EE464 Groebner Bases

Ideal membership and division

We have seen that testing feasibility of a set of polynomial equations over $\mathbb{C}^n$ can be solved if we can test ideal membership.

given $f, g_1, \ldots, g_m \in \mathbb{C}[x_1, \ldots, x_n]$, is it true that

$$f \in \operatorname{ideal}\{g_1, \ldots, g_m\}$$

- We would like to *divide* the polynomial f by the g_i, that is, find quotients $q_1, \ldots, q_m$ and remainder r such that

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

- Clearly, if $r = 0$ then $f \in \operatorname{ideal}\{g_1, \ldots, g_m\}$.
- The converse is not true unless we use a special generating set for the ideal, called a *Groebner basis*.

monomials

A monomial x^α is defined by a point $\alpha \in \mathbb{N}^n$; e.g.,

$$\alpha = (1, 0, 2) \qquad \Longrightarrow \qquad x^\alpha = x_1 x_3^2$$

in the scalar division algorithm, we repeatedly subtract a multiple of the divisor g from f

- the multiple is chosen to cancel the *leading term*
- the algorithm stops when the remainder is as small as possible

we need to specify an *ordering* on monomials for both of these steps

e.g., if $f = x^2$ and $g = x^2 - y^2$, then

$$f = 0\, g + x^2 \qquad \text{and} \qquad f = 1\, g + y^2$$

which is the *smaller* remainder?

note orderings are also important in Gaussian elimination

lex order

in *lexicographic order*, define $\alpha < \beta$ if the leftmost non-zero entry of $\beta - \alpha$ is positive; e.g.,

$$\begin{aligned}
(1,0,0) &< (2,0,0) & x &< x^2 \\
(1,2,0) &< (1,2,1) & xy &< xyz \\
(0,1,0) &< (8,0,0) & y &< x^8 \\
(0,8,0) &< (1,0,0) & y^8 &< x
\end{aligned}$$

called *lexicographic* after dictionary ordering; think of α_i as letters

the order depends on the ordering of the variables

in a polynomial, order the terms in *decreasing* order

$$f = \underbrace{-5x^3y}_{x^3} + \underbrace{7x^2y^2 + 3x^2y}_{x^2} + \underbrace{4xy^2z}_{x^1} + \underbrace{4yz^2}_{x^0}$$

grlex order

in *graded lexicographic order*, define $\alpha < \beta$ if

$$|\alpha| < |\beta| \qquad \text{or} \qquad |\alpha| = |\beta| \text{ and } \alpha <_{\mathsf{lex}} \beta$$

i.e., smallest degree always comes first; break ties using lex order

$$f = -5x^3y + 7x^2y^2 + 4xy^2z + 3x^2y + 4yz^2$$

order properties

both of these orderings have important properties

- for any α, β, exactly one of the following holds

$$\alpha < \beta \qquad \text{or} \qquad \alpha = \beta \qquad \text{or} \qquad \alpha > \beta$$

- if $x^\alpha < x^\beta$ then $x^\gamma x^\alpha < x^\gamma x^\beta$ for all $\gamma \in \mathbb{N}^n$

- $\alpha \geq 0$ for all $\alpha \in \mathbb{N}^n$

notation

ordering the terms in a polynomial

$$f = -5x^3y + 7x^2y^2 + 3x^2y + 4xy^2z + 4yz^2$$

defines

- the leading term $\mathrm{lt}(f) = -5x^3y$
  leading coefficient $\mathrm{lc}(f) = -5$
  leading monomial $\mathrm{lm}(f) = x^3y$
- we say f has multidegree $\mathrm{multideg}(f) = (3, 1, 0)$
- if f and g are nonzero then

$$\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$$

multivariable division

now we have an ordering, we can do division, for example

using lex order, with $y < x$,

$$
\begin{array}{r|l}
 & x - y \\
\cline{2-2}
x^2y + xy^2 + 1 & x^3y + xy^2 + 1 \\
 & x^3y + x^2y^2 + x \\
\cline{2-2}
 & \quad -x^2y^2 + xy^2 - x + 1 \\
 & \quad -x^2y^2 - xy^3 - y \\
\cline{2-2}
 & \qquad xy^3 + xy^2 - x + y + 1
\end{array}
$$

$$q = x - y \qquad r = xy^3 + xy^2 - x + y + 1$$

order dependence

but the result depends on the monomial ordering

same example as before, using lex order, with $x < y$,

$$
\begin{array}{r|l}
 & \quad 1 \\
\cline{2-2}
y^2x + yx^2 + 1 & y^2x + yx^3 + 1 \\
 & y^2x + yx^2 + 1 \\
\cline{2-2}
 & \qquad yx^3 - yx^2
\end{array}
$$

$$q = 1 \qquad r = yx^3 - yx^2$$

stopping criterion

in division of scalar polynomials, the algorithm halts if $\mathrm{lt}(g)$ does not divide $\mathrm{lt}(r)$;

