LECTURE NOTES:

A self-contained proof of the Hilbert's Nullstellensatz

Jesús A. De Loera
Univ. of California, Davis

1 Introduction

Hilbert Nullstellensatz is a central result that tells us a necessary and sufficient condition for when a system of equations has a no solution. This theorem was first proven by David Hilbert in 1900. Here we present a self-contained proof.

Theorem 1.1 (Hilbert's Nullstellensatz (HNS)) *Let $f_1 = 0, f_2 = 0, ..., f_s = 0$ be a system of polynomials in $\mathbb{C}[x_1, ..., x_m]$, then the system has no root, or solution, if and only if there exist polynomials $\alpha_1, \alpha_2, ..., \alpha_s \in \mathbb{C}[x_1, ..., x_m]$ such that $1 = \sum_{i=1}^{n} \alpha_i(x_1, ..., x_m) f_i(x_1, ..., x_m)$*

The idea of the proof is by induction on the number of variables. One settles it first for one variable and in the case one has more than one variable one needs to have a way to eliminate variables one at a time (this is done using resultants). The proof of the Hilbert Nullstellensatz in in one variable uses a familiar notion:

Definition 1.2 *Let $f_1, ..., f_s$ be univariate polynomials in $\mathbb{C}[x]$ (e.g. $f_1(x) = x^{700} - 72x^3 + 3$) We say a polynomial h is a Greatest Common Divisor (GCD) of $f_1, ..., f_s$ if*

1) $h|f_1$, $h|f_2$, ..., $h|f_s$ 2) $p|f_i$ for $i = 1, ..., s \implies p|h$

The centuries old Euclidean division algorithm allow us to compute the GCD. Recall

Algorithm: (GCD computation)

Input: $f, g \in \mathbb{C}[x]$
Output: $gcd(f, g)$

Set $i = 1$
Set $h_0 = f$, $h_1 = g$
while $h_i \neq 0$ do
    divide h_{i-1} by h_i
        $h_{i-1} = q_i h_i + r_i$ where r_i equals remainder(h_{i-1}, h_i)
        Set $h_i = r_i$
        $i = i + 1$

Lemma 1.3 *Suppose f, g are univariable polynomials with complex coefficients.*

1) If we know q, r, f satisfy $f = qg + r$, then $GCD(f, g) = GCD(g, f - qg) = GCD(g, r)$

2) $GCD(f_1, f_2, ..., f_s) = GCD(f_1, GCD(f_2, ..., f_s))$

3) If g_1, g_2 are both $GCD(f_1, ..., f_s)$, then $g_1 = cg_2$ where c is a constant.

Proof: : For part (1) $GCD(f,g)|g$, and $GCD(f,g)|f - qg = r$ this implies $GCD(f,g)|GCD(g,r)$ by definition: $GCD(g,r)|g$, and $GCD(g,r)|r = f - qg$, which implies $GCD(g,r)$ must divides f. Also implies $GCD(g,r)|GCD(f,g)$

For the proof of part (3) $GCD(f_1, f_2 \ldots f_s)|f_i$; for $i = 1, \ldots, s$. This implies $GCD(f_1, f_2, \ldots, f_s)|GCD(f_2, \ldots, f_s)$ and it also divides f_1. Therefore $GCD(f1, GCD(f_2, f_3, \ldots, f_s))$ is divided by $GCD(f1, f_2, f_3, \ldots, f_s)$. Given these two quantities, if $h|f_1$ and $h|GCD(f_2, f_3, \ldots, f_s)$ then $h|f_i$ for $i = 1$ to s. Thus $GCD(f1, f_2, f_3, \ldots, f_s)$ must divide $GCD(f1, GCD(f_2, f_3, \ldots, f_s))$. This proves they are equal.

Theorem 1.4 *Euclidean Algorithm works: It returns the $GCD(f,g)$.*

Proof: : We know h_{i+1} = remainder(h_{i-1}, h_i) Which can means $h_{i+1} = h_i - qh_i(h_{i-1})$ By the lemma above $GCD(h_{i-1}, h_i) = GCD(h_{i+1}, h_i)$, Since the degrees decrease and eventually $h_n = 0$, for some n,

$$h_{n-1} = GCD(h_{n-2}, h_{n-3}) = GCD(h_{n-3}, h_{n-4}) = \ldots = GCD(h_0, h_1).$$

Now, we clearly obtain then an algorithm to compute GCD $(f_1, f_2, \ldots f_s)$ using Lemma part (3). But remember our main goal, to find solutions of the system of polynomial equations. How can we determine whether system $g_1(x) = 0, \ldots, g_r(x) = 0$ has a common root? The key point is that if a is a common root, $(x - a)$ is a common factor. Then when $GCD(g_1(x), \ldots, g_r(x)) \neq 1$, then you have a common solution, any of the roots of this GCD will be a common root.

