PREMUR 2007 - Seminar
Week 3 Discussions – Elimination theory and applications

Day 1: First applications, elimination of variables

Today, we want to begin looking at some of the (mathematical) applications of Gröbner bases. Applications to other real world problems are often made by translating the question under consideration into a question about systems of polynomial equations, then proceeding as below.

Discussion Questions

A) ("warmup") Show that if $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis for $I = \langle f_1, \ldots, f_s\rangle$, then

$$\mathbf{V}(g_1, \ldots, g_t) = \mathbf{V}(f_1, \ldots, f_s)$$

in k^n.

B) Using Mathematica, I computed a Gröbner basis for the ideal $I = \langle x^2+y^2+z^2-4, xz-y, y^2-z^2+1\rangle$ with respect to the *lex* order, $x > y > z$, and found:

$$[2z^4 - 4z^2 - 1, y^2 - z^2 + 1, x - 2yz^3 + 4yz].$$

1) Using the Elimination Theorem, give Gröbner bases for the elimination ideals $I_1 = k[y, z]$ and $I_2 = k[z]$.
2) What does the Extension Theorem say about the number of points in the variety $\mathbf{V}(I) \in \mathbf{R}^2$? What are those points?

C) Let V be a finite set in $\mathbf{R}^n$ (or $\mathbf{C}^n$, and let $I = \mathbf{I}(V) = \langle f_1, \ldots, f_s\rangle \subset \mathbf{R}[x_1, \ldots, x_n]$ be the ideal of all polynomials that are zero at all the points of V.

1) Show that for each i, $1 \leq i \leq n$, I must include a nonzero polynomial p_i that depends only on the variable x_i.
2) Explain why if we compute a Gröbner basis G for I with respect to a lex order $>_i$ with x_i as the *last - i.e. smallest* variable, then a polynomial $p_i(x_i)$ as in part 1 must appear in that Gröbner basis G. (Hint: If $cx_i^\alpha = LT_{>_i}(p_i(x_i))$ is the leading term of $p_i(x_i)$, then some Gröbner basis element g in G must have a leading term (with respect to this special *lex* order $>_i$ which divides cx_i^α. What does that say about the form of g?

"Extra Credit" Question

Let V be a finite set in $\mathbf{R}^3$ which is in *"general position" in the sense that the z-coordinates of the points of V are distinct*. Let $I = \mathbf{I}(V)$. What does the Gröbner basis for $I = \mathbf{I}(V)$ with respect to the *lex* order, $x > y > z$ look like?

The answer is a result sometimes called the "Shape Lemma". Some suggestions: First note that the "general position" hypothesis is *not* satisfied, for instance, for the Gröbner basis from question B above(!) (*Why not?*) Then think about what part 2 of Question C from above tells you here. You will get one of the Gröbner basis elements that way. Then, what do the others look like? For instance, is there a polynomial of the form $y - f(z)$ in the ideal (hence in the first elimination ideal $I \cap \mathbf{R}[y,z]$? Must it appear in the *lex* Gröbner basis? If so, why? Then, what about polynomials involving x?

Day 2: The Implicitization Problem

Today, we will reconsider the implicitization problem for polynomial parametric curves and surfaces. Our goal is to show that any such curve or surface is (at least) contained in a variety.

Discussion Questions

We consider parametric curves in the plane, given as $x = f(t), y = g(t)$, where $f(t), g(t) \in \mathbf{R}[t]$.

A) Show that for all $m \geq 0$, the total number of monomials $x^a y^b$ of total degree $a + b \leq m$ is equal to the binomial coefficient $\binom{m+2}{2}$.

B) Show that if we substitute $x = f(t)$ and $y = g(t)$ into all of the monomials $x^a y^b$ with $a + b \leq m$, then for m sufficiently large, we obtain a *linearly dependent* collection of polynomials in $k[t]$.

C) Deduce from question B that every parametric curve in $\mathbf{R}^2$ defined by $x = f(t)$, $y = g(t)$ for some polynomials $f(t), g(t) \in \mathbf{R}[t]$ is contained in $\mathbf{V}(F)$ for some nonzero $F(x,y) \in \mathbf{R}[x,y]$ (that is, $F(f(t), g(t)) = 0$ as a polynomial in t).

D) Show that if

$$I = \langle x - f(t), y - g(t) \rangle \subset \mathbf{R}[t, x, y],$$

then $F(x,y)$ from part C is an element of the elimination ideal

$$I_1 = I \cap \mathbf{R}[x,y].$$

E) Generalize your arguments in questions A,B,C,D to show that every surface in $\mathbf{R}^3$ with a polynomial parametrization

$$x = f(t,u), y = g(t,u), z = h(t,u)$$

is contained in $\mathbf{V}(F)$ for some nonzero $F(x,y,z) \in \mathbf{R}[x,y,z]$, and if

$$I = \langle x - f(t,u), y - g(t,u), z - h(t,u) \rangle \subset \mathbf{R}[t,u,x,y,z],$$

then

$$F \in I_2 = I \cap \mathbf{R}[x,y,z].$$

Day 3: Unique factorization and resultants

We have now introduced notion of irreducible polynomials, irreducible factorizations, and the Sylvester resultant of two polynomials, whose original purpose was to detect common irreducible factors of two polynomials.

Discussion Questions

A) In this problem you will develop a proof of the uniqueness of irreducible factorizations from Theorem 5 on page 149 of the text. The existence of the irreducible factorization follows from Proposition 2.