$$
\begin{array}{r|l}
 & x^2 \\
\cline{2-2}
xy^2 + 1 & x^3y^2 + x^2y + x^2 + xy^2 \\
 & x^3y^2 + x^2 \\
\cline{2-2}
 & \qquad\quad x^2y + xy^2
\end{array}
$$

at this point, the remainder $r = x^2y + xy^2$

even though $\mathrm{lt}(r)$ is not divisible by $\mathrm{lt}(g)$, the second term in r is

so we can continue, if we ignore the leading term of r

stopping criterion

keep track of ignored remainders, and continue dividing

$$
\begin{array}{r|l l}
 & x^2+1 & \\
\cline{2-2}
xy^2+1 & x^3y^2 + x^2y + x^2 + xy^2 & \\
 & x^3y^2 + x^2 & \\
\cline{2-2}
 & \quad x^2y + xy^2 & \mathrm{lt}\ \text{does not divide by } \mathrm{lt}(g) \\
 & \quad xy^2 & \longrightarrow x^2y \text{ remainder} \\
 & \quad xy^2 + 1 & \\
\cline{2-2}
 & \qquad -1 & \\
 & \qquad\ \ 0 & \longrightarrow x^2y - 1
\end{array}
$$

the algorithm halts when no term in the remainder is divisible by $\mathrm{lt}(g)$

multiple divisors

we can divide f by multiple polynomials $g_1, \ldots, g_m$ to find quotients $q_1, \ldots, q_m$ and remainder r such that $f = q_1 g_1 + \cdots + q_m g_m + r$

$$
\begin{array}{llll}
 & q_1 : x + y & & \\
 & q_2 : 1 & & \\
\begin{array}{r} xy - 1 \\ y^2 - 1 \end{array} & \overline{\left| \; x^2y + xy^2 + y^2 \right.} & & \text{divides by } g_1 \\
 & x^2y \;\; \underline{-x} & & \\
 & \quad xy^2 + x + y^2 & & \text{divides by } g_1 \\
 & \quad xy^2 \;\; \underline{-y} & & \\
 & \qquad x + \;\; y^2 - y & & \\
 & \qquad\qquad y^2 - y & & \longrightarrow x \text{ rem, then divide by } g_2 \\
 & \qquad\qquad \underline{y^2 - 1} & & \\
 & \qquad\qquad\quad y + 1 & & \\
 & \qquad\qquad\qquad\qquad 0 & & \longrightarrow x + y + 1 \text{ rem}
\end{array}
$$

division algorithm

the algorithm is

$q_1 = 0;\ \dots\ q_m = 0;$

$r = 0; p = f;$

while $p \neq 0$

let i be the smallest i such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(p)$

if such i exists

$q_i = q_i + \mathrm{lt}(p)/\,\mathrm{lt}(g_i)$

$p = p - g_i\,\mathrm{lt}(r)/\,\mathrm{lt}(g_i)$

else

$r = r + \mathrm{lt}(p)$

$p = p - \mathrm{lt}(p)$

division algorithm

the division algorithm works because

- after every pass through the loop, we have

$$f = q_1 g_1 + \cdots + q_m g_m + r + p$$

- we update p every time we pass through the loop, and each time its multidegree drops (relative to the monomial ordering)

division theorem

suppose $f, g_1, \ldots, g_m \in \mathbb{K}[x_1, \ldots, x_n]$;

there exist $r, q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

and either

- $r = 0$ or
- none of the monomials of r divide by any of $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)$

also, $\mathrm{multideg}(q_i g_i) \le \mathrm{multideg}(f)$ w.r.t. the monomial order

nonuniqueness

there is no uniqueness; both quotients and remainder may change, if we

- reorder the g_i polynomials
- change the monomial ordering

example

dividing $f = x^2y + xy^2 + y^2$ by

$$g_1 = xy - 1, \qquad g_2 = y^2 - 1$$

gives $f = (x+y)(xy-1) + (y^2-1) + (x+y+1)$

Reversing the order of the g_i's gives

$$f = x(xy-1) + (x+1)(y^2-1) + (2x+1)$$

testing ideal membership

if the remainder on division is zero, then we have

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

but the converse is not true

example

$$f = xy^2 - x, \qquad g_1 = xy + 1, \qquad g_2 = y^2 - 1$$

division gives $q_1 = y$, $q_2 = 0$, and $r = -x - y$

but we have $f = xg_2$ so clearly $f \in \mathrm{ideal}\{g_1, g_2\}$

testing ideal membership

we would like to test if

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

the division algorithm stops when all terms of the remainder are not divisible by any $\mathrm{lt}(g_i)$

for example, if

$$g_1 = x^2 - y \qquad g_2 = x^2 - z$$

in lex order $z < y < x$, then the leading x^2 terms mask information about terms in y and z; e.g., $y - z \in \mathrm{ideal}\{g_1, g_2\}$ but does not divide by g_1, g_2

this suggests picking a basis $h_1, \ldots, h_s$ of the ideal where the $\mathrm{lt}(h_i)$ terms contain enough information to specify the ideal

