# A FULL NULLSTELLENSATZ FOR FINITE ALGEBRAIC SETS

PETE L. CLARK

Abstract. Inspired by Alon's Combinatorial Nullstellensatz, we give a full Nullstellensatz for finite algebraic sets. Our approach is self-contained and elementary: we do not assume familiarity with Nullstellensätze, nor indeed with any commutative algebra beyond the Chinese Remainder Theorem.

## 1. Introduction

### 1.1. The Combinatorial Nullstellensatz and the Polynomial Method.

This note concerns the following celebrated result of N. Alon.

**Theorem 1.** *(Alon's Combinatorial Nullstellensatz) Let $F$ be an integral domain, let $X_1, \ldots, X_n \subset F$ be nonempty and finite, and $X = \prod_{i=1}^n X_i$. For $1 \leq i \leq n$, put*

$$\varphi_i(t_i) = \prod_{x_i \in X_i} (t_i - x_i) \in F[t_i] \subset F[t] = F[t_1, \ldots, t_n]. \tag{1}$$

*Let $f \in F[t]$ be a polynomial which vanishes on all the common zeros of $\varphi_1, \ldots, \varphi_n$: that is, for all $x \in F^n$, if $\varphi_1(x) = \ldots = \varphi_n(x) = 0$, then $f(x) = 0$. Then:*
*a) There are polynomials $h_1, \ldots, h_n \in F[t]$ such that*

$$f(t) = \sum_{i=1}^n h_i(t)\varphi_i(t). \tag{2}$$

*b) Moreover the $h_1, \ldots, h_n$ may be chosen so as to satisfy*

$$\forall 1 \leq i \leq n,\ \deg h_i \leq \deg f - \deg \varphi_i. \tag{3}$$

Using Theorem 1, Alon deduced the following result.

**Corollary 2.** *(Alon's Polynomial Method) Let $F$ be an integral domain, $n \in \mathbb{Z}^+$, $a_1, \ldots, a_n \in \mathbb{N}$, and let $f \in F[t] = F[t_1, \ldots, t_n]$. We suppose:*
*(i) $\deg f \leq a_1 + \ldots + a_n$.*
*(ii) The coefficient of $t_1^{a_1} \cdots t_n^{a_n}$ in $f$ is nonzero.*
*Then, for any subsets $X_1, \ldots, X_n$ of $F$ with $\#X_i = a_i + 1$ for $1 \leq i \leq n$, there is $x = (x_1, \ldots, x_n) \in X = \prod_{i=1}^n X_i$ such that $f(x) \neq 0$.*

Alon used Corollary 2 to derive various old and new results in number theory and combinatorics, starting with Chevalley's Theorem that a homogeneous polynomial of degree $d$ in at least $d+1$ variables over a finite field has a nontrivial zero. The use of polynomial methods has burgeoned to a remarkable degree in recent years. We recommend the recent survey [Ta13], which lucidly describes the main techniques but also captures the sense of awe and excitement at the extent to which these very simple ideas have cracked open the field of combinatorial number theory and whose range of future applicability seems almost boundless.

In [Al99], the term "Combinatorial Nullsetellensatz" is used for both Theorem 1 and Corollary 2. Most later references to the "Combinatorial Nullstellensatz" mean Corollary 2. More recently attention has focused on the following result.

**Theorem 3.** *(*[Sc08, Thm. 3.2], [La10, Thm. 3], [KP12, Thm. 4]*) Let $F$ be an integral domain, and let $f \in F[t]$. Let $a_1, \ldots, a_n \in \mathbb{N}$ be such that $\deg f \leq a_1 + \ldots + a_n$. For each $1 \leq i \leq n$, let $X_i \subset F$ with $\#X_i = a_i + 1$, and let $X = \prod_{i=1}^n X_i$. Let $c_a = c_{a_1,\ldots,a_n}$ be the coefficient of $t_1^{a_1} \cdots t_n^{a_n}$ in $f$. Then*

$$c_a = \sum_{x=(x_1,\ldots,x_n)\in X} \frac{f(x)}{\prod_{i=1}^n \prod_{y_i \in X_i \setminus \{c_i\}} (x_i - y_i)}. \tag{4}$$

Theorem 3 implies Corollary 2, and the above papers do a good job of showing that it really is an improvement. For instance, from Theorem 3 we get:

