6.966 Algebra and Computation October 28, 1998

Lecture 15

Lecturer: Madhu Sudan *Scribe: Ted Allison*

1 Variable Elimination

In this section we will examine what happens when variables are eliminated from a set of polynomials and how this affects the common zeros of the polynomials. To do this we will look at a new way of creating an ideal.

Definition 1 *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in $k[x_1, \ldots, x_n]$. Then define $I_T = I \cap k[x_1, \ldots, x_n - T]$, where $T \subset \{x_1, \ldots, x_n\}$. If $T = \{x_1, \ldots, x_l\}$, then I_T is called the l^{th}* **elimination ideal** *of I and is denoted I_l.*

This naturally raises the usual questions for an ideal: what is a basis for I_l? how do we determine membership in I_l? These questions are addressed by the elimination theorem. A related question is answered by the extension theorem: given a point $(a_2, \ldots, a_n) \in \mathbf{V}(I_{\{x_1\}})$, when can we find a value a_1 such that $(a_1, \ldots, a_n) \in \mathbf{V}(I)$? In other words, given a partial solution to a system, when does a complete solution exist? The concept of elimination ideals will be useful in solving this problem.

Theorem 1 (Elimination Theorem) *Let G be a Groebner basis for an ideal I under lexicographic order, $x_1 > x_2 > \cdots > x_n$. Then $G_l = G \cap k[x_{l+1}, \ldots, x_n]$ is a Groebner basis for $I_l = I \cap k[x_{l+1}, \ldots, x_n]$, the l^{th} elimination ideal of I.*

Proof: Since $G_l \subset I_l$, it suffices to show that $\langle \mathtt{LT}(G_l) \rangle = \langle \mathtt{LT}(I_l) \rangle$, and one direction is trivial.

To show $\langle \mathtt{LT}(I_l) \rangle \subset \langle \mathtt{LT}(G_l) \rangle$, choose a polynomial $f \in I_l$. Because G is a Groebner basis of I, $\mathtt{LT}(f)$ is divisible by $\mathtt{LT}(g)$ for some $g \in G$. But $\mathtt{LT}(f)$ contains none of the variables $x_1, \ldots, x_l$, so neither does $\mathtt{LT}(g)$. Then by the monomial ordering, neither does any other term of g. Thus $g \in G_l$, which shows that $\mathtt{LT}(f) \in \langle \mathtt{LT} G_l \rangle$, and the desired inclusion is proved. ■

Theorem 2 (Extension Theorem) *Given a set of polynomials $f_i(x, y_1, y_2, \ldots, y_n), 1 \le i \le s$ over an algebraically closed field k, write each f_i in the form $f_i(x, y_1, \ldots, y_n) = g_i(y_1, \ldots, y_n)x^{d_i} +$ [terms of lower degree in x], and let $I = \langle f_1, \ldots, f_s \rangle$. If $(a_1, \ldots, a_n) \in \mathbf{V}(I_{\{x\}})$ and $(a_1, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$, then there is some $a \in k$ such that $(a, a_1, \ldots, a_n) \in \mathbf{V}(I)$.*

Before proving the theorem, let us look at some examples of how extensions of partial might not exist if one of the hypotheses fails to hold.

First consider $\langle x - y^2 \rangle$ with the monomial ordering $y > x$. It is easy to see that I_y is the trivial ideal $\{0\}$, which would seem to imply that for any value of y, there is a value for x which yields a complete solution. But this is obviously not true over a field such as the real numbers which is not algebraically closed.

Next consider $I = \langle xy - 1, xz - 1 \rangle$ using the ordering $x > y > z$ over an algebraically closed field. Then $z - y = y(xz - 1) - z(xy - 1) \in I_x$, and in fact $I_x = \langle z - y \rangle$. Clearly $(0, 0) \in \mathbf{V}(I_x)$, but there is no value for x which extends to a complete solution $(x, 0, 0)$ for the polynomials in I. On closer inspection we see that the polynomials g_i defined in the theorem are

$$g_1 = y$$

and

$$g_2 = z.$$

Then we have $\mathbf{V}(g_1, g_2) = \mathbf{V}(y, z) = \{(0, 0)\}$, and so no extension was expected for this point.

