Notes 14: Applications of Groebner Bases

Ideal Membership Problem: Let $I \subseteq k[x_1, x_2, \ldots, x_n]$ be an ideal and $G$ be a Groebner basis of $I$ with respect to some monomial order. We have seen that

$$f \in I \iff \overline{f}^G = 0.$$ 

Solving Equations by Elimination: We outline how to use Groebner bases to solve polynomial equations in many variables. We do not give proofs here.

Example 1. Find the common solutions of the equations

$$f_1 = x^2 + y^2 + z^2 - 1 = 0,$$
$$f_2 = x^2 + z^2 - y = 0$$
$$f_3 = x - z = 0$$

We compute a Groebner basis of the ideal generated by $\{f_1, f_2, f_3\}$ with respect to the lexicographic order $x > y > z$. I have added a mathematica notebook showing how to do the calculation. The Groebner basis is

$$\{-1 + 2z^2 + 4z^4, y - 2z^2, x - z\}$$

We can back solve this equation. First we solve for $z$, then $y$, and finally $x$. The first member of the G-basis only involves $z$. The second only involves $y$ and $z$, and the last adds the last variable $x$ to the mix. If we change the monomial order the results change. The Groebner basis with respect to the monomial order $y > z > x$ is $\{-1 + 2x^2 + 4x^4, -x + z, -2x^2 + y\}$.

We return to the first G-basis. Solving for $x$ by setting $z^2 = u$ and solving $4u^2 + 2u - 1 = 0$ gives

$$z = \pm(1/2)\sqrt{\pm5} - 1.$$ 

The last two equations in the Groebner basis determine $x, y$ uniquely so there are four solutions.

Example 2. We partially solve a max-min problem in several variables. We find the critical points of the function $f(x, y) = 4 + x^3 + y^3 - 3xy$. This means we find the common zeros of $f_x = 0$ and $f_y = 0$, that is we find the points in the variety

$$V(3x^2 - 3y, 3y^2 - 3x).$$

The Groebner basis of the ideal $< 3x^2 - 3y, 3y^2 - 3x >$ is $y^4 - y, x - y^2$. The associated equations are easily solved.

Example 3. We solve a Lagrange Multipliers Problem. Find the dimensions of rectangular the box with largest volume if the surface area is 64. We wish to maximize $V = xyz$ subject to the constraint $2(xy + xz + yz) - 64 = 0$. We wish to find a point $P$ where the surfaces $F(x, y, z) = 2(xy + xz + yz) - 64 = 0$ and $G(x, y, z) = xyz - V = 0$ intersect
and have parallel tangent planes at the point $P$. The direction of the tangent plane to a surface at a point is determined by its gradient at that point. The tangent plane at a point is perpendicular, that is, normal to the gradient at that point. To say that gradients of $F$ and $G$ point in the same direction is to say that there is a non-zero number $u$ so that $\nabla G = u \nabla F$. Thus we wish to solve the equations

$$
F_x = u G_x \\
F_y = u G_y \\
F_z = u G_z \\
F = 0.
$$

In our case we wish to solve the equations

$$(2y + 2z) - u(yz) = 0$$
$$(2x + 2z) - u(xz) = 0$$
$$(2x + 2y) - u(xy) = 0$$
$$2(xy + xz + yz) - 64 = 0$$

The Groebner basis of the appropriate ideal is

$$\{-32 - 3z^2, y - z, x - z, 8u - 3z\}.$$ 

Note that $x = y = z$ so the solution is a cube.

**Example 4.** We describe a mechanism that draws a cissoid and find the equation of the resulting curve. We start with a point on the $y$-axis, $Q = (0, v)$. A fixed point $A = (1, 0)$ on the $x$-axis. Let $S = (w, z)$ be a point so that its distance to $Q$ is 2. We require that the angle $ASQ$ is a right angle. Let $P = (x, y)$ be the midpoint of the line segment $SQ$. Our problem is to find the equation of the locus of points $P$ as $Q$ moves along the $y$-axis.

