A duality based proof of the Combinatorial Nullstellensatz

Omran Kouba

Department of Mathematics
Higher Institute for Applied Sciences and Technology
P.O. Box 31983, Damascus, Syria
omran_kouba@hiast.edu.sy

Submitted: Dec 21, 2008; Accepted: Mar 5, 2009; Published: Mar 13, 2009
Mathematics Subject Classifications: 05A99, 15A03

Abstract

In this note we present a proof of the combinatorial nullstellensatz using simple arguments from linear algebra.

The *combinatorial nullstellensatz* [1] is an elegant tool which has many applications in combinatorial number theory, graph theory and combinatorics (see [1] and [2]). In this note we present a proof of this result using simple arguments from linear algebra. In Theorem 1, we recall the statement of the combinatorial nullstellensatz:

Theorem 1. *Let P be a polynomial in m variables $X_1, X_2, \ldots, X_m$ over an arbitrary field $\mathbb{K}$. Suppose that the coefficient of the monomial $X_1^{n_1} X_2^{n_2} \cdots X_m^{n_m}$ in P is nonzero, and that the total degree of P is $\sum_{j=1}^{m} n_j$. Then, if $S_1, S_2, \ldots, S_m$ are subsets of $\mathbb{K}$ such that $\operatorname{card}(S_j) > n_j$ (for $1 \leq j \leq n$,) there is some $(t_1, t_2, \ldots, t_m)$ in $S_1 \times S_2 \times \cdots \times S_m$ so that $P(t_1, t_2, \ldots, t_m) \neq 0$.*

Our proof is based upon a simple lemma concerning linear forms on the vector space $\mathbb{K}[T]$ of polynomials in one variable T over an arbitrary field $\mathbb{K}$. In the dual space $(\mathbb{K}[T])^*$, we consider the dual basis $(\varphi_m)_{m\geq 0}$ of the canonical basis $(T^m)_{m\geq 0}$ of $\mathbb{K}[T]$, this means that $\varphi_m(P)$ is the coefficient of T^m in P, in other words $\varphi_i(T^j) = \delta_{ij}$ where δ_{ij} is the Kronecker symbol. We also denote by $\mathbb{K}_n[T]$ the subspace of $\mathbb{K}[T]$ formed of polynomials of degree at most n.

With the above notation we have the following lemma :

Lemma 2. *Let S be a subset of $\mathbb{K}$ such that $\operatorname{card}(S) = m + 1$. Then there is a family $(\lambda_t^S)_{t\in S}$ of elements in $\mathbb{K}$ such that*

$$\forall\, P \in \mathbb{K}_m[T], \quad \varphi_m(P) = \sum_{t\in S} \lambda_t^S P(t).$$

Proof. Consider, for $t \in S$, the linear form $\mu_t : \mathbb{K}_m[T] \longrightarrow \mathbb{K}, \mu_t(P) = P(t)$. The family $(\mu_t)_{t\in S}$ constitutes a basis of the dual space $(\mathbb{K}_m[T])^*$. (To see this, note that if $(\ell_t)_{t\in S}$ denotes the basis of $\mathbb{K}_m[T]$ formed by the Lagrange intepolation polynomials : $\ell_t(T) = \prod_{s\in S\setminus\{t\}} \frac{T-s}{t-s}$, then $\mu_u(\ell_v) = \delta_{uv}$. This proves that $(\mu_t)_{t\in S}$ is the dual basis of $(\ell_t)_{t\in S}$.)

Now, the linear form $P \mapsto \varphi_m(P)$ defines an element from $(\mathbb{K}_m[T])^*$ and, consequently, it has a unique expression as a linear combination of the elements of the basis $(\mu_t)_{t\in S}$. This proves the existence of a familly of scalars $(\lambda_t^S)_{t\in S}$, such that $\varphi_m(P) = \sum_{t\in S} \lambda_t^S \mu_t(P)$ for any polynomial P in $\mathbb{K}_m[T]$, and achieves the proof of Lemma 2. □

Before proceeding with the proof of Theorem 1, let us recall that the total degree of a polynomial P from $\mathbb{K}[X_1, \ldots, X_m]$ is the largest value of $d_1 + d_2 + \cdots + d_m$ taken over all monomials $X_1^{d_1} X_2^{d_2} \cdots X_m^{d_m}$ with nonzero coefficients in P.

