6.S897 Algebra and Computation April 11, 2012

Hilbert Nullstellensatz & Quantifier Elimination

Instructor: Madhu Sudan *Scribe: Alessandro Chiesa*

Throughout, $\mathbb{K}$ will denote an algebraically closed field.

Recall that, given a (commutative) ring R, an *ideal* I of R if $I \subseteq R$, I is closed under addition (i.e., $a, b \in I \implies a + b \in I$) and under multiplication by elements of R (i.e., $a \in I, r \in R \implies ra \in I$).

Also recall that a subset V of $\mathbb{K}^n$ is an *(affine) variety* if it is the locus of points where some set of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ vanish simultaneously.

For more details about ideals and varieties (including further discussions and more detailed proofs for the Hilbert Nullstellensatz, which we will cover today), see [CLO07].

1 From Ideals to Varieties and Back

When studying polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, we can choose an algebraic or geometric perspective; these two perspectives respectively give rise to the notions of the ideal and the variety of $\{f_1, \ldots, f_m\}$.

Definition 1.1. *The* ideal *of* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *is the set of polynomials*

$$\text{Ideal}(f_1, \ldots, f_m) = \left\{ \sum_{i=1}^{m} q_i f_i \;\middle|\; q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n] \right\} .$$

Definition 1.2. *The* variety *of* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *is the set of points*

$$\text{Var}(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n \mid f_1(a_1, \ldots, a_n) = \cdots = f_m(a_1, \ldots, a_n) = 0\} .$$

More generally, given a variety V in $\mathbb{K}^n$ and an ideal I in $\mathbb{K}[x_1, \ldots, x_n]$, we can define

$$\begin{aligned} \text{Ideal}(V) &= \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in \mathbb{K}^n\} , \\ \text{Var}(I) &= \{(a_1, \ldots, a_n) \in \mathbb{K}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\} . \end{aligned}$$

2 Radical of an Ideal

An important notion that we shall need today is the radical of an ideal:

Definition 2.1. *The* radical *of an ideal* I*, denoted* $\text{Rad}(I)$*, is the set defined as follows:*

$$\text{Rad}(I) = \left\{ f \in \mathbb{K}[x_1, \ldots, x_n] \;\middle|\; \textit{there is a positive integer } d \textit{ s.t. } f^d \in I \right\} .$$

The radical of an ideal is in fact an ideal itself:

Lemma 2.2. *If* I *is an ideal, then so is* $\text{Rad}(I)$*.*

Proof. Suppose that $f \in \mathrm{Rad}(I)$ and let $h \in \mathbb{K}[x_1, \ldots, x_n]$. From the definition of $\mathrm{Rad}(I)$, we know that there is a positive integer d such that $f^d \in I$. Since I is an ideal, we also know that $h^d f^d \in I$. But this means that $hf \in \mathrm{Rad}(I)$ as well.

Let $g \in \mathrm{Rad}(I)$. Again from the definition of $\mathrm{Rad}(I)$, we know that there is a positive integer e such that $g^e \in I$. Note that $(f+g)^{d+e} = \sum_{i=0}^{d+e} \binom{d+e}{i} f^i g^{d+e-i}$ is a sum of terms each of which is divisible by either f^d or g^e, so that $(f+g)^{d+e} \in I$, and thus $f+g \in \mathrm{Rad}(I)$. □

Note also that $\mathrm{Rad}(\cdot)$ is idempotent: $\mathrm{Rad}(\mathrm{Rad}(\cdot)) = \mathrm{Rad}(\cdot)$.

3 The Hilbert Nullstellensatz

Note that $\mathrm{Var}(\mathrm{Ideal}(f_1, \ldots, f_m)) = \mathrm{Var}(f_1, \ldots, f_m)$. However, $\mathrm{Ideal}(\mathrm{Var}(f_1, \ldots, f_m))$ contains, **but is not necessarily equal to**, $\mathrm{Ideal}(f_1, \ldots, f_m)$. So when does the sequence of operations $\mathrm{Ideal}(\mathrm{Var}(\mathrm{Ideal}(\mathrm{Var}(\cdots))))$ converge?

