Gröbner bases and polynomial equations

John B. Little

Department of Mathematics and Computer Science, College of the Holy Cross

little@mathcs.holycross.edu

University of South Alabama Mathematics Department Colloquium

April 5, 2007
Outline of Talk

• "Applied Algebra"

• Polynomials and Ideals

• Gröbner Bases

• Solving Polynomial Systems

• More Sophisticated Methods
§1. “Applied Algebra”

Many problems in areas such as

- geometric design and robotics
- error-control coding theory
- operations research
- statistics/bioinformatics, etc.

can be phrased in terms of polynomials in several variables (solving polynomial equations and other operations). Makes contact with well-developed areas of pure mathematics (commutative algebra, algebraic geometry) and recently-developed computational tools!
2. Polynomials and Ideals

- Given a field $k$ (e.g. $k = \mathbb{Q}, \mathbb{R}$, but all fields work similarly), let $k[x_1, \ldots, x_n]$ denote the ring of polynomials in $n$ variables with coefficients in $k$.

- To solve a system of polynomial equations
  
  $$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0,$$

  it is often useful to consider (polynomial) combinations

  $$g_1f_1 + \cdots + g_sf_s = 0,$$

  (e.g. to eliminate variables).

- This leads naturally to the ideal $I$ generated by $f_1, \ldots, f_s$:

  $$I = \langle f_1, \ldots, f_s \rangle = \{g_1f_1 + \cdots + g_sf_s\}$$

  where the $g_i$ are arbitrary polynomials.
Basic Facts

The set $I = \langle f_1, \ldots, f_s \rangle$ is closed under sums, and under products by arbitrary polynomials (the definition of an ideal in a ring from abstract algebra). Other subsets of the polynomial ring with this property:

- If $S \subseteq k^n$ is some set,
  $$I(S) = \{ f \in k[x_1, \ldots, x_n] : f(p_1, \ldots, p_n) = 0 \text{ for all } (p_1, \ldots, p_n) \in S \}.$$

- If $I$ is an ideal,
  $$\sqrt{I} = \{ f \in k[x_1, \ldots, x_n] : f^p \in I, \text{ some } p \geq 1 \}.$$

**Hilbert Basis Theorem.** Every ideal $I$ in the ring $k[x_1, \ldots, x_n]$ is generated by some finite set of polynomials: $I = \langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s$. 

4
Motivating Questions and Problems

Aim: find constructive methods for questions on polynomial ideals, e.g.

- **Ideal Membership Problem**: Given $I = \langle f_1, \ldots, f_s \rangle$ and $f$, determine whether $f \in I$.

- **Radical Problem**: Given $I = \langle f_1, \ldots, f_s \rangle$, determine a set of generators for $\sqrt{I}$.

- **Solving Polynomial Systems**: Given $I = \langle f_1, \ldots, f_s \rangle$, determine

$$V(I) = \{ a \in k^n : f(a) = 0 \text{ all } f \in I \}$$
Polynomials and Division

- For polynomials in 1 variable, we have *polynomial division*.

- Via the Euclidean algorithm, every ideal in $k[x]$ can be generated by a single polynomial: $I = \langle g(x) \rangle$ for some $g$.

- Then, given any $f \in k[x]$, we can divide $g$ into $f$:

$$f(x) = q(x)g(x) + r(x),$$

and $f \in I = \langle g(x) \rangle \iff r(x) = 0$, which gives a solution of the Ideal Membership Problem in this case.
Monomial Orders

- To generalize the *degree ordering*
  
  \[ 1 < x < x^2 < x^3 < \cdots \]

  used in division in \( k[x] \), start from a *monomial order*: a well-ordering \( > \) on set of monomials compatible with ring multiplication. \( x^\alpha > x^\beta \Rightarrow x^\alpha \cdot x^\gamma > x^\beta \cdot x^\gamma \)

- **Example.** *Lexicographic* (lex, or “dictionary”) order on \( k[x, y, z] \) with \( x > y > z \): \( x^5 y > y^{12} z, xy^2 > xyz \).

- **Example.** *Graded lexicographic* order on \( k[x, y, z] \) with \( x > y > z \): Compare total degrees first, then “break ties” with lex order). Have \( x^5 y < y^{12} z, xy^2 > xyz \).

