SIMU 1999 - Gröbner Bases Seminar
Week 3 Discussions

Day 1: S-Polynomials and Buchberger's Algorithm

The S-polynomial of two polynomials f, g with respect to a monomial order $>$ is defined in "IVA" as:

$$S(f,g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g,$$

where $x^\gamma = LCM(LM(f), LM(g))$. By Buchberger's Criterion, we know that $G = \{g_1, \ldots, g_t\} \subset I$ is a Gröbner basis for I if and only if

$$\overline{S(g_i, g_j)}^G = 0$$

for all pairs (i, j) with $1 \leq i < j \leq t$.

This gives the idea behind an algorithm for computing Gröbner bases we discussed in class, starting from an arbitrary ideal basis $F = \{f_1, \ldots, f_s\}$ for I. We start with $G = F$, compute S-polynomial remainders, and adjoin any non-zero polynomials we find to the set G. This process is iterated until Buchberger's Criterion is satisfied, and we have a Gröbner basis. The resulting algorithm is called *Buchberger's Algorithm* for Gröbner bases.

Discussion Questions

A) Let $f_1 = x^3y - x$ and $f_2 = y^2 - 1$.
   1) Is $\{f_1, f_2\}$ a Gröbner basis for $I = \langle f_1, f_2 \rangle$ with respect to the *lex* order, $x > y$? Why or why not?
   2) Apply Buchberger's Algorithm to find a Gröbner basis for this ideal.

B) Pick a monomial order $>$, and let $f, g \in k[x_1, \ldots, x_n]$ be two polynomials such that the leading coefficient in each is 1, and $LM(f)$ and $LM(g)$ are *relatively prime* (that is, the gcd of the leading monomials is 1).

   1) Show that in this situation

$$S(f,g) = -(g - LT(g))f + (f - LT(f))g$$

   2) From part 1, show that $LT(S(f,g))$ is still divisible by either $LT(f)$ or $LT(g)$ (in fact if we write $g - LT(g) = q$ and $f - LT(f) = p$, then show that $LT(S(f,g))$ is equal either to $-LT(f)LT(q)$ or to $LT(g)LT(p)$.
   3) Suppose we are performing Buchberger's Algorithm and we notice that in our $F = (f_1, \ldots, f_s)$ two of the polynomials (say f_i and f_j) have leading terms that are relatively prime. Does this mean that $\overline{S(f_i, f_j)}^F = 0$? Why or why not? (*Be careful!*)

It can be shown (even taking 3 into account), that in Buchberger's Algorithm, it is not necessary to check that $\overline{S(f_i, f_j)}^F = 0$ whenever $LT(f_i)$ and $LT(f_j)$ are relatively prime. This leads to savings in computational effort in many examples!

Day 2: Solving Systems of Equations

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) 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 Maple, 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:

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

What does this 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 $\mathbf{R}^n$, and let $I = I(V) = \langle f_1, \ldots, f_s \rangle \subset \mathbf{R}[x_1, \ldots, x_n]$ 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 $p_i(x_i)$ 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?

Day 3: 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 $f(t), g(t) \in \mathbf{R}[t]$ first.

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 $F(x, y) \in \mathbf{R}[x, y]$.

D) Generalize your arguments in questions A,B,C 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 $F(x, y, z) \in \mathbf{R}[x, y, z]$.

Day 4: The "Shape" of the lex Gröbner basis for $I = \mathbf{I}(V)$ for a finite set

Today, we want to try to put together a lot of what we have studied to answer the following 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 on Day 2(!) (*Why not?*) Then think about what part 2 of Question C from Day 2 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?