Lemma 1.5 *if $h = GCD(f_1, f_2, \ldots f_s)$, there exists polynomials $a_1, a_2, \ldots a_s$ such that*

$$h = a_1\ f_1 + \ldots + a_s f_s$$

Proof: This is proved by induction on the number of polynomials. Say for $n = 2$, apply Euclidean algorithm to f_1, f_2. while keeping track of divisors in each iteration $h_{i+1} = h_i - g_{i+1}h_{1-1}$. We can start by observing $GCD = h_{n-1} = h_{n-2} - q_{n-1}h_{n-3}(*)$ In each iteration: $h_{n-2} = h_{n-3} - q_{n-2}h_{n-4}(**)$ Substitute (**) into (*) and we obtain: $GCD(f_1, f_2) = (1 - q_{n-1})h_{n-3} - q_{n-2}h_{n-4}$

Repeat such back substitution using the identities $h_{i+1} = h_i - g_{i+1}h_{1-1}$. Eventually, $a_1\ f_1 + a_2\ f_2 = GCD(f_1, f_2)$. Assume lemma is true for $S-1$ polynomials or less. We know $GCD(f_1, f_2, \ldots f_s) = GCD(f_1, GCD(f_2, \ldots f_s))$. Thus by induction:

$GCD(f_2, \ldots f_s)$ can be written as $h = GCD(f_2, \ldots f_s) = \ b_2\ f_2 + \ldots + b_s\ f_s$. Which, by the case of 2 polynomials, gives, as desired: $GCD(f_1, f_2, \ldots f_s) = GCD(f_1, h) = r_1\ f_1 + sh = \ r_1\ f_1 + s(b_2\ f_2 + \ldots + b_s\ f_s) = \ r_1\ f_1 + sb_2\ f_2 + \ldots + sb_s\ f_s; then r_1 = a_1, sb_2 = a_2, \ldots, sb_s = a_s$.

Corollary 1.6 *In the case of one variable, a system of equations* $f_1(x) = 0, \ldots, f_s(x) = 0$ *has no common root if and only if*

$1 = a_1\ f_1 + \ldots + a_s f_s$; *for some polynomials* $a_1, a_{2,\ldots} a_s$.

Now that we have the Nullstellensatz for systems of polynomials in one single variable we will use Resultants to reduce any other system to this simpler case. The resultant will be a special determinant obtained from f, g polynomials in $R[x]$, where R is any integral domain (Think $R = K[y_1, \ldots, y_n]$, or $R = \mathbb{Z}$). The Sylvester matrix $syl(f, g)$ will have the following crucial property:

Theorem 1.7 *Let* R *be an integral domain. The polynomials* f, g *have a common root factor in* $R[X]$ *if and only if* $det(syl(f, g)) = 0$.

Lemma 1.8 *Let* f *and* g *be polynomials in* $R[x]$ *such that* $f,\ g$ *are nonzero, where* R *is an integral domain, and* $deg(f) = n, deg(g) = m$, *then* $f,\ g$ *have a common factor if and only if* $A,\ B$ *polynomials exist in* $R[x]$ *such that*

1. $Af + Bg = 0 \Rightarrow Bg = -Af$.
2. $deg\ (A) < m$, $deg\ (B) < n$.
3. A and B are nonzeros.

Proof: ($\Rightarrow$)
Suppose $f = f_1 h,\ g = g_1 h$, for some common h. Let $A = g_1$ and $B = -f_1$, then $g_1 f + -f_1 g = g_1 f_1 h - g_1 f_1 h = 0$.

($\Leftarrow$) By contradiction.
Suppose $f,\ g$ have no common factor, that implies $\exists\ \tilde{A},\ \tilde{B}$ polynomials in $k[x]$ such that $\tilde{A}f + \tilde{B}g = 1$. Then $B = B\tilde{A}f + B\tilde{B}g = B\tilde{A}f - \tilde{B}Af = (B\tilde{A} - \tilde{B}A)f$ implies $deg(B) > n$, thus this contradicts our assumption that $deg(B) < n$.

