Advanced Robotics

Lecture 5
ALGEBRAIC EQUATIONS
2000-1600 BC:

Old Babylonian Mathematics was able to solve quadratic equations

\[ x^2 + b \cdot x = c \]

with positive \( c \) using the formula

\[ x = -\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + c} \]

and some simpler cubic equations, e.g.

\[ x^3 + x^2 = c \]
The word algebra is derived from operations described in the treatise written by the Persian mathematician Muhammad ibn Musa al-Kwarizmi titled Al-Kitab al-Jabr wa-l-Muqabala (meaning “The Compendious Book on Calculation by Completion and Balancing”) on the systematic solution of linear and quadratic equations.
1608, Petrus Roth:

“A polynomial equation of degree $n$ (with real coefficients) may have $n$ solutions”

1806, Jean-Robert Argand:

A rigorous proof of the Fundamental Theorem of Algebra:

*Every complex polynomial $p(z)$ in one variable and of degree $n \geq 1$ has some complex root.*
1799 Paolo Ruffini,
1824 Niels Henrik Abel,
1832 Évariste Galois:

“Abel–Rufini Impossibility Theorem”

The solution of fifth degree algebraic equations cannot in all cases be expressed by starting with the coefficients and using only finitely many of the operations of addition, subtraction, multiplication, division and root extraction.

An example: \[ x^5 - x + 1 = 0 \]
1888, David Hilbert: “Finitness theorem”

Every ideal has a finite generating set
1964, Heisuke Hironaka: “Standard basis”  
1965, Bruno Buchberger: “Gröbner basis”

→ an algorithm for solving systems polynomial equations

**Algorithm:**

\[ \{ f_1, \ldots, f_s \} \text{ polynomials in } k[x_1, \ldots, x_n] \]

**Input:** \( F = (f_1, \ldots, f_s) \) \hspace{1cm} **Output:** a Groebner basis \( G = (g_1, \ldots, g_t) \)

\( G_1 := F \)

**Repeat**

**Until** \( G = G' \)

\( G' := G \)

**For** each pair \( (p, q) \in \{1, \ldots, s\}^2 \), \( p \neq q \) **Do**

\( S = \sum (p, q) G' \)

**If** \( S \neq 0 \) **Then** \( G := G \cup S \setminus \{ \} \)

**Until** \( G = G' \)
One algebraic equation in one variable
SOLVING 1 ALGEBRAIC EQUATION

1 equation, 1 variable $\rightarrow$ companion matrix $\rightarrow$ eigenvalues

$f(x) = x^3 + 4x^2 + x - 6 = -6 + 1x + 4x^2 + 1x^3$

$$M_x = \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -1 \\ 0 & 1 & -4 \end{bmatrix}$$

... a simple rule

$$>> e = \text{eig}(M_x)$$

$$e = \begin{bmatrix} 1 \\ -2 \\ -3 \end{bmatrix} \quad x_1 = 1, \ x_2 = -2, \ x_3 = -3$$

It works when eig works, i.e. order 100 in Matlab is often OK.
SOLVING 1 ALGEBRAIC EQUATION

Linear mapping \( M \in \mathbb{R}^{n\times n} \)

Eigenvalues \( Mx = \lambda x \)

\[ Mx - \lambda x = 0 \]

\[ (M - \lambda I)x = 0 \]

\( x \neq 0 \) \( \Rightarrow \) rank\((M - \lambda I)\) < \( n \)

\[ \det(M - \lambda I) = 0 \]
SOLVING 1 ALGEBRAIC EQUATION

algebraic equation

\[ f(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = \det(-M + x I) \]

\[ -M + x I = \begin{bmatrix} x & & a_0 \\ -1 & x & \\ & -1 & x \\ & & -1 & x + a_3 \end{bmatrix} \]

\[ f(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \]
Polynomials in one variable

**Leading term:** a non-zero polynomial

\[ f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0 \quad \in k[x] \]

\[ a_m \neq 0 \quad \text{LT}(f) = a_m x^m = \text{the leading term} \]

