# An algebraic proof of Alon's Combinatorial Nullstellensatz *

Nisheeth K. Vishnoi †

**Abstract**

In [1], Alon proved the following: Let $k$ be a field and $f \in k[x_1, x_2, \ldots, x_n]$. Given non-empty subsets $S_1, \ldots, S_n \subset k$, for $1 \leq i \leq n$, define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If $f$ vanishes on $S_1 \times \cdots \times S_n$, then $f = \sum_{i=1}^{n} h_i g_i$, for some $h_i \in k[x_1, \ldots, k_n]$, $1 \leq i \leq n$. In this note we give an algebraic proof of the same fact which uses some basic ideas from commutative algebra.

## 1 Introduction

Let $k$ be a field and let $f \in k[x_1, x_2, \ldots, x_n]$. In [1], Alon proved the following important result which has surprising applications.

**Theorem 1.** *(***Combinatorial Nullstellensatz [1]***) Given nonempty subsets $S_1, \ldots, S_n \subset k$, for $1 \leq i \leq n$, define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If $f$ vanishes on $S_1 \times \cdots \times S_n$, then $f = \sum_{i=1}^{n} h_i g_i$, for some $h_i \in k[x_1, \ldots, k_n]$, $1 \leq i \leq n$.*

The numerous applications of this Theorem motivated us to give another proof. Notice that the Theorem is a stronger form of Hilbert's nullstellensatz for the specific case (refer [2]). Before we proceed to give the algebraic proof of Theorem 1, we need some preliminary definitions. Let $A$ be a commutative ring with identity. An ideal $I$ of a ring $A$ is a subset of $A$ which is an additive subgroup of $A$ and, if $a \in A$ and $x \in I$, then $ax \in I$. An ideal $M$ of a ring $A$ is said to be *maximal* if $M \neq A$ and there is no proper ideal $U$ of $A$ which strictly contains $M$. If $I, J$ are ideals of $A$. Then the *sum* , *product* and *radical* ideals are defined as follows

$$I + J := \{a + b \mid a \in I, b \in J\}, \tag{1}$$

*Presented in 32nd Southeastern Conference on Combinatorics, Graph Theory and Computing, LSU.

†College of Computing, Georgia Institute of Technology, Atlanta, GA 30332. Email: nkv@cc.gatech.edu

$$IJ := \left\{ \sum_{i=1}^{m} a_i b_i \mid a_i \in I, b_i \in J, \quad \text{for some} \quad m \geq 0 \right\}, \qquad (2)$$

$$\sqrt{I} := \{ f \mid f^m \in I, \quad m \geq 0 \}.$$

These can be seen to be ideals of $A$. If $I = \sqrt{I}$, then $I$ is called a *radical* ideal. If $I + J = A$, then $I$ and $J$ are said to be *coprime*. Note that two distinct maximal ideals are coprime.

**Proposition 2.** *Let $A$ be a ring, if $I_1, \cdots, I_m$ are pairwise coprime, then*

$$I_1 I_2 \cdots I_m = I_1 \cap \cdots \cap I_m.$$

The proof of this can be found in [2]. If $k$ is a field, and given a set of polynomials $h_1, \ldots, h_m \in k[x_1, \ldots, x_n]$, denote by $V(h_1, \ldots, h_m)$, the *variety* or the set of common zeros of $h_1, \ldots, h_m$ in $k^n$ and by $\langle h_1, \ldots, h_m \rangle$, the ideal generated by $h_1, \ldots, h_m$.

## 2 The algebraic proof

**Proof of Theorem 1**. Let $k$, $S_i$, $g_i$, for $1 \leq i \leq n$ and $f$ be as in Theorem 1. Denote by $\Omega = V(g_1, \ldots, g_n) = S_1 \times \cdots \times S_n$. We are given that $\Omega \subset V(f)$. Let $a := (a_1, \ldots, a_n) \in \Omega$ and the maximal ideal associated to it in $k[x_1, \ldots, x_n]$, $M_a = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$. For $a \in \Omega$, if $f$ is not in $M_a$ then there exists $P_1, P_2 \in k[x_1, \cdots, x_n]$ such that $P_1 f + P_2 M_a = 1$. Then $(P_1 f + P_2 M_a)(a_1, \cdots, a_n) = 0 \neq 1$, a contradiction. Thus $f \in M_a$, $\forall\ a \in \Omega$. Thus $f \in \cap_{a \in \Omega} M_a$. By proposition 2, $\prod_{a \in \Omega} M_a = \cap_{a \in \Omega} M_a$. Thus $f \in \prod_{a \in \Omega} M_a$. We claim that

$$\prod_{a \in \Omega} M_a \quad \subseteq \qquad \langle g_1(x_1), \ldots, g_n(x_n) \rangle.$$

By definition

$$\prod_{a \in \Omega} M_a = \left\{ \sum_{j=1}^{m} \prod_{a \in \Omega} h_a^{(j)}, \quad \text{for some} \quad m \geq 0 \right\},$$

where each $h_a^{(j)}$, for $a = (a_1, \ldots, a_n)$, is of the form

$$h_a^{(j)}(x_1, \ldots, x_n) = p_1^{(j)}(x_1 - a_1) + \cdots p_n^{(j)}(x_n - a_n),$$

for $p_j^{(i)} \in k[x_1, \ldots, x_n]$. Let $p \in \prod_{a \in \Omega} M_a$. Then $p = \sum_{j=1}^{m} \prod_{a \in \Omega} h_a^{(j)}$. It will be sufficient to show that for any $1 \leq j \leq m$,

$$\prod_{a \in \Omega} h_a^{(j)} \in \quad \langle g_1(x_1), \ldots, g_n(x_n) \rangle.$$

We drop the superscript $(j)$ for simplicity. Let $h = \prod_{a \in \Omega} h_a$. It is easy to see as in the expansion of $h$, each term must be of the type

$qg_i(x_i)$ for some $i$ and some $q \in k[x_1, \dots, x_n]$. Thus $h \in \langle g_1, \dots, g_n \rangle$. Hence

$$f \in \cap_{a\in\Omega} M_a = \prod_{a\in\Omega} M_a \subseteq \langle g_1, \dots, g_n \rangle.$$

Note that we have shown that $\langle g_1, \dots, g_n \rangle$ is a radical ideal.

# References


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

[2] M.F. Atiyah, I.G. MacDonald, *Introduction to Commutative Algebra*, Addison- Wesley, 1969.