**Corollary 4.** *(Schauz* [Sc08, Cor. 3.4]*) Let $F$ be a field, and let $f \in F[t]$. Let $X_1, \ldots, X_n$ be nonempty finite subsets of $F$ such that $\sum_{i=1}^n (\#X_i - 1) > \deg f$. Let $\mathfrak{u}_X = \#\{x \in X \mid f(x) \neq 0\}$. Then $\mathfrak{u}_X \neq 1$.*

(So if $P \in \mathbb{F}_q[t_1, \ldots, t_n]$ has degree $d < n$, apply Corollary 4 with $X_1 = \ldots = X_n = \mathbb{F}_q$ and $f(t) = 1 - P(t)^{q-1}$, and note that $f(x) = 1$ if $P(x) = 0$ and $f(x) = 0$ otherwise. Thus $P$ cannot have precisely one zero, proving Chevalley's Theorem!)

Thus the lack of interest in Theorem 1 *per se* seems likely to continue.

### 1.2. **Alon's Nullstellensatz versus Hilbert's Nullstellensatz.**

In particular the prospect of improving Theorem 1 *as a Nullstellensatz* has not been explored, perhaps because the notion of a Nullstellensatz, though seminal in algebra and geometry, is less familiar to researchers in combinatorics. But it was certainly familiar to Alon, who began [Al99] by recalling the following result.

**Theorem 5.** *(Hilbert's Nullstellensatz) Let $F$ be an algebraically closed field, let $g_1, \ldots, g_m \in F[t]$, and let $f \in F[t]$ be a polynomial which vanishes on all the common zeros of $g_1, \ldots, g_m$. Then there is $k \in \mathbb{Z}^+$ and $h_1, \ldots, h_m \in F[t]$ such that*

$$f^k = \sum_{i=1}^m h_i g_i.$$

Let us compare Theorems 1 and 5. They differ in the following points:
• In Alon's Nullstellensatz, $F$ can be any field (and in fact any integral domain, but for our main result we need to work over a field). In Hilbert's Nullstellensatz, $F$ must be algebraically closed. Really must: if $f$ is not algebraically closed, then there is a nonconstant polynomial $g(t_1)$ without roots in $F$; taking $m = 1$, $g_1 = g$ and $f = 1$ we see that the conclusion fails.
• In Alon's Nullstellensatz, the conclusion is that $f$ itself is a linear combination of the $\varphi_i$'s with polynomial coefficients, but in Hilbert's Nullstellensatz we must allow taking a power of $f$. Really must: e.g. take $k \in \mathbb{Z}^+$ $m = 1$, $g_1 = t_1^k$ and $f = t_1$.
• Alon's Nullstellensatz is **effective**: it gives upper bounds on $\deg h_i$. Hilbert's Nullstellensatz is not effective. It can be made so: effective versions of Hilbert's Nullstellensatz have been given by Brownawell [Br87], Kollár [Ko88] and others, but their bounds are much more complicated than the ones in Theorem 1.

• In Alon's Nullstellensatz the $\varphi_i$'s are extremely restricted. On the other hand, in Hilbert's Nullstellensatz the $g_i$'s can be any set of polynomials. Thus Theorem 5 is a *full Nullstellensatz*, whereas Theorem 1 is a *partial Nullstellensatz*.

### 1.3. **The Finitely Restricted Nullstellensatz.**

Let $F$ be any field. The main result of this note gives a full Nullstellensatz for finite algebraic subsets which includes as a special case Theorem 1 for $F$ without the upper bounds on the degree. We supplement this with another, very simple, result, which when combined with the main result recovers the degree conditions of Theorem 1 (and holds over any integral domain $F$).

Our main result is more general than Theorem 1 in a further sense: we consider *arbitrary* finite subsets of $F^n$, not just the *cylindrical* subsets $\prod_{i=1}^n X_i$.

We now set up the formalism for a **restricted variable Nullstellensatz**. The key observation: in Theorem 1, the $\varphi_1, \ldots, \varphi_n$ are chosen to have common zero set $X = \prod_{i=1}^n X_i$, so the condition on $f \in F[t]$ that for all $x \in F^n$, $\varphi_1(x) = \ldots = \varphi_n(x) = 0 \implies f(x) = 0$ is equivalent to: for all $x \in X$, $\varphi_1(x) = \ldots = \varphi_n(x) = 0 \implies f(x) = 0$. We will replace $X$ by any finite subset of $F^n$ and replace the special polynomials $\varphi_1, \ldots, \varphi_n$ by an arbitrary set of polynomials.