A first observation is that, given an ideal I, $\mathrm{Ideal}(\mathrm{Var}(I))$ contains not only I but also its radical $\mathrm{Rad}(I)$. It actually turns out that $\mathrm{Ideal}(\mathrm{Var}(I))$ contains nothing more than $\mathrm{Rad}(I)$ — and thus we learn than the alternate application of $\mathrm{Ideal}(\cdot)$ and $\mathrm{Var}(\cdot)$ "stabilizes" at the radical.

Theorem 3.1 (Strong Hilbert Nullstellensatz (SHN))**.** *For any ideal I in $\mathbb{K}[x_1, \ldots, x_n]$,*

$$\mathrm{Ideal}(\mathrm{Var}(I)) = \mathrm{Rad}(I) \ .$$

In particular, $\mathrm{Ideal}(\mathrm{Var}(\mathrm{Rad}(I))) = \mathrm{Rad}(I)$.

The proof of the SHN relies on the following simpler theorem, which states that the only way that a variety of an ideal can be empty is if the ideal contains all the possible polynomials:

Theorem 3.2 (Weak Hilbert Nullstellensatz (WHN))**.** *For any ideal I in $\mathbb{K}[x_1, \ldots, x_n]$,*

$$\mathrm{Var}(I) = \emptyset \ \Leftrightarrow \ 1 \in I \ .$$

(Note that $1 \in I \ \Leftrightarrow \ I = \mathbb{K}[x_1, \ldots, x_n]$.)

Let us begin by showing the equivalence of the SHN and the WHN (and afterwards we shall prove WHN):

Lemma 3.3. *The SHN and the WHN are equivalent statements.*

Proof. Both the SHN and the WHN have trivial directions (respectively, $\mathrm{Ideal}(\mathrm{Var}(I)) \supseteq \mathrm{Rad}(I)$ and $\mathrm{Var}(I) = \emptyset \Leftarrow 1 \in I$), so we only need to prove the equivalence of the non-trivial directions of the SHN and the WHN (respectively, $\mathrm{Ideal}(\mathrm{Var}(I)) \subseteq \mathrm{Rad}(I)$ and $\mathrm{Var}(I) = \emptyset \Rightarrow 1 \in I$).

The easy implication is SHN $\implies$ WHN so let us begin with this one. So suppose that $\mathrm{Var}(I) = \emptyset$. Then, by the SHN, $\mathrm{Rad}(I) = \mathrm{Ideal}(\mathrm{Var}(I)) = \mathrm{Ideal}(\emptyset) = \mathbb{K}[x_1, \ldots, x_n]$. Hence, $1 \in \mathrm{Rad}(I)$ and thus $1 \in I$, as claimed in the WHN.

So let us turn to the other implication, WHN $\implies$ SHN; this direction follows what is known as the Rabinowitsch trick [Rab30].

Let $f \in \text{Ideal}(\text{Var}(I))$; we need to show that $f \in \text{Rad}(I)$. If f is identically 0, we are done; so assume that f is not identically 0. Consider the ideal J in $\mathbb{K}[x_1, \ldots, x_n, y]$, where y is an auxiliary variable, defined by $J = \text{Ideal}(I, 1 - yf)$.

Notice that $\text{Var}(J) = \emptyset$. Indeed, suppose by way of contradiction that there is $(a_1, \ldots, a_n, b) \in \text{Var}(J)$; then $(a_1, \ldots, a_n) \in \text{Var}(I)$ and thus $f(a_1, \ldots, a_n) = 0$, and thus $1 - bf(a_1, \ldots, a_n) = 1 - 0 = 1 \neq 0$; we conclude that $\text{Var}(J)$ must indeed be empty.