We have 5 variables: $v, x, y, w, z$. We have 4 equations:

- The distance from $S$ to $Q$ is 2, so $(z - v)^2 + w^2 - 4 = 0$.
- The angle between $AS$ and $QS$ is $\pi/2$, so the dot product of the vectors $\vec{AS}$ and $\vec{QS}$ is zero. This gives the equation $(1 - w, -z) \cdot (w, v - z) = w^2 - w + z^2 - vz = 0$.
- The point $P$ is the midpoint of $SQ$. This implies that
  $$x - w/2 = 0$$
  $$y - (v + z)/2 = 0.$$ 

Using Mathematica we obtain the equation

$$16 - 40x + 105x^2 - 100x^3 + 100x^4 - 20y^2 + 16xy^2 - 32x^2y^2 + 4y^4 = 0$$

for the cissoid.
Why Does a Groebner Basis Allow Us To Perform Elimination?

Finding solutions to sets of equations in many variables consist of two steps:

Step One: Say you have equations in variables $x_1, x_2, \cdots, x_n$. Eliminating variables so that you are able to find a solution of an equation in one variable, $x_n$.

Step Two: Once you have a solution in a single variable, extending it two a solution in the remaining variables one at a time.

We show how Groebner bases performs the elimination step.

Notation: Let $I \subseteq k[x_1, x_2, \cdots, x_n]$ be an ideal. We set

$$I_l = I \cap k[x_{l+1}, x_{l+2}, \cdots, x_n]$$

It is an exercise to show that $I_l$ is an ideal, the $l$-th elimination ideal.

**Theorem 1.** Let $G$ be a $G$-basis of an ideal $I \subseteq k[x_1, x_2, \cdots, x_n]$ with respect to the lex ordering with $x_1 > x_2, \cdots$. Then

$$G_l := G \cap k[x_{l+1}, x_{l+2}, \cdots, x_n]$$

is a Groebner basis for $I_l$.

**Proof.** We need two facts

- Let $x^\alpha, x^\beta$ be two monomials in $k[x_1, x_2, \cdots, x_n]$. Assume that we are given a monomial order. If $x^\alpha$ divides $x^\beta$, then $x^\alpha < x^\beta$. For a proof see notes 8.

- Let $h \subseteq I, I$ an ideal in $k[x_1, x_2, \cdots, x_n]$. If

  $$<\text{LT}(H)> = <\text{LT}(I)>,$$

  then $<H> = I$.

Since $G_l \subseteq I_l$, it suffices to show that $<\text{LT}(G_l)> = <\text{LT}(I_l)>$ by one of the facts above.

We show that $<\text{LT}(G_l)> = <\text{LT}(I_l)>$. Since $G_l \subseteq I_l$, we have

$$<\text{LT}(G_l)> \subseteq <\text{LT}(I_l)>.$$

We now show $<\text{LT}(I_l)> \subseteq <\text{LT}(G_l)>$. Let $f \in <\text{LT}(I_l)>$. Since $G$ is a Groebner basis for $I$ there is some element $g$ that divides $f$. The other fact implies that $\text{LT}(g) < \text{LT}(f)$. This is impossible if there is a positive power of any of the variables $x_1, x_2, \cdots, x_l$ appearing in $\text{LT}(g)$. This implies that $g \in G_l$ and $\text{LT}(f) \in <\text{LT}(G_l)>$.  

3
The Extension theorem

Let $I \subseteq k[x_1, x_2, \ldots, x_n]$ be an ideal, $G_1$ a Groebner basis of $I$, and let $(a_{l+1}, a_{l+2}, \ldots, a_n)$ satisfy all the equations in $G_1$. We want to know if there is an element $(a_1, a_2, \ldots, a_n) \in V(I)$, that is, an element $(a_1, a_2, \ldots, a_n)$ that satisfies all the equations in $G$. This is asking: Can we extend $a_{l+1}, \ldots, a_n$ to an element of $V(I)$? We do this step by step, first extending to a partial solution $(a_1, a_{l+1}, \ldots, a_n)$, that is, we wish to find $(a_1, a_{l+1}, \ldots, a_n)$ that satisfies the equations in $I_{l-1}$. We then try to find a partial solution $(a_{l-1}, a_l, \ldots, a_n)$ and so forth.

