Division Algorithms and Term Orderings for Symbolic Computation

Motivating Gröbner Bases and their computation

Priyank Kalla

Associate Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
`http://www.ece.utah.edu/~kalla`

Lectures: Sep 29 - Oct 1, 2014

Agenda:

- Wish to build a polynomial algebra model for hardware
- Modulo arithmetic model is versatile: can represent both *bit-level* and *word-level* constraints
- To build the algebraic/modulo arithmetic model:
  - Rings, Fields, Modulo arithmetic
  - Polynomials, Polynomial functions, Polynomial Rings
  - Ideals, Varieties, Symbolic Computing and Gröbner Bases
  - Decision procedures in verification

- Ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq R = \mathbb{F}[x_1, \ldots, x_d]$ generated by any set of polynomials $f_1, \ldots, f_s$
- $J = \langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} f_i \cdot h_i \ : \ h_i \in R\}$
- Many ideal generators: $J = \langle f_1, \ldots, f_s \rangle = \cdots = \langle g_1, \ldots, g_t \rangle$
  - Given: $F = \{f_1, \ldots, f_s\} \in R$
  - Gröbner basis: $G = \{g_1, \ldots, g_t\}$ a canonical representation of ideal $J = \langle F \rangle = \langle G \rangle$
  - Buchberger's algorithm computes a Gröbner basis, which we will study soon
- Variety: the set of all solutions to $f_1 = \cdots = f_s = 0$
- Variety depends on the ideal J, not just on $f_1, \ldots, f_s$
- $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t) = V(J)$

Some facts about ideals and varieties

- When ideal $J = \langle 1 \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, then $J = F[x_1, \ldots, x_d]$
- $J = \langle 1 \rangle \iff V(J) = \emptyset$; as the polynomial $1 = 0$ has no solutions
- Variety: Set of ALL solutions to a given system of polynomial equations: $V(f_1, \ldots, f_s)$
  - $V(x^2 + y^2 - 1) = \{\textit{all points on circle} : x^2 + y^2 - 1 = 0\}$
  - $V_{\mathbb{R}}(x^2 + 1) = \emptyset$;
  - $V_{\mathbb{C}}(x^2 + 1) = \{(\pm i)\}$
- Important to analyze variety over a specific field ($V_{\mathbb{R}}$ versus $V_{\mathbb{C}}$)
- Modern algebraic geometry does not explicitly solve for the varieties. Rather, it reasons about the Variety by analyzing the Ideals!
  - Solving for varieties is extremely hard
  - Reasoning about their presence, absence, union/intersection is easier
  - We need to do the same for hardware verification

Formally define a variety

- Let $R = \mathbb{F}[x_1, \ldots, x_d]$ be a ring, $f \in R$ be a polynomial and $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{F}^d$ be a point
- We say that f vanishes on $\mathbf{a}$ when $f(\mathbf{a}) = 0$

Definition

For any ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, the *affine variety* of J over $\mathbb{F}$ is:

$$V(J) = \{\mathbf{a} \in \mathbb{F}^d : \forall f \in J, f(\mathbf{a}) = 0\}.$$

Algebraically Closed Fields (ACFs)

- A field $\overline{\mathbb{F}}$ is algebraically closed, when every non-constant univariate polynomial $f \in \overline{\mathbb{F}}[x]$ has a root in $\overline{\mathbb{F}}$
- Every field is either algebraically closed, or it is contained in an algebraically closed one
- Algebraically closed fields are infinite fields
- Only over algebraically closed fields can one reason (unambiguously) about presence or absence of solutions (varieties)
    - Many famous mathematical results valid (only!) over ACFs
- Examples: $\mathbb{R}$ is not ACF as $V_{\mathbb{R}}(x^2 + 1) = \emptyset$;
- $\mathbb{C}$ is ACF; in fact $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ ($\mathbb{R} \subset \mathbb{C}$)
- Finite (Galois) fields are NOT ACF!
    - But every GF $\mathbb{F}_{p^k} \subset \overline{\mathbb{F}_{p^k}}$, where $\overline{\mathbb{F}_{p^k}}$ is the algebraic closure of $\mathbb{F}_{p^k}$
- So how will we reason about $V_{\mathbb{F}_{2^k}}(J)$? We will, using some funky Galois field results (Galois fields are awesome!)

