Hilbert's Nullstellensatz

Rahul Murthy

May 21, 2016

Abstract

This paper will examine Hilbert's Nullstellensatz, specifically a formulation of the Nullstellensatz involving polynomial rings. We begin by reviewing some definitions and the Euclidean Algorithm for finding the greatest common divisor of two polynomials. Then we will formally state and give examples of the Nullstellensatz. We will conclude with a proof of the Nullstellensatz.

Introduction

If we consider the solvability of a system of equations $P_1(X) = \cdots = P_d(X) = 0$ an obstruction to solvability would be if the system is inconsistent. Specifically, if it is possible to find polynomials $Q_1, ..., Q_m \in F[X]$ such that $P_1Q_1 + ... + P_mQ_m = 1$ then it is impossible to solve $P_1(X) = \cdots = P_m(X) = 0$. The Weak Nullstellensatz claims that the existence of such a collection of polynomials is the only obstacle to the solvability of our system of equations. The Strong Nullstellensatz is a further generalization of this claim. The word "Nullstellensatz" literally translates to "zero locus theorem", but it more commonly translated as the theorem of zeroes. This theorem was developed by David Hilbert in Germany around the turn of the 20th century.

1 Background

1.1 Definitions

Definition 1.1 (2)**.** A *group*, denoted $\langle G, * \rangle$, is a set G equipped with a binary operation $*$ which satisfies the following axioms

I. The operation $*$ is associative on G; that is, for all a, b, c in G, $(a * b) * c = a * (b * c)$.

II. G contains an identity element; that is, there exists an element e in G such that $e * x = x * e = x$, for all $x \in G$.

III. G contains an inverse for each of its elements; that is, for every element x in G there is an element y in G such that $x * y = y * x = e$.

Example 1.2. An example of a group would be the integers under addition, $\langle \mathbb{Z}, + \rangle$. The integers under multiplication $\langle \mathbb{Z}, \cdot \rangle$ is not a group because there exist elements that have no inverses under this operation.

Definition 1.3 (2)**.** A *ring*, denoted $\langle R, +, \cdot \rangle$, is a set R equipped with two binary operations $+$ and $\cdot$ that satisfies the following three axioms:

I. $\langle R, + \rangle$ is an commutative group.

II. The operation $\cdot$ is associative in R; that is, for all a, b, c in R, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

III. The operation $\cdot$ distributes over the operation $+$ in R; that is, for all a, b, c in R, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Example 1.4. Examples of rings include: $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$.

Definition 1.5 (2)**.** Let R be a ring, $R[x] = \{\sum_{i=0}^{\infty} a_i x^i | a_i \in R, a_i = 0$ for all but a finite number of $a_i\}$ is a /textitpolynomial ring, a polynomial with coefficients in R. If for some $i \geq 0$ it is the case that $a_i \neq 0$ the largest such value of i is the *degree* of $f(x)$. Futhermore, we can have a polynomial ring in many indeterminates $R[x_1, x_2, \ldots, x_d]$ which we will denote as $R[X]$, where $X = (x_1, \ldots, x_d)$ is a collection of d indeterminats.

Example 1.6. For example we have the polynomial $7x^3 - 3x^2 + 11$, which is in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$. Also, $7x^3 - 3x^2 + 11$ has a degree of 2.

Definition 1.7 (2)**.** A *monic polynomial* is a polynomial with one indeterminate in which the coefficent of the indeterminate of the highest degree is equal to 1.

Definition 1.8 (2)**.** A *field* is a ring $\langle R, +, \cdot \rangle$ such that $\langle R^*, \cdot \rangle$ is a commutative group.

Example 1.9. $\mathbb{Q}$ is a field, but $\mathbb{Z}$ is not because it does not form a commutative group under multiplication.

Definition 1.10 (2)**.** A field F is said to be *algebraically closed* if every non constant polynomial in $F[x]$ has a zero in F.

Example 1.11. $\mathbb{R}$ is not algebraically closed because the equation $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. No sub field of $\mathbb{R}$ is algebraically closed. $\mathbb{C}$ is algebraically closed, via the fundamental theorem of algebra.

Definition 1.12. An *Ideal*, I is a an additive subgroup of a ring, R, that satisfies the following conditions

I. $\langle I, + \rangle$ is a subgroup of $\langle R, + \rangle$.

II. $\forall x \in I, \forall r \in R$: $x\dot{r}, r\dot{x} \in I$

Theorem 1.13 (The Fundamental Theorem of Algebra)**.** *Every non-constant single variable polynomial in* $\mathbb{C}[x]$ *has a root in* $\mathbb{C}$.

