EE464 Elimination
ideal membership

given \( h, f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_m] \), we’d like to test if

\[
h \in \text{ideal}\{f_1, \ldots, f_m\}
\]

procedure

\begin{itemize}
  \item compute the Groebner basis \( g_1, \ldots, g_s \) for \( f_1, \ldots, f_m \)
  \item divide \( h \) by \( g_1, \ldots, g_s \); the remainder \( r = 0 \) if and only if

\[
h \in \text{ideal}\{f_1, \ldots, f_m\}
\]
\end{itemize}

this works independent of the monomial order or the order in which division is performed.
example

for $f_1 = xz - y^2$, $f_2 = x^3 - z^2$ in grlex order, the Groebner basis is

$$xz - y^2, \quad x^3 - z^2, \quad x^2 y^2 - z^3, \quad xy^4 - z^4, \quad y^6 - z^5$$

check membership of $h = -4x^2y^2z^2 + y^6 + 3z^5$, we find

$$h = (-4xy^2z - 4y^4)(xz - y^2) + (-3)(y^6 - z^5)$$

so $h \in \text{ideal}\{f_1, f_2\}$

also if $t = xy - 5z^2 + x$, then $t$ is not in the ideal, since its leading term is not divisible by any of the leading terms of the Groebner basis
example: solving polynomial equations

consider the equations

\[ x^2 + y^2 + z^2 - 1 = 0 \]
\[ x^2 - y + z^2 = 0 \]
\[ x - z = 0 \]

a Groebner basis in *lex order* gives equivalent equations

\[ x - z = 0 \]
\[ y - 2z^2 = 0 \]
\[ 4z^4 + 2z^2 - 1 = 0 \]

the third equation depends only on \( z \); so we can solve it, then substitute to find \( x \) and \( y \)
example 2

we’d like to solve the following equations

\[-2 \, w \, x + 3 \, x^2 + 2 \, y \, z = 0\]
\[-2 \, w \, y + 2 \, x \, z = 0\]
\[-2 \, w \, z + 2 \, x \, y - 2 \, z = 0\]
\[x^2 + y^2 + z^2 - 1 = 0\]
example 2 continued

a Groebner basis in lex order $w > x > y > z$ gives equivalent equations

$$7670w - 11505x - 11505yz - 335232z^6 + 477321z^4 - 134419z^2 = 0$$

$$x^2 + y^2 + z^2 - 1 = 0$$

$$3835xy - 19584z^5 + 25987z^3 - 6403z = 0$$

$$-3835xz - 3835y^2 + 1152z^5 + 1404z^3 - 2556z = 0$$

$$-3835y^3 - 3835yz^2 + 3835y + 9216z^5 - 11778z^3 + 2562z = 0$$

$$3835y^2z - 6912z^5 + 10751z^3 - 3839z = 0$$

$$118yz^3 - 118yz - 1152z^6 + 1605z^4 - 453z^2 = 0$$

$$-1152z^7 + 1763z^5 - 655z^3 + 44z = 0$$

again, the Groebner basis eliminates variables successively

similar to back-substitution in Gaussian elimination
Elimination

- the above examples illustrate *elimination*

- the Groebner basis algorithm successively removes terms
  this is similar to Gaussian elimination; a *triangular* structure results, i.e,
    some polynomials depend only on $x_n$
    some polynomials depend only on $x_{n-1}, x_n$
    some polynomials depend only on $x_{n-2}, x_{n-1}, x_n$
    etc.
**Implicitization**

A parametrization of the circle is

\[
x = \frac{1 - t^2}{1 + t^2}
\]

\[
y = \frac{2t}{1 + t^2}
\]

clear denominators

\[
t^2 y - 2t + y = 0 \quad t^2 x + t^2 + x - 1 = 0
\]

Groebner basis in lex order \( t > x > y \) is

\[
t x + t - y \quad t y + x - 1 \quad x^2 + y^2 - 1
\]

so for any \( t \) every \((x, y)\) lies on the circle
if \{ f_1, \ldots, f_m \} and \{ g_1, \ldots, g_m \} are two bases for the same ideal, then they have the same feasible sets.

