What are Gröbner bases and what are they useful for?

Michael Monagan

The CECM Research Centre, SFU

What are the most important/useful tools/algorithms in mathematics?

Useful tools/algorithms in Mathematics

1. The Fundamental Theorem of Calculus:
   If $g(x) = \int f(x)dx$ then $\int_a^b f(x)dx = g(b) - g(a)$.
2. Gaussian elimination and reduced row Echelon form
3. The Fast Fourier Transform, Cooley and Tukey, 1965.
4. **Gröbner bases**, Buchberger, 1965.
5. ...

I'll cover 1 and 3 in MATH 801, Computer Algebra, Spring 2027

Gemini answered

Useful tools/algorithms in Mathematics

1. The Fundamental Theorem of Calculus:
   If $g(x) = \int f(x)dx$ then $\int_a^b f(x)dx = g(b) - g(a)$.
2. Gaussian elimination and reduced row Echelon form
3. The Fast Fourier Transform, Cooley and Tukey, 1965.
4. **Gröbner bases**, Buchberger, 1965.
5. ...

I'll cover 1 and 3 in MATH 801, Computer Algebra, Spring 2027

Gemini answered

The Fast Fourier Transform, Newton's method, and the simplex algorithm.

Solving linear systems and polynomial systems

Let $\mathbb{F}$ be a field. E.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Q}(\alpha), \mathbb{F}_q$.
Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$.
Let $\mathbb{V}(F) = \{a \in \mathbb{F}^n : f_1(a) = 0, f_2(a) = 0, \ldots, f_s(a) = 0\}$.

Question 1: How can we compute $\mathbb{V}(F)$?
Question 2: What is the dimension of $\mathbb{V}(F)$? How many variables are free?

Solving linear systems and polynomial systems

Let $\mathbb{F}$ be a field. E.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Q}(\alpha), \mathbb{F}_q$.
Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$.
Let $\mathbb{V}(F) = \{a \in \mathbb{F}^n : f_1(a) = 0, f_2(a) = 0, \ldots, f_s(a) = 0\}$.

Question 1: How can we compute $\mathbb{V}(F)$?
Question 2: What is the dimension of $\mathbb{V}(F)$? How many variables are free?

Example 1: $F = \{x_1 + x_2 - 1, x_1 + x_3 - 2, x_2 - x_3 + 1\}$. Using Gaussian elimination we have

$$[A|b] = \left[\begin{array}{ccc|c} 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & -2 \\ 0 & 1 & -1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 1 & -2 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right] \Longrightarrow \left\{\begin{array}{c} x_1 = -2 - x_3 \\ x_2 = 1 + x_3 \\ x_3 = t \end{array}\right\}$$

What if $F = \{x_1^2 + x_2^2 + x_3^2 - 5,\ x_1x_2x_3 - 1,\ x_1 + x_2 + x_3\}$?

Ideals in $\mathbb{F}[x_1, x_2, \ldots, x_n]$

Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$.

Let $V = Span(f_1, f_2, \ldots, f_s) = \{\sum_{i=1}^{s} c_i f_i : c_i \in \mathbb{F}\}$. ;

Let $I = \langle f_1, f_2, \ldots, f_s \rangle = \left\{\sum_{i=1}^{s} h_i f_i : h_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]\right\}$.

V is a vector space and I is an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Ideals in $\mathbb{F}[x_1, x_2, \ldots, x_n]$

Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$.

Let $V = Span(f_1, f_2, \ldots, f_s) = \{\sum_{i=1}^{s} c_i f_i : c_i \in \mathbb{F}\}$. ;

Let $I = \langle f_1, f_2, \ldots, f_s \rangle = \left\{\sum_{i=1}^{s} h_i f_i : h_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]\right\}$.

V is a vector space and I is an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Example 2: Let $f_1 = x + y^2, f_2 = xy + y$.
Then $f_3 = y f_1 + (-1) f_2 = y^3 - y \in I$. Also $f_2 = y f_1 - f_3$ so

$$I = \underbrace{\langle x + y^2, xy + y \rangle}_{f_1, f_2} = \underbrace{\langle x + y^2, xy + y, y^3 - y \rangle}_{f_1, f_2, f_3} = \underbrace{\langle x + y^2, y^3 - y \rangle}_{f_1, f_3}.$$

We say $F_1 = \{f_1, f_2\}$, $F_2 = \{f_1, f_2, f_3\}$ and $F_3 = \{f_1, f_3\}$ are bases for I.
It turns out that F_2 and F_3 are Gröbner bases (nice bases) for I but F_1 is not.