The answer is: Not Always. Often we can; we will find conditions insuring that we can extend our partial solution to a complete solution.

Example 5. Let $f_1 = (x^2 - 1)y - 1$, $f_2 = (x^2 - 1)z - 1$. A Groebner basis for the ideal $J = \langle f_1, f_2 \rangle$ with respect to the lex ordering $x > y > z$ is $g_1 = x^2 z - z - 1$, $g_2 = y - z$.

The equation $y - z = 0$ with no $x$ appearing says that $(y = a, z = a)$ is a solution to the equations in $G_1$. Can we find an $b \in k$ so that $(b, a, a)$ is an element $V(I)$? The answer is no if $a = 0$. If $a \neq 0$ there is a solution.

Theorem 2. Let $I = \langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$. Let $I_1$ be the first elimination ideal if $I$ (so we have only eliminated the first variable $x_1$). For all $i$ write

$$f_i(x_1, x_2, \ldots, x_n) = g(x_2, x_3, \ldots, x_n)x_1^m + \text{ terms involving lower powers of } x_1.$$  

Let $(a_2, a_3, \ldots, a_n)$ be an element of $V(I_1)$. If $(a_2, a_3, \ldots, a_n) \notin V(g_1, g_2, \ldots, g_s)$, then $(a_2, a_3, \ldots, a_n)$ extends to a solution of all the equations $f_i = 0$.

Theorem says that we can lift a partial solution $(a_2, a_3, \ldots, a_n)$ to a complete solution when one of the coefficients of $x_1$ is not zero at $(a_2, a_3, \ldots, a_n)$. In particular, we have the

Corollary 1. Assume that $f_i = c_i x_1^m + \text{ terms of lower degree in } x_1$ with $c_i$ a non-zero constant. Then every partial solution lifts.

Example 6. We use the extension theorem in a step by step fashion. We find the solutions to

$$f_1 = x^2 - y^2 + z^2 - 1 = 0$$
$$f_2 = x(y^2 - 1)z - 1 = 0$$

We compute a Groebner basis with respect to the lex order $x > y > z$. We obtain

$$g_1 = -1 + z^2 - y^2 z^2 - y^4 z^2 + y^6 z^2 - z^4 + 2 y^2 z^4 - y^4 z^4, \quad g_2 = x + z - y^4 z - z^3 + y^2 z^3.$$  

We set up some notation. We let $I = \langle f_1, f_2 \rangle$, and $I_2 = I \cap k[z]$, $I_1 = k[x, y] \cap I$.

Note that $I_2 = 0$. This says that any value of $z = a$ is a partial solution. Which ones lift to a solution to the equations in $I_1$, that is, to a partial solution $y = b, z = a$. By the extension theorem applied to the situation $k[z] \subseteq k[y, z]$ we see that $z = a$ extends to $y = b, z = a$ provided the coefficient of the highest power of $y$ in

$$g_1 = -1 + z^2 - y^2 z^2 - y^4 z^2 + y^6 z^2 - z^4 + 2 y^2 z^4 - y^4 z^4.$$  

4
is not zero at \( z = a \). The coefficient of \( y^6 \), the highest power of \( y \), is \( z^2 \). Hence the solution extends provided \( z \neq 0 \).

The next step is to find which solutions \((y = b, z = a)\) extend to a solution \( x = c, y = b, z = a \). We look at the generators of \( I \) that involve \( x \). We see that the coefficient of the highest power of \( x \) is 1. This means that all partial solutions extend.