**Example:**

\[ f = 2x^3 - 4x + 3 \quad \Rightarrow \quad \text{LT}(f) = 2x^3 \]
Division of terms

\[ \alpha, \beta \in \mathbb{Z}_{\geq 0}^n, \ a_\alpha \cdot b_\beta \in k, \ x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in k[x_1, \ldots, x_n] \text{ monomials} \]

\[ a_\alpha x^\alpha \text{ divides } b_\beta x^\beta \overset{\text{def}}{=} \beta_i - \alpha_i \geq 0, \quad i = 1, \ldots, n \]

If \( a_\alpha x^\alpha \text{ divides } b_\beta x^\beta \), then there is exactly one monomial

\[ c_\gamma x^\gamma = \frac{b_\beta}{a_\alpha} \cdot x^{\beta - \alpha} \]

such that \( b_\beta x^\beta = a_\alpha x^\alpha \cdot c_\gamma x^\gamma \)
"Division" of polynomials in one variable

Polynomials cannot be divided but can be "divided"

\[
f : g \quad \text{def} \quad f = qg + r, \quad r = 0 \lor \deg(r) < \deg(g)
\]

Example \( f = 2x^3 - 4x + 3 \mid g(x) = x - 1 \)

\[
f : g \equiv 2x^3 - 4x + 3 = 2x^2(x - 1) + 2x^2 - 4x + 3 = (2x^2 + 2x)(x - 1) - 2x + 3 = (2x^2 + 2x - 2)(x - 1) + 1
\]

Notice that: \( \deg(f) = \deg(\text{LT}(f)) \)

\( \text{LT}(g) \) divides \( \text{LT}(f) \) \( \iff \) \( \deg(\text{LT}(g)) \leq \deg(\text{LT}(f)) \) \( \iff \) \( \deg(g) \leq \deg(f) \)

\( \text{LT}(g) \) divides \( \text{LT}(f) \) \( \iff \) \( \deg(g) \leq \deg(f) \)
Let $k$ be a field and $g$ be a non-zero polynomial in $k[x]$.

(i) Then every $f \in k[x]$ can be written as

$$f = qg + r$$

where $q, r \in k[x]$, and either

$$r = 0 \text{ or } \deg(r) < \deg(g)$$

(ii) Furthermore, $q$ and $r$ are unique.
Proof: "Division algorithm"

Input: \( g, f \)
Output: \( q, r \)

\( q := 0 \)
\( r := f \)

WHILE \( r \neq 0 \) AND \( \text{LT}(g) \) divides \( \text{LT}(r) \) DO

\[
q := q + \frac{\text{LT}(r)}{\text{LT}(g)}
\]

\[
r := r - \frac{\text{LT}(r)}{\text{LT}(g)} \cdot g
\]

END
Observe that \( f = q \cdot g + r \) holds true.

(a) \( q = 0 \) \& \( r = f \) \( \Rightarrow \) \( 0 \cdot g + f = f \)

(b) Let \( q_i, r_i \) be such that \( f = q_i \cdot g + r_i \), then

\[
q_{i+1} \cdot g + r_{i+1} = \left( q_i + \frac{\text{LT}(r_i)}{\text{LT}(g)} \right) g + \left( r_i - \frac{\text{LT}(r_i)}{\text{LT}(g)} \cdot g \right) = q_{i+1} \cdot g + r_{i+1} = f
\]

If the algorithm terminates, then either

\( r = 0 \) or

\( \text{LT}(g) \) does not divide \( \text{LT}(r) \) \( \iff \) \( \text{deg}(r) < \text{deg}(g) \)
Let us show that the algorithm terminates.

Assume that the algorithm does not terminate. Then, $\text{LT}(g)$ divides $\text{LT}(r)$ and $r \neq 0$.

