Math 332

Gröbner Bases

David Perkinson

Reed College
Portland, OR

Spring 2009

Gröbner Bases

Gröbner bases are the central tool of computational algebraic geometry.

Examples of computations for which they are useful:

- the ideal membership problem: $f \overset{?}{\in} I$;
- Hilbert functions;
- resolutions;
- elimination theory;
- finding solutions to systems of equations;
- intersections of ideals.

Main Idea

Reduce all problems in polynomial rings to problems concerning monomials.

Notation

$R = k[x_1, \ldots, x_n]$.

- monomial: $x^a = x_1^{a_1} \cdots x_n^{a_n}$
- exponent vector for x^a: $a = (a_1, \ldots, a_n)$
- degree: $\deg x^a = |a| = \sum_i a_i$
- term: αx^a where $\alpha \in k$
  - Every polynomial is a sum of terms.
- monomial ideal: an ideal generated by monomials
- division of monomials: $x^a | x^b$ if $x^b = f\, x^a$ for some $f \in R$.
  - $x^a | x^b$ iff $b \geq a$, i.e., $b_i \geq a_i$ for all i.

Membership problem

$$1 \overset{?}{\in} (x^2 + y - 3,\ xy^2 + 2x,\ y^3)$$

Yes!

$$\begin{aligned} 1 \quad = \quad & \frac{-1}{27}(y^2 + 3y + 9)(x^2 + y - 3) \\ & -\frac{1}{108}(xy^4 + 3xy^3 + 7xy^2 - 6xy - 18x)(xy^2 + 2x) \\ & +\frac{1}{108}(x^2y^3 + 3x^2y^2 + 9x^2y + 4)y^3 \end{aligned}$$

The problem is easier for monomial ideals. . .

Proposition

Let $I \subseteq R$ be a monomial ideal generated by a set of monomials M. Then $f \in I$ iff each term of f is divisible by some monomial in M.

Proof.

Exercise. □

Corollary

Every monomial ideal is generated by a finite set of monomials.

Proof.

Hilbert basis theorem and the above Proposition. □

Monomial Orderings

Definition

A monomial ordering on $R = k[x_1, \ldots, x_n]$ is a total ordering on the monomials of R such that

1. $x^b > x^a \implies x^c x^b > x^c x^a$ for all x^c;
2. 1 is the smallest monomial.

lex: Lexicographical Ordering

$x^b >_{\mathrm{lex}} x^a$ if the left-most nonzero entry of $b - a$ is positive. (Mantra: more of the early variables)

$$x^2 > xy > xz > x > y^2 > yz > y > z^2 > z > 1$$

deglex: Degree Lexicographical Ordering

$x^b >_{\mathrm{deglex}} x^a$ if $|b| > |a|$ or if $|b| = |a|$ and $x^b >_{\mathrm{lex}} x^a$. (Mantra: By degree, breaking ties with lex)

$$x^2 > xy > xz > y^2 > yz > z^2 > x > y > z > 1$$

drlex: Degree Reverse Lexicographical Ordering

$x^b >_{\mathrm{drlex}} x^a$ if $|b| > |a|$ or if $|b| = |a|$ and the right-most nonzero entry of $b - a$ is negative. (Mantra: fewer of the late variables)

$$x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1$$

Notes

- From now on, fix a monomial ordering, $>$, on $R = k[x_1, \ldots, x_n]$.
- We will also compare terms: for nonzero $\alpha, \beta \in k$,

$$\alpha x^b > \beta x^a \text{ if } x^b > x^a.$$

Definition

- The initial term of $f \in R$, denoted $\mathrm{in}_>(f)$, is the largest term of f with respect to $>$.
- The initial ideal of an ideal I is the monomial ideal

$$\mathrm{in}_>(I) = (\mathrm{in}_>(f) : f \in I).$$

Macaulay's Theorem

A preliminary

Lemma

Every nonempty set of monomials $\{x^{a_i}\}$ *has a least element.*

Proof.

Since R is Noetherian the ideal generated by the monomials is generated by a finite subset. Take a least element of this subset. □

Theorem (Macaulay)

Let $I \subseteq R$ be an ideal and $>$ a monomial ordering. Let B be the set of monomials of R not contained in $in_>(I)$. Then B is a k-vector space basis for R/I.

Proof.

Exercise (minimal criminal argument). □

Division Algorithm

One variable

Input: $f, g \in k[x]$ with $g \neq 0$.

Output: $f = q\,g + r$ with $\deg r < \deg g$.

Idea: Start with f. At each step subtract off the leading term of the remainder using g.