In particular, in the above example, this implies that every solution to the implicit equations satisfies

\[ x^2 + y^2 = 1 \]

that is \( \mathcal{V}\{ f_1, \ldots, f_m \} \subset \mathcal{V}\{ g_3 \} \)

but the set on the RHS is strictly bigger; it contains \((-1, 0)\)

because we have ignored \( g_1 \) and \( g_2 \)
**the elimination ideal**

the Groebner basis \( G = \{g_1, \ldots, g_m\} \) w.r.t. lex order consists of

- polynomials in \( I = \text{ideal}\{g_1, \ldots, g_m\} \)
- which do not contain variables \( x_1, \ldots, x_k \) for some \( k \)

that is, it finds polynomials in

\[
I_k = \text{ideal}\{g_1, \ldots, g_m\} \cap \mathbb{K}[x_{k+1}, \ldots, x_n]
\]

- \( I_k \) is called the \( k \)'th elimination ideal of \( I \)
- it is an ideal in \( \mathbb{K}[x_{k+1}, \ldots, x_n] \)
- every \( f \in I_k \) is a *polynomial consequence* of \( g_1, \ldots, g_m \)
  which depends only on \( x_{k+1}, \ldots, x_n \)
the elimination theorem

suppose \( G = \{g_1, \ldots, g_m\} \) is a Groebner basis for \( I \) w.r.t. lex order with \( x_1 > x_2 > \cdots > x_n \); then

\[
G_k = G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]
\]

is a Groebner basis for \( I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n] \)

we need to show

\[
\text{ideal}\{\text{lt}(I_k)\} = \text{ideal}\{\text{lt}(G_k)\}
\]

since \( I_k \supseteq G_k \), all we need to show is LHS \( \subseteq \) RHS

any \( f \in I_k \) is divisible by \( \text{lt}(g_i) \) for some \( g_i \), and \( f \) does not contain variables \( x_1, \ldots, x_k \), so neither does \( \text{lt}(g_i) \);

since we are using lex order, neither does \( g_i \), so \( g_i \in G_k \)
example

consider polynomials \( x^2 + y + z - 1, \ x + y^2 + z - 1, \ x + y + z^2 - 1 \)

Groebner basis is

\[
\begin{align*}
g_1 &= x + y + z^2 - 1 \\
g_2 &= y^2 - y - z^2 + z \\
g_3 &= 2yz^2 + z^4 - z^2 \\
g_4 &= z^6 - 4z^4 + 4z^3 - z^2
\end{align*}
\]

so we have

\[
I_1 = I \cap \mathbb{K}[y, z] = \text{ideal}\{g_2, g_3, g_4\}
\]

\[
I_2 = I \cap \mathbb{K}[z] = \text{ideal}\{g_4\}
\]

\[\text{\textbullet\quad} I_{n-1} \text{ is always principal}\]

\[\text{\textbullet\quad} \text{any polynomial in } I \text{ which does not contain } x, y \text{ is a multiple of } g_4\]
geometric interpretation

In parametrization or elimination, we are interested in

\[ \left\{ (x_{k+1}, \ldots, x_n) \mid \text{there exists } x_1, \ldots, x_k \text{ such that } x \in \mathcal{V}\{f_1, \ldots, f_m\} \right\} \]

this is the projection of \( \mathcal{V}(f_1, \ldots, f_m) \) onto \( x_1 = 0, \ldots, x_k = 0 \)

denote the projection map by

\[ P_k : \mathbb{R}^n \to \mathbb{R}^{n-k} \]

\[ x \mapsto (0, \ldots, 0, x_{k+1}, \ldots, x_n) \]

we have

\[ P_k \mathcal{V}(I) \subset \mathcal{V}(I_k) \]
projection

suppose $I$ is an ideal, and $I_k$ is the $k$'th elimination ideal; then

$$P_k\mathcal{V}(I) \subset \mathcal{V}(I_k)$$

because if $f \in I_k$ then $f(x) = 0$ for all $x \in \mathcal{V}(I)$

but since $f$ doesn't depend on $x_1, \ldots, x_k$,

$$f(P_kx) = 0 \quad \text{for all} \quad x \in \mathcal{V}(I)$$

which means

$$f(y) = 0 \quad \text{for all} \quad y \in P_k\mathcal{V}(I)$$