Observe that for

$$ r_{i+1} = r_i - \frac{\text{LT}(r_i)}{\text{LT}(g)} \cdot g $$

either

$$ r_{i+1} = 0 $$

or

$$ \deg(r_{i+1}) < \deg(r_i) $$

Write

$$ r_i = a_0 x^m + a_1 x^{m-1} + \ldots + a_m $$

with $m \geq \ell$

and

$$ g = b_0 x^\ell + b_2 x^{\ell-1} + \ldots + b_\ell $$

($\text{LT}(g)$ divides $\text{LT}(r_i)$)
\[ r_{i+1} = r_i - \frac{\text{LT}(r_i)}{\text{LT}(p_i)} \cdot g = (a_0 x^m + a_1 x^{m-1} + \ldots) - \frac{a_o}{b_o} x^{m-1} (b_0 x^e + b_1 x^{e-1} + \ldots) \]

\[ = (a_1 x^{m-1} + \ldots) - \left(\frac{a_o}{b_o} b_1 x^{m-1} + \ldots\right) \]

\[ = (a_1 - \frac{a_o}{b_o} b_1) x^{m-1} + (a_2 - \frac{a_o}{b_o} b_2) x^{m-2} + \ldots \]

and therefore we see that

either \( r_{i+1} = 0 \) if all coefficients vanish

or \( \deg(r_{i+1}) \leq m-1 < m = \deg(r_i) \)
Monomial ordering

Monomials in one variable are easy to order by their degree, i.e.

\[ x^0 <_{\text{deg}} x^1 <_{\text{deg}} x^2 <_{\text{deg}} \ldots \]

Also notice that \( x^m \prec_{\text{deg}} x^n \iff x^m \text{ divides } x^n \)

Not so simple with more variables

Consider \( xy^2 \prec x^2y \ldots \) neither one divides the other but

\[ \deg(xy^2) = 1+2 = 3 = 2+1 = \deg(x^2y) \]
A monomial ordering on \( k[x_1, \ldots, x_n] \) is any ordering relation \( < \) on \( \mathbb{Z}_{\geq 0}^n \) satisfying:

(i) \( \forall \alpha, \beta : \alpha > \beta \) or \( \alpha < \beta \)

(ii) \( \alpha > \beta \) \& \( \gamma \in \mathbb{Z}_{\geq 0} \) \( \Rightarrow \alpha + \gamma > \beta + \gamma \)

(iii) \( \forall \alpha : \alpha > 0 \)

we write \( x^\alpha > x^\beta \) def \( \alpha > \beta \)
Lexicographic order

\[ \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m), \quad \beta = (\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{Z}_{\geq 0}^m \]

\[ \lambda \prec \beta \quad \text{if the left-most non-zero element of} \]

\[ \lambda - \beta \quad \text{is positive or} \quad \lambda - \beta = 0. \]

Examples

\[ (1, 2, 0) \prec \lambda (0, 3, 4) \leq (1, -1, -4) \]

\[ (3, 2, 4) \prec \lambda (3, 2, 1) \leq (0, 1, 3) \]

Behold!

\[ \begin{array}{c}
X_1 X_2 X_3 \xrightarrow{\text{rename}} X_3 X_2 X_1 \\
\end{array} \]

There is \( m! \) lex orders

\[ (1, 0, 1) \succ (0, 1, 1) \succ (0, 1, 0) \]

\[ \begin{array}{c}
X_1 X_2 X_3 \xrightarrow{\text{rename}} X_3 X_2 X_1 \\
\end{array} \]

\[ (1, 0, 1) \succ (0, 1, 1) \succ (0, 1, 0) \]

\[ \begin{array}{c}
X_3 X_2 X_1 \xrightarrow{\text{rename}} X_1 X_2 X_3 \\
\end{array} \]
The lex ordering on $\mathbb{Z}_2^n$ is a monomial ordering

$\prec_{\text{lex}}$ is an ordering ($a \succ b \iff a \succ b_1$)

(a) $\alpha - \beta = 0 \Rightarrow \alpha \succ_{\text{lex}} \beta$

$\exists i, j \in \mathbb{Z}_{\geq 0}$ such that $(\alpha - \beta)_k = 0$ and $(\beta - \gamma)_m = 0$ for $k < i, m < j$