Recall also remember the resultant function. Given two polynomials $h_1(x) = c_0 + c_1 x + \cdots + c_n x^n$ and $h_2(x) = d_0 + d_1 x + \cdots + d_m x^m$, with $c_n \neq 0$ and $d_m \neq 0$, the question arises, can we find two lower degree polynomials $u(x) = u_0 + u_1 x + \cdots + u_{m-1}x^{m-1}$ and $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$ such that $u(x)h_1(x) + v(x)h_2(x) = 1$? This reduces to a system of linear equations in the coefficients of x represented by the matrix:

$$\begin{bmatrix} c_0 & & & & d_0 & & & \\ c_1 & c_0 & & & d_1 & d_0 & & \\ & c_1 & \ddots & & & d_1 & \ddots & \\ \vdots & & \ddots & c_0 & \vdots & & \ddots & d_0 \\ c_n & \vdots & & c_1 & d_m & \vdots & & d_1 \\ & c_n & & & & d_m & & \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & c_n & & & & d_m \end{bmatrix}$$

The determinant of this matrix is the resultant of h_1 and h_2 with respect to x, $Res(h_1, h_2, x)$. Of course, if the coefficients c_i and d_j are polynomials in variables y_k, then the resultant will also be a polynomial in these variables.

Now we are ready to prove the extension theorem.

Proof: We will begin with the special case $n = 0, s = 2$. This is equivalent to asking, "Do the polynomials $f_1(x)$ and $f_2(x)$ have a common root?" Symbolically, this becomes

$$\begin{aligned} \exists a : f_1(a) = f_2(a) = 0 \quad &\Leftrightarrow \quad gcd(f_1, f_2) \neq 1 \\ &\Leftrightarrow \quad \forall u(x) \forall v(x), uf_1 + vf_2 \neq 1 \\ &\Leftrightarrow \quad 1 \notin \langle f_1, f_2 \rangle \\ &\Leftrightarrow \quad \langle 1 \rangle \neq I_x \end{aligned}$$

Note that I_x is either $\{0\}$ or $\langle 1 \rangle$, and these two cases are equivalent to the existence and nonexistence of a solution, respectively.

The next case to consider is again $s = 2$, but with $n > 0$. Let the two polynomials be $f_1(x, y_1, \ldots, y_n)$ and $f_2(x, y_1, \ldots, y_n)$ and let $I = \langle f_1, f_2 \rangle$. Let $p(y_1, \ldots, y_n) = Res(f_1, f_2, x)$, and note that $p \in I_x$. Let $(a_1, \ldots, a_n) \in \mathbf{V}(I_x)$. Then $p(a_1, \ldots, a_n) = 0$. It must now be shown that there is some a such that $f_1(a, a_1, \ldots, a_n) = f_2(a, a_1, \ldots, a_n) = 0$ if $(a_1, \ldots, a_n) \notin \mathbf{V}(g_1, g_2)$.

Define $h_i(x) = f_i(x, a_1, \ldots, a_n)$. Assuming $(a_1, \ldots, a_n) \notin \mathbf{V}(g_1, g_2)$, it cannot be that both $g_1(a_1, \ldots, a_n)$ and $g_2(a_1, \ldots, a_n)$ are zero. If neither are zero, then

$$\begin{aligned} Res(h_1, h_2, x) &= Res(f_1, f_2, x)(a_1, \ldots, a_n) \\ &= p(a_1, \ldots, a_n) \\ &= 0. \end{aligned}$$

But this means that there are no polynomials $u(x), v(x)$ such that $u(x)h_1(x) + v(x)h_2(x) = 1$, which from above implies that h_1 and h_2 have a common root a. This root provides an extension to the partial solution such that $f_1(a, a_1, \ldots, a_n) = f_2(a, a_1, \ldots, a_n) = 0$.

