A proof of Combinatorial Nullstellensatz over Integral Domains

Himanshu Shukla[1] *

Department of Mathematics and Statistics
Indian Institute of Technology, Kanpur

Abstract. In this article, we present an alternative proof of Combinatorial Nullstellensatz over which was first proved by Noga Alon. We prove the theorem for integral domains. This version of Nullstellensatz by Alon haS diverse applications in various areas of Mathematics such as Graph Theory, Additive Number Theory, and Algebra itself.

1 Theorem

Theorem 1. *Let R be an Integral Domain, and let $f = f(x_1, ..., x_n)$ be a polynomial in $R[X_1, ..., X_n]$. Let $S_1, ..., S_n$ be nonempty subsets of R and define $g_i(x_i) = \Pi_{s \in S_i}(x_i - s)$. If f vanishes over all the common zeros of $g_1, ..., g_n$ (that is; if $f(s_1, ..., s_n) = 0$ for all $s_i \in S_i$), then there are polynomials $h_1, ...h_n \in R[X_1, ..., X_n]$ satisfying deg(h_i) $\leq$ deg(f) - deg(g_i), so that*

$$f = \sum_{i=1}^{n} g_i h_i \tag{1}$$

Proof. We will use induction on number of variables. For $n = 1$, let s_i represent the zeros. $f(X) = \Sigma_{i=1}^{n} a_i X^i$, rewrite X as $(X - s_1) + s_1$ and expand using binomial to get

$$f(X) = \Sigma_{i=1}^{n} b_i (X - s_1)^i + c_0 \tag{2}$$

where c_0 is a constant, but note that $0 = f(s_1) = 0 + c_0 \Rightarrow c_0 = 0$. Now, $f(X) = (X - s_1)(\Sigma_{i=1}^{n} b_i (X - s_1)^{i-1})$ and observe that $(\Sigma_{i=1}^{n} b_i (s_2 - s_1)^{i-1}) = 0$ as $f(s_2) = 0$. Now, the summation can be written as a polynomial in $(X - s_2)$ and hence we get, $f(X) = (X - s_1)(\Sigma_{i=1}^{n-1} b_i (X - s_2)^i) + (X - s_1)c_1$. Since $f(s_2) = 0$ and R is an integral domain which implies that $c_1 = 0$. It is evident that we can continue this process and in the end we will have $f = gh$, where g and h are as required. Also, the degree bound on h is also clear from the expression. Now, assume the case is true for $n - 1$ variables. Let f be a polynomial in n variables and let its degree in variable X_i be n_i. Also, denote the elements of S_i by s_{ij}, where j varies from 1 to n_i. Let $f = \Sigma_{i=0}^{n} a_i (X_2, ..., X_n) X_1^i$, where a_i is a polynomial in n-1 variables. Write X_1 as $(X_1 - s_{11}) + s_{11}$ and use binomial expansion. What you get is

$$f = (X_1 - s_{11}) \Sigma_{i=0}^{n-1} a'_i (X_1 - s_{11})^i + a'_0 (X_2, ..., X_n) \tag{3}$$

* hshukla.math04@gmail.com

Here a'_i is also a polynomial in n-1 variables. Note that a'_0 vanishes on all tuples of form $(s_{2i_1}, s_{3i_2}, ...)$. So, by induction hypothesis, a'_0 can be written in desired form (from now I will refer it to as D_0), which is actually $\Sigma g_i h_i$, where $deg(h_i) \leq deg(a'_0) - deg(g_i) \leq deg(f) - n_1 - deg(g_i)$. Now consider the term in the summation which is $f = \Sigma_{i=0}^{n-1} a'_i (X_1 - s_{11})^i$ and call it D_1. So, observe that $D_1(s_{1i}, s_{2i_1}, s_{3^i_2} .....) = 0$, except at $i = 1$. So, we can do the same "rewriting" of the polynomial as we did twiw before to get,

$$P_1 = \Sigma_{i=1}^{n_1-1} b_i(X_2, ...X_n)(X_1 - s_{12})^i + b_0(X_2, ...X_n) \tag{4}$$

where b_0 vanishes on tuples of form $(s_{2i_1}, s_{3i_2}, ...)$. Now, if we look back at f, we have

$$f = (X_1 - s_{11})(X_1 - s_{12})(\Sigma_{i=0}^{n_1-2} b_i(X_2, ...X_n)(X_1 - s_{12})) + (X_1 - s_{11})(b_0(X-2, ...X_n)) + D_0 \tag{5}$$

Note that b_0 can also be written in desired form. Observe that summation (call it D_2) vanishes on tuples of form $(s_{1i}, s_{2i_1}, s_{3^i_2} .....) = 0$, except at $i = 1$ and $i = 2$. So, for this summation we would do the same thing as for f. This process keeps going on till we extract out all the $s_{1i's}$. So we will finally get an equation of following form,

$$f = \Sigma_{j=0}^{m_1-1} (\Pi_{i=1}^{m_1-j} (X_1 - s_{1i})(D_{m_1-j}(X_2, ...X_n))) + D_0$$

where all these $D_i s$ can be written in desired form. So, except the first term all terms can be combined together to be written in the form of $\Sigma_{g_i} h'_i$, where

$$deg(h_i) \leq deg(h_i) + m_1 - 1 \leq deg(h_i) + n_1 \leq deg(f) - deg(g_i) \tag{6}$$

Hence, it completes the proof.

□