(b) $\alpha \succ_{\text{lex}} \beta, \beta \succ_{\text{lex}} \gamma \iff (\alpha - \beta)_i > 0 \& (\beta - \gamma)_j > 0$

$\ (\alpha - \beta)_k = 0 \ \ \ \ k = 1, \ldots, \min (i, j) - 1 \quad \alpha_k = \beta_k = \gamma_k$

$\ (\alpha - \beta)_{\min (i, j)} > 0 \quad \left\{ \begin{array}{l}
\min (i, j) = i \quad \alpha_i \geq \beta_i = \gamma_i \\
\min (i, j) = j \quad \alpha_j \geq \beta_j \geq \gamma_j
\end{array} \right.$

$\Rightarrow \alpha \succ_{\text{lex}} \gamma$

(c) $\alpha \succ_{\text{lex}} \beta \& \beta \succ_{\text{lex}} \alpha \Rightarrow \{\begin{array}{l}
either \alpha - \beta = 0 \\
\exists i \in \mathbb{Z}_{\geq 0} \quad ((\alpha - \beta)_i > 0 \& (\beta - \alpha)_i > 0)
\end{array}\} \Rightarrow \alpha - \beta = 0$
The lex ordering is a monomial ordering

(i) \( \nabla \alpha, \beta : \alpha \preceq \beta \text{ or } \beta \preceq \alpha : \)

\[ c = \alpha - \beta = 0 \Rightarrow \alpha = \beta \text{ or there is the first non-zero element } c_i \]

If \( c_i > 0 \), then \( \alpha > \beta, \beta \preceq \alpha \text{ otherwise.} \)

(ii) \( \alpha \preceq \beta \text{ and } \gamma \in \mathbb{Z}_{\geq 0}^m \Rightarrow \alpha + \gamma \preceq \beta + \gamma \)

\[ \alpha + \gamma - (\beta + \gamma) = \alpha - \beta \]

(iii) \( \forall \alpha : \alpha > 0 \)

\[ (\alpha - 0)_i \geq 0 \]
A non-zero $f = \sum_{\alpha} a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ has a monomial ordering $>$. 

**Multidegree** of $f$ \( \text{multideg}(f) = \max \{ \alpha \in \mathbb{Z}_{\geq 0}^n \mid a_\alpha \neq 0 \} \)

**Leading term** \( \rightarrow \text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f) \)

- Leading coefficient \( \text{LC}(f) = a_{\text{multideg}(f)} \)
- Leading monomial \( \text{LM}(f) = x^{\text{multideg}(f)} \)

**Example:**

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

\[ = 4x^{(1,2,1)} + 4x^{(0,0,2)} - 5x^{(3,0,0)} + 7x^{(2,1,2)} \]

\( \text{multideg}(f) = (3,0,0) \)

\( \text{LC}(f) = -5 \)

\( \text{LM}(f) = x^3 \)

\( \text{LT}(f) = -5x^3 \)
Polynomial division with more divisors in more variables
"Division" by more than one polynomial

\[ f = 3x^4 - x^2 + 2x \quad | \quad f_1 = x - 1 \quad | \quad f_2 = x^2 + 1 \]

\[ f = 3(x-1) = 0 \cdot (x^2 + 1) + 3x^4 - x^2 + 2x + 0 \]

\[ = 3x^3(x-1) = 0 \cdot (x^2 + 1) + 3x^3 - x^2 + 2x + 0 \]

\[ = (3x^3 + 3x^2)(x-1) + 0 \cdot (x^2 + 1) + 2x^2 + 2x + 0 \]

\[ = (3x^3 + 3x^2 + 2x)(x-1) + 0 \cdot (x^2 + 1) + 4x + 0 \]

\[ = (3x^3 + 3x^2 + 2x + 4)(x-1) + 0 \cdot (x^2 + 1) + 4 \]

\[ = 3x(x^2 + 1) + 0 \cdot (x-1) - x^2 - x + 0 \]

\[ = (3x - 1)(x^2 + 1) + 0 \cdot (x - 1) - x + 1 + 0 \]

\[ = (3x - 1)(x^2 + 1) - 1 \cdot (x - 1) + 0 \]