Proposition 1: If $F = \{f_1, f_2, \ldots, f_s\}$ and $G = \{g_1, g_2, \ldots, g_t\}$ are bases for I then

$$\mathbb{V}(F) = \mathbb{V}(G).$$

Monomial Orderings

Definition 1: Let $M_n = \{x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} : e_i \in \mathbb{Z}_{\geq 0}\}$. Let $X, Y, Z \in M_n$.
A **monomial ordering** on M_n is an order relation $<$ such that

1. $<$ is a total ordering, i.e.,
   (i) $X \leq Y$ or $Y \leq X$ (totality)
   (ii) $X \leq Y$ and $Y \leq X$ implies $X = Y$ (antisymmetry)
   (iii) $X \leq Y$ and $Y \leq Z$ implies $X \leq Z$ (transitivity)
2. $X < Y$ implies $ZX < ZY$
3. $<$ is a well ordering

Monomial Orderings

Definition 1: Let $M_n = \{x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} : e_i \in \mathbb{Z}_{\geq 0}\}$. Let $X, Y, Z \in M_n$.
A **monomial ordering** on M_n is an order relation $<$ such that

1. $<$ is a total ordering, i.e.,
   (i) $X \leq Y$ or $Y \leq X$ (totality)
   (ii) $X \leq Y$ and $Y \leq X$ implies $X = Y$ (antisymmetry)
   (iii) $X \leq Y$ and $Y \leq Z$ implies $X \leq Z$ (transitivity)
2. $X < Y$ implies $ZX < ZY$
3. $<$ is a well ordering

Lexicographical monomial ordering with $x_1 > x_2 > x_3$.

$$x_1^2 x_2 > x_1 x_2 > x_1 x_3^3 > x_2^3.$$

Graded monomial ordering with $x_1 > x_2 > x_3$.
Sort first by total degree then break ties with lexicographical order.

$$x_1 x_3^3 > x_1^2 x_2 > x_2^3 > x_1 x_2.$$

Definition of a Gröbner basis

Definition 2: Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $<$ be a monomial ordering on M_n.
$LT(f), LC(f), LM(f)$ are the leading term, leading coefficient and leading monomial of f.

Example 3: In graded lex with $x_1 > x_2 > x_3$

For $f = 2x_1x_3^3 + 3x_1^2x_2 + 4x_2^3 + 5x_1x_2,$, we have $LM(f) = x_1x_3^3,\ LC(f) = 2,\ LT(f) = 2x_1^2x_3^3$.

Definition 3: Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$. Let $I = \langle f_1, f_2, \ldots, f_s \rangle$.
Let $LM(I) = \langle LM(f) : f \in I \rangle$. The set F is a Gröbner basis for I if

$$J := \langle LM(f_i) : 1 \leq i \leq s \rangle = \langle LM(I) \rangle.$$

Proposition 2: Every ideal in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ has a Gröbner basis.

Example 4: $f_1 = x + y^2, f_2 = xy + y$ in lex with $x > y$. Here

$$J = \langle LM(f_1), LM(f_2) \rangle = \langle x, xy \rangle = \langle x \rangle.$$

But since $f_3 = yf_1 - f_2 = y^3 - y \in I$ and $LM(f_3) = y^3$ is not in J, $F = \{f_1, f_2\}$ is not a GB for I.

Division by a F, a set of polynomials

Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$ and let $I = \langle f_1, f_2, \ldots, f_s \rangle$.
Fix a monomial ordering $<$ on M_n.
Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. How do we compute $f \div F$?
Compute quotients $q_1, q_2, \ldots, q_s$ and a remainder r such that $f = q_1 f_1 + \ldots q_s f_s + r$ and no term in r is divisible by any $LM(f_i)$.