- This is a good time to first think in terms of a canonical representation of ideals — i.e. a Gröbner Bases
- Recall:
- Given polynomials $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_d]$. Let $F = \{f_1, \ldots, f_s\}$ be the given set of polynomials
- Then ideal $J = \langle F \rangle \subset \mathbb{F}[x_1, \ldots, x_d]$
- Find another set of polynomials $G = \{g_1, \ldots, g_t\} \in \mathbb{F}[x_1, \ldots, x_d]$ such that:
  - $J = \langle F \rangle = \langle G \rangle$
  - $V(J) = V(\langle F \rangle) = V(\langle G \rangle)$
  - The set G has some nice properties that F does not have
  - The set G is called a Gröbner basis of ideal J

The power of Gröbner bases

- A Gröbner basis G can help us solve (unambiguously) many polynomial decision questions:

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Hilbert's Nullstellensatz: The polynomial SAT/UNSAT problem

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, is $V(J) = \emptyset$?

The polynomial #SAT problem

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq R = \mathbb{F}[x_1, \ldots, x_d]$, is $V(J)$ infinite or finite? If finite, then $|V(J)| = ?$ [i.e. how many solutions to $V(J)$?]

Elimination ideals: help in solving polynomial equations

Generalize triangularization to polynomial equations

A Gröbner basis example [From Cox/Little/O'Shea]

Solve the system of equations:

$$f_1 : x^2 - y - z - 1 = 0$$
$$f_2 : x - y^2 - z - 1 = 0$$
$$f_3 : x - y - z^2 - 1 = 0$$

Gröbner basis with lex term order $x > y > z$

$$g_1 : x - y - z^2 - 1 = 0$$
$$g_2 : y^2 - y - z^2 - z = 0$$
$$g_3 : 2yz^2 - z^4 - z^2 = 0$$
$$g_4 : z^6 - 4z^4 - 4z^3 - z^2 = 0$$

- Is $V(\langle G \rangle) = \emptyset$? No, because $G \neq \{1\}$
- G tells me that $V(\langle G \rangle)$ is finite!
- G is *triangular*: solve g_4 for z, then g_2, g_3 for y, and then g_1 for x

To start thinking in terms of Gröbner bases....

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?

To start thinking in terms of Gröbner bases....

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?
- Divide f by f_1, obtain quotient and remainder (q_1, r_1)

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?
- Divide f by f_1, obtain quotient and remainder (q_1, r_1)
- Then, divide r_1 by f_2, obtain (q_2, r_2)

To start thinking in terms of Gröbner bases....

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?
- Divide f by f_1, obtain quotient and remainder (q_1, r_1)
- Then, divide r_1 by f_2, obtain (q_2, r_2)
- If $r_2 = 0$, then $f = q_1 f_1 + q_2 f_2$, so $f \in \langle f_1, f_2 \rangle$.

Ideal Membership Testing

Given ideal $J = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{F}[x_1, \dots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?
- Divide f by f_1, obtain quotient and remainder (q_1, r_1)
- Then, divide r_1 by f_2, obtain (q_2, r_2)
- If $r_2 = 0$, then $f = q_1 f_1 + q_2 f_2$, so $f \in \langle f_1, f_2 \rangle$.
- But, what if we divide f by f_2 first and then by f_1?

To start thinking in terms of Gröbner bases....

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?
- Divide f by f_1, obtain quotient and remainder (q_1, r_1)
- Then, divide r_1 by f_2, obtain (q_2, r_2)
- If $r_2 = 0$, then $f = q_1 f_1 + q_2 f_2$, so $f \in \langle f_1, f_2 \rangle$.
- But, what if we divide f by f_2 first and then by f_1?
- The culprits are: term ordering issues and the division algorithm

Ideal Membership Testing

Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$, and a polynomial f, is $f \in J$?