- Many others too, and can “tailor” monomial orders for particular applications.
Leading Terms and Division

• Any monomial order $>$ selects a leading term $LT_>(f)$ from each polynomial (sometimes omit the subscript $>$).

• Can follow 1-variable case to define a division procedure, but allowing several divisors and quotients.

• Example: $f_1 = xy - 1$, $f_2 = x^2 + y^2 - 2$

• Take $>$ to be lex order with $x > y$: then $LT(xy - 1) = xy$ and $LT(x^2 + y^2 - 2) = x^2$.

• If $f = x^2y + x^2 - 1$, for instance, then we can divide $f_1$ and $f_2$ into $f$ to get an expression

$$f = x \cdot f_1 + 1 \cdot f_2 + x - y^2 + 1$$

(the “remainder” $x - y^2 + 1$ contains no monomials divisible by $LT(f_1)$ or $LT(f_2)$)

8
Problems With This Idea

As it stands, this division process doesn’t have the nice properties of the one-variable version.

- Reordering the divisors can change quotients and remainder: interchange $f_1, f_2$, same $f$, and apply same process we get

$$x^2y + x^2 - 1 = (y+1)(x^2+y^2-2)+0\cdot(xy-1)-y^3-y^2+2y+1$$

- Worse, polynomials in $I = \langle f_1, f_2 \rangle$ can have nonzero remainders on division! Note

$$-x(xy - 1) + y(x^2 + y^2 - 2)$$

$$= x + y^3 - 2y \in I,$$

but $x = LT(x + y^3 - 2y) \notin \langle xy, x^2 \rangle$. 
§3. Gröbner Bases

The solutions to these problems come from the idea of a Gröbner basis (developed by Bruno Buchberger of University of Linz – Wolfgang Gröbner was his Ph.D. thesis advisor).

**Definition.** Given an ideal \( I \subseteq k[x_1, \ldots, x_n] \), a Gröbner basis for \( I \) w.r.t. a monomial order \( > \) is a set \( G \subseteq I \) such that for all \( f \in I \), there exist some \( g \in G \) such that \( \text{LT}_>(g) | \text{LT}_>(f) \).

This implies \( I = \langle G \rangle \), by division.

**Example.** A Gröbner basis for our example ideal \( I = \langle xy - 1, x^2 + y^2 - 2 \rangle \) w.r.t. lex order, \( x > y \), is

\[
G = \{ y^4 - 2y^2 + 1, x + y^3 - 2y \}
\]
Good Properties of GB’s

- **Buchberger’s algorithm** computes a Gröbner basis $G$ from any generating set for $I$ as input.

- This algorithm can be seen as a *common generalization* of Euclidean algorithm for polynomials in 1 variable, and Gaussian elimination (row-reduction) for linear polynomials in any number of variables.

- There is a *unique* reduced Gröbner basis for $I$ with respect to each monomial order (analogous to row-reduced echelon or Gauss-Jordan form for linear systems)

- Remainders on division with respect to a Gröbner basis are *unique*. 
Good Properties, cont.

• If we divide by a Gröbner basis $G$, then we get $f \in I = \langle G \rangle \Leftrightarrow$ remainder is zero. (That is, GB’s give an algorithmic solution of the Ideal Membership Problem mentioned before.)

• Software for Gröbner basis computation is widely available – implemented in Maple, Mathematica.

• There are also more powerful special-purpose programs: Singular, CoCoA, Macaulay 2, Magma, etc.

• These are now very widely-used standard tools for research in commutative algebra, algebraic geometry, applications.
Elimination Theory

An interesting pattern is evident in the lex Gröbner bases we have seen.

Given $I \subset k[x_1, \ldots, x_n]$, for $1 \leq m \leq n - 1$, let

$$I_m = I \cap k[x_{m+1}, \ldots, x_n]$$

(called the $m$th elimination ideal of $I$).

For instance, let $I = \langle xy - 1, x^2 + y^2 - 2 \rangle$ as before. In the lex Gröbner basis from before

$$G = \{y^4 - 2y^2 + 1, x + y^3 - 2y\},$$

(lex with $x > y$) we have

$$y^4 - 2y^2 + 1 \in I \cap k[y] = I_1.$$
Elimination Theorem

In fact, \textit{lex} Gröbner bases eliminate variables systematically, in this sense:

\textbf{Elimination Theorem.} If $G$ is a Gröbner basis for $I$ w.r.t. the \textit{lex} order with $x_1 > \cdots > x_n$, then for all $m$, $1 \leq m \leq n-1$,

$$G_m = G \cap k[x_{m+1}, \ldots, x_n]$$

is a Gröbner basis for $I_m$.