2 The Nullstellensatz

We begin by first reviewing the Euclidean Algorithms as a process for finding the greatest common divisor of two integers, and then we will generalize the algorithm to handle polynomials as well.

2.1 Preliminaries

Euclidean algorithm

The Euclidean Algorithm is a procedure that is employed to find the greatest common divisor of two numbers. [4]

Extended Euclidean Algorithm

The Extended Euclidean Algorithm is an extension of the Euclidean Algorithm which can be used to express the greatest common divisors of $a, b \in \mathbb{Z}$ as a linear combination of a and b. That is, it produces $x, y \in \mathbb{Z}$ such that $xa + yb = \gcd a, b$. The algorithm behaves according to the following procedure in order to find $\gcd(a, b)$.

$$r_0 = a \qquad r_1 = b$$
$$s_0 = 0 \qquad s_1 = 1$$
$$t_0 = 1 \qquad t_1 = 0$$

$r_{i+1} = r_{i-1} - q_i r_i$ or $r_{i-1} = q_i r_i + r_{i+1}$
$s_{i+1} = s_{i-1} - q_i s_i$
$t_{i+1} = t_{i-1} - q_i t_i$
We continue on in this manner until we obtain $r_{i+1} = 0$ for some i.Then $\gcd a, b = r_i$ A more intuitive way to achive the same end result is to simply calculate the gcd and then work back up to our inputs by rearranging our equations and substituting.

Example 2.1. To calculate the greatest common divisors of $24, 33$ we can first work through

the standard euclidean algorithm

$$\begin{aligned} 33 &= (1 * 24) + 9 \\ 24 &= (2 * 9) + 6 \\ 9 &= (1 * 6) + 3 \\ 6 &= 2 * 3 \end{aligned}$$

So because there is no remainder in our final calculation we can see that $\gcd 33, 24 = 3$; now we can work our way back up.

$$\begin{aligned} 3 &= 9 - (1 * 6) \\ 3 &= 9 - (24 - (2 * 9)) \\ 3 &= 33 - 24 - (24 - 2(33 - 24)) \\ 3 &= 3 * 33 - 4 * 24 \end{aligned}$$

We can use the Extended Euclidean Algorithm for Polynomials in order to find the greatest common divisor $D(x)$ of some number of nonzero $P_i(x)$ from some collection of polynomials. We can iteratively apply the algorithm to any number of polynomials, which will give us the gcd of the entire collection. The algorithm will supply us with polynomials $Q_1(x), \ldots, Q_m(x)$ such that

$$P_1(x)Q_1(x) + \cdots + P_m(x)Q_m(X) = D(X)$$

Example 2.2. Suppose $P(x) = x + 2$ and $Q(x) = x^2 - x + 1$. In order to find the greatest common divisor of these polynomials, we start by writing the polynomial with the larger degree as $a(x)$ and the smaller degree polynomial as $b(x)$. So $a(x) = x^2 - x + 1$ and $b(x) = x + 2$. Now we can follow the algorithm :

$$\begin{aligned} r_0(x) &= x^2 - x + 1 & \qquad r_1(x) &= x + 2 \\ s_0(x) &= 1 & \qquad s_1(x) &= 0 \\ t_0(x) &= 0 & \qquad t_1(x) &= 1 \end{aligned}$$

$r_2(x) = r_0(x) - q_1(x)r_1(x) = (x^2 - x + 1) - q_1(x)(x + 2)$
Now we can divide to find $q_1(x)$ and $r_2(x)$

$$
\begin{array}{rl}
 & \quad\;\; x-3 \\
\cline{2-2}
x+2\big) & \;\; x^2 \;\; -x+1 \\
 & -x^2-2x \\
\cline{2-2}
 & \quad -3x+1 \\
 & \quad\;\; 3x+6 \\
\cline{2-2}
 & \qquad\;\; 7
\end{array}
$$