Example:

$f = 2x^3 + 4x - 2$
$g = 2x^2 + 3x + 9$

Solution:

$A = a_1 x + a_0$
$B = b_2 x^2 + b_1 x + b_0$
$0 = Af + Bg = (a_1 x + a_0)(2x^3 + 4x - 2) + (b_2 x^2 + b_1 x + b_0)(2x^2 + 3x + 9)$
$0 = (2a_1 + 2b_2)x^4 + (2a_0 + 3b_2 + 3b_1)x^3 + (4a_1 + 9b_2 + 3b_1 + 2b_0)x^2 + (-2a_1 + 4a_0 + 9b_1 + 3b_0)x + (-2a_0 + 9b_0)$

setting the coefficients equal to zero:

$$\begin{aligned} 2a_1 + 2b_2 &= 0 && (1)\\ 2a_0 + 3b_2 + 2b_1 &= 0 && (2)\\ 4a_1 + 9b_2 + 3b_1 + 2b_0 &= 0 && (3)\\ -2a_1 + 4a_0 + 9b_1 + 3b_0 &= 0 && (4)\\ -2a_0 + 9b_0 &= 0 && (5) \end{aligned}$$

form the Sylvester matrix ($S(f,g)$):

$$\underbrace{\begin{bmatrix} 2 & 0 & 2 & 0 & 0\\ 0 & 2 & 3 & 2 & 0\\ 4 & 0 & 9 & 3 & 2\\ -2 & 4 & 0 & 9 & 3\\ 0 & -2 & 0 & 0 & 9 \end{bmatrix}}_{S(f,g)} \begin{bmatrix} a_1\\ a_0\\ b_2\\ b_1\\ b_0 \end{bmatrix} = \begin{bmatrix} 0\\ 0\\ 0\\ 0\\ 0 \end{bmatrix}$$

$$det(S(f,g)) = 1163 \neq 0$$

Therefore, there is no common factor.

ALGORITHM:
Input: $f, g \in R[x]$
Output: Yes/No depending on whether they have a common factor.

Step 1: Compute the Sylvester matrix $S(f,g)$.
Step 2: Compute its determinant ($= Resultant$).
If $Resultant = 0$,
Return Yes there's a common factor.
Else Resultant $\neq 0$
Return No, there's no common factor.

Properties of Resultants :

1. $Resultant \neq 0 \Leftrightarrow GCD(f,g) = 1$.
2. $Resultant(f,g)$ is a polynomial whose variables are the coefficients of $f\&g$ and it has integer coefficients.
3. There exists polynomials $C, D \in k[x]$, such that $Cf+Dg = Resultant(f,g)$

Proof:

1. By lemma, $resultant \neq 0 \Leftrightarrow$ there is no common factor $\Leftrightarrow GCD(f,g) = 1$.

2. $Resultant(f,g) = \det \begin{bmatrix} a_n & 0 & \dots & 0 & b_m & 0 & \dots & 0 \\ a_{n-1} & a_n & \ddots & 0 & b_{m-1} & b_m & \ddots & 0 \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & b_{m-1} & \ddots & 0 \\ a_0 & \vdots & \ddots & a_n & b_0 & \vdots & \ddots & b_m \\ 0 & a_0 & \dots & \vdots & 0 & b_0 & \dots & \vdots \\ 0 & 0 & \dots & a_0 & 0 & 0 & \dots & b_0 \end{bmatrix}$ (m columns, n columns)

3. $Resultant(f,g) = 0$. Take $C = 0, D = 0$, then we are Done.
$Resultant(f,g) \neq 0 \Rightarrow det[S(f,g)] \neq 0$ Because $Resultant(f,g) \neq 0$
$\Rightarrow GCD(f,g) = 1$. Then there exist $Cf + Dg = 1$

$$\begin{bmatrix} & & \\ & Sylvester & \\ & & \end{bmatrix} \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_0 \\ d_m \\ d_{m-1} \\ \vdots \\ d_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

By Cramer's Rules:
C_i's and D_j's can be written in the form:

$$\frac{\begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}}{Resultant(f,g)} \qquad Cf + Dg = 1$$

multiply by $Resultant(f,g)$. The denominators cancel, hence $\tilde{C}f + \tilde{D}g = Resultant(f,g)$.