1) Show that if f is irreducible and f divides a product $g_1 g_2 \ldots g_s$, then f divides g_j for some i.
2) The key step in the proof of uniqueness of factorizations is the following. Assume

   $$f_1 f_2 \cdots f_r = g_1 g_2 \cdots g_s, \tag{1}$$

   where all the f_i and g_j are irreducible. Show using part 1 that $f_1 = c g_j$ for some constant c and some j.
3) Show how the idea in part 2 leads to a proof by induction on the total degree of f. (Note: We cannot do induction on the numbers of factors r, s because part of what we are trying to show is that $r = s$, so we cannot assume that.)

B) Another interesting formula for the resultant involves the roots of the polynomials f, g.

1) Compute the resultant of $f = (x - a_1)(x - a_2)$ and $g = (x - b_1)(x - b_2)$.
2) It can be shown in general that if f, g are monic, f has degree n and has roots $a_1, \ldots, a_n$ (possibly in some field containing k), then

   $$Res(f, g, x) = \prod_{i=1}^{n} g(a_i).$$

   Assuming this, show that if g of degree m also has roots $b_1, \ldots, b_m$ in some field containing k, then

   $$\mathrm{Res}(f, g, x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (a_i - b_j).$$

   (Note that this gives another proof of Corollary 2 in §6 of Chapter 3.

C) One important application of resultants is determining when polynomials have multiple roots. For the purposes of this problem, assume that $k \subset \mathbf{Q}$. Under this assumption, it is true that f is constant $\Leftrightarrow f' = 0$. (Note: This is not true for fields of *characteristic* p – fields containing $\mathbf{Z}/p\mathbf{Z}$. The polynomial x^p has derivative identically zero, but is not constant.)

1) Let $f \in k[x]$, and assume that f has the irreducible factorization

$$f = f_1^{r_1} \cdots f_s^{r_s},$$

where no f_i is a constant multiple of f_j for $j \neq i$. Show that

$$\gcd(f, f') = f_1^{r_1 - 1} \cdots f_s^{r_s - 1}.$$

2) Let $f = a_0 x^n + \cdots + a_{n-1} x + a_n \in k[x]$, where $a_0 \neq 0$ (that is, f has degree exactly n). The *discriminant* of f is

$$\operatorname{disc}(f) = \frac{(-1)^{n(n-1)/2}}{a_0} \operatorname{Res}(f, f', x).$$

Show that f has a multiple root (that is f is divisible by h^2 for some irreducible h) if and only if $\operatorname{disc}(f) = 0$.

3) Does $f(x) = 6x^4 - 23x^3 + 32x^2 - 19x + 4$ have a multiple root? If so, what is it?

4) Compute the discriminant of $f(x) = a_0 x^2 + a_1 x + a_2$. How does this relate to the quadratic formula?

Day 4: More on resultants

Background

The Sylvester determinant formula for $\operatorname{Res}(f, g, x)$ is not an efficient way to compute the resultant when f and g have large degrees in x. In today's problems, you will see that there is actually another, much more efficient, way to compute the resultant in these cases by following the Euclidean algorithm for the gcd. The idea is that by considering properties of determinants, we can show that if f has degree ℓ in x, $g = b_0 x^m + \cdots + b_m$ has degree m in x, and if the result of dividing g into f is

$$f = qg + r, \qquad \deg(r) < \deg(g),$$

then

$$\operatorname{Res}(f, g, x) = (-1)^{m(\ell - \deg(r))} b_0^{\ell - \deg(r)} \operatorname{Res}(r, g, x)$$

(see problem 16 below). Then we can reverse r, g (which changes the resultant by a sign) and apply the same formula again, dividing r into g as in the Euclidean algorithm!

Discussion Questions

Do problems 14, 15, 16, 17 from Chapter 3, §6 of "IVA". Some comments:

1) Problem 14 deals with the case where either f or g is constant. This will be needed at the end of the procedure for the case where $\gcd(f, g) = 1$.

2) Problem 16 gives the proof of the key formula above.

3) Problem 17 assembles the various pieces discussed above into an algorithm for resultants. When programs like Mathematica or Maple compute resultants, they are using this method rather than the Sylvester determinant formula.

Day 5: Resultants and the proof of the Extension Theorem

Background

We have seen the definition of the *generalized resultants* of $f_1, f_2, \ldots, f_s$ with respect to x_1: If we write

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) u^\alpha,$$

then the generalized resultants are the $h_\alpha \in k[x_2, \ldots, x_n]$.

Discussion Questions

A) Let $f, g_1, \ldots, g_s \in k[x]$. Prove that f is a common divisor of $g_1, \ldots, g_s$ if and only if f divides $u_1 g_1 + \cdots + u_s g_s$ in $k[x, u_1, \ldots, u_s]$.

B) Let

$$\begin{aligned} f_1 &= x^4 - 2xy^2 + zw \\ f_2 &= wx^2 - w^2 z + y \\ f_3 &= x^3 + 3w \end{aligned}$$

Compute the generalized resultants of f_1, f_2, f_3 with respect to w (that is follow the definition above to find $\mathrm{Res}(f_1, u_2 f_2 + u_3 f_3, w)$. In the lab today, you will be able to check your work. You will also see that the generalized resultants *do not* generate the elimination ideal

$$\langle f_1, f_2, f_3 \rangle \cap k[x, y, z].$$

C) Exactly *how many* generalized resultants with respect to x_1 are there when f_1 has degree m_1 in x_1, and $f_2, \ldots, f_s$ have degrees $m_2 \geq m_3 \geq \cdots \geq m_s$ with respect to x_1? Prove your assertion.

D) Show that the generalized resultants are always elements of the elimination ideal

$$\langle f_1, f_2, \ldots, f_s \rangle \cap k[x_2, \ldots, x_n].$$

(Note: This shown in the text, but try to work out a proof yourself using Proposition 1 on page 158 before looking for it.)