By the WHN, since $\text{Var}(J) = \emptyset$, we know that $1 \in J$, so that there must exist $p \in \mathbb{K}[x_1, \ldots, x_n, y]$ and $q_1, \ldots, q_d \in I$ such that $1 = p(1 - yf) + \sum_{i=0}^{d} y^i q_i$. This polynomial identity holds in $\mathbb{K}[x_1, \ldots, x_n, y]$, and thus also in $\mathbb{K}(x_1, \ldots, x_n)[y]$; furthermore, since f is not identically 0, $1/f$ is a valid element in $\mathbb{K}(x_1, \ldots, x_n)$. By setting $y = 1/f$, we deduce that $1 = \sum_{i=0}^{d} f^{-i} q_i$, and thus $f^d = \sum_{i=0}^{d} f^{d-i} q_i$, which means that f^d is in I, and thus $f \in \text{Rad}(I)$, as we wanted to show. □

Having established that the SHN and the WHN are equivalent statements, we concentrate on proving the WHN. The proof relies on the following lemma (which we shall prove in the next section):

Lemma 3.4 (Extension Lemma)**.** *Let $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ be monic in x_n and $I = \text{Ideal}(f_1, \ldots, f_m)$. Let $J = I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$. If $(a_1, \ldots, a_{n-1}) \in \text{Var}(J)$ then there is $a_n \in \mathbb{K}$ such that $(a_1, \ldots, a_n) \in \text{Var}(I)$.*

Proof of the WHN based on the Extension Lemma. Recall that the non-trivial direction of the WHN is to show that if $\text{Var}(I) = \emptyset \implies 1 \in I$. The proof is by induction on n.

The base case $n = 1$ is simple. In this case, I is a principal ideal, say, $I = \text{Ideal}(f)$ for some $f \in \mathbb{K}[x_1]$. Then $\text{Var}(I)$ is the set of roots of f. Since $\mathbb{K}$ is algebraically closed, every non-constant polynomial in $\mathbb{K}[x_1]$ has a root in $\mathbb{K}$, and thus f has to be a constant polynomial. Thus, $1/f \in \mathbb{K}$ and thus $1 = (1/f) \cdot f \in I$, as desired.

So suppose that the statement holds for $n - 1$. We wish to prove the statement for n. Say that $I = \text{Ideal}(f_1, \ldots, f_m)$ (recalling that every ideal is indeed finitely generated) and suppose that each f_i is a non-constant polynomial of degree d_i (for otherwise we are done for trivial reasons). For any $b_1, \ldots, b_{n-1} \in \mathbb{K}$, consider the linear transformation

$$x_1 = y_1 + b_1 y_n \ , \ x_2 = y_2 + b_2 y_n \ , \ \ldots \ , \ x_{n-1} = y_{n-1} + b_{n-1} y_n \ , \ x_n = y_n \ .$$

Note that, for $i = 1, \ldots, m$,

$$\begin{aligned} f_i(x_1, \ldots, x_n) =& f_i(y_1 + b_1 y_n, \ldots, y_{n-1} + b_{n-1} y_n, y_n) \\ =& p_i(b_1, \ldots, b_{n-1}) y_n^{d_i} + \text{ terms in which } \deg(y_n) < d_i \ . \end{aligned}$$

Because each $p_i(b_1, \ldots, b_{n-1})$ is some polynomial in $b_1, \ldots, b_{n-1}$ and $\mathbb{K}$ is algebraically closed (and thus, in particular, infinite), there are choices of $b_1, \ldots, b_{n-1}$ for which all the $p_i(b_1, \ldots, b_{n-1})$ are not equal to 0. Since the constant polynomial 1 is not affected by the transformation, this means that if $1 \in I'$ then $1 \in I$, where $I' = \text{Ideal}(f'_1, \ldots, f'_m) \subseteq \mathbb{K}[y_1, \ldots, y_n]$ is the ideal induced by the transformation by mapping each f_i to a corresponding *monic* polynomial f'_i. Also note that $\text{Var}(I) = \emptyset \implies \text{Var}(I') = \emptyset$.

Let $J' = I' \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$ and suppose by way of contradiction that $1 \notin I'$ so that, in particular, $1 \notin J'$. By the inductive assumption, we know that there is $(a_1, \ldots, a_{n-1}) \in \text{Var}(J')$. Then, by invoking the Extension Lemma on the monic $f'_1, \ldots, f'_m$, we know that there is $a_n \in \mathbb{K}$ such that $(a_1, \ldots, a_n) \in \text{Var}(I')$, which is a contradiction. □

4 Proving the Extension Lemma

Recall that, for a ring R, given two polynomials f and g in $R[x]$ of positive degree n and m respectively, their *resultant*, denoted $\text{Res}(f, g)$, is the determinant of their corresponding $(n+m) \times (n+m)$ Sylvester matrix. The $\text{Res}(f, g)$ is in the ideal $\text{Ideal}(f, g)$ and, moreover, is equal to 0 if and only if there is $h \in R[x]$ of positive degree that divides both f and g.