If one is zero, say $g_2(a_1, \ldots, a_n)$, then it is not true that $Res(h_1, h_2, x) = Res(f_1, f_2, x)(a_1, \ldots, a_n)$, since the definition of the resultant requires nonzero leading coefficients. But consider the ideal $\langle f_1, f_2 + x^r f_1 \rangle$. It is easy to see that this ideal is identical to $\langle f_1, f_2 \rangle$, so a solution to one pair of functions is a solution to the other. Furthermore, it is always possible to choose r high enough that, viewing f_1 and f_2 as polynomials in x with coefficients which are polynomials in y, the leading coefficient of $f_2 + x^r f_1$ is the same as the leading coefficient of f_1. Then the leading coefficients of both functions are nonzero at the partial solution $(a_1, \ldots, a_n)$, and the existence of an extension to a complete solution is guaranteed by the previous argument.

Now the proof is complete in the case where $s = 2$. In the case where $s > 2$, we will reduce to the proven case by trading off excess polynomials for additional variables.

Let $f_1, \ldots, f_s$ be given, and let $(a_1, \ldots, a_n) \in \mathbf{V}(I_x(f_1, \ldots, f_s))$ be a partial solution. Order the f_i so that $g_1(a_1, \ldots, a_n) \neq 0$.

Define $U(x, y_1, \ldots, y_n, u_2, \ldots, u_n) = \sum_{i=2}^{s} u_i f_i(x, y_1, \ldots, y_n)$. Consider the resultant of U and f_1 with respect to x written as a sum of monomials in the new variables u_i with coefficients which are polynomials in y_i. Let the coefficients be h_α; then $Res(f_1, U, x) = \sum_\alpha h_\alpha(y_1, \ldots, y_n) u^\alpha$. It can be shown that $h_\alpha \in \langle f_1, \ldots, f_s \rangle_{\{x\}}$. This means that $h_\alpha(a_1, \ldots, a_n) = 0$, so $Res(f_1, U, x)(a_1, \ldots, a_n, u_2, \ldots u_s) = 0$.

Now let $\tilde{f_1}(x) = f_1(x, a_1, \ldots, a_n)$ and $\tilde{U}(x, u_2, \ldots, u_s) = U(x, a_1, \ldots, a_n, u_2, \ldots, u_s)$. As in the previous case, we have, possibly after replacing $\tilde{U}$ with $\tilde{U} + x^r f_1$, $Res(\tilde{f_1}, \tilde{U}, x) = 0$. This implies that $\tilde{f_1}(x)$ and $\tilde{U}(x, u_2, \ldots, u_s)$ have a common factor, which must be of the form $(x - a)$ for some a since $\tilde{f_1}$ does not contain any of the u_i. But then $\tilde{U}(a, u_2, \ldots, u_s) = 0$, from which it is easy to see that $f_i(a, a_1, \ldots, a_n) = 0$ for all i. Thus an extension exists in this final case, and the theorem is proved. ■

2 Hilbert's Nullstellensatz

Now that we have answered the question of when we can find a point in a variety of a set of polynomials, it is logical to ask when we cannot. In other words, given a set of polynomials $f_1, \ldots, f_s$, how can we claim that $\forall a_1, \ldots, a_n, \exists i : f_i(a_1, \ldots, a_n) \neq 0$, or, equivalently, $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$?

Consider a random invertible linear transform R and define $(y_1, \ldots, y_n)^T = R^{-1}(x_1, \ldots, x_n)^T$. Set $\tilde{f_i}(y_1, \ldots, y_n) = f_i(R(y_1, \ldots, y_n))$. The new functions $\tilde{f_i}$ will have a common root if and only if the original f_i do. Note that because R has no effect on constant polynomials, $1 \in \tilde{I} = \langle \tilde{f_1}, \ldots, \tilde{f_s} \rangle \Rightarrow \langle f_1, \ldots, f_s \rangle$.

There is some transform R such that the new polynomials $\tilde{f_i}$ are monic in y_1. By the extension theorem, if $\tilde{I_1}$ has a common root, then it extends to a common root of $\tilde{I}$. Assuming then that there is no root, it can be shown by induction that $1 \in \tilde{I_1}$, which implies that $1 \in \tilde{I}$, which agin implies that $1 \in \langle f_1, \ldots, f_s \rangle$.

This argument shows that the Extension Theorem leads to the following result, due to Hilbert.

Theorem 3 (Weak Nullstellensatz) *Given a set of polynomials $f_1, \ldots, f_s$ over an algebraically closed field, $1 \in \langle f_1, \ldots, f_s \rangle$ if and only if $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$.*