Lemma 1.9 *$B(x_1, x_2, ...x_n) \epsilon \mathbb{C}[x_1, x_2, ...x_n]$ polynomial that is not identically zero, then $\exists Z_1, Z_2, ...Z_n \epsilon C$ such that $B(Z_1, Z_2, ..., Z_n) \neq 0$*

Proof: By induction on n the number of variables. If $n = 1$ we are done, because univariate polynomials have finitely many roots, thus $B(x_1) \neq 0$ in infinitely values. Suppose the Lemma is true for $n - 1$ variables and take

$B(x_1, x_2, ...x_n)$ not identically zero. Expand it in terms of x_n, $B(x_1, x_2, ...x_n) = P_d(x_1, x_2, ...x_{n-1})x_n^d + P_{d-1}(x_1, x_2, ..., x_{n-1})z_n^{d-1} + ... + P_1(x_1, x_2, ...x_{n-1})$.

$\Rightarrow$ by hypothesis, $P_i(x_1, x_2, ...x_n)$ is not identically zero for some i. Thus by induction $\exists z_1, z_2, ...z_{n-1} \epsilon \mathbb{C}$ where $P_i(z_1, z_2, ...z_{n-1}) \neq 0$. Substitute $x_k = z_k$ for $k = 1, 2, ..., n-1$. In B, $B(z_1, z_2, ..., z_{n-1}, z_n)$, compute its root $\beta_1, \beta_2, ..., \beta_n$, let z_n be any complex number $\neq \beta_i$.

Lemma 1.10 *(Make me monic!) Let $b(x_1, x_2, ..., x_n)$ be a polynomial all of whose monomials have total degree $\leq d$*

There exist a change of coordinates

$$x_1 = \lambda_1 y_1 + y_n, x_2 = \lambda_2 y_2 + y_n, \ldots, x_i = \lambda_i y_i + y_n$$

$$x_n = y_n$$

such that $B(y_1 + \lambda_1 y_n, ..., y_{n-1} + \lambda_{n-1} y_n, y_n) = P(y_1, ...y_n)$ is a monic polynomial with respect to the variable y_n. This means

$$P(y_1, ...y_n) = C_d(y_1, ...y_{n-1})y_n^d + ... + C_0(y_1, ..., y_{n-1})$$

with $C_d = 1$.

Proof: Do substitution with parameter $\lambda_1, \lambda_2, ..., \lambda_{n-1}$; say d is the highest degree for y_n. The leading coefficient, will be the polynomial in $\lambda_1, \lambda_2, ..\lambda_{n-1}$ call leading coefficient C_d. From previous lemma we can find $\lambda_1, \lambda_2, ..\lambda_{n-1}$ values in $\mathbb{C}$ that make $C_d \neq 0$. Divide by constant $C_d(\lambda_1, \lambda_2, ..\lambda_{n-1}) \neq 0$, $P_1(y_1, ...y_n) = 1 * y_n^d +$ junk.

Theorem 1.11 *(Hilbert's Nullstellensatz) Let $f_1 = 0, f_2 = 0, ..f_s = 0$ be a system of polynomial equation, $f_1, ..f_s \epsilon \mathbb{C}[x_1, ...x_n]$ then there is no common solution over $\mathbb{C}^n \iff \exists \alpha_1, \alpha_2, ..\alpha_s \epsilon \mathbb{C}[x_1, .., x_n]$ such that $\alpha_1 f_2 + \alpha_2 f_2 + .. + \alpha_s f_s = 1$*

Proof: By induction on the number of variables. We already proved it for $n = 1$ using the GCD properties. Suppose true for $n-1$ variables, you are now given a system with n variables. (1) By Lemma about changes of variables you can assume f_1 is monic with respect to x_n. (2) Let y be an auxiliary variable. Let $Q(x_1, x_2, ..., x_n, y) = f_2 + yf_3 + y^2 f_4 + ... + y^{s-2} f_s$.

(3) Compute the resultant of f_1,Q with respect to x_n namely $Res(f_1, Q) = R_d(x_1, .., x_{n-1})y^d + R_{d-1}(x_1, .., x_{n-1})y^{d-1} + .. + R_0(x_1, .., x_{n-1})$ We saw there exist $A, B \in \mathbb{C}[x_1, ..., x_n, y]$ $Af + BQ = Res(f_1, Q, x_n)$ Because of induction, if I can prove $R_0 = 0, R_1 = 0, .., R_d = 0$ has no common root then done. Thus we know now how, given a system of polynomials without a common root, we can construct a new polynomial whose resultant must also have no solution. Here is all as a lemma.