monomial ideals

an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is called a *monomial ideal* if it is generated by a set of monomials $W \subset \mathbb{N}^n$

$$I = \mathrm{ideal}\{\, x^\alpha \mid \alpha \in W \,\}$$

monomial ideals

suppose I is the monomial ideal $I = \mathrm{ideal}\{\, x^\alpha \mid \alpha \in W \,\}$; then

$$x^\beta \in I \qquad \Longrightarrow \qquad x^\beta = x^\gamma x^\alpha \text{ for some } \alpha \in W$$

proof; since $x^\beta \in I$, we have

$$x^\beta = \sum_{i=1}^{m} h_i x^{\alpha(i)} \qquad \text{where } \alpha(1), \ldots, \alpha(m) \in W$$

every term on the RHS has the property that

there exists some i such that $x^{\alpha(i)}$ divides it

so every term on the LHS does also; but there is only one term on the LHS

monomial ideals

a similar argument, expanding f in terms of the generators, shows

$f \in I$ if and only if every term of f is in I

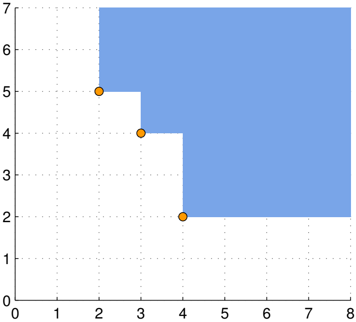
and this then implies

two monomial ideals are the same if and only if they contain the same monomials

monomial ideals

monomial ideals are defined by the monomials they contain; e.g.

$$I = \mathrm{ideal}\{x^4y^2, x^3y^4, x^2y^5\}$$



we can plot these in $\mathbb{N}^n$

the picture should convince you of *Dickson's Lemma*

Every monomial ideal is finitely generated

the Hilbert basis theorem

Every ideal in $\mathbb{K}[x_1, \ldots, x_n]$ is finitely generated

- we know that $\mathrm{ideal}\{f_1, \ldots, f_m\}$ is finitely generated
- but what about $\mathcal{I}(S)$ when S is a variety?

the Hilbert basis theorem

to see this, suppose I is an ideal; then

$$\mathrm{ideal}\{\mathrm{lt}(I)\} \text{ is a monomial ideal}$$

so it is finite generated by some monomials $w_1, \ldots, w_m$

these monomials are in $\mathrm{ideal}\{\mathrm{lt}(I)\}$ since they are generators for it

we can also choose them in $\mathrm{lt}(I)$, by the proof of Dickson's Lemma

since they are in $\mathrm{lt}(I)$, they are the leading terms of some elements of I, say $g_1, \ldots, g_m$

proof continued

so far, we have $\mathrm{ideal}\{\mathrm{lt}(I)\}$ is finitely generated by the leading terms of some $g_i \in I$

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

we'll show $I = \mathrm{ideal}\{g_1, \ldots, g_m\}$

suppose $f \in I$, then division gives

$$f = q_1 g_1 + \ldots q_m g_m + r$$

if $r \neq 0$ we have a contradiction, since $r \in I$, hence

$$\mathrm{lt}(r) \in \mathrm{lt}(I) \subset \mathrm{ideal}\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$$

hence $\mathrm{lt}(r)$ is divisible by some $\mathrm{lt}(g_i)$; contradicting the division theorem

consequences of the Hilbert basis theorem

$g_1, \ldots, g_m \in \mathbb{K}[x_1, \ldots, x_n]$ are called a *Groebner basis* for I if

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

the Hilbert basis theorem gives a condition for ideal membership

$$f \in I \quad \Longleftrightarrow \quad \text{remainder } r = 0 \text{ when dividing } f \text{ by } g_1, \ldots, g_m$$

so far, we do not know how to construct a Groebner basis

properties of Groebner bases

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

- whether $g_1, \ldots, g_m$ is a Groebner basis for I depends on the monomial ordering

- for any $f \in \mathbb{K}[x_1, \ldots, x_n]$ the remainder on division by $g_1, \ldots, g_m$ is independent of how we order the g_i

  but we have to use the same monomial ordering in the division

  and the *quotients* may change under reordering of g_i

- proof of the HB theorem showed that a Groebner basis always exists

consequences of the Hilbert basis theorem

an important consequence is

> every variety $S \subset \mathbb{R}^n$ is the feasible set of a *finite* set of polynomial equations

because if $S = \mathcal{V}(P)$, for some possibly infinite set $P \subset \mathbb{K}[x_1, \ldots, x_n]$

then $\mathcal{V}(\mathcal{I}(S)) = S$ since S is a variety and $\mathcal{I}(S)$ is finitely generated, so there exists $f_1, \ldots, f_m$ such that

$$\mathcal{V}(\mathrm{ideal}\{f_1, \ldots, f_m\}) = S$$

and $\mathcal{V}(\mathrm{ideal}\{f_1, \ldots, f_m\}) = \mathcal{V}(f_1, \ldots, f_m)$