We see that \( f : (f_1, f_2) \neq f : (f_2, f_1) \Rightarrow f : E_{f_1, f_2} \) not well-defined.
"Division theorem" for more than one divisor in $k[x_1, \ldots, x_n]$

Let $>$ be a monomial order on $\mathbb{Z}^m_+$ and $F = (f_1, \ldots, f_s)$ an ordered $s$-tuple, $f_i \in k[x_1, \ldots, x_n]$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

$a_i, r \in k[x_1, \ldots, x_n]$ and either

$r = 0$ or none of the monomials of $r$ is divisible by any of $\text{LT}(f_1), \ldots, \text{LT}(f_s)$.

Furthermore

$$a_i f_i \neq 0 \Rightarrow \text{multideg}(f) \geq \text{multideg}(a_i f_i)$$

$r \equiv \text{remainder of } f \text{ on division by } F \ldots \ r = \frac{f}{F}$

with the notation $F = (f_1, \ldots, f_s)$
"Division algorithm" for more than one divisor in $k[x_1, \ldots, x_m]$

Input: $F = (f_1, \ldots, f_s)$, $f$ 
Output: $a_1, \ldots, a_s$, $r \equiv \overline{F}$  

$a_1 = a_2 = \cdots = a_s = r := 0$, $p := f$

WHILE $p \neq 0$ DO

\[ i := 1 \]

\[ \text{divisionoccurred} := \text{FALSE} \]

WHILE $i \leq s$ AND \text{divisionoccurred} = \text{FALSE} DO

\[ \text{IF } \text{LT}(f_i) \text{ divides } \text{LT}(p) \text{ THEN} \]

\[ a_i := a_i + \frac{\text{LT}(p)}{\text{LT}(f_i)} \]

\[ p := p - \frac{\text{LT}(p)}{\text{LT}(f_i)} \cdot f_i \]

\[ \text{divisionoccurred} := \text{TRUE} \]

ELSE \[ i := i + 1 \]

IF \text{divisionoccurred} = \text{FALSE} THEN

\[ r := r + \text{LT}(p) \]

\[ p := p - \text{LT}(p) \]

Proof as for 1 variable degree \rightarrow multidegree

$r \rightarrow p$
Example

\[ x \geq 0, \quad y \geq 0 \]

\[ f = xy^2 + x + 1, \quad f_1 = xy + 1, \quad f_2 = y + 1 \]

\[
\begin{array}{cccc}
(1,2) & (1,0) & (0,0) & \\
\downarrow & \downarrow & \downarrow & \\
(1,1) & (0,1) & (0,0) & \\
\end{array}
\]

\[ f = y(x+1) + x - y + 1 = y(xy+1) - 1(y+1) + \frac{x+2}{r} \]

\[
\begin{array}{cccc}
(1,0) & (0,1) & (0,0) & \\
\downarrow & \downarrow & \downarrow & \\
(1,0) & (0,1) & (0,0) & \\
\end{array}
\]

\[ f = 0 \cdot f_1 + 0 \cdot f_2 + xy^2 + x + 1 + 0 \]

\[ = y \cdot f_1 + 0 \cdot f_2 + x - y + 1 + 0 \]

\[ = y \cdot f_1 + 0 \cdot f_2 - y + 1 + x \]

\[ = y \cdot f_1 - 1 \cdot f_2 + 2 + x \]

\[ = y \cdot f_1 - 1 \cdot f_2 + x + 2 \]
Example:

\[ f = xy^2 - x \quad f_1 = xy + 1 \quad f_2 = y^2 - 1 \]

\[ x \geq y \quad \forall x \geq y \]

\( a \) \quad f : (f_1 \mid f_2)

\[ xy^2 - x = y \cdot (xy + 1) + o \cdot (y^2 - 1) + o \cdot (-x - y) \]

