COMBINATORIAL NULLSTELLENSATZ

SHAMIL ASGARLI

I learnt the following proof from Corrine Yap, who kindly shared it with me when I was teaching a week-long minicourse on this topic during MathILy 2019. I am also grateful to Brian Freidin who helped me understand the proof better. The purpose of this document is to fill in all the details carefully.

Theorem. Let K be a field, and $F \in K[x_1, ..., x_n]$. Suppose that the monomial $x_1^{d_1} \cdots x_n^{d_n}$ appears with a non-zero coefficient in F such that $d_1 + \cdots + d_n = d$ is the maximum degree among all the monomials in F. Let $S_1, ..., S_n$ be finite subsets of K such that $|S_i| > d_i$ for each i. Then there exists $a_i \in S_i$ for $1 \le i \le n$ such that $F(a_1, ..., a_n) \neq 0$.

Proof. We begin by proving a lemma regarding polynomials of one variable. In particular, the lemma proves the result when $n = 1$.

Lemma. Let $S \subset K$ be a finite subset such that $s := |S| > d$. Write $S = \{u_1, ..., u_s\}$. There exist constants $\beta_1, \dots, \beta_s$ in K (depending only on S) such that for every polynomial f of degree d,

$$\sum_{i=1}^{s} \beta_i f(u_i) \neq 0$$

In particular, $f(u_i) \neq 0$ for some $u_i \in S$.

Proof of the lemma. In fact, we will show that a stronger conclusion holds: we will prove existence of $\beta_1, ..., \beta_s \in K$ such that for every polynomial $f(x) = c_d x^d + \cdots + c_1 x + c_0$,

$$\sum_{i=1}^{s} \beta_i f(u_i) = c_d \neq 0$$

The idea of extracting the leading coefficient will be beneficial when we extend the result for polynomials in many variables. As for the proof, consider the matrix

$$A_m = \begin{bmatrix} 1 & 1 & \dots & 1 \\ u_1 & u_2 & \dots & u_s \\ \vdots & \vdots & \ddots & \vdots \\ u_1^m & u_2^m & \dots & u_s^m \end{bmatrix}$$

defined for each $m \in \mathbb{N}$. To prove the lemma, it suffices to find $\beta_1, ..., \beta_s$ such that

$$A_d \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{s-1} \\ \beta_s \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ u_1 & u_2 & \dots & u_s \\ \vdots & \vdots & \ddots & \vdots \\ u_1^{d-1} & u_2^{d-1} & \dots & u_s^{d-1} \\ u_1^d & u_2^d & \dots & u_s^d \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{s-1} \\ \beta_s \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

Indeed, if $\{\beta_i\}_{i=1}^s$ satisfies the condition above, then

$$\sum_{i=1}^{s} \beta_i f(u_i) = \sum_{i=1}^{s} \beta_i \sum_{j=0}^{d} c_j u_i^j = \sum_{j=0}^{d} c_j \sum_{i=1}^{s} \beta_i u_i^j = c_d$$

since $\sum_{i=1}^{s} \beta_i u_i^j = 0$ for all $0 \leq j < d$, and $\sum_{i=1}^{s} \beta_i u_i^d = 1$ by construction. Note that $\beta_1, ..., \beta_s$ gives rise to a vector $\mathbf{b} = [\beta_1, ..., \beta_s]^T$ such that $\mathbf{b} \in \ker(A_{d-1})$ but $\mathbf{b} \notin \ker(A_d)$. Conversely, any element in $\ker(A_{d-1}) \backslash \ker(A_d)$ gives rise to, possibly after scaling, a vector $\mathbf{b} = [\beta_1, ..., \beta_s]^T$ satisfying the above properties. The task has been reduced to demonstrating that $\ker(A_d) \subsetneq \ker(A_{d-1})$. Note that the last row of A_d is not in the span of first d rows, because otherwise such a linear dependence would produce a non-zero polynomial of degree d that vanishes at s distinct points $u_1, ..., u_s$ which is impossible as $s > d$. It follows that $\text{rank}(A_d) > \text{rank}(A_{d-1})$. Viewing $A_d : K^s \to K^{d+1}$ and $A_{d-1} : K^s \to K^d$ as linear transformations, the rank-nullity theorem implies that $\dim \ker(A_d) < \dim \ker(A_{d-1})$. □

We can rephrase the content of the lemma as follows. There exists a function $\beta : S \to K$ such that

$$\sum_{s \in S} \beta(s) s^j = \begin{cases} 1 & \text{if } j = d \\ 0 & \text{if } j < d \end{cases}$$

To prove the theorem, consider the sets $S_1, ..., S_n$ in the hypothesis. For each S_i, use the lemma above to construct $\beta^{(i)} : S_i \to K$. Now define $\alpha : S_1 \times \cdots \times S_n \to K$ by assigning for each $\mathbf{s} = (s_1, ..., s_n) \in S_1 \times \cdots \times S_n$,

$$\alpha(\mathbf{s}) := \beta^{(1)}(s_1)\beta^{(2)}(s_2) \cdots \beta^{(n)}(s_n)$$

We claim that for each monomial $\mathbf{x}^\mathbf{j} = x_1^{j_1} \cdots x_n^{j_n}$ with $j_1 + \cdots + j_n \leq d$,

$$\sum_{\mathbf{s} \in S_1 \times \cdots \times S_n} \alpha(\mathbf{s}) \mathbf{s}^\mathbf{j} = \begin{cases} 1 & \text{if } j_i = d_i \text{ for every } i \\ 0 & \text{if } j_i < d_i \text{ for at least one } i \end{cases}$$

Indeed, assume $j_i = d_i$ for every i. Then the right hand side becomes:

$$\sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \cdots \sum_{s_n \in S_n} \beta^{(1)}(s_1) \cdots \beta^{(n)}(s_n) s_1^{d_1} \cdots s_n^{d_n} = \prod_{i=1}^{n} \left(\sum_{s \in S_i} \beta^{(i)}(s) s^{d_i} \right) = \prod_{i=1}^{n} 1 = 1$$

If $j_i < d_i$ for some i, then $\sum_{s \in S_i} \beta^{(i)}(s) s^{d_i} = 0$ for that value of i, so the product in the last displayed equation is zero, and the claim is proved.

As a consequence,

$$\sum_{\mathbf{s} \in S_1 \times \cdots \times S_n} \alpha(\mathbf{s}) F(\mathbf{s}) = c_{d_1 d_2 \ldots d_n} \neq 0$$

where $c_{d_1 d_2 \ldots d_n}$ is the coefficient of the monomial $x_1^{d_1} \cdots x_n^{d_n}$ appearing in F. In particular, there exists a choice of $\mathbf{s} = (s_1, ..., s_n) \in S_1 \times \cdots \times S_n$ for which $F(\mathbf{s}) \neq 0$, as desired.

□