EE464 More Groebner Bases
example

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

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

suppose $p = x^2 + \frac{1}{2}y^2z - z - 1$; 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

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

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

if for every \( p \in I \),

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

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 \( \text{lt}(f_i) \) divides \( y^2 \)
the set of polynomials \( \{g_1, \ldots, g_m\} \subset I \) is a Groebner basis for ideal \( I \) if and only if

\[
\text{for all } f \in I \quad \text{there is some } i \text{ such that } \text{lt}(g_i) \text{ divides } \text{lt}(f)
\]

we’ll show this is equivalent to our previous definition
example

Suppose \( I = \text{ideal}\{f_1, f_2\} \) where

\[
\begin{align*}
f_1 &= x^3 + 2x^2 - 5x + 2 \\ f_2 &= x^2 + 3x - 4
\end{align*}
\]

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 \( \text{lt}(f_i) \)

\[
\begin{align*}
\text{cancel } x^3 \text{ terms:} & \quad f_3 = xf_2 - f_1 = x^2 + x - 2 \text{ is in } I \\
\text{cancel } x^2 \text{ terms:} & \quad p = f_2 - f_3 = 2x - 2
\end{align*}
\]
equivalence of Groebner basis conditions

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

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

then

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

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

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

the RHS is a monomial ideal, so membership implies \( \text{lt}(f) \) is a multiple of one of the \( \text{lt}(g_i) \)
equivalence of Groebner basis conditions

suppose \(\{g_1, \ldots, g_m\} \subset I\) and

\[
\text{for all } f \in I \quad \text{there is some } i \text{ such that } \text{lt}(g_i) \text{ divides } \text{lt}(f)
\]

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

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

\[I_1 = \text{ideal}\{\text{lt}(I)\} \text{ and } I_2 = \text{ideal}\{\text{lt}(g_1), \ldots, \text{lt}(g_m)\}\]

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 \(x^\beta \in \text{lt}(I)\);

this means \(x^\beta = \text{lt}(f)\) for some \(f \in I\), so by the hypothesis it is divisible by some \(\text{lt}(g_i)\), hence so is \(x^\gamma\), so \(x^\gamma \in I_2\)
equivalence of Groebner basis conditions

\[ I_1 = \text{ideal}\{\text{lt}(I)\} \] and \[ I_2 = \text{ideal}\{\text{lt}(g_1), \ldots, \text{lt}(g_m)\} \]

now we’ll show \( I_2 \subset I_1 \);

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

since \( g_i \in I \), we have \( \text{lt}(g_i) \in \text{lt}(I) \) 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 \( I = \text{ideal}\{g_1, \ldots, g_m\} \)

this set of polynomials is \textit{not} a Groebner basis for \( I \) if there is some \( f \in I \) such that
\[
\text{lt}(f) \notin \text{ideal}\{\text{lt}(g_1), \ldots, \text{lt}(g_m)\}
\]

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

\textbf{example}

in \textit{grlex} order
\[
g_1 = x^3 - 2xy \quad g_2 = x^2y - 2y^2 + x
\]

we have \(-yg_1 + xg_2 = x^2\), so \( x^2 \in \text{ideal}\{g_1, \ldots, g_2\} \)

but \( \text{lt}(x^2) \notin \text{ideal}\{\text{lt}(g_1), \ldots, \text{lt}(g_m)\} \)
the least common multiple of monomials $x^\alpha$ and $x^\beta$ is $x^\gamma$, where

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

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

for \( f, g \in K[x_1, \ldots, x_n] \), define the **syzygy polynomial** (S-polynomial)

\[
S(f, g) = \frac{x^\gamma}{\mathrm{lt}(f)} f - \frac{x^\gamma}{\mathrm{lt}(g)} g
\]

where \( x^\gamma = \text{lcm}(\text{lm}(f), \text{lm}(g)) \)

**example**

in grlex order

\[
f = x^3 y^2 - x^2 y^3 + x \quad g = 3x^4 y + y^2
\]

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

\[
S(f, g) = xf - \frac{1}{3}yg
\]

\[
= -x^3 y^3 - \frac{y^3}{3} + x^2
\]
cancellation and syzygy polynomials

suppose $f_1, \ldots, f_m$ each have $\text{multideg}(f_i) = \delta$, 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.,

$$\text{multideg}(h) < \max_i \text{multideg}(f_i)$$

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

\[ f_1 = x^3y^2 + x \quad f_2 = 2x^3y^2 + y^2 \quad f_3 = x^3y^2 - xy + x^2 \]

