6.885 Algebra and Computation November 21, 2005

Lecture 20

Lecturer: Madhu Sudan *Scribe: Eitan Reich*

1 Today

- Hilbert's Nullstellensatz

2 Generic/Random Linear Transformations

Given an ideal in $K[x_1, ..., x_n]$, our goal is to find a basis for this ideal that is in a nice form. For example, we might want a basis consisting of only monic polynomials.

We use the notion of a linear map ϕ on our variables that defines a mapping over $K[x_1, ..., x_n]$ as follows:

$$f(x_1, ..., x_n) \rightarrow \tilde{f}(x_1, ..., x_n) = f(\phi(x_1, ..., x_n))$$

The transformation ϕ can be represented by a lower-triangular matrix $[\lambda_{i,j}]$ where the $\lambda_{i,i} \neq 0$. This gives us an associated map from $K^n \rightarrow K^n$ given by $a \rightarrow \tilde{a} = \phi^{-1}(a)$, in addition to our map from $K[x] \rightarrow K[x]$ mapping f to $\tilde{f}$, such that the following properties hold:

- $f(a) = 0 \iff \tilde{f}(\tilde{a}) = 0$
- $f \tilde{+} g = \tilde{f} + \tilde{g}$
- $\tilde{fg} = \tilde{f}\tilde{g}$
- deg $f \geq$ deg $\tilde{f}$

Claim 1 *With high probability over the choices of $\{\lambda_{i,j}\}$, $\tilde{f}$ is monic in the variable x_1.*

Proof Given a polynomial f, we first write $f(x_1, ..., x_n) = g(x_1, ..., x_n) + g_1(x_1, ..., x_n)$ where g is homogeneous of deg f and g_1 has a smaller degree than f. To see that $\tilde{f}$ is monic in x_1, we subsitute 0 for all of the other variables: $\tilde{f}(x_1, 0, ..., 0) = f(\lambda_{1,1}x_1, \lambda_{2,1}x_1, ..., \lambda_{n,1}x_1) = g(\lambda_{1,1}, \lambda_{2,1}, ..., \lambda_{n,1})x_1^{degf} + g_1(\lambda_{1,1}x_1, \lambda_{2,1}x_1, ..., \lambda_{n,1}x_1)$. Since with high probability the coefficient of the x_1^{degf} term is nonzero, and the g_1 term has smaller degree, we know that the polynomial $\tilde{f}$ is monic in x_1. ■

3 Varieties and Radicals

- Given an ideal I in $K[x_1, ..., x_n]$, we define $V(I) = \{\bar{a} \in K^n | f(\bar{a}) = 0 \forall f \in I\}$
- A set $V \subseteq K^n$ is a variety if there exists an ideal $I \subseteq K[x]$ such that $V = V(I)$
- Given a variety V, we define $I(V) = \{f \in K[x] | f(a) = 0 \forall a \in V\}$. We note that it is clear to show that $I \subseteq I(V(I))$
- Given an ideal I, we define the Radical of I by $Rad(I) = \{f \in K[x] | \exists m \in Z, f^m \in I\}$. It is also clear that $Rad(I) \subseteq V(I)$

4 Weak and Strong Nullstellensatz

Theorem 2 (Weak Nullstellensatz) *For an ideal I, $V(I) = \emptyset \iff 1 \in I$*

In other words, this theorem states that functions $f_1...f_m(x_1, ..., x_n)$ don't have simultaneous roots if and only if $\exists q_1, ..., q_m$ such that $1 = \Sigma f_i q_i$. The Strong Nullstellensatz will be used to help prove the Weak Nullstellensatz.

Theorem 3 (Strong Nullstellensatz) $\forall I \subseteq K[x_1, ..., x_n]$, *$K$ algebraically closed* $\Rightarrow$ *$Rad(I) = I(V(I))$*

We will begin by proving the easy directions for both the Weak and Strong Nullstellensatz.

Lemma 4 (Easy Part of Weak Nullstellensatz) *For an ideal I, $1 \in I \Rightarrow V(I) = \emptyset$*

Proof $1 \in I(f_1, ..., f_m) \Rightarrow \exists q_1, ..., q_m$ such that $1 = \Sigma q_i f_i$ by the definition of the ideal. Given arbitrary $a \in K^n$ we know $1 = \Sigma q_i(a) f_i(a)$ by substitution. This implies $\exists i, f_i(a) \neq 0 \Rightarrow a \notin V(I)$. Since a was chosen arbitrarily in K^n, this implies that $V(I) = \emptyset$. ■

Lemma 5 (Easy Part of Strong Nullstellensatz) $\forall I \subseteq K[x_1, ..., x_n]$, *$K$ algebraically closed*
$\Rightarrow$ *$Rad(I) \subseteq I(V(I))$*

Proof Given $f \in Rad(I)$, we wish to show that $f \in I(V(I))$. $f \in Rad(I) \Rightarrow f^D \in I$ by the definition of the radical. Because f^D is in the ideal, we know that $f^D = \sum_{i=1}^{m} q_i f_i$. By substution we see that $\forall a \in V(I), f^D(a) = \sum_{i=1}^{m} q_i(a) f_i(a) = 0 \Rightarrow f(a) = 0 \Rightarrow f \in I(V(I))$. ■

To prove the other directions of the Weak and Strong Nullstellensatz, we will first prove that they are equivalent and then use an extension lemma to prove the Weak Nullstellensatz.