The division implies that $q_1(x) = x - 3$ and $r_2(x) = 7$, thus
$r_0 = x^2 - x + 1 = (x - 3)(x + 2) + 7$

$$
\begin{array}{lll}
r_{i-1}(x) = q_i(x)r_i(x) + r_{i+1}(x) & r_0(x) = q_1(x)r_1(x) + r_2(x) & r_0(x) = x^2 - x + 1 = (x-3)(x+2) + 7 \\
s_{i+1}(x) = s_{i-1}(x) - q_i(x)s_i(x) & s_2(x) = s_0(x) - q_1(x)s_1(x) & s_2(x) = 1 - (x-3)(0) = 1 \\
t_{i+1}(x) = t_{i-1}(x) - q_i(x)t_i(x) & t_2(x) = t_0(x) - q_1(x)s_1(x) & t_2(x) = 0 - (x-3)(1)
\end{array}
$$

$r_1(x) = (x + 2) = 7(\frac{1}{7}x + \frac{2}{7}) + 0$
So since $r_2 = 0$ the greatest common divisor of $P(x) = x + 2$ and $Q(x) = x^2 - x + 1$ is 7.

Throughout this paper F will be an algebraically closed field (such as $\mathbb{C}$). Also $P_1(X) = 0, \ldots, P_m(X) = 0$ is a system of polynomial equations in d indeterminates $X = (x_1, ..., x_d) \in F^d$ over F, thus $P_1(X), ..., P_m(X) \in F[X]$ are polynomials in d indeterminates.

2.2 The Weak Nullstellensatz

Consider the polynomials $P_1, P_2, \ldots, P_m \in F[X]$ where $X = (x_1, \ldots, x_d)$. If $P_1(X) = 0, P_2(X) = 0, \ldots, P_m(X) = 0$ has no solution then we call the system inconsistant. If it is possible to find polynomials $Q_1, \ldots, Q_m \in F[X]$ such that $P_1(X)Q_1(X) + \cdots + P_m(X)Q_m(X) = 1$ then it is impossible to solve $P_1(X) = 0, P_2(X) = 0, \ldots, P_m(X) = 0$. The Weak Nullstellensatz claims that the existence of such a collection of polynomials, $Q_1, \ldots, Q_m$ is the only obstacle to the solvability of our system of equations. [3]

Theorem 2.3. *(The Weak Nullstellensatz) Let $P_1, ..., P_m \in F[X]$ where $X = (x_1, ..., x_d)$. Exactly one of the following statements is true.*

I. The system of equations $P_1(X) = 0, P_2(X) = 0, \ldots, P_m(X) = 0$ *has a solution in* F^d.

II. There exists $Q_1, ..., Q_m \in F[X]$ *such that*

$$P_1(X)Q_1(X) + \cdots + P_m(X)Q_m(X) = 1$$

Example 2.4. Consider the equations $x = 0$ and $x + 1 = 0$, we can easily see that there will not be a solution to this system. Furthermore it is possible to find $Q(x)$'s such that the system will be equal to 1, in our case these are simply constants.

$$(-1)(x) + (1)(x + 1) = 1$$

2.3 The Strong Nullstellensatz

The Strong Nullstellensatz expands upon the second statement of the Weak Nullstellensatz

$$P_1(X)Q_1(X) + \cdots + P_m(X)Q_m(X) = 1$$

to a more general condition,

$$P_1(X)Q_1(X) + \cdots + P_m(X)Q_m(X) = R(X)^r$$

where $R(X)$ is a non-zero polynomial, $R(X) \neq 0$ and $r \in \mathbb{N}$. The Weak Nullstellensatz is simply a special case of the Strong Nullstellensatz, with $R(X)$ equal to a non-zero constant. It also modifies the first statement of the Nullstellensatz, as seen below.

Theorem 2.5. *(The Strong Nullstellensatz) Let* $P_1, ..., P_m, R \in F[X]$ *be polynomials where* $X = (x_1, \ldots, x_d)$. *Then exactly one of the following statements holds.*

I. The system of inequations $P_1(X) = \cdots = P_m(X) = 0; R(X) \neq 0$ *has a solution* $X \in F^d$.

II. There exist some polynomials $Q_1(X), \ldots, Q_m(X) \in F[X]$ *and a natural number* r *such that* $P_1(X)Q_1(X) + \cdots + P_m(X)Q_m(X) = R(X)^r$.