\( b \) \quad f : (f_2 \mid f_1)

\[ xy^2 - x = x \cdot (y^2 - 1) + o \cdot (xy + 1) + o \]

The order of polynomials in F matters
Affine varieties

\[ f_k(x_1, x_2, \ldots, x_n) \ldots \text{algebraic equations} \]

Algebraic variety = the set of points for which all equations \( f_k \) are satisfied

\[ V = \{ (x_1, x_2, \ldots, x_n) \mid f_k(x_1, x_2, \ldots, x_n) = 0, \ k = 1, 2, \ldots, n \} \]

Examples:

\[ \begin{align*}
\{ x^2 + y^2 = 2 \} \\
\{ x^2 + y^2 = 0 \} \\
\{ x^2 = 1 \} \\
\{ x^2 + y^2 = 1, \ x y = 1 \}
\end{align*} \]
For solving IKU, we are interested in situations when there is a finite number of solutions \( \equiv \) finite affine varieties

Notice that:

1. \( f(a_1, a_2, \ldots, a_m) = 0 \) \& \( g \in k[x_1, x_2, \ldots, x_m] \Rightarrow (f \cdot g)(a_1, a_2, \ldots, a_m) = 0 \)

2. \( f(a_1, a_2, \ldots, a_m) = 0 \) \& \( g(a_1, a_2, \ldots, a_m) = 0 \Rightarrow (f + g)(a_1, a_2, \ldots, a_m) = 0 \)

\( \Rightarrow \) there is an infinite number of different sets of algebraic equations defining the same variety.

New "true" equations can be generated by algebraic operations with polynomials.
Ideal generated by polynomials

**Ideal:** A subset $I \subseteq k[x_1, x_2, \ldots, x_n]$ is an ideal if it satisfies:

(i) $0 \in I$

(ii) $f, g \in I \Rightarrow f + g \in I$

(iii) $f \in I$ & $h \in k[x_1, x_2, \ldots, x_n] \Rightarrow h \cdot f \in I$

All polynomials
Ideal generated by a variety

Theorem: Let $V$ be an affine variety. Then

$$I(V) = \{ f \in k[x_1, \ldots, x_n] | f(x) = 0, \forall x \in V \}$$

is an ideal.

Proof:

(i) $0(x) = 0$

(ii) $f, g \in I \Rightarrow f + g \in I$

(iii) $f \in I \& h \in k[x_1, x_2, \ldots, x_n] \Rightarrow h \cdot f \in I$

$f(x) = 0 \& g(x) = 0$

$\Rightarrow (f + g)(x) = f(x) + g(x) = 0 + 0 = 0$

$f(x) = 0$

$\Rightarrow (f \cdot h)(x) = f(x) \cdot h(x) = 0 \cdot h(x) = 0$
Ideal generated by polynomials and by the corresponding variety

\[ \{f_1, f_2, \ldots, f_s^3 \} \rightarrow \mathcal{V}(\{f_1, f_2, \ldots, f_s^3 \}) \]

\[ \mathcal{I}(\{f_1, f_2, \ldots, f_s^3 \}) \subset \mathcal{I}(\mathcal{V}) \]

The ideal generated by polynomials \( \{f_1, f_2, \ldots, f_s^3 \} \)

The ideal generated by variety \( \mathcal{V} \)
Example

\[ \mathfrak{I}(x^2, y^2) \rightarrow \mathfrak{V}(x^2, y^2) \]

\[ \mathfrak{I}(x^2, y^2) \subseteq \mathfrak{I}(\mathfrak{V}(x^2, y^2)) \]

\[ \mathfrak{V}(x^2, y^2) = \mathfrak{I}(0, 0)^3 \]

\[ \mathfrak{I}(\mathfrak{V}(x^2, y^2)) = \mathfrak{I}(x, y)^3 \]

\[ \mathfrak{I}(x^2, y^2) \subset \mathfrak{I}(x, y)^3 \]