Proof of Theorem 1. For each j in $\{1, \ldots, m\}$, we may assume that $\operatorname{card}(S_j) = n_j + 1$ (by discarding the extra elements if necessary,) then, using Lemma 2, we find a familly of scalars $(\lambda_t^{S_j})_{t\in S_j}$ such that

$$\forall\, P \in \mathbb{K}_{n_j}[T], \quad \varphi_{n_j}(P) = \sum_{t\in S_j} \lambda_t^{S_j} P(t). \tag{1}$$

Then, we consider the linear form Φ on $\mathbb{K}[X_1, \ldots, X_m]$ defined by :

$$\Phi(Q) = \sum_{(t_1,\ldots,t_m)\in S_1\times\cdots\times S_m} \lambda_{t_1}^{S_1} \lambda_{t_2}^{S_2} \cdots \lambda_{t_m}^{S_m} Q(t_1, t_2, \ldots, t_m).$$

Clearly, we have

$$\begin{aligned}\Phi(X_1^{d_1} X_2^{d_2} \cdots X_m^{d_m}) &= \sum_{t_1\in S_1} \sum_{t_2\in S_2} \cdots \sum_{t_m\in S_m} \lambda_{t_1}^{S_1} \lambda_{t_2}^{S_2} \cdots \lambda_{t_m}^{S_m} t_1^{d_1} t_2^{d_2} \ldots t_m^{d_m} \\ &= \prod_{j=1}^{m} \left(\sum_{t\in S_j} \lambda_t^{S_j} t^{d_j} \right).\end{aligned}$$

So we have the following two properties:

i. If there is some k in $\{1, \ldots, m\}$ such that $d_k < n_k$, then by (1) we have

$$\sum_{t\in S_k} \lambda_t^{S_k} t^{d_k} = \varphi_{n_k}(T^{d_k}) = 0,$$

and therefore, $\Phi(X_1^{d_1} X_2^{d_2} \cdots X_m^{d_m}) = 0$.

ii. On the other hand,

$$\Phi(X_1^{n_1}X_2^{n_2}\cdots X_m^{n_m}) = \prod_{j=1}^{m}\varphi_{n_j}(T^{n_j}) = 1.$$

Let us suppose that

$$P = \sum_{(d_1,d_2,\ldots,d_m)\in\mathcal{D}} b_{d_1,d_2,\ldots,d_m} X_1^{d_1}X_2^{d_2}\cdots X_m^{d_m},$$

where we collected in $\mathcal{D}$ the multi-indexes $(d_1, d_2, \ldots, d_m)$ satisfying $b_{d_1,d_2,\ldots,d_m} \neq 0$.

Now, if $(d_1, d_2, \ldots, d_m)$ is an element from $\mathcal{D}$ which is different from $(n_1, n_2, \ldots, n_m)$, then there is some k in $\{1, \ldots, m\}$ such that $d_k < n_k$ because $\deg(P) = \sum_{j=1}^m n_j$. Therefore, by (*i.*), if $(d_1, d_2, \ldots, d_m)$ is an element from $\mathcal{D}$ which is different from $(n_1, n_2, \ldots, n_m)$, then $\Phi(X_1^{d_1}X_2^{d_2}\cdots X_m^{d_m}) = 0$, and if we use (*ii.*) we conclude that

$$\Phi(P) = \sum_{(d_1,d_2,\ldots,d_m)\in\mathcal{D}} b_{d_1,d_2,\ldots,d_m}\Phi(X_1^{d_1}X_2^{d_2}\cdots X_m^{d_m}) = b_{n_1,n_2,\ldots,n_m} \neq 0.$$

Finally, the conclusion of the theorem follows since

$$\sum_{(t_1,\ldots,t_m)\in S_1\times\cdots\times S_m} \lambda_{t_1}^{S_1}\lambda_{t_2}^{S_2}\cdots\lambda_{t_m}^{S_m} P(t_1, t_2, \ldots, t_m) = \Phi(P) \neq 0.$$

This ends the proof of Theorem 1. □

References

[**1**] Alon, N., Combinatorial Nullstellensatz. *Recent trends in combinatorics. (Mátraháza, 1995). Combin. Probab. Comput.* 8 (1999), 7–29.

[**2**] Shirazi, H. and Verstraëte, J., A note on polynomials and f-factors of graphs. *Electronic J. of Combinatorics,* 15 (2008), #N22.