Note that if our system has multiple polynomials that are of the form $R_1(X) \neq 0, \ldots, R_m(X) \neq 0$ then these can be combined into a single inequation $R_1(X) \ldots R_n(X) \neq 0$, but this is not especially significant beyond simplifying the statement of the Nullstellensatz. There no way for us to get $R_1(X)R_2(X) \ldots R_n(X) = 0$ because $F[X]$ is an integral domain, there are no nonzero polynomials twhose product is zero. [2]

Example 2.6. Consider the equations $x = 0$, $x+1 = 0$, and $x^2+1 \neq 0$; We can again easily see that there will be no solution to this system. Furthermore it is possible to find $Q(x)$'s such that the system will be equal to a power of $x^2 + 1$, in our case this power is simply 1.

$$(x-1)(x) + (1)(x+1) = (x^2+1)^1$$

2.4 Proof of Nullstellensatz

We will prove the Strong Nullstellensatz by induction on d, the number of indeterminants in the system of equations.

Proof. (The Strong Nullstellensatz) Base Case: Suppose $P_1, ..., P_m, R \in F[x]$. Recall that a collection of polynomials $(P_1, ..., P_m, R)$ is said to *obey the Nullstellensatz* if one of the following are true.

I. The system of equations $P_1(X) = \cdots = P_d(X) = 0; R(X) \neq 0$ has a solution $X \in F^d$

II. There exist some polynomials $Q_1, \ldots, Q_m \in F[X]$ and a natural number r such that $P_1Q_1 + \cdots + P_mQ_m = R^r$

These statements cannot both be true because if there did exist a solution to the system of equations $P_1(X) = 0, \ldots, P_m(X) = 0, R(X) \neq 0$, then each P_i would vanish simultaniously at some point and there would be no way for us to find a nonzero linear combination of the P_i's.

Without loss of Generality, suppose that none of the P_i is identically zero. Suppose the system of equations has no solution; Then we can employ the Extended Euclidean Algorithm for Polynomials to find the greatest common divisor $D(X)$ of the $P_i(x)$. Since $D(X)$ is the greatest common divisor of $(P_1(x), ..., P_m(x))$, the collection of polynomials $(P_1(x), ..., P_m(x), R(x))$ obeys the Nullstellensatz if and only if $(D; R)$ obeys the Nullstellensatz. This effectively reduces the number of to 1.

Suppose that $\gcd D, R = D'$ there there exist $A(x), B(x) \in F[x]$ such that $D' = DA + RB$.

We can now factor

$$\begin{aligned} D' &= DA + RB \\ D' &= (D'S)A + (D'T)B \\ 1 &= SA + TB \end{aligned}$$

where S and T are polynomials.

Furthermore if some power of D' is a multiple of S then some power of R is a multiple of D. So if $(S; D')$ obeys the Nullstellensatz then so too must $(D; R)$. By the Extended Euclidean Algorithm for polynomials, we see that the degree of S and D' is less than the degree of D and R unless R is constant. We reduce our polynomials to the case where R is constant by repeatedly applying the algorithm. Now our polynomials R and D will be one of three possible states.

I. If R is zero then we are in the second case of the Nullstellensatz, we can simply assign each Q_i to be identically zero.

II. If we assume R to be non-zero and D to be constant then we are again in the second case of the Nullstellensatz, we can multiply our non-zero R by some Q such that some combination of them will be D.

III. If D is not constant and R is non-zero then we are in the first case of the Nullstellensatz because we will have a solution by the fundamental theorem of algebra.

This proves the base case.

Induction Hypothesis: Suppose that $P_1, .., P_m, R \in F[x_1, ..., x_{\ell-1}]$ then $(P_1, ..., P_m, R)$ obeys the Nullstellensatz.

The Inductive Case $d = \ell$:

The basic idea is to view the system of equations in ℓ variables as a $\ell - 1$ dimensional family of of systems in a single variable. We will apply the induction hypothesis to every system in this family.

We start by writing the variable $X \in F^d$ as $X = (Y, t)$ with $Y \in F^{d-1}$ and $t \in F$. We can now view the ring $F[X]$ in d variables as the ring $F[Y][t]$ in a single variable t, in which the coefficeients are in the $F[Y]$. If we let I be the ideal generated by $P_1, \ldots, P_m$ then either we can solve the system

$$P_1(Y,t) = 0, \ldots, P_m(Y,t) = 0; R(Y,t) \neq 0$$

Which is exactly the first statement of the Nullstellensatz or we can show that

$$R^r = 0 \bmod I$$

for some $r \in \mathbb{N}$ which is equivelent to the second statement of the Nullstellensatz.