Can you think of an approach to decide ideal membership?

- Let $f = y^2x - x, \quad f_1 = yx - y, \quad f_2 = y^2 - x; \quad (y > x)$
- Is $f \in \langle f_1, f_2 \rangle$?
- Divide f by f_1, obtain quotient and remainder (q_1, r_1)
- Then, divide r_1 by f_2, obtain (q_2, r_2)
- If $r_2 = 0$, then $f = q_1 f_1 + q_2 f_2$, so $f \in \langle f_1, f_2 \rangle$.
- But, what if we divide f by f_2 first and then by f_1?
- The culprits are: term ordering issues and the division algorithm
- Let us study these in detail

The one variable case of $\mathbb{F}[x]$

- $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$
- The terms of f are ordered according to (descending) degrees
- $\deg(f) = n$ is the degree of f
- $lt(f) = a_n x^n$ is the leading term of f
- $lm(f) = x^n$ is the leading monomial of f [often also called the leading power of $f(lp(f))$]
- $lc(f) = a_n$ is the leading coefficient of f
- lt, lm, lc are the main tools of the division algorithm

Polynomial Long Division (say, in $\mathbb{Q}[x]$)

Divide f by g, get q, r s.t. $f = qg + r$, with $r = 0$ or $deg(r) < deg(g)$

Polynomial Long Division (say, in $\mathbb{Q}[x]$)

Divide f by g, get q, r s.t. $f = qg + r$, with $r = 0$ or $deg(r) < deg(g)$
Divide $f = x^3 - 2x^2 + 2x + 8$ by $g = 2x^2 + 3x + 1$

Polynomial Long Division (say, in $\mathbb{Q}[x]$)

Divide f by g, get q, r s.t. $f = qg + r$, with $r = 0$ or $deg(r) < deg(g)$
Divide $f = x^3 - 2x^2 + 2x + 8$ by $g = 2x^2 + 3x + 1$

$$
\begin{array}{r|rrrr}
\multicolumn{1}{r}{} & & & \frac{1}{2}x & -\frac{7}{4} \\ \cline{2-5}
2x^2+3x+1 & x^3 & -2x^2 & +2x & +8 \\
& -x^3 & -\frac{3}{2}x^2 & -\frac{1}{2}x & \\ \cline{2-4}
& & -\frac{7}{2}x^2 & +\frac{3}{2}x & +8 \\
& & \frac{7}{2}x^2 & +\frac{21}{4}x & +\frac{7}{4} \\ \cline{3-5}
& & & \frac{27}{4}x & +\frac{39}{4}
\end{array}
$$

Polynomial Long Division (say, in $\mathbb{Q}[x]$)

Divide f by g, get q, r s.t. $f = qg + r$, with $r = 0$ or $deg(r) < deg(g)$
Divide $f = x^3 - 2x^2 + 2x + 8$ by $g = 2x^2 + 3x + 1$

$$
\begin{array}{r|rrrr}
 & & & \frac{1}{2}x & -\frac{7}{4} \\
\hline
2x^2 + 3x + 1 & x^3 & -2x^2 & +2x & +8 \\
 & -x^3 & -\frac{3}{2}x^2 & -\frac{1}{2}x & \\
\hline
 & & -\frac{7}{2}x^2 & +\frac{3}{2}x & +8 \\
 & & \frac{7}{2}x^2 & +\frac{21}{4}x & +\frac{7}{4} \\
\hline
 & & & \frac{27}{4}x & +\frac{39}{4}
\end{array}
$$

- Multiply g by $\frac{1}{2}x$ and then compute: $r = f - \frac{1}{2}xg$
- The key step in division: $r = f - \frac{lt(f)}{lt(g)}g$
- One-step reduction of f by g to r: $f \xrightarrow{g} r$
- Repeatedly apply reduction: f reduces to g modulo r: $f \xrightarrow{g}_{+} r$

Inputs: $f, g \in \mathbb{F}[x], g \neq 0$
Outputs: q, r s.t. $f = qg + r$ with $r = 0$ or $deg(r) < deg(g)$