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

\[ s_{12} = x - \frac{y^2}{2} \quad s_{13} = -x^2 + xy + x \quad s_{23} = -x^2 + xy + \frac{y^2}{2} \]
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 $\text{lt}(g_i)$ divides $\text{lt}(f)$
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 \( \text{lt}(g_i) \) divides \( \text{lt}(f) \); this holds if

\[
\text{multideg}(f) = \max_i \text{multideg}(h_i g_i)
\]

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

\[
\text{multideg}(f) < \max_i \text{multideg}(h_i g_i)
\]

for all choices of the \( h_i \) such that \( f = \sum h_i g_i \)
from all choices of \( h \) such that \( f = \sum h_i g_i \), let \( \delta \) be the minimum of the max multidegrees

\[
\delta = \min_h \max_i \text{multideg}(h_i g_i)
\]

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

\[
f = \sum_i h_i g_i \quad \text{and} \quad \max_i \text{multideg}(h_i g_i) = \delta
\]

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

we’ll show that this contradicts the choice of \( \delta \) as minimal; i.e, we can find \( \tilde{h}_i \) such that

\[
f = \sum_i \tilde{h}_i g_i \quad \text{and} \quad \max_i \text{multideg}(\tilde{h}_i g_i) < \delta
\]
proof, continued

write \( f \) as a sum of terms in which cancellation occurs

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

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

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

each \( S \)-poly has \( \text{multideg} < \delta \), and is a multiple of an \( S \)-poly of the \( g_i \)

\[
S(\text{lt}(h_j)g_j, \text{lt}(h_k)g_k) = p_{j,k} S(g_j, g_k)
\]
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

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

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

$$\text{multideg}(p_{jk} q_{ijk} g_i) \leq \text{multideg} \left( S(\text{lt}(h_j) g_j, \text{lt}(h_k) g_k) \right)$$

$$< \delta$$
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 $\text{multideg}(\tilde{h}_i q_i) < \delta$,

as required, this contradicts the assumption that $\delta$ was minimal

this proves the result
the Buchberger algorithm

given \( f_1, \ldots, f_m \), the following algorithm constructs a Groebner basis for 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
we’d like to find a Groebner basis for \( I = \text{ideal}\{f_1, f_2\} \) using grlex order

\[
f_1 = x^3 - 2xy \quad f_2 = x^2y - 2y^2 + x
\]

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 \( G = \{f_1, f_2, f_3\} \)  \quad 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

$$I_k = I_N \quad \text{for all } k \geq N$$
termination of the Buchberger algorithm

the algorithm generates an ascending chain

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

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 $\text{ideal}\{\text{lt}(G_k)\} \neq \text{ideal}\{\text{lt}(G_{k+1})\}$ 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 $\text{lt}(G_k)$, so

$$\text{lt}(r) \not\in \text{ideal}\{\text{lt}(G_k)\}$$
minimal Groebner bases

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

we can remove polynomial $g_i$, leaving $G \setminus \{g_i\}$ a Groebner basis, if $\text{lt}(g_i)$ is divisible by $\text{lt}(g_j)$ for some $j \neq i$

this holds because removing $g_i$ does not change the monomial ideal

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

a Groebner basis where all such redundant polynomials have been removed is called \textit{minimal}
the following polynomials are a Groebner basis w.r.t. grlex order

\[ f_1 = x^3 - 2xy \quad f_2 = x^2y - 2y^2 + x \quad f_3 = -x^2 \]
\[ f_4 = -2xy \quad f_5 = -2y^2 + x \]

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

since \( \text{lt}(f_2) = -\frac{1}{2}x \text{lt}(f_4) \), 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 $G \setminus \{g_i\}$

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

\[
\begin{align*}
g_1 &= x^2 \\
g_2 &= xy \\
g_3 &= y^2 - \frac{1}{2}x
\end{align*}
\]
example: linear equations

consider the system of linear equations

\[
\begin{align*}
3x - 6y - 2z &= 0 \\
2x - 4y + 4w &= 0 \\
x - 2y - z - w &= 0
\end{align*}
\]

which is

\[
\begin{bmatrix}
3 & -6 & -2 & 0 \\
2 & -4 & 0 & 4 \\
1 & -2 & -1 & -1
\end{bmatrix}
\begin{bmatrix}
x \\
y \\
z \\
w
\end{bmatrix} = 0
\]

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