6.966 Algebra and Computation	November 2, 1998
Lecture 16	
Lecturer: Madhu Sudan	*Scribe: Leonid Reyzin*

Nullstellensatz

To review, we've been considering the following two questions, given s polynomials $f_1, \ldots, f_s$ in n variables over a field K of maximum total degree d.

1. Do they have a common zero? That is, is their variety non-empty?
2. Is a given polynomial f in the ideal $I(f_1, \ldots, f_s)$? That is, do there exist polynomials $q_1, \ldots, q_s \in K[x_1, \ldots, x_n]$ such that $f = \sum q_i f_i$.

Two lectures ago we proved a doubly exponential upper bound on the q_i's for question 2. One lecture ago we proved a relationship between the two questions (for $f = 1$) with the theorem known as "Hilbert's Nullstellensatz." We review the main idea of the proof below.

In order to find the answer to the first question, we can try to find a point $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$. We can reduce the number of dimensions by considering

$$\Pi_1 = \{(a_2, \ldots, a_n) | \exists a_1 : (a_1, a_2, \ldots, a_n) \in V(f_1, \ldots, f_s)\}.$$

Then we can first look for a point in Π_1 and then extend it to a point in $V(f_1, \ldots, f_s)$ by looking for a common zero of the s univariate polynomials $f_i(x_1, a_2, \ldots, a_n)$ for $1 \leq i \leq s$.

It seems that, at least in principle, finding a common zero should not be hard. The hard part is looking for the point in Π_1. The hope is that Π_1 is itself a variety : $\exists g_1, \ldots, g_t \in K[x_2, \ldots, x_n]$ such that $\Pi_1 = V(g_1, \ldots, g_t)$.

We weren't quite able to prove that. We were able to prove, however, that Π_1 contains a variety if K is algebraically closed and $f_1, \ldots, f_s$ are monic in x_1 (this is the Extension Theorem). More specifically, let

$$f_i = x_1^{d_i} g_i(x_2, \ldots, x_n) + x_1^{d_i - 1} \ldots$$

and let

$$\begin{aligned} I_1 &= I(f_1, \ldots, f_s) \cap K[x_2, \ldots, x_n] \\ J &= I(g_1, \ldots, g_s). \end{aligned}$$

For a point $(a_2, \ldots, a_n) \in V(I_1) - V(J)$, there exists an extension a_1 such that $(a_1, a_2, \ldots, a_n) \in V(I)$. So, we get that $V(I_1) - V(J) \subseteq \Pi_1$. This was enough to prove the following theorem.

Theorem 1 *(Hilbert's Weak Nullstellensatz.) If K is algebraically closed, then $(f_1, \ldots, f_s)$ have a common zero if and only if $1 \notin I(f_1, \ldots, f_s)$.*

We will now work towards a strong version of Nullstellensatz.

So far, we have been considering the case of $V = \emptyset$ or $V \neq \emptyset$. But varieties have more geometric meaning, and we'd like to look more closely at the ideals when $V \neq \emptyset$.

Let V be a set of points in K^n. Define the ideal defining V as $I(V) = \{f \in K[x_1, \ldots, x_n] | f(x) = 0\ \forall x \in V\}$.

To better understand the definition, consider the following examples. Let $f_1 = x^2 - y^2$ and $f_2 = x + y$. Then $V(f_1, f_2) = \{(x, y) | x + y = 0\}$. Therefore, $I(V(f_1, f_2)) = \{(x+y)p(x, y) | \forall p(x, y) \in K[x, y]\} = I(x+y) = I(f_1, f_2)$. Now let $f_1 = (x+y)^2(x-y)^2$ and $f_2 = (x+y)^2$. Note that $V(f_1, f_2)$ is still the same, and therefore $I(V(f_1, f_2)) = I(x+y)$, even though $I(f_1, f_2) = I((x+y)^2)$.

Definition 2 *A radical for an ideal I is* $\mathrm{Rad}(I) = \{f | \exists m > 0 : f^m \in I\}$.

$\mathrm{Rad}(I)$ is an ideal. The proof is left as an exercise to the reader.

This definition together with the following theorem explain what happened in the example above.

Theorem 3 *(Strong Nullstellensatz.) If K is algebraically closed, and $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, then* $\mathrm{Rad}(I(f_1, \ldots, f_s)) = I(V(I(f_1, \ldots, f_s)))$.