Example 5: In lex with $x > y$.

$$
\begin{array}{lll}
 & q_1 = y & \\
 & q_2 = 1 & \\
f_1 = xy + y &) \overline{xy^2 + x = f} & \\
f_2 = x - y & \underline{-(xy^2 + y^2)} & \\
 & x - y^2 & \\
 & \underline{-(x - y)} & \\
 & -y^2 + y = r &
\end{array}
\qquad
\begin{array}{lll}
 & q_1 = y^2 + 1 & \\
 & q_2 = 0 & \\
f_1 = x - y &) \overline{xy^2 + x = f} & \\
f_2 = xy + y & \underline{-(xy^2 - y^3)} & \\
 & x + y^3 & \\
 & \underline{-(x - y)} & \\
 & y^3 + y = r &
\end{array}
$$

Proposition 3: If G is any Gröbner basis for I then the remainder $r = f \mod G$ is unique.

Syzergy polynomials

How can we compute a Gröbner basis for $I = \langle f_1, f_2, \ldots, f_s \rangle$?

Definition 4: Let $f_1, f_2 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $>$ be a monomial ordering on M_n. Let $L = \mathrm{lcm}(LM(f_1), LM(f_2))$. Then **the Syzergy polynomial**

$$S(f_1, f_2) = \frac{L}{LT(f_1)} f_1 - \frac{L}{LT(f_2)} f_2.$$

Example 6: Let $f_1 = x + y^2, f_2 = xy + y$, $L = xy$.

$$S(f_1, f_2) = \frac{xy}{x} f_1 - \frac{xy}{xy} f_2 = y f_1 - f_2 = y^3 - y$$

Proposition 4: Buchberger's S-polynomial criterion
Let $G = \{g_1, g_2, \ldots, g_t\}$ be a basis for $I = \langle f_1, f_2, \ldots, f_s \rangle$.
G is a Gröbner basis for I if and only if

$$S(g_i, g_j) \mod G = 0 \text{ for all } i \neq j.$$

Buchberger's Algorithm

Input $F = \{f_1, f_2, \ldots, f_s\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $<$ a monomial ordering on M_n.
Output a Gröbner basis for $I = \langle f_1, f_2, \ldots, f_s \rangle$ w.r.t. $<$.

1. $G_1 := F$; $k := 1$;
2. **repeat** the following
   Set $k := k + 1$ and $G_k := G_{k-1}$.
   Compute $r_{ij} := S(G_i, G_j) \mod G$ for all $i \neq j$.
   If any $r_{ij} \neq 0$ then $G_k := G_k \cup \{r_{ij}\}$.
3. **until** $G_k = G_{k-1}$.
4. Output G_k.

Example 4 continued: $G_1 := \{f_1 f_2\} = \{x + y^2, xy + y\}$ Since $r_{12} = S(f_1, f_2) \mod G_1 = y^3 - y$ we have

$$G_2 := \{f_1, f_2, r_{12}\} = \{x + y^2, xy - y, y^3 - y\}$$

G_2 is a GB for I. So is $G = \{x + y^2, y^3 - y\}$.
In fact G is the unique reduced Gröbner basis for I.

Some more properties of Gröbner bases

Let $F = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$.
Let $I = \langle f_1, f_2, \ldots, f_s \rangle$.
Let $G = \{g_2, g_2, \ldots, g_t\}$ be a Gröbner basis for I wrt a monomial ordering $<$.

Proposition 5: For $\mathbb{F} = \mathbb{C}$, $|\mathbb{V}(F)|$ is finite if and only if, for all $1 \leq i \leq n$, $\exists g_i \in G$ such that $LM(g_i) = x_i^{m_i}$. Moreover $|\mathbb{V}(F)| \leq \prod_{i=1}^{n} m_i$.

Proposition 6: (The elimination theorem). If $<$ is lex with $x_1 > x_2 > \cdots > x_n$ then $G \cap \mathbb{F}[x_i, \ldots, x_n]$ is a Gröbner basis for $I \cap \mathbb{F}[x_i, \ldots, x_n]$.

Example 7: $f_1 = x + y^2, f_2 = xy + y$, $I = \langle f_1, f_2 \rangle$.
$G_2 := \{x^1 + y^2, xy - y, y^3 - y\}$
So $I \cap \mathbb{C}[y] = \langle y^3 - y \rangle$ and $|\mathbb{V}(F)| \leq 3$.