Lemma 6 (Strong Nullstellensatz $\Rightarrow$ Weak Nullstellensatz) *For an ideal I, $I(V(I)) \subseteq Rad(I)$, $V(I) = \emptyset \Rightarrow 1 \in I$*

Proof

We first show that $1 \in I(V(I))$. This is true since $V(I) = \emptyset$ and $I(\emptyset) = K[x]$ which contains 1. By the Strong Nullstellensatz, which tells us that $I(V(I)) \subseteq Rad(I)$, we know that $1 \in Rad(I)$. By the definition of the radical, this implies that there is some integer D such that $1^D \in I$. But $1^D = 1$ for all D, which means that $1 \in I$. ■

Lemma 7 (Weak Nullstellensatz $\Rightarrow$ Weak Nullstellensatz (Rabinowich's Trick)) $(V(I) = \emptyset \Rightarrow 1 \in I) \Rightarrow I(V(I)) \subseteq Rad(I)$

Proof We begin by taking an arbitrary polynomial $f \in I(V(I))$ and we wish to show $f \in Rad(I)$. We know $f(a) = 0$ whenever $f_1, ..., f_m(a) = 0$ by the definition of the variety. We wish to show that there exists some integer D and polynomials q_i such that $f^D = \Sigma q_i f_i$.

We want a polynomial g that is not zero whenever $f_1, ..., f_m = 0$. So we take $g = 1 - yf(x_1, ..., x_n)$ and look at the ideal I' generated by $f_1, ..., f_n$ and the polynomial g. Because $g \neq 0$ whenever the $f_i = 0$, the polynomials generating I' can never all be zero at the same time, which means that $V(I') = \emptyset$. By the Weak Nullstellensatz, this implies that $1 \in I'$. So there exists $q'_1, ..., q'_m, q \in K[x_1, ..., x_n, y]$ such that $1 = \Sigma q'_i f_i + qg$. Using this identity over $K(x_1, ..., x_n)[y]$ and substituting $y = \frac{1}{f(x_1,...,x_n)}$ (which is a valid element since f is not zero), we get $1 = \Sigma q'_i(x_1, ..., x_n, \frac{1}{f(x_1,...,x_n)}) f_i + q[1 - \frac{1}{f} f] =$

$\Sigma q_i'(x_1, ..., x_n, \frac{1}{f})f_i$. Multiplying both sides of this equality by a sufficiently large power of f, f^D. gives us $f^D = \Sigma(q_i'(x_1, ..., x_n, \frac{1}{f})f^D)f_i$, where $q_i'(x_1, ..., x_n, \frac{1}{f})f^D = q_i \in K[x_1, ..., x_n]$, so that f^D is generated by the f_i over polynomials in $K[x_1, ..., x_n]$ which proves that $f \in Rad(I)$. ■

Now we just need to prove a single direction of either the Weak or Strong Nullstellensatz to complete our proof. We will do this by using the following extension lemma, which we will prove later, to prove the direction needed in the Weak Nullstellensatz.

Lemma 8 (Extension Lemma) *Given polynomials $f_1, ..., f_m(x_1, ..., x_n) \in (K[x_1, ..., x_{n-1}])[x_n]$ monic in x_n, let $I' = I(f_1, ..., f_m) \cap K[x_1, ..., x_{n-1}]$. Suppose $(a_1, ..., a_{n-1}) \in V(I')$. Then $\exists a_n$ such that $(a_1, ..., a_n) \in V(I(f_1, ..., f_m))$.*

We will prove this lemma later, but use it now to prove the Weak Nullstellensatz.
Proof [of Weak Nullstellensatz assuming extension lemma] Given our ideal I, we will assume $1 \notin I$. We wish to show that $V(I) \neq \emptyset$. Let I' be the ideal defined in the extension lemma. Because this ideal is contained in I, $1 \notin I \Rightarrow 1 \notin I'$. By our induction hypothesis, we can assume that $\exists(a_1, ..., a_{n-1}) \in I'$. By the extension lemma, this implies that there exists some a_n such that $(a_1, ..., a_n) \in V(I)$. This implies that $V(I) \neq \emptyset$. ■

In order to prove our extension lemma, we will have an aside on classical resultants.