because \( x_1 y \in \mathfrak{I}(x, y)^3 \) but \( x_1 y \notin \mathfrak{I}(x^2, y^2) \)

as every \( \partial \left( h_1(x_1 y) x^2 + h_2(x_1 y) y^2 \right) \) has total degree at least two
the affine variety defined by \( \{f_1, f_2, \ldots, f_5\} \)

\[ V(\{f_1, f_2, \ldots, f_5\}) \]

\[ I(\{f_1, f_2, \ldots, f_5\}) = \text{all polynomials that can be "algebraically" generated from } \{f_1, f_2, \ldots, f_5\} \]

\[ I(V) = \text{all polynomials that are } 0 \text{ on all points of } V \]
Groebner basis is a special basis of the Ideal

Basis: $B = \{f_1, f_2, \ldots, f_s\}$

Algebraic manipulation

Groebner basis w.r.t. $<_{lex}$:
$G = \{g_1, g_2, \ldots, g_n\}$

The affine variety defined by $\{f_1, f_2, \ldots, f_s\}$

$I(V)$ contains all polynomials that are $= 0$ on all points of $V$

$k[x_1, \ldots, x_n]$ all polynomials
Theorem 3: Let $G$ be a Groebner basis constructed by the Buchberger algorithm w.r.t. $x_1, x_2, \ldots, x_n$ from polynomials $\{f_1, \ldots, f_s\} \subseteq \mathbb{C}[x_1, \ldots, x_n]$ for which equations $\partial f_i = 0$ have a finite number of solutions. Then $G$ contains a polynomial $g \in \mathbb{C}[x_n]$.

There is often even more:

$G$ often consists of a set of polynomials

$g_n(x_n)$

$g_{n-1}(x_n, x_{n-1})$

$g_{n-2}(x_n, x_{n-1}, x_{n-2})$

$\vdots$

$g_1(x_n, x_{n-1}, x_{n-2}, \ldots, x_1)$
A working definition of a

Groebner basis (of an ideal)

(A basis) $G_1 = (g_1, \ldots, g_t)$ (of an ideal $I$) is a Groebner basis

if the remainder on division of $f \in k[x_1, \ldots, x_n]$ by $G_1$ does not depend on the ordering of $g_i$ in $G_1$.

\textbf{Beware!} Only \( r \) is unique - \( a_i \)'s need not be unique.
Least common multiple of monomials

Let \( x^\alpha, x^\beta \in k[x_1, \ldots, x_m] \) be monomials, then \( x^\gamma \) with

\[
\gamma_i = \max(\alpha_i, \beta_i), \quad i = 1, \ldots, m
\]

is the least common multiple \( \text{LCM}(x^\alpha, x^\beta) \) of \( x^\alpha, x^\beta \)

**Example:**

\[
x^\alpha = x y^3 z^2, \quad x^\beta = y z^6
\]

\[
\alpha = (1, 3, 2), \quad \beta = (0, 1, 6)
\]

\[
\gamma = \max((1, 3, 2), (0, 1, 6)) = (1, 3, 6)
\]

\[
x^\gamma = x y^3 z^6
\]
The S-polynomial (designed to cancel the leading terms)

The S-polynomial of \( f, g \in k[x_1, \ldots, x_n] \) is the (algebraic) combination

\[
S(f, g) = \frac{\text{LCM}(\text{LT}(f), \text{LT}(g))}{\text{LT}(f)} \cdot f - \frac{\text{LCM}(\text{LT}(f), \text{LT}(g))}{\text{LT}(g)} \cdot g
\]

Example:

\[
f = x^3y^2 - x^2y^3 + x \quad g = 3x^4y + y^2 \in R[x_1, y]
\]

with \( x > \leq y \)

\[
S(f, g) = \frac{\text{LCM}(x^3y^2, x^4y)}{x^3y^2} \cdot f - \frac{\text{LCM}(x^3y^2, x^4y)}{3x^4y} \cdot g = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g
\]

\[
= x \cdot f - \frac{4}{3} y \cdot g = x^4y^2 - x^3y^3 + x^2 - x^4y^2 - \frac{4}{3} y^3 = -x^3y^3 + x^2 - \frac{1}{3} y^3
\]

\[\underline{\text{cancel}}\]
Characterization of Groebner bases in terms of S-polynomials

A set $G = \{ g_1, \ldots, g \}$ of polynomials in $k[x_1, \ldots, x_n]$ is a Groebner basis if for all $i, j \in 1, \ldots, t$, $i \neq j$, the remainder on division of $S(g_i, g_j)$ by $G$ (with arbitrary but fixed order of $g_k$) is zero.