For a set $Z$, let $2^Z$ be the set of all subsets of $Z$. For a subset $J$ of a ring $R$, let $\langle J \rangle$ denote the ideal of $R$ generated by $J$, and let $\operatorname{rad} J = \operatorname{rad}\langle J \rangle$ denote the set of all $f \in R$ such that $f^k \in \langle J \rangle$ for some $k \in \mathbb{Z}^+$. An ideal $J$ is **radical** if $J = \operatorname{rad} J$.

Let $F$ be a domain, $F[t] = F[t_1, \ldots, t_n]$, and let $X \subset F^n$. For $x \in X,\ f \in F[t]$, put

$$I(x) = \{f \in F[t] \mid f(x) = 0\},$$

$$V_X(f) = \{x \in X \mid f(x) = 0\}.$$

We extend $I$ and $V_X$ to maps on power sets as follows:

$$I : 2^X \to 2^{F[t]},\ A \subset X \mapsto I(A) = \bigcap_{a \in A} I(a) = \{f \in F[t] \mid \forall a \in A,\ f(a) = 0\},$$

$$V_A : 2^{F[t]} \to 2^X,\ J \subset F[t] \mapsto V_A(J) = \bigcap_{f \in J} V_A(f) = \{x \in X \mid \forall f \in J,\ f(a) = 0\}.$$

The maps $I$ and $V_A$ are **antitone**:

$$A_1 \subset A_2 \subset X \implies I(A_1) \supset I(A_2),$$

$$J_1 \subset J_2 \subset F[t] \implies V_A(J_1) \supset V_A(J_2),$$

and thus their compositions are **isotone**:

$$A_1 \subset A_2 \subset X \implies V_X(I(A_1)) \subset V_X(I(A_2)),$$

$$J_1 \subset J_2 \subset F[t] \implies I(V_X(J_1)) \subset I(V_X(J_2)).$$

We have $X = V_X(0)$, so

$$\forall J \subset F[t],\ I(V_X(J)) \supset I(V_X(0)) = I(X).$$

**Lemma 6.** *For all ideals $J_1, \ldots, J_m$ of $F[t]$, we have $V_X(J_1 \cdots J_m) = \bigcup_{i=1}^m V_X(J_i)$.*

*Proof.* We do intend to allow $m = 0$, in which case the identity reads $V_X(\langle 1 \rangle) = \varnothing$, which is true. Having established that, we immediately reduce to the case $m = 2$. Since $J_1 J_2 \subset J_i$ for $i = 1, 2$, $V_X(J_1 J_2) \supset V_X(J_i)$ for $i = 1, 2$, thus $V_X(J_1 J_2) \supset V_X(J_1) \cup V_X(J_2)$. Now let $x \in X \setminus (V_X(J_1) \cup V_X(J_2))$. For $i = 1, 2$ there is $f_i \in J_i$ with $f_i(x) \neq 0$. Since $F$ is a domain, $f_1(x) f_2(x) \neq 0$, so $x \notin V_X(J_1 J_2)$. □

If $A \subset X$, then $I(A)$ is an ideal of $F[t]$, and in fact a radical ideal: if $f \in F[t]$ and $f^k \in I(A)$ for some $k \in \mathbb{Z}^+$, then for all $a \in A$ we have $f(x)^k = 0$, hence – since $F$ is a domain – $f(x) = 0$, and thus $f \in I(A)$. It follows that

$$\forall J \subset F[t],\ I(V_X(J)) \supset \operatorname{rad}(J + I(X)) \supset \operatorname{rad} J + I(X) \supset J + I(X). \tag{5}$$

It is a well known fact (but see § 2.3 for a proof) that for any infinite field $F$, the only polynomial which vanishes at every point of $F^n$ is the zero polynomial: $I(F^n) = \{0\}$. This serves to motivate the following restatement of Hilbert's Nullstellensatz.[1]

**Theorem 7.** *Let $F$ be an algebraically closed field. For all $J \subset F[t]$,*

$$I(V_{F^n}(J)) = \operatorname{rad} J.$$

Here is the main result of this note.