Idea of proof: By definition of a Gröbner basis, given any $f \in I_m \subset I$, there must be some $g \in G$ such that $LT_{\text{lex}}(g) | LT_{\text{lex}}(f)$.

But $LT_{\text{lex}}(f)$ contains only $x_{m+1}, \ldots, x_n$, so the same is true of $LT_{\text{lex}}(g)$.

In the \textit{lex} order, any monomial containing $x_i$ for some $i \geq m$ is greater than all monomials containing only $x_{m+1}, \ldots, x_n$. This implies that $g \in G_m$. 

14
Extension of Solutions

Elimination of $x_1$ corresponds geometrically to projection of the set $V(I)$ of solutions onto the $x_2, \ldots, x_n$-coordinate hyperplane.

The projection need not be a variety (solution set of a polynomial system) itself, but working over $\mathbb{C}$ now, $V(I_1)$ is the smallest variety containing it (its Zariski closure).

If $(a_2, \ldots, a_n) \in V(I_1)$, can ask: when it can be extended to a solution $(a_1, a_2, \ldots, a_n)$ of the whole system?

The **Extension Theorem** gives a sufficient condition: Suppose $G = \{g_1, \ldots, g_s\} \cup G_1$ and

$$g_i = h_i(x_2, \ldots, x_n)x_1^{m_i} + \cdots.$$ 

If $h_i(a_2, \ldots, a_n) \neq 0$ for some $i$, then the solution extends over $\mathbb{C}$. 

15
Quotient Rings

Can guess from this example that the properties of $\mathbf{V}(I)$ are “encoded” in the algebra of $k[x_1, \ldots, x_n]/I$.

- Indeed, Buchberger’s original motivation was to give a good way to make computations in quotient rings $k[x_1, \ldots, x_n]/I$ — elements are cosets modulo $I$, so $[f] \equiv [g]$ if $f - g \in I$.

- If $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis for $I$, then the set $\mathcal{B}(G)$ of monomials in the complement of

$$\langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$$

gives a vector space basis for $k[x_1, \ldots, x_n]/I$.

- Example. $G = \{y^4 - 2y^2 + 1, x + y^3 - 2y\}$

$B(G) = \{1, y, y^2, y^3\}$
Arithmetic in $k[x_1, \ldots, x_n]/I$

Remainders on division by a Gröbner basis for $I$ give “normal forms” of elements of the quotient.

- Can take $[p] \leftrightarrow \overline{p}^G = \text{remainder on division by } G$.

- Then

$$[f] + [g] \leftrightarrow \overline{f + g} = \overline{f}^G + \overline{g}^G$$

$$[f] \cdot [g] \leftrightarrow \overline{f}^G \cdot \overline{g}^G$$

To conclude the talk, we’ll indicate some ways this additional algebra can yield improvements over the basic methods for solving equations described before.
§5. More Sophisticated Methods

• Let $k \supset Q$. $I$ is said to be “zero-dimensional” if $B(G)$ is finite.

• $\iff$ set of common zeroes over $C$ is finite.

• **Example.** Exactly 4 points in $C^2$ in

  \[ V(xy - 1, x^2 + y^2 - 2), \]

  all real.

• All information about the zero locus

  \[ V(I) = \{ p \in C^n : f(p) = 0; \text{all } f \in I \} \]

  is contained in (linear) algebra of

  \[ A = k[x_1, \ldots, x_n]/I \]

  and *multiplication maps* $m_f : A \to A$, $f \in A$. 