Algorithm:

\{ $f_1, \ldots, f_s$ \} polynomials in $k[x_1, \ldots, x_n]$

Input: $F = (f_1, \ldots, f_s)$ \hspace{1cm} Output: a Groebner basis $G = (g_1, \ldots, g_t)$

$G_1 := F$

REPEAT

\$ G' := G \$

FOR each pair $(p, q) \in G'$, $p \neq q$ DO

\$ S = S(p, q)^G' \$

IF $S \neq 0$ THEN $G := G \cup \{ S \}$

UNTIL $G = G'$


Example: \( k \in \mathbb{R} \), \( x > 0 \), \( y \)

\[ F = (f_1, f_2) = (x^3 - 2xy, x^2y - 2y^2 + x) \]

\( F \) is not GB: 

\[
S(f_1, f_2) = \frac{x^3}{x^2} f_1 - \frac{x^2 y}{x^2} f_2 = y f_1 - x f_2 = -2xy^2 + 2y^2 - x^2 = -x^2
\]

and \( S(f_1, f_2) \neq 0 \)

\[ G_1 = F \cup \mathbb{R} \cdot x^2 \cdot 3 = (f_1, f_2, x^2) \]

\[
S(f_1, x^2) = \frac{x^3}{x^3} f_1 - \frac{x^2 y}{x^2} x^2 = -2xy, \quad S(f_1, x^2) G_1 = -2xy
\]

\[
S(f_2, x^2) = \frac{x^2 y}{x^2 y} f_2 - \frac{x^2 y}{x^2 y} x^2 = -2y^2 + x, \quad S(f_2, x^2) G_1 = -2y^2 + x
\]

\[ G_2 = (f_1, f_2, x^2, -2xy, x, -2y^2) = (f_1, f_2, f_3, f_4, f_5) \]

\[
S(f_1, f_4) = \frac{x^3 y}{x^3} f_1 - \frac{x^3 y}{2xy} f_4 = -2xy^2, \quad S(f_1, f_4) G_2 = 0
\]

\[
S(f_2, f_4) = \frac{x^2 y}{x^2 y} f_2 - \frac{x^2 y}{-2xy} f_4 = x - 2y^2, \quad S(f_2, f_4) G_2 = 0
\]

\[
S(f_4, f_5) = \frac{xy}{-2xy} f_4 - \frac{xy}{x} f_5 = 3y^3, \quad S(f_4, f_5) G_2 = 3y^3
\]
\[ G_3 = (x^3 - 2xy, x^2y - 2y^2 + x, -x^2 - 2xy, x - 2y^2, 3y^3) \]

\[
\begin{align*}
  f_1 &= -x f_3 + f_4 \\
  f_2 &= -y f_3 + f_5 \\
  f_3 &= -x f_5 + y f_4 \\
  f_4 &= -2y f_5 - \frac{4}{3} f_6
\end{align*}
\]

\[ G_4 = (x - 2y^2, 3y^3) \]

\[ S(f_5, f_6) = \frac{xy^3}{x} f_5 - \frac{xy^3}{3y^3} f_6 = -2y^5 \]

\[ -2y^5 G_4 = 0 \]

Therefore, \( G_3 \) is a Groebner basis. It contains \( f_1 \) and \( f_2 \).

\( G_4 \) is also a Groebner basis. It generates the same ideal as \( G_3 \).
Click to start

IRO-2007-Solving-by-GB.mws

Click to start