1: $q \leftarrow 0$; $r \leftarrow f$
2: **while** $(r \neq 0$ AND $deg(g) \leq deg(r))$ **do**
3: $\quad q \leftarrow q + \frac{lt(r)}{lt(g)}$
4: $\quad r \leftarrow r - \frac{lt(r)}{lt(g)} \cdot g$
5: **end while**
6: return q, r;

Algorithm 1: Univariate Division of f by g

Run the algorithm on the previous example
Does this algorithm run on $\mathbb{Z}_p[x]$ as is? Say, over $\mathbb{Z}_{11}[x]$ for the previous example? What about over $\mathbb{Z}_8[x]$?

- Remember: Division is modeled as cancellation of leading terms ($lt(f)$) by leading terms ($lt(g)$)
- For $r = f - \frac{lt(f)}{lt(g)} g = f - \frac{lc(f)}{lc(g)} \cdot \frac{lm(f)}{lm(g)} \cdot g$
- Requires computation of inverse of $lc(g)$
- This division algorithm works over fields $\mathbb{F} = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p, \mathbb{F}_{2^k}$, etc.
- This division algorithm does not always work over $\mathbb{Z}, \mathbb{Z}_n, n \neq p$.

Application to Ideal Membership Test

- Let $f = x$; $f_1 = x^2$; $f_2 = x^2 - x$ in $\mathbb{Q}[x]$

- Let $f = x; \quad f_1 = x^2; \quad f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?

Application to Ideal Membership Test

- Let $f = x$; $f_1 = x^2$; $f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?
- $f = f_1 - f_2$, so surely $f \in J$?

- Let $f = x$; $f_1 = x^2$; $f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?
- $f = f_1 - f_2$, so surely $f \in J$?
- $f \xrightarrow{f_1} f \xrightarrow{f_2} f \neq 0$

- Let $f = x$; $f_1 = x^2$; $f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?
- $f = f_1 - f_2$, so surely $f \in J$?
- $f \xrightarrow{f_1} f \xrightarrow{f_2} f \neq 0$
- $f \xrightarrow{f_2} f \xrightarrow{f_1} f \neq 0$

Application to Ideal Membership Test

- Let $f = x; \quad f_1 = x^2; \quad f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?
- $f = f_1 - f_2$, so surely $f \in J$?
- $f \xrightarrow{f_1} f \xrightarrow{f_2} f \neq 0$
- $f \xrightarrow{f_2} f \xrightarrow{f_1} f \neq 0$
- What's happening?

- Let $f = x$; $f_1 = x^2$; $f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?
- $f = f_1 - f_2$, so surely $f \in J$?
- $f \xrightarrow{f_1} f \xrightarrow{f_2} f \neq 0$
- $f \xrightarrow{f_2} f \xrightarrow{f_1} f \neq 0$
- What's happening?
- $F = \{f_1, f_2\}$ is not a Gröbner basis of J

Application to Ideal Membership Test

- Let $f = x$; $f_1 = x^2$; $f_2 = x^2 - x$ in $\mathbb{Q}[x]$
- Is $f \in J = \langle f_1, f_2 \rangle$?
- $f = f_1 - f_2$, so surely $f \in J$?
- $f \xrightarrow{f_1} f \xrightarrow{f_2} f \neq 0$
- $f \xrightarrow{f_2} f \xrightarrow{f_1} f \neq 0$
- What's happening?
- $F = \{f_1, f_2\}$ is not a Gröbner basis of J
- Cannot decide ideal membership without Gröbner basis!