18
The One-variable Case

The one variable case of this construction is probably familiar. If \( A = k[x]/\langle p(x) \rangle \), \( p \) monic of degree \( n \), then the matrix of \( m_x \) on \( A \) w.r.t. basis \( \{1, x, x^2, \ldots, x^{n-1}\} \) for \( A \) is the companion matrix of \( p(x) \):

\[
C_p = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & -a_0 \\
1 & 0 & 0 & \cdots & 0 & -a_1 \\
0 & 1 & 0 & \cdots & 0 & -a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & -a_{n-1}
\end{pmatrix}
\]

Recall: The eigenvalues of \( C_p \) are the roots of \( p \), since \( p \) is the characteristic polynomial of \( C_p \).
Eigenvalues

In general,

- The multiplication maps $m_{x_i} : A \to A$ are linear.

- When $I$ is zero-dimensional, the eigenvalues of $m_{x_i}$ are the $x_i$-coordinates of points in $V(I)$.

- “Hybrid” symbolic-numeric techniques for polynomial system solving based on eigenvalue methods have been introduced and studied in recent years.
“Good” Bases for $A$

- In fact, we can even generalize a bit and consider monomial bases $B$ for

\[ A = k[x_1, \ldots, x_n]/I \]

satisfying:

\[ x^\alpha \in B \text{ and } x^\beta | x^\alpha \Rightarrow x^\beta \in B. \]

- The monomial basis $B(G)$ for $A$ (monomials in the complement of $\langle LT(G) \rangle$ for a Gröbner basis $G$) has this property, but there are examples that don’t come from this construction.
Border Bases

Suppose $B$ is such a basis for $A$.

- The *border* of $B$ is:
  \[ B^+ = \{ x_i \cdot x^\alpha \notin B : x^\alpha \in B, 1 \leq i \leq n \} \]

- $x^\beta \in B^+ \Rightarrow$ there exist $a_{\beta \alpha} \in \mathbb{Q}$ such that
  \[ g_\beta = x^\beta - \sum_{x^\alpha \in B} a_{\beta \alpha} x^\alpha \in I \]

- Call the collection of all these $g_\beta$ a *border basis* for $I$.

- **Proposition.** The $g_\beta$ generate $I$. 
Multiplication maps

The $g_\beta$ in a border basis are closely related to the multiplication maps

$$m_{x_i} : A \rightarrow A$$

$$f \mapsto x_i \cdot f$$

In fact, the matrix $M_i$ of $m_{x_i}$ with respect to $B$ can be "read off" the $g_\beta$ directly:

**Proposition 3.** If $x^\alpha \in B$ and $x_i \cdot x^\alpha \in B$ get a column in $M_i = [m_{x_i}]$ with one 1 in row corresponding to $x_i \cdot x^\alpha \in B$ all other entries zero. If $x_i x^\alpha = x^\beta \in B^+$, get a column in $M_i$ consisting of the vector of coefficients from $g_\beta$.

Note: By construction, $M_i M_j = M_j M_i$ for all $i, j$. 

23
Example, continued

With \( V = \{(0,0), (1,1), (2,2), (1,2)\} \), and \( \mathcal{B} = \{1, x, y, xy\} \), get \( \mathcal{B}^+ = \{x^2, x^2y, xy^2, y^2\} \) and border basis:

\[
\begin{align*}
g(2,0) &= x^2 - x + y - xy \\
g(2,1) &= x^2y + 2y - 3xy \\
g(1,2) &= xy^2 + 2x - 3xy \\
g(0,2) &= y^2 + 2x - 2y - xy
\end{align*}
\]

So for instance

\[
[m_x] = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -2 \\ 0 & 1 & 1 & 3 \end{pmatrix}
\]

and it’s easy to check that the eigenvalues are 0, 1 (multiplicity 2), and 2.
Conclusions and Extensions

- Gröbner bases and border bases give powerful tools for constructive treatment of systems of polynomial equations

- Also the basis for algorithms for many other constructions in commutative algebra (ideal intersections, colon ideals and saturations, computations on modules, syzygies and free resolutions, Hilbert functions, ... )

- The theory can also be “localized” (Mora’s algorithm, used in singularity theory)

- Many interesting applications!
References

To get started:

- Cox, - , O’Shea, “Ideals, Varieties, and Algorithms” (suitable for undergrads)

- Kreuzer and Robbiano, “Computational Commutative Algebra I,II” (CoCoA)

- Greuel and Pfister, “A Singular Introduction to Commutative Algebra”

For applications to numerical polynomial system solving:

- Cox, - , O’Shea, “Using Algebraic Geometry”

- Stetter, “Numerical Polynomial Algebra”