Lemma 1.12 *Given the system of polynomials $f_1 = f_2 = \cdots = f_s = 0$ without a common root, we let $Q(x_1, x_2, \ldots, x_n, y) = f_2 + yf_3 + y^2 f_4 + \cdots + y^{s-2} f_s$.*

Next, we compute the resultant:

$Res(f_1, Q, x_1) = R_d(x_1, \ldots, x_{n-1})y^d + R_{d-1}(x_1, \ldots, x_{n-1})y^{d-1} + \cdots + R_0(x_1, \ldots, x_n)$

And find the system $R_d = R_{d-1} = \cdots = R_0 = 0$, which also has no solution.

Proof: By contradiction, suppose not true, therefore, there must exist a solution to the system constructed. Specifically, $\exists a_1, a_2, \ldots, a_{n-1}$ (let these be denoted by $\bar{a}$) such that $R_d(\bar{a}) = R_{d-1}(\bar{a}) = \cdots = R_0(\bar{a}) = 0$.

Thus, $Res(f_1, Q, x_n)(\bar{a}) = 0$.

Remember, since the resultant equals zero, the polynomials $f_1(\bar{a}, x_n)$ and $Q(\bar{a}, x_n, y)$ must have a common factor. This means that they share a root. Let this root be denoted as β. So, $f_1(\bar{a}, \beta) = Q(\bar{a}, y, \beta) = 0$, for any value of y. Since y is unconstrained, the only way Q can be distinctly zero is if $f_2(\bar{a}, \beta) = f_3(\bar{a}, \beta) = \cdots = 0$. Therefore, we have found a solution.

We will now use Hilbert's Nullstellensatz to prove the fundamental theorem that characterises which polynomials vanish in a variety!

Theorem 1.13 (The Strong Hilbert Nullstellensatz) *Let $h_i, g \in \mathbb{C}[x_1, ..., x_m]$. We define the* hypothesis variety *as follows $V = \{\bar{x} | h_1(\bar{x}) = h_2(\bar{x}) = ... = h_n(\bar{x}) = 0\}$. Here V can be interpreted as the set of all "positions" or "configurations" where the hypotheses are satisfied, then $g(\bar{x}) = 0\ \forall \bar{x} \in V \iff g^r(x_1, ..., x_m) = \sum_{i=1}^{n} \alpha_i(x_1, ..., x_m)h_i(x_1, ..., x_m)$ where $\alpha_i \in \mathbb{C}[x_1, ..., x_m]$.*

Proof: ($\Longrightarrow$) Suppose $g(\bar{x}) = 0\ \forall \bar{x} \in V$. Let f_i be defined as follows:

$f_0 = 1 + g(x)t \in \mathbb{C}[x_1, x_2, ..., x_m, t]$

$f_1 = h_1$

$f_2 = h_2$

$\vdots$

$f_i = h_i$.

There is no solution of this system ($1 \neq 0$) thus the Hilbert's Nullstellensatz implies $1 = \alpha_0(1+tg(x)) + \alpha_1 h_1 + \alpha_2 h_2 + ... + \alpha_n h_n$ where $\alpha_i \in \mathbb{C}[x_1, x_2, ..., x_m, t]$. If we set $t = -1/g$, then we get $1 = \alpha_1(x_1, ..., x_m, -1/g)h_1(x_1, ..., x_m) + ... + \alpha_n(x_1, ..., x_m, -1/g)h_n(x_1, ..., x_m)$ where the denominators look like $g(x_1, ..., x_m)^k$. Then pick the highest power of g that appears in the denominator, and multiply the expression by it. we get the desired statement.

Now let us prove the converse, which is easy. Given

$$g^n(x_1, ..., x_m) = \sum_{i=1}^{n} \alpha_i(x_1, \ldots, x_m)h_i(x_1, \ldots, x_m),$$

when $\bar{x}$ is a root of the system of equations means $\Longrightarrow h_i(\bar{x}) = 0 \Longrightarrow g^r(\bar{x}) = 0 \Longrightarrow g(\bar{x}) = 0$.

References

[1] Cox, D., Little, J., and O'Shea, D. *Ideals, varieties, and Algorithms*, Springer Verlag, Undergraduate Text, 2nd Edition, 1997.

[2] Cox, D., Little, J., and O'Shea, D. *Using Algebraic Geometry*, Springer Verlag, Undergraduate Text, 2nd Edition, 1997.

[3] Sturmfels, B. *Gröbner bases and convex polytopes*, university lecture series, vol. 8, AMS, Providence RI, (1996).