Gröbner Bases over Univariate Polynomial Rings $\mathbb{F}[x]$

- When $\mathbb{F}$ is a field, Every ideal J of $\mathbb{F}[x]$ is generated by only one element (polynomial).
  - These rings $\mathbb{F}[x]$ are principal ideal domains (PID)
  - *E.g.* $\mathbb{Z}_p[x] =$ PID, but multivariate rings are not PIDs (*e.g* $\mathbb{Z}_p[x_1, x_2] \neq$ PID)
  - Ideal of vanishing polynomials is a good example: $\langle x^p - x \rangle$ versus $\langle x_1^p - x_1, x_2^p - x_2 \rangle$
- Gröbner Basis of $\{f_1, f_2\} = \text{GCD}(f_1, f_2)$
- Gröbner Basis of $\{f_1, \ldots, f_s\} = \text{GCD}(f_1, \text{GCD}(f_2, \ldots, f_s))$
- The Euclidean Algorithm computes the GCD of two polynomials
- The algorithm is given in any math textbook, and can also be found on wikipedia (Internet)
- Homework assignment for you..... Euclidean algorithm
- Univariate rings are of not much use in hardware verification

- Divide $f = y^2x + 4yx - 3x^2$ by $g = 2y + x + 1$

- Divide $f = y^2x + 4yx - 3x^2$ by $g = 2y + x + 1$
- Recall: Division is cancellation by leading terms

- Divide $f = y^2x + 4yx - 3x^2$ by $g = 2y + x + 1$
- Recall: Division is cancellation by leading terms
- What are $lt(f), lt(g)$?

- Divide $f = y^2x + 4yx - 3x^2$ by $g = 2y + x + 1$
- Recall: Division is cancellation by leading terms
- What are $lt(f), lt(g)$?
- We need to figure out how to order the terms of f, g

Monomial (Term) Orderings

Power product: $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_d^{\alpha_d}, \alpha_i \in \mathbb{Z}_{\geq 0}$.

For simplicity: $x_1^{\alpha_1} \dots x_d^{\alpha_d} = \mathbf{x}^{\alpha},\ \alpha \in \mathbb{Z}_{\geq 0}^{d}$.

- Term $= a \cdot \mathbf{x}^{\alpha} =$ coeff. times a power product
- $\mathbb{T}^d = \{\mathbf{x}^{\alpha} : \alpha \in \mathbb{Z}_{\geq 0}\}$ is the set of all power products
- A multivariate polynomial is a sum of terms

A total order $<$ on $\mathbb{T}^d$, and it should be a well-ordering:

- Total order: One and only one of the following should be true: $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ or $x^\alpha < x^\beta$.
- $1 < x^\alpha, \quad \forall x^\alpha \quad (x^\alpha \neq 1)$
- $x^\alpha < x^\beta \implies x^\alpha \cdot x^\gamma < x^\beta \cdot x^\gamma$.

Definition (LEX)

Lexicographic order: Let $x_1 > x_2 > \cdots > x_d$ lexicographically. Also let $\alpha = (\alpha_1, \ldots, \alpha_d)$; $\beta = (\beta_1, \ldots, \beta_d) \in \mathbb{Z}^d_{\geq 0}$. Then we have:

$$x^\alpha < x^\beta \iff \begin{cases} \text{Starting from the left, the first co-ordinates of } \alpha_i, \beta_i \\ \text{that are different satisfy } \alpha_i < \beta_i \end{cases}$$

For 2-variables: $1 < x_2 < x_2^2 < \cdots < x_1 < \ldots x_2 x_1 < \cdots < x_1^2 < \ldots$

Definition (DEGLEX)

Degree Lexicographic order: Let $x_1 > x_2 > \cdots > x_d$ lexicographically. Also let $\alpha = (\alpha_1, \ldots, \alpha_d)$; $\beta = (\beta_1, \ldots, \beta_d) \in \mathbb{Z}^d_{\geq 0}$. Then we have:

$$x^\alpha < x^\beta \iff \begin{cases} \sum_{i=1}^d \alpha_i < \sum_{i=1}^d \beta_i & \text{OR} \\ \sum_{i=1}^d \alpha_i = \sum_{i=1}^d \beta_i \text{ AND } x^\alpha < x^\beta & \text{w.r.t. LEX order} \end{cases}$$

Definition (DEGREVLEX)