5 Classical Resultants

The classical resultant is defined in terms of polynomials and their roots.

Definition 9 *Suppose we are working over an algebraically closed field K, with monic polynomials $f(x)$ and $g(x)$ that factor into $f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_m)$ and $g(x) = (x - \beta_1)(x - \beta_2)...(x - \beta_n)$. We define the resultant of f and g by $Res(f, g) = \Pi_i \Pi_j (\alpha_i - \beta_j)$.*

The resultant as defined above has the following properties:

- $Res(f, g) = 0 \iff f, g$ have a common root over K, where K is the algebraic clousure of $\tilde{R}$,
- $Res(f, g) \in R$
- $Res(f, g) = 0 \iff f, g$ have a common factor in $R[x]$

We use the idea of resultants to answer the question of finding polynomials $a(x)$ and $b(x)$ of degrees smaller than g and f respectivelysuch that $a(x)f(x) + b(x)g(x) = 1$ for monic polynomials f and g that have no common factor in $\tilde{R}[x]$. If $f_0, ..., f_n$ are the coefficients of f and $g_0, ..., g_m$ are the coefficients of g, then this amounts to finding coefficients $a_0, ..., a_{m-1}$ and $b_0, ...b_{n-1}$ such that $\Sigma a_j f_{i-j} + \Sigma b_j gi - j = \delta_{i0}$ where $\delta_{i0} = 1$ if $i = 0$ and 0 otherwise. This amounts to solving a system of linear equations whose determinant is nonzero only if the system is solvable. Call the matrix of this system M. Then we know:

- $Det(M) \neq 0 \rightarrow$ we can solve the linear system.
- $Det(M) = Res(f, g) \iff Res(f, g) \in K$
- $Res(f, g) \in I(f, g)$

We can now use this relationship between resultants and the determinant of M to prove the extension lemma which we define again here.

Lemma 10 (Extension Lemma) *Given polynomials $f_1, ..., f_m(x_1, ..., x_n) \in (K[x_1, ..., x_{n-1}])[x_n]$ monic in x_n, let $I' = I(f_1, ..., f_m) \cap K[x_1, ..., x_{n-1}]$. Suppose $(a_1, ..., a_{n-1}) \in V(I')$. Then $\exists a_n$ such that $(a_1, ..., a_n) \in V(I(f_1, ..., f_m))$.*

Proof We begin with the proof for the special case that $m = 2$. We have two polynomails $f_1(x_1, ..., x_n)$ and $f_2(x_1, ..., x_n)$ and we would like to find a common root. We look at the resultant $R(x_1, ..., x_{n-1}) = Res_{x_n}(f_1, f_2) \in I'$. By assumption we have $(a_1, ..., a_{n-1}) \in V(I')$, $R(a_1, ..., a_{n-1}) = 0$. We set $h_1(x_n) = f_1(a_1, ..., a_{n-1}, x_n), h_2(x_n) = f_2(a_1, ..., a_{n-1}, x_n)$ and look at their resultant: $Res_{x_n}(h_1, h_2) = R(a_1, ..., a_{n-1}) = 0$ which implies that h_1 and h_2 have a common factor. Since we are working over an algebraically closed field, this implies that h_1 and h_2 have a common root, so that there is some one degree polynomial $(x - a_n)$ that divides both h_1 and h_2. So we have a common zero $(a_1, ..., a_n)$ of $f_1(x_1, ..., x_n)$ and $f_2(x_1, ..., x_n)$.

To prove the general case for arbitrary m, we begin with m polynomials $f_1, ..., f_m(x_1, ..., x_n)$ and we would like to find a common root for these polynomials. We combine these into a single polynomial with more variables as follows:

$$F_2(x_1, ..., x_n, y_2, ..., y_m) = \sum_{i=2}^{m} f_i(x_1, ..., x_n) y_i$$

We then look at the resultant of f_1 and F_2:

$$R(x_1, ..., x_{n-1}, y_2, ..., y_m) = Res_{x_n}(f_1, F_2) = \sum_{\bar{\alpha}} h_\alpha(x_1, ..., x_{n-1}) \bar{y}^{\bar{\alpha}}, h_\alpha \in I' \rightarrow R(a_1, ..., a_{n-1}, y_2, ..., y_m) = 0$$

This will allow us to find a common factor:

$$(x - a_n(y_2 ... y_m)) | f_1(a_1, ..., a_{n-1}, x_n), F_2(a_1, ..., a_{n-1}, x_n, y_2, ..., y_m)$$

But $a_n(y_2 ... y_m) \in K$, which implies that $(x - a_n)$ divides the two polynomials. This means that $(x - a_n)$ is a common factor of all of the f_i. ■