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

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

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

$$f = q_1g_1 + \cdots + q_mg_m + r$$

Clearly, if $r = 0$ then $f \in \text{ideal}\{g_1, \ldots, g_m\}$.

The converse is not true unless we use a special generating set for the ideal, called a Groebner basis.
monomials

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

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

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

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

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.,

\[
(1, 0, 0) < (2, 0, 0) \quad \quad x < x^2 \\
(1, 2, 0) < (1, 2, 1) \quad \quad xy < xyz \\
(0, 1, 0) < (8, 0, 0) \quad \quad y < x^8
\]

called *lexicographic* after dictionary ordering; think of $\alpha_i$ as letters

the order depends on the ordering of the variables

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

\[
f = -5x^3y + 7x^2y^2 + 3x^2y + 4xy^2z + 4yz^2
\]
grlex order

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

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

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 $\alpha, \beta$, exactly one of the following holds

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

• 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 \( \text{lt}(f) = -5x^3 \)
- leading coefficient \( \text{lc}(f) = -5 \)
- leading monomial \( \text{lm}(f) = x^3 \)

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

- if \( f \) and \( g \) are nonzero then

\[ \text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g) \]
multivariable division

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

using lex order, with $y < x$,

\[
x^2y + xy^2 + 1 \bigg| \begin{array}{c}
x - y \\
x^3y + x^2y^2 + x \\
x^3y + xy^2 + 1 \\
x^2y^2 + xy^2 - x + 1 \\
x^2y^2 - xy^3 - y \\
xy^3 + xy^2 - x + y + 1
\end{array}
\]

\[q = x - y \quad r = xy^3 + xy^2 - x + y + 1\]
order dependence

but the result depends on the monomial ordering

same example as before, using lex order, with \( x < y \),

\[
y^2x + yx^2 + 1 \div \begin{array}{c}
y^2x + yx^3 + 1 \\
y^2x + yx^2 + 1 \\
yx^3 - yx^2
\end{array}
\]

\( q = 1 \quad r = yx^3 - yx^2 \)
stopping criterion

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

\[
\begin{array}{c|ccccc}
 & x^2 y^2 + 1 & x^3 y^2 + x^2 y + x^2 + xy^2 \\
\hline
 & x^3 y^2 + x^2 & \hline
 & \"x^2 y + xy^2" \\
\end{array}
\]

at this point, the remainder \( r = x^2 y + xy^2 \)

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

\[
\begin{align*}
xy^2 + 1 & \divides x^2y + xy^2 \\
& \divides x^2y + xy^2 \\
x^2y + xy^2 & \rightarrow x^2y \text{ remainder} \\
xy^2 & \rightarrow x^2y - 1
\end{align*}
\]

the algorithm halts when no term in the remainder is divisible by \(\text{Lt}(g)\)
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 $f = q_1 g_1 + \cdots + q_m g_m + r$

\[
\begin{align*}
q_1 : x + y \\
q_2 : 1 \\
x y - 1 & \overline{\begin{array}{c}
x^2 y + x y^2 + y^2 \\
y^2 - 1 & \end{array}} \\
x^2 y - x & \overline{\begin{array}{c}
xy^2 + x + y^2 \\
xy^2 - y & \end{array}} \\
x + y^2 - y & \overline{\begin{array}{c}
y^2 - y \\
y^2 - 1 \\
0 & \end{array}} \\
\end{align*}
\]

divides by $g_1$
divides by $g_1$\[\rightarrow x \text{ rem, then divide by } g_2\]\[\rightarrow x + y + 1 \text{ rem}\]
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 \( \text{lt}(g_i) \) divides \( \text{lt}(p) \)

if such \( i \) exists

\[ q_i = q_i + \frac{\text{lt}(p)}{\text{lt}(g_i)} \]
\[ p = p - g_i \frac{\text{lt}(r)}{\text{lt}(g_i)} \]

else

\[ r = r + \text{lt}(p) \]
\[ p = p - \text{lt}(p) \]
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

\[
f = q_1g_1 + \cdots + q_mg_m + r
\]

and either

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

also, \( \text{multideg}(q_ig_i) \leq \text{multideg}(f) \) 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

\[
g_1 = xy - 1, \quad g_2 = y^2 - 1
\]
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

\[ f \in \text{ideal}\{g_1, \ldots, g_m\} \]

but the converse is not true

example

\[ f = xy^2 - x, \quad g_1 = xy + 1, \quad g_2 = y^2 - 1 \]

division gives \( q_1 = y, \ q_2 = 0, \) and \( r = -x - y \)

but we have \( f = xg_2 \) so clearly \( f \in \text{ideal}\{g_1, g_2\} \)
testing ideal membership

we would like to test if

\[ f \in \text{ideal}\{g_1, \ldots, g_m\} \]

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

for example, if

\[ g_1 = x^2 - y \quad g_2 = x^2 - z \]

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

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

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

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

properties

• if $x^\beta \in I$ then $x^\beta$ is a multiple of $x^\alpha$ 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., $y^2 \not\in \text{ideal}\{y^2 - x^3\}$

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

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

\[
x^\beta \in I \implies x^\beta = x^\gamma x^\alpha \text{ for some } \alpha \in W
\]

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

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

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

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

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.

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

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 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

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

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

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

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

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

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

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

we’ll show $I = \text{ideal}\{g_1, \ldots, g_m\}$

suppose $f \in I$, then division gives

$$f = q_1g_1 + \ldots + q_mg_m + r$$

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

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

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

\[
\text{ideal}\{\text{lt}(I)\} = \text{ideal}\{\text{lt}(g_1), \ldots, \text{lt}(g_m)\}
\]

the Hilbert basis theorem gives a condition for ideal membership

\[
f \in I \quad \iff \quad \text{remainder } r = 0 \text{ when dividing } f \text{ by } g_1, \ldots, g_m
\]

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

- \( I = \text{ideal}\{g_1, \ldots, g_m\} \)

- 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 \textit{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

\[
\text{every variety } S \subset \mathbb{R}^n \text{ is the feasible set of a finite set of polynomial equations}
\]

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

\[
\mathcal{V}(\text{ideal}\{f_1, \ldots, f_m\}) = S
\]

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