We view the polynomials $P_1(Y,t), \ldots, P_m(Y,t); R(Y,t)$ as polynomials in $F[t]$ whose coefficients lie in F and depend on Y. For emphasis we will rewrite $P_j(Y,t)$ as $P_{j,Y}(t)$ and $R(Y,t)$ as $R_Y(t)$. From our assumption there is no t for which

$$P_{1,Y}(t) = 0, \ldots, P_{m,Y}(t) = 0; R_Y(t) \neq 0$$

From the base case we can now conclude that there are polynomials $Q_{1,y}, \ldots, Q_{m,y} \in F[t]$ and $r = r_y \geq 0$ such that

$$P_{1,Y}(t)Q_{1,Y}(t) + \cdots + P_{m,Y}(t)Q_{m,Y}(t) = R_Y^{r_Y}(t).$$

If r_Y is a constant in Y and the coefficients of $Q_{1,Y}, \ldots, Q_{m,Y}$ depend on Y then we are in the second case of the Nullstellensatz and therefore done.

We can multiply both sides of the above formula by $R_Y(t)$ which will remove $r = r_Y$ dependence on Y and that will give us

$$P_1(Y,t)Q_{1,Y}(t) + \cdots + P_m(Y,t)Q_{m,Y}(t) = R^r(Y,t)$$

The coefficients on Q are piecewise rational in Y. From the $d = 1$ case we can observe that the proceedure that we used makes a finite number of steps, which depend on whether or not polynomials of Y, which we will now call $T(Y)$ will be zero or not. At the termination

of the procedure we are provided with polynomials $Q_{1,Y}, \ldots, Qm, Y$ which have coefficents that are combinations of the coefficients of $P_{1,Y}, \ldots, P_{m,Y}$ and so are functions of X. Also, all the division operations of the Euclidean Algorithm are by polynomials of Y which will be non-zero at some stage of the process so the denominator of these coefficients is some product of the $T(y)$'s that will be not zero.

There are only finitely many routes that the Euclidean Algorithm may take. Some of the routes may not be feasible, there are no $Y \in F^{d-1}$ which can trace these routes. An infeasible path can be thought of as an impossible path, there is no way for us to get there or move on from there. However, from any feasible route, such as one where polynomials which we will call $S_1(Y), \ldots, S_a(Y)$ are zero and polynomials $T_1(Y), \ldots, T_b(Y)$ are nonzero. Since we assume that there is no solution to the system of equations we know that the algorithm will eventually return an identity of the form

$$P_1(Y,t)Q_{1,Y}(t) + \cdots + P_m(Y,t)Q_{m,Y}(t) = R^r(Y,t)$$

where the coefficients of $Q_{1,Y}, \ldots, Q_{m,Y}$ are polynomials in Y with denominators that will be the products of $T_1, \ldots, T_b$. We can clear the denominators, while enlarging r if we have to, giving us polynomials which we will call $U_1(Y,t), \ldots, U_m(Y,t)$. This will then give us

$$P_1(Y,t)U_1(Y,t) + \cdots + P_m(Y,t)U_m(Y,t) = (T_1(Y) \ldots T_b(Y)R(Y))^r$$

This equation holds whenever we have a Y such that $S_1(Y), \ldots, S_a(Y)$ are zero and $T_1(Y), \ldots, T_b(Y)$ are nonzero. The only reason that we need $T_1(Y), \ldots, T_b(Y)$ to be non-zero was to be able to use them in division. If we clear out the denominators everwhere we can remove the previous constraint, thus the equation above will hold whenever $S_1(Y), \ldots, S_a(Y)$ are zero. Furthermore, if $S_1(Y), \ldots, S_a(Y)$ will be non-zero then they only add additonal terms to the previous equation which will be combinations of $S_1, \ldots, S_a$. So for any feasibly path, we can obtain an identity in $F[Y,t]$ with the form

$$P_1U_1 + \cdots + P_mU_m = (T_1 \ldots T_bR)^r + S_1V_1 + \cdots + S_aV_a$$

for some polynomials $U_1, \ldots U_m, V_1, \ldots V_a \in F[Y,t]$. So we can see that

$$(T_1 \ldots T_bR)^r = 0 \bmod I, S_1, \ldots, S_a$$

for any possible feasible path.

