7. Groebner Bases

- Monomials
- Lexicographic and graded lexicographic order
- Properties of orders
- Multivariable division
- Stopping criteria for the division algorithm
- The division algorithm
- Testing ideal membership
- Monomial ideals
- Dickson's Lemma
- The Hilbert basis theorem
- 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

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

We would like to *divide* the polynomial f by the g_i; i.e. 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 $f \in \mathbf{ideal}\{g_1, \ldots, g_m\}$.

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?

lex order

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

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

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

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

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 $\alpha \in \mathbb{N}^n$

- every nonempty subset of $\mathbb{N}^n$ has a smallest element

notation

ordering the terms in a polynomial

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

defines

- the leading term $\mathbf{lt}(f) = -5x^3$
  leading coefficient $\mathbf{lc}(f) = -5$
  leading monomial $\mathbf{lm}(f) = x^3$

- we say f has multidegree $\mathbf{multideg}(f) = (3,1,0)$

- if f and g are nonzero then

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

multivariable division

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

using lex order, with $y < x$,

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

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

order dependence

but the result depends on the monomial ordering

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

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

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

stopping criterion

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

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

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

even though $\mathbf{lt}(r)$ is not divisible by $\mathbf{lt}(g)$, 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

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

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

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

$$
\begin{array}{r|l}
 & q_1 : x + y \\
 & q_2 : 1 \\
\hline
\begin{array}{r} xy - 1 \\ y^2 - 1 \end{array} & x^2y + xy^2 + y^2 \\
 & x^2y \ \underline{-x} \\
 & \quad xy^2 + x + y^2 \\
 & \quad xy^2 \ \underline{-y} \\
 & \qquad x + \ y^2 - y \\
 & \qquad\quad y^2 - y \\
 & \qquad\quad \underline{y^2 - 1} \\
 & \qquad\qquad y + 1 \\
 & \qquad\qquad\quad 0
\end{array}
$$

divides by g_1

divides by g_1

$\longrightarrow x$ rem, then divide by g_2

$\longrightarrow x + y + 1$ rem

division algorithm

the algorithm is

$$q_1 = 0; \ \ldots \ q_m = 0;$$

$$r = 0; p = f;$$

while $p \neq 0$

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

if such i exists

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

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

else

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

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

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 $\mathbf{lt}(g_1), \ldots, \mathbf{lt}(g_m)$

also, $\mathbf{multideg}(q_i g_i) \leq \mathbf{multideg}(f)$ 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

$$f \in \mathbf{ideal}\{g_1, \dots, g_m\}$$

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 $f \in \mathbf{ideal}\{g_1, g_2\}$

testing ideal membership

we would like to test if

$$f \in \mathbf{ideal}\{g_1, \dots, g_m\}$$

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

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., $y - z \in \mathbf{ideal}\{g_1, g_2\}$ but does not divide by g_1, g_2

this suggests picking a basis $h_1, \dots, h_s$ of the ideal where the $\mathbf{lt}(h_i)$ 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 $W \subset \mathbb{N}^n$

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

properties

- if $x^\beta \in I$ then x^β is a multiple of x^α for some $\alpha \in W$
- $f \in I$ if and only if every term of f is in I
  most ideals do not satisfy this; e.g., $y^2 \notin \mathbf{ideal}\{y^2 - x^3\}$
- two monomial ideals are the same if and only if they contain the same monomials

monomial ideals

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

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

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

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

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

$$\boxed{f \in I \text{ if and only if every term of } f \text{ is in } I}$$

and this then implies

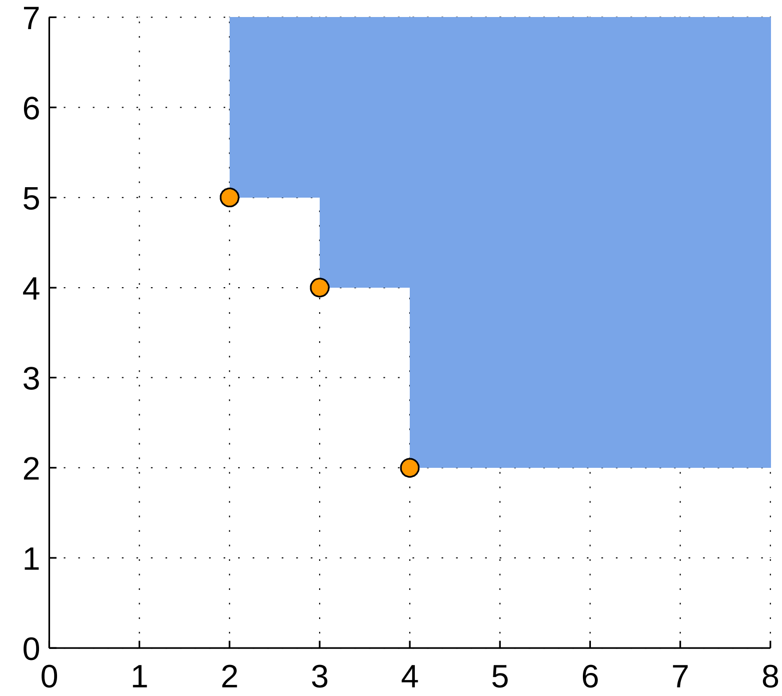
> two monomial ideals are the same if and only if
> they contain the same monomials

monomial ideals

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

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

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



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

$$\boxed{\text{Every monomial ideal is finitely generated}}$$

the Hilbert basis theorem

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

- we know that $\mathbf{ideal}\{f_1, \ldots, f_m\}$ 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

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

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

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

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

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

proof continued

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

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

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

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

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

hence $\mathbf{lt}(r)$ is divisible by some $\mathbf{lt}(g_i)$; 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

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

the Hilbert basis theorem gives a condition for ideal membership

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

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

properties of Groebner bases

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

- 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

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

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