Degree Reverse Lexicographic order: Let $x_1 > x_2 > \cdots > x_d$ lexicographically. Also let $\alpha = (\alpha_1, \ldots, \alpha_d)$; $\beta = (\beta_1, \ldots, \beta_d) \in \mathbb{Z}^d_{\geq 0}$. Then we have:

$$x^\alpha < x^\beta \iff \begin{cases} \sum_{i=1}^d \alpha_i < \sum_{i=1}^d \beta_i \text{ or} \\ \sum_{i=1}^d \alpha_i = \sum_{i=1}^d \beta_i \text{ AND the first co-ordinates} \\ \alpha_i, \beta_i \text{ from the RIGHT, which are different, satisfy } \alpha_i > \beta_i \end{cases}$$

Term Ordering Examples

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:

Term Ordering Examples

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:
- $f = 2x^2yz + 3xy^3 - 2x^3$

Term Ordering Examples

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:
- $f = 2x^2yz + 3xy^3 - 2x^3$
- DEGREVLEX $x > y > z$: f is:

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:
- $f = 2x^2yz + 3xy^3 - 2x^3$
- DEGREVLEX $x > y > z$: f is:
- $f = 3xy^3 + 2x^2yz - 2x^3$

Term Ordering Examples

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:
- $f = 2x^2yz + 3xy^3 - 2x^3$
- DEGREVLEX $x > y > z$: f is:
- $f = 3xy^3 + 2x^2yz - 2x^3$

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:
- $f = 2x^2yz + 3xy^3 - 2x^3$
- DEGREVLEX $x > y > z$: f is:
- $f = 3xy^3 + 2x^2yz - 2x^3$

Always fix a term order over a ring, and stick to it!

Term Ordering Examples

$f = 2x^2yz + 3xy^3 - 2x^3$

- LEX with $x > y > z$, f is:
- $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: f is:
- $f = 2x^2yz + 3xy^3 - 2x^3$
- DEGREVLEX $x > y > z$: f is:
- $f = 3xy^3 + 2x^2yz - 2x^3$

Always fix a term order over a ring, and stick to it!

$f = c_1X_1 + c_2X_2 + \cdots + c_tX_t$ implies $X_1 > \cdots > X_t$

Multi-variate Division

Divide $f = y^2x + 4yx - 3x^2$ by $g = 2y + x + 1$ with DEGLEX $y > x$ in $\mathbb{Q}[x, y]$

Multi-variate Division

Divide $f = y^2x + 4yx - 3x^2$ by $g = 2y + x + 1$ with DEGLEX $y > x$ in $\mathbb{Q}[x, y]$

Solved on the board in the classroom

Divide f by g: denoted $f \xrightarrow{g} h$, where $h = f - \frac{X}{\text{lt}(g)} g$. Here, X may not be the leading term.

Definition

Let $f, f_1, \ldots, f_s, h \in \mathbb{F}[x_1, \ldots, x_n], f_i \quad \neq 0; \quad F = \{f_1, \ldots, f_s\}$. Then f reduces to h modulo F:

$$f \xrightarrow{F}_+ h$$

if and only if there exists a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ and a sequence of polynomials $h_1, \ldots, h_{t-1} \in k[x_1, \ldots, x_n]$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$$

$f_1 = yx - y, f_2 = y^2 - x, \quad f = y^2x$; DEGLEX $y > x$ in $\mathbb{Q}[x]$. Divide $f \xrightarrow{f_1, f_2}_+ h$:

- To divide f by $F = \{f_1, \ldots, f_3\}$ (say)
- Impose term order on the ring
- Impose the given order on polynomials of F: $f_1 > f_2 > f_3$
- Divide f by f_1 first:
  - Analyze terms of $f = c_1X_1 + c_2X_2 + \cdots + c_tX_t$ in order
  - Does $lt(f_1) \mid c_1X_1$? If so, divide (or cancel lt(f)), update f, and check if $lt(f_1) \mid$ the new $lt(f)$ (in updated f)?
  - Otherwise, does $lt(f_2) \mid c_1X_1$? And so on...
- If $lt(f)$ is not divisible by any $lt(f_i)$, then move $lt(f)$ into the remainder ($r = r + lt(f)$), and update f ($f = f - lt(f)$)
- Repeat... [See the algorithm in the next slides]

Definition

If $f \xrightarrow{F}_{+} r$, then no term in r is divisible by $\mathrm{LT}(f_i)$, $\forall f_i \in F$. Then r is reduced w.r.t. F and it is called the remainder.