First, we'd like to note that Strong Nullstellensatz easily implies Weak Nullstellensatz, as expected. Indeed, if $V(f_1, \ldots, f_s) = \emptyset$, then $1 \in I(V(f_1, \ldots, f_s))$ (by definition of the ideal defining a variety), so $1 \in \mathrm{Rad}(I(f_1, \ldots, f_s))$ (by Strong Nullstellensatz), so $1 \in I(f_1, \ldots, f_s)$. The converse doesn't even need Strong Nullstellensatz: if $1 \in I(f_1, \ldots, f_s)$, then $1 = \sum q_i f_i$; if all the f_i's have a common zero, evaluate at it to get $1 = 0$.

We will now use the Weak Nullstellensatz to prove the Strong Nullstellensatz. Note that we are not involved in circular reasoning here, because we originally proved the Weak Nullstellensatz without the Strong Nullstellensatz.

Proof Let $I = I(f_1, \ldots, f_s)$ and $V = V(I)$. Suppose $f \in \mathrm{Rad}(I)$. We need to show that $f \in I(V)$, i.e., that f vanishes on every point in V. Since $f \in \mathrm{Rad}(I)$, $f^m \in I$, so f^m vanishes on every point in V. Therefore, so does f.

Now, suppose $f \in I(V)$. We need to show that $f \in \mathrm{Rad}(I)$. If $f = 0$, we are done. So assume $f \neq 0$. We will use Rabinowitsch's trick. Consider the polynomials $f_1, \ldots, f_s, 1 - yf$, for a new variable y. Note that if for some point $a = (a_1, \ldots, a_n, b)$ we have that $f_1(a) = \cdots = f_s(a) = 0$, then $f(a) = 0$ (because $(a_1, \ldots, a_n) \in V$ and f vanishes on V), so $1 - yf \neq 0$. Therefore, $V(f_1, \ldots, f_s, 1 - yf) = \emptyset$. Therefore, by the Weak Nullstellensatz, $1 \in I(f_1, \ldots, f_s, 1 - yf)$. Therefore, for some $q_1, \ldots, q_s$ and $p \in K[x_1, \ldots, x_n, y]$ we have that

$$1 = \left(\sum_{i=1}^{s} q_i(x_1, \ldots, x_n, y) f_i(x_1, \ldots, x_n) \right) + (1 - yf(x_1, \ldots, x_n))\, p(x_1, \ldots, x_n).$$

Note that this identity holds over $K[x_1, \ldots, x_n, y]$ and therefore also over $K(x_1, \ldots, x_n)[y]$. Now substitute $y = \frac{1}{f(x_1, \ldots, x_n)}$ ($f \neq 0$, so this is allowed). Then

$$1 = \sum_{i=1}^{s} q_i \left(x_1, \ldots, x_n, \frac{1}{f} \right) f_i(x_1, \ldots, x_n).$$

If we let m be the maximum degree of q_i in y, then multiplying through by f^m we get rid of the denominators to get

$$f^m = \sum_{i=1}^{s} \left(f^m q_i \left(x_1, \ldots, x_n, \frac{1}{f} \right) \right) f_i(x_1, \ldots, x_n).$$

Since f is a polynomial only in $x_1, \ldots, x_n$, this identity holds in $K[x_1, \ldots, x_n]$. Therefore, we expressed f^m as a linear combination of $f_1, \ldots, f_s$, so $f^m \in I$, so $f \in \mathrm{Rad}(I)$. ■

The above proof shows that $f \in \mathrm{Rad}(I(f_1, \ldots, f_s))$ if $1 \in I(f_1, \ldots, f_s, 1 - yf)$. The converse also holds: if $1 \notin I(f_1, \ldots, f_s, 1 - yf)$, then by Nullstellensatz some point $(a_1, \ldots, a_n, b)$ is a common zero for $(f_1, \ldots, f_s, 1 - yf)$. Note that $f(a_1, \ldots, a_n) \neq 0$, because otherwise the last polynomial would 1. Therefore, f is not zero at some point where $f_1, \ldots, f_s$ are zero; therefore, $f^m \notin I(f_1, \ldots, f_s)$ for any m, and hence $f \notin \mathrm{Rad}(I(f_1, \ldots, f_s))$.