Now all we need to do is simplify the previous equation until we obtain the second statement of the Nullstellensatz. We claim that previous equation will hold for not just complete feasible routes, in which we can follow the Euclidean Algorithm all the way to its conclusion, but also for partial feasible paths in which we follow the algorithm for some number of steps and then halt where there is at least one $Y \in F^{d-1}$ that can solve all of the constraints reached as yet. The empty feasible path will then immediately give the second statement of the Nullstellensatz.

To prove this claim we must induct backwards on the number of steps in the partial path. Suppose there exists a partial route which requires $S_1(Y), \ldots, S_a(Y)$ to be zero and $T_1(Y), \ldots, T_b(Y)$ to be nonzero to get to where we are in this route. If the route is complete then we are done, so we will suppose that there are further steps to be done. Let the polynomial that the algorithm will operate on be $W(Y)$. At least one of the cases $W(Y) = 0$ and $W(Y) \neq 0$ must be feasible, meaning we are able to continue the algorithm in one or both cases. Now we can observe the three possible cases.

Case 1: $W(Y) = 0$ is feasible and $W(Y) \neq 0$ is infeasible. Following the $W(Y) = 0$ route and by using our inductive hypothesis we can get the equation

$$(T_1 \ldots T_b R)^r = 0 \bmod I, S_1, \ldots, S_a, W$$

for some $r \in \mathbb{N}$. But, because $W(Y) \neq 0$ we can see that the system

$$S_1(Y) = \cdots = S_a(Y) = 0; T_1 \ldots T_b W(Y) \neq 0$$

has no solution. Since we assume the Nullstellensatz will hold for $d-1$ indeterminants we can conclude

$$(T_1 \ldots T_b W)^(r') = 0 \bmod S_1, \ldots S_a.$$

for some r'. If we raise

$$(T_1 \ldots T_b R)^r = 0 \bmod I, S_1, \ldots, S_a, W$$

to the power r' by $(T_1 \ldots T_b R)^{r'}$, we can conclude that we are in the second statement of the Nullstellensatz.

Case 2: $W(Y) = 0$ is an infeasible route and $W(Y) \neq 0$ is a feasible route. Following the $W(Y) \neq 0$ route we can obtain the equation

$$(T_1 \dots T_b W R)^{r''} = 0 \bmod I, S_1, \dots, S_a.$$

for some $r'' \in \mathbb{N}$, while the infeasibility of the $W(y) = 0$ route means that there is no solution to

$$S_1(y) = \dots = S_a(y) = W(y) = 0; T_1(y) \dots T_b(y) \neq 0$$

And so by the induction hypothesis we have

$$(T_1 \dots T_b)^{r'''} = WZ \bmod S_1, \dots S_a$$

for some polynomial Z and some $r''' \in \mathbb{N}$. Also we can now multiply the equation

$$(T_1 \dots T_b W R)^{r'''} = 0 \bmod I, S_1, \dots, S_a.$$

by $Z^{r''}$ to eliminate W we again see that we are in the second statement of the Nullstellensatz.

Case 3: $W(Y) = 0$ and $W(Y) \neq 0$ are both feasible routes for the Euclidean algorithm. In this case we obtain the same equations as in the previous cases. We can rewrite

$$(T_1 \dots T_b R)^r = 0 \bmod I, S_1, \dots, S_a, W$$

as

$$(T_1 \dots T_b R)^r = WZ \bmod S_1, \dots, S_a$$

for some polynomial Z. We can then multiply

$$(T_1 \dots T_b W R)^{r''} = 0 \bmod I, S_1, \dots, S_a.$$

by Z^r to eliminate W and obtain

$$(T_1 \dots T_b R)^r = 0 \bmod I, S_1, \dots, S_a$$

as desired.

These three cases establish the above equation for all partial branching paths, eventually leading to the second statement of the Nullstellensatz as desired. □

3 Applications

Hilbert's Nullstellensatz is primarily used to provide a bridge between Abstract Algebra and Algebraic Geometry.

References:

[1] Alon, Noga. Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing*, 8, 7-29, (1999).

[2] Fraleigh, John B. *A First Course in Abstract Algebra*, Seventh Edition, 2002.

[3] Tao, Terry. Hilbert's Nullstellensatz: https://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz (updated November 26, 2007).

[4] T. Gowers, J. Barrow-Green, I. Leader. *The Princeton Companion to Mathematics*, First edition, 2008.