We begin by proving the Extension Lemma in the special case $m = 2$:

Proof of the Extension Lemma when $m = 2$. Define $p(x_1, \ldots, x_{n-1}) = \text{Res}_{x_n}(f_1, f_2)$. Since $p \in I = \text{Ideal}(f_1, f_2)$, we also know that $p \in J = I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$. Since $(a_1, \ldots, a_{n-1}) \in \text{Var}(J)$, we have that $p(a_1, \ldots, a_{n-1}) = 0$. Define $h_1(x_n) = f_1(a_1, \ldots, a_{n-1}, x_n)$ and $h_2(x_n) = f_2(a_1, \ldots, a_{n-1}, x_n)$. Since f_1 and f_2 are monic in x_n, both h_1 and h_2 have positive degree, and thus $\text{Res}_{x_n}(h_1, h_2) = \text{Res}_{x_n}(f_1, f_2)|_{a_1,\ldots,a_{n-1}} = p(a_1, \ldots, a_{n-1}) = 0$. Thus, there must exist $g(x_n) \in \mathbb{K}[x_n]$ dividing both h_1 and h_2. Since $\mathbb{K}$ is algebraically closed, there must exist $a_n \in \mathbb{K}$ such that $g(a_n) = 0$.

Therefore, $h_1(a_n) = h_2(a_n) = 0$, and we conclude that $f_1(a_1, \ldots, a_n) = f_2(a_1, \ldots, a_n) = 0$, and $(a_1, \ldots, a_n)$ is the point in $\text{Var}(I)$ that we wanted. □

We now prove the general case of the Extension Lemma by building on ideas for the $m = 2$ case:

Proof of the Extension Lemma. As before, let $I = I(f_1, \ldots, f_n) \subseteq \mathbb{K}[x_1, \ldots, x_n]$ with $f_1, \ldots, f_m$ all monic in x_n. Define $J = I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$ and let $(a_1, \ldots, a_{n-1}) \in \text{Var}(J)$. Consider the new ideal $I' = \text{Ideal}(f_1, F) \subseteq \mathbb{K}[x_1, \ldots, x_n, y_2, \ldots, y_m]$ where $F(x_1, \ldots, x_n, y_2, \ldots, y_m) = \sum_{i=2}^{m} f_i(x_1, \ldots, x_n) y_i$.

Define $p(x_1, \ldots, x_{n-1}, y_2, \ldots, y_m) = \text{Res}_{x_n}(f_1, F)$. Note that $p(a_1, \ldots, a_{n-1}, y_2, \ldots, y_m)$ is identically zero. To show this, it suffices to prove that for all $b_2, \ldots, b_m \in \mathbb{K}$ we have $p(a_1, \ldots, a_{n-1}, b_2, \ldots, b_m) = 0$. To see this, notice that $p(x_1, \ldots, x_{n-1}, b_2, \ldots, b_m) = \text{Res}_{x_n}(f_1, F(x_1, \ldots, x_n, b_2, \ldots, b_m)) \in \text{Ideal}(f_1, F(x_1, \ldots, x_n, b_2, \ldots, b_m))$ and thus is also in the ideal $I = \text{Ideal}(f_1, \ldots, f_m)$. We conclude that $p(x_1, \ldots, x_{n-1}, b_2, \ldots, b_m) \in J$, so that $p(a_1, \ldots, a_{n-1}, b_2, \ldots, b_m) = 0$.