Example

$$f = x^3 - 2x + 1, \qquad g = x - 2$$

$$
\begin{array}{r|rrrr}
 & x^2 & +2x & +2 & \\
\hline
x-2\,) & x^3 & & -2x & +1 \\
 & x^3 & -2x^2 & & \\
\hline
 & & 2x^2 & -2x & +1 \\
 & & 2x^2 & -4x & \\
\hline
 & & & 2x & +1 \\
 & & & 2x & -4 \\
\hline
 & & & & 5
\end{array}
$$

$$
\begin{array}{ccccc}
f & = & q & g & +r \\
x^3 - 2x + 1 & = & (x^2 + 2x + 2) & (x - 2) & +5
\end{array}
$$

Applications

- $f(\alpha) = 0$ iff $x - \alpha$ divides f.
- $k[x]$ is a PID.

  Proof. If $I \subset k[x]$ is a nonzero ideal, choose $g \in I$ of least non-negative degree. Then $I = (g)$.
- membership problem: $f \in (g)$ iff $f = qg + 0$, i.e., $r = 0$.

Several variables

Input: $f, g_1, \ldots, g_s \in R = k[x_1, \ldots, x_n]$, ordering $>$.

Output: $f = \sum_i f_i g_i + r$ where no term of r is divisible by any $\text{in}_>(g_i)$, and $\text{in}_>(f) \geq \text{in}(f_i g_i)$ for all i.

Idea: Start with f. At each step subtract off the largest term of the remainder divisible by some $\text{in}_>(g_i)$.

Example

$$f = x^3 + 2xy^2 - y^3 + x, \quad g_1 = xy + 1,\ g_2 = x^2 + y$$

$$\begin{array}{l}
xg_2 + 2yg_1 - g_1 \\
\hline\hline
x^3 + 2xy^2 - y^3 + x \\
x^3 + xy \\
\hline
2xy^2 - y^3 - xy + x \\
2xy^2 + 2y \\
\hline
-y^3 - xy + x - 2y \\
-xy - 1 \\
\hline
-y^3 + x - 2y + 1 = r
\end{array}$$

$$f = (2y - 1)g_1 + xg_2 + r$$

It's not the answer.

$$x^2 + y \overset{?}{\in} (x^2, x^2 + y)$$

$$f = x^2 + y, \qquad g_1 = x^2, \quad g_2 = x^2 + y$$

$$r = y \quad \text{or} \quad r = 0 \quad \text{depending on order}$$

- The remainder depends on the ordering of $g_1, \ldots, g_s$.
- The division algorithm does not solve the ideal membership problem.

Gröbner Bases

Definition

Let $I \subseteq R$ be an ideal, and let $>$ be a monomial ordering on R. A Gröbner basis for I w.r.t. $>$ is a subset

$$\{g_1, \ldots, g_s\} \subset I$$

such that

$$(\mathrm{in}_>(g_1), \ldots, \mathrm{in}_>(g_s)) = \mathrm{in}_>(I).$$

Example

$$\{x^2 + y, y\} \subset (x^2, x^2 + y).$$

Proposition

Let $J \subseteq I$ be ideals of $R = k[x_1, \ldots, x_n]$. Then

$$in_>(J) = in_>(I) \implies J = I.$$

Proof. HW (minimal criminal argument).

Corollary

$$\{g_1, \ldots, g_s\} \text{ a GB for } I \implies (g_1, \ldots, g_s) = I.$$

Ideal Membership Problem

Let $\{g_1, \ldots, g_s\}$ be a Gröbner basis for I.

Proposition

$f \in I$ iff the division algorithm applied to f w.r.t. $g_1, \ldots, g_s$ gives a remainder of 0.

Proof.

($\Leftarrow$) Duh.

($\Rightarrow$) Consider the initial term of the remainder,

$$r = f - \sum_i f_i g_i \in I.$$

and remember that no term of r is divisible by any $\text{in}_>(g_i)$. □

Normal form

Let $\{g_1, \ldots, g_s\}$ be a Gröbner basis for I.

Proposition

R/I has a k-vector space basis B consisting of monomials not divisible by any $in_>(g_i)$.

Proof. Macaulay's theorem.

Fact

The remainder of $f \in R$ upon division by $g_1, \ldots, g_s$ is the unique expression of $f \in R/I$ in terms of the basis B.

Buchberger Algorithm

Input: $g_1, \ldots, g_s$ generating $I \subseteq R$, ordering $>$.
Output: a Gröbner basis for I.

Let $C = \{(i,j) : 1 \leq i < j \leq s\}$, $\mathcal{G} = \{g_1, \ldots, g_s\}$.