Thus, to check if $f \in \mathrm{Rad}(I(f_1, \ldots, f_s))$ one can just check if $1 \in I(f_1, \ldots, f_s, 1 - yf)$. This is a PSPACE question (because, by some recent results, checking if 1 is a member of an ideal is in PSPACE). On the other hand, to check if $f \in I(f_1, \ldots, f_s)$ is EXPSPACE-complete.

Quantifier Elimination

Suppose we are given a boolean formula φ in s variables. Let $f_1, \ldots, f_s$ be n-variate polynomials of maximum total degree d over an algebraically closed field K. Let $Q_1, \ldots, Q_w$ be quantifiers ($Q_i \in \{\forall, \exists\}$). And finally, let $x_1, \ldots x_n$ be n variables divided into $w+1$ blocks $x^{[0]}, x^{[1]}, \ldots, x^{[w]}$. Note that whether $f_i(x_1, \ldots, x_n) = 0$ is a boolean variable whose value depends on $x_1, \ldots, x_n$. This boolean variable can be used as input to φ. Then we can consider the following quantified formula:

$$F(x^{[0]}) = Q_1 x^{[1]} \ldots Q_w x^{[w]} \varphi(f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0),$$

whose boolean value depends on the variables in the block $x^{[0]}$. Let m be the number of variables in $x^{[0]}$.

(Note that if $f_i = 1 - x_i$, then deciding the value of this formula is a complete problem for a level of the polynomial hierarchy (if w is bounded) or for PSPACE (if w is unbounded).)

We are required to output a boolean formula ψ on t variables and polynomials $g_1, \ldots, g_t$ in m variables of degree at most D such that

$$\psi(g_1(x^{[0]}) = 0, \ldots, g_t(x^{[0]}) = 0) = F(x^{[0]}).$$

Note that *a priori* it's not even clear that it is possible to eliminate quantifiers, i.e., that such ψ exists. Here and in the next lecture we will prove that they do and obtain reasonable bounds on t, D and the size of ψ.

A simple special case

Consider the case when $w = 1$, $Q_1 = \exists$, and $\varphi = \wedge$. Then

$$F(x^{[0]}) = \exists x^{[1]} \bigwedge_{i=1}^{s} (f_i(x^{[0]}, x^{[1]}) = 0).$$

By the Nullstellensatz, we know that for any particular $x^{[0]}$, $\neg F(x^{[0]}) \Leftrightarrow \exists q_1, \ldots, q_s \in K[x^{[1]}]$ s.t. $1 = \sum_{i=1}^{s} q_i f_i$.

Thus, all we need to do is to attempt to find such $q_1, \ldots, q_s$. We can do so by setting up a system of linear equations $Ay = b$, where A is a matrix and b is a vector with coefficients from $K[x^{[0]}]$. This system has a solution if and only if $\mathrm{rank}(A) \geq \mathrm{rank}(A|b)$. Thus, we can construct ψ as follows:

$$\psi(x^{[0]} = \bigwedge_{k} (\mathrm{rank}(A|b) < k \vee \mathrm{rank}(A) \geq k)$$

The only remaining question now is how to express for some matrix X that $\mathrm{rank}(X) < k$?

For a set S of row-numbers and T of column-numbers such that $|S| = |T| = i$, let $A_{S,T}$ denote the $i \times i$ minor of the matrix A consisting of the entries at the intersections of the rows whose numbers are in S and the columns whose numbers are in T. Consider $\det(A_{S,T})$. It is a polynomial in $x^{[0]}$ of degree about D^n. Denote it by $p_{S,T}(x^{[0]})$.

We can now express $\mathrm{rank}(A) < k$ by a statement that the determinants of all the minors of size k are 0:

$$\bigwedge_{S,T,|S|=|T|=k} (p_{S,T}(x^{[0]}) = 0).$$

This looks promising, except for one problem: there are too many elements under the $\bigwedge$, because there are too many size k minors possible. However, all we need is a small subset of all possible $p_{S,T}$: namely, those that generate an ideal that contains the rest. Since there are about D^{n^2} coefficients in each $p_{S,T}$, there can't be too many linearly independent polynomials. So, all we need to do is to find a linearly independent subset of all $p_{S,T}$ that generates the rest. Such a set can be found using Gaussian elimination. The details are left as an exercise to the reader.

In the next lecture, we will perform a series of generalizations to show how to do quantifier elimination for any formula.