\mathrm{lt}(f_3)$, we can remove f_1

since $\mathrm{lt}(f_2) = -\frac{1}{2}x\,\mathrm{lt}(f_4)$, we can remove f_2

so a minimal Groebner basis is $\{f_3, f_4, f_5\}$

it is not unique; e.g., we can replace f_3 by $f_3 + cf_4$ for any $c \in \mathbb{K}$

reduced Groebner bases

suppose $G = \{g_1, \ldots, g_m\}$ is a minimal Groebner basis; we can normalize each element as follows

replace g_i by the remainder on dividing g_i by $G \backslash \{g_i\}$

if each element is monic, and normalized as above, then G is called a *reduced* Groebner basis

for a given ideal and monomial ordering, it is unique

for the previous example, we have the reduced Groebner basis

$$g_1 = x^2 \qquad g_2 = xy \qquad g_3 = y^2 - \tfrac{1}{2}x$$

example: linear equations

consider the system of linear equations

$$\begin{aligned} 3x - 6y - 2z &= 0 \\ 2x - 4y + 4w &= 0 \\ x - 2y - z - w &= 0 \end{aligned} \qquad \text{which is} \qquad \begin{bmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \\ 1 & -2 & -1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = 0$$

the Buchberger algorithm gives the reduced Groebner basis

$$\begin{bmatrix} 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = 0$$

i.e., it performs Gaussian elimination to *reduced row echelon form*

properties of the Buchberger algorithm

- again, it's linear algebra in disguise
- for polynomials in one variable, the Buchberger algorithm returns the gcd of $f_1, \ldots, f_m$
- for linear polynomials, the Buchberger algorithm performs Gaussian elimination
- many refinements of the algorithm are possible to achieve faster performance