Definition

Let $f, f_1, \ldots, f_s, r \in \mathbb{F}[x_1, \ldots, x_n], f_i \quad \neq 0; \quad F = \{f_1, \ldots, f_s\}$. Then f reduces to r modulo F:

$$f \xrightarrow{F}_{+} r$$

then

$$f = u_1 f_1 + \cdots + u_s f_s + r$$

and we have that:

- r is reduced w.r.t. F
- $u_1, \ldots u_s \in \mathbb{F}[x_1, \ldots, x_n]$
- $\mathrm{LP}(f) = \mathrm{MAX}(\mathrm{LP}(f_1)\mathrm{LP}(u_1), \ldots \mathrm{LP}(f_s)\mathrm{LP}(u_s), r)$

Inputs: $f, f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n], f_i \neq 0$
Outputs: $u_1, \ldots, u_s, r$ s.t. $f = \sum f_i u_i + r$ where r is reduced w.r.t. $F = \{f_1, \ldots, f_s\}$ and $\max(lp(u_1)lp(f_1), \ldots, lp(u_s)lp(f_s), lp(r)) = lp(f)$

$u_i \leftarrow 0$; $r \leftarrow 0$, $h \leftarrow f$
while $(h \neq 0)$ **do**
  if $\exists i$ s.t. $lm(f_i) \mid lm(h)$ **then**
    choose i least s.t. $lm(f_i) \mid lm(h)$
    $u_i = u_i + \frac{lt(h)}{lt(f_i)}$
    $h = h - \frac{lt(h)}{lt(f_i)} f_i$
  else
    $r = r + lt(h)$
    $h = h - lt(h)$
  end if
end while

Algorithm 2: Multivariate Division of f by $F = \{f_1, \ldots, f_s\}$

Motivate Gröbner basis

Let $F = \{f_1, \ldots, f_s\}$; $J = \langle f_1, \ldots, f_s \rangle$ and let $f \in J$. Then we should be able to represent $f = u_1 f_1 + \cdots + u_s f_s + r$ where $r = 0$. If we were to divide f by $F = \{f_1, \ldots, f_s\}$, then we will obtain an intermediate remainder (say, h) after every one-step reduction. The leading term of every such remainder $(\mathrm{LT}(h))$ should be divisible by the leading term of at least one of the polynomials in F. Only then we will have $r = 0$.

Definition

Let $F = \{f_1, \ldots, f_s\}$; $G = \{g_1, \ldots, g_t\}$;
$J = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. Then G is a **Gröbner Basis** of J

$$\Longleftrightarrow$$

$$\forall f \in J \;\; (f \neq 0), \quad \exists i : \mathrm{LM}(g_i) \mid \mathrm{lm}(f)$$

Gröbner Basis

Definition

$G = \{g_1, \ldots, g_t\} = GB(J) \iff \forall f \in J, \exists g_i \text{ s.t. } lm(g_i) \mid lm(f)$

Definition

$G = GB(J) \iff \forall f \in J, f \xrightarrow{g_1, g_2, \cdots, g_t}_+ 0$

Implies a "decision procedure" for ideal membership

Buchberger's Algorithm

INPUT : $F = \{f_1, \ldots, f_s\}$
OUTPUT : $G = \{g_1, \ldots, g_t\}$
$G := F;$
REPEAT
  $G' := G$
  For each pair $\{f, g\}, f \neq g$ in G' DO
    $S(f, g) \xrightarrow{G'}_{+} r$
    IF $r \neq 0$ THEN $G := G \cup \{r\}$
UNTIL $G = G'$

$$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$$

$L = \text{LCM}(lm(f), lm(g))$, $lm(f)$: leading monomial of f