1. If $C = \emptyset$, stop. Otherwise, pick $(i,j) \in C$ and delete it.
2. $$m_{ij} := \frac{\mathrm{in}(g_i)}{\gcd(\mathrm{in}(g_i), \mathrm{in}(g_j))}, \qquad s_{ij} := m_{ji} g_i - m_{ij} g_j$$
   $$h_{ij} := \text{remainder of } s_{ij} \text{ upon division by } \mathcal{G}$$
3. If $h_{ij} = 0$, go to step 1. Otherwise,
   3.1. Set $g_{s+1} = h_{ij}$, and add it to $\mathcal{G}$.
   3.2. Add $(i, s+1)$ to C for $1 \leq i \leq s$.
   3.3. Replace s by $s+1$.
   3.4. Go to step 1.

Example

$I = (x^2, xy + y^2)$ with DegLex term-ordering.

- $\mathcal{G} = \{g_1 = x^2, g_2 = xy + y^2\}$, $C = \{(1,2)\}$. Choose $(1,2)$.

$$\begin{aligned} s_{12} = y(x^2) - x(xy + y^2) &= -xy^2 \\ &\to -xy^2 + y(xy + y^2) = y^3 = h_{12} \end{aligned}$$

- $\mathcal{G} = \{x^2, xy + y^2, y^3\}$, $C = \{(1,3),(2,3)\}$. Choose $(1,3)$.

$$s_{13} = y^3(x^2) - x^2(y^3) = 0 = h_{13}.$$

- $\mathcal{G} = \{x^2, xy + y^2, y^3\}$, $C = \{(2,3)\}$. Choose $(2,3)$.

$$s_{23} = y^2(xy + y^2) - x(y^3) = y^4 \to 0 = h_{23}.$$

- $C = \emptyset$.

Gröbner basis for I: $\{x^2, xy + y^2, y^3\}$.

Elimination

Problem: Let $R = k[x_1, \ldots, x_n]$ and let $I \subseteq R[y_1, \ldots, y_m]$ be an ideal. Compute

$$I \cap R.$$

Definition

A monomial ordering $>$ on $R[y_1, \ldots, y_m]$ is an elimination ordering if

$$f \in R[y_1, \ldots, y_m] \quad \text{and} \quad \text{in}_>(f) \in R \quad \Longrightarrow \quad f \in R.$$

Example

Lexicographical ordering with $y_1 > \cdots > y_m > x_1 > \cdots > x_n$.

Algorithm

Input: $I = (f_1, \ldots, f_s) \subseteq R[y_1, \ldots, y_m]$.

Output: ideal generators for $I \cap R$.

Idea: Compute a Gröbner basis $\mathcal{G}$ for I w.r.t. an elimination ordering. Output $\mathcal{G} \cap R$.

Example

```
Use R::=Q[a[1..4],b[1..4],z[1..6]],Lex;
M:=Mat([a,b]);
N:=Minors(2,M);
I:=Ideal(z-N);
I;
Ideal(-a[1]b[2] + a[2]b[1] + z[1], -a[1]b[3] + a[3]b[1] + z[2],
-a[1]b[4] + a[4]b[1] + z[3], -a[2]b[3] + a[3]b[2] + z[4],
-a[2]b[4] + a[4]b[2] + z[5], -a[3]b[4] + a[4]b[3] + z[6])
-------------------------------
GBasis(I);
[-a[3]b[4] + a[4]b[3] + z[6], -a[2]b[4] + a[4]b[2] + z[5],
-a[2]b[3] + a[3]b[2] + z[4], -a[1]b[4] + a[4]b[1] + z[3],
-a[1]b[3] + a[3]b[1] + z[2], -a[1]b[2] + a[2]b[1] + z[1],
b[2]z[6] - b[3]z[5] + b[4]z[4], b[1]z[6] - b[3]z[3] + b[4]z[2],
b[1]z[5] - b[2]z[3] + b[4]z[1], -a[2]z[6] + a[3]z[5] - a[4]z[4],
z[1]z[6] - z[2]z[5] + z[3]z[4],  -- <<-----***
b[2]z[2]z[5] - b[2]z[3]z[4] - b[3]z[1]z[5] + b[4]z[1]z[4],
a[2]z[2]z[5] - a[2]z[3]z[4] - a[3]z[1]z[5] + a[4]z[1]z[4],
-a[1]z[6] + a[3]z[3] - a[4]z[2],-a[1]z[5] + a[2]z[3] - a[4]z[1],
b[1]z[4] - b[2]z[2] + b[3]z[1], -a[1]z[4] + a[2]z[2] - a[3]z[1]]
-------------------------------
```