Next, define $f_1'(x_n) = f_1(a_1, \ldots, a_{n-1}, x_n)$ and $H(x_n, y_2, \ldots, y_m) = F(a_1, \ldots, a_{n-1}, x_n, y_2, \ldots, y_m)$. Define $\mathbb{L} = \overline{\mathbb{K}(y_2, \ldots, y_m)}$ and note that $f_1', H \in \text{Ł}[x_n]$. Due to the previous paragraph, we know that f_1' and H share a root $a_n \in \mathbb{L}$. Since all the roots of f_1' are in $\mathbb{K}$, we know that in fact $a_n \in \mathbb{K}$.

We conclude by noting that $(x_n - a_n)$ divides both $f_1(a_1, \ldots, a_{n-1}, x_n)$ and $\sum_{i=2}^{m} f_i(a_1, \ldots, a_{n-1}, x_n) y_i$ so that $(x_n - a_n)$ divides each $f_i(a_1, \ldots, a_{n-1}, x_n)$. The point $(a_1, \ldots, a_n)$ is the point in $\text{Var}(I)$ that we were looking for. □

5 Degree Bounds for the Hilbert Nullstellensatz

If $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ each have degree at most d and there exist $q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n]$ such that $1 = \sum_{i=1}^{m} q_i f_i$, then what is the smallest degree bound $D_{n,m,d}$ on the q_i? The smaller $D_{n,m,d}$ can be shown to be, the easier it is to determine whether a system of polynomial equations has a solution; indeed, by the WHN, $1 \in \text{Ideal}(f_1, \ldots, f_m) \Leftrightarrow \text{Var}(f_1, \ldots, f_m) = \emptyset$.

- By invoking the degree bound analysis of Hermann [Her26] for the ideal membership problem, we know that $D_{n,m,d} \leq (mdn)^{2^{O(n)}}$.
- Using complex analysis, Brownawell [Bro87] showed that $D_{n,m,d} \leq (md)^n$; this bound is good enough to put the problem of deciding whether $1 \in I$ in PSPACE (as opposed to EXPSPACE with Hermann's weaker bound).
- Using cohomology, János [Kol88] showed the same bound, $D_{n,m,d} \leq (md)^n$.
- Using combinatorial counting arguments, Dubé [Dub93] also showed the same bound, $D_{n,m,d} \leq (md)^n$.
- Under the Generalized Riemann Hypothesis, Koiran [Koi96] showed that deciding whether $\mathrm{Var}(f_1, \ldots, f_m) = \emptyset$ is in AM (can be decided via an Arthur-Merlin protocol with two messages in which Arthur moves first).

6 Quantifier Elimination

Given $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, the question of whether $\mathrm{Var}(f_1, \ldots, f_m) = \emptyset$ is the question of whether there is $(a_1, \ldots, a_n) \in \mathbb{K}^n$ with $f_1(a_1, \ldots, a_n) = \cdots = f_m(a_1, \ldots, a_n) = 0$.

The existential quantification in such a question is merely the "first level" of a question with more quantifiers we could ask. For example, at the second level, we could ask the following question:

$$\text{Is it the case that } \forall\,(a_1, \ldots, a_n) \in \mathbb{K}^n\ \exists\,(b_1, \ldots, b_n) \in \mathbb{K}^n \text{ s.t } \begin{cases} f_1(a_1, \ldots, a_n, b_1, \ldots, b_n) = 0 \\ \vdots \\ f_m(a_1, \ldots, a_n, b_1, \ldots, b_n) = 0 \end{cases} ?$$

More generally, we could also consider both equalities and *disequalities* (i.e., asking when a certain polynomial is not equal to 0).

How much harder are problems with such additional quantifiers relative to the basic existential question? It turns out that such problems can also be solved reasonably efficiently by showing that quantifiers can be eliminated with not too much overhead.

References

[Bro87] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *The Annals of Mathematics*, 126(3):577–591, 1987.

[CLO07] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[Dub93] Thomas W. Dubé. A combinatorial proof of the effective Nullstellensatz. *Journal of Symbolic Computation*, 15(3):277–296, 1993.

[Her26] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Mathematische Annalen*, 95:736–788, 1926.

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996.

[Kol88] János Kollár. Sharp effective Nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988.

[Rab30] J. L. Rabinowitsch. Zum Hilbertschen Nullstellensatz. *Mathematische Annalen*, 102:520–520, 1930.