**Theorem 8.** *(Finitely Restricted Nullstellensatz) Let $F$ be a field, and let $X \subset F^n$ be a finite subset.*
*a) For all ideals $J$ of $F[t]$, we have*

$$I(V_X(J)) = J + I(X). \tag{6}$$

*In particular, if $J \supset I(X)$ then $I(V_X(J)) = J$.*
*b) Suppose that $X = \prod_{i=1}^n X_i$ for finite nonempty subsets $X_i$ of $F$. Define $\varphi_i(t_i) \in F[t_i]$ as in (1) above. Then*

$$I(X) = \langle \varphi_1, \ldots, \varphi_n \rangle. \tag{7}$$

*c) If $X = \prod_{i=1}^n X_i$, then*

$$I(V_J(\langle \varphi_1, \ldots, \varphi_n \rangle)) = \langle \varphi_1, \ldots, \varphi_n \rangle + I(X) = I(X) + I(X) = I(X).$$

We will prove parts a) and b) of Theorem 8 in § 2. Theorem 8c) follows immediately. Moreover, part c) is precisely the ineffective part of Alon's Combinatorial Nullstellensatz (Theorem 1a)) when $F$ is a field.

We immediately deduce the following result of G. Terjanian [Te66].

**Corollary 9.** *(Finite Field Nullstellensatz) Let $\mathbb{F}_q$ be a finite field. Then for all ideals $J$ of $\mathbb{F}_q[t]$ we have*

$$I(V_{\mathbb{F}_q^n}(J)) = J + \langle t_1^q - t_1, \ldots, t_n^q - t_n \rangle.$$

*Proof.* Apply Theorem 8 with $F = X_1 = \ldots = X_n = \mathbb{F}_q$. □

[1]The equivalence of the two formulations uses the Hilbert Basis Theorem.

1.4. **Supplement on Cylindrical Reduction.**

**Proposition 10.** *(Cylindrical Reduction) Let $F$ be an integral domain. For $1 \leq i \leq n$, let $\varphi_i(t_i) \in F[t_i]$ be monic of degree $d_i$. Put $\Phi = \langle \varphi_1, \ldots, \varphi_n \rangle$ and $d = (d_1, \ldots, d_n)$. Say $f \in F[t]$ is **d-reduced** if for all $1 \leq i \leq n$, $\deg_{t_i} f < d_i$. Then:*
*a) The set $\mathcal{R}_d$ of all d-reduced polynomials is a free $F$-module of rank $d_1 \cdots d_n$.*
*b) For all $f \in F[t]$, there are $h_1, \ldots, h_n \in F[t]$ such that $\deg h_i \leq \deg f - \deg \varphi_i$ and $\overline{f} = f - \sum_{i=1}^n h_i \varphi_i$ is d-reduced.*
*c) The composite map*

$$R : \mathcal{R}_d \hookrightarrow F[t] \to F[t]/\Phi$$

*is an $F$-module isomorphism.*
*d) For all $f \in F[t]$, there is a unique $\overline{f} \in \mathcal{R}_d$ such that $f - \overline{f} \in \langle \varphi_1, \ldots, \varphi_n \rangle$.*
*e) If $f \in \Phi$, then $f = \sum_{i=1}^n h_i \varphi_i$ with $\deg h_i \leq \deg f - \deg \varphi_i$ for all $1 \leq i \leq n$.*

*Proof.* a) Indeed $\{t_1^{a_1} \cdots t_n^{a_n} \mid 0 \leq a_i < d_i\}$ is a basis for $\mathcal{R}_d$.
b) Our argument directly generalizes an **explicit reduction procedure** given by Alon when the $\varphi_i$'s are given by (1). Nevertheless let us give the details.

For any domain $T$, if $a(t_1), b(t_1) \in T[t_1]$ with $b(t_1)$ monic, then the usual long-division algorithm yields unique polynomials $q(t_1), r(t_1) \in T[t_1]$ with $a(t_1) = q(t_1)b(t_1) + r(t_1)$ and $\deg r < \deg b$. Or: we may write $b(t_1) = t_1^{d_1} - (\beta_{d_1-1} t_1^{d_1-1} + \ldots + \beta_0)$ and obtain $r(t_1)$ by repeatedly substituting $\beta_{d_1-1} t_1^{d_1-1} + \ldots + \beta_0$ for $t_1^{d_1}$ until we obtain a polynomial of degree smaller than $d_1 = \deg b$. The latter description makes it easy to see that if $T$ is itself a polynomial ring in other indeterminates $t_2, \ldots, t_n$ then $r_1$ not only has smaller $t_1$-degree than $b(t_1)$ but has total degree at most that of $a_1$.
Returning to our $f \in F[t]$: we divide $f(t)$ by $\varphi_1(t_1)$, then divide the remainder $r_1$ by $\varphi_2(t_2)$, and so forth, finally dividing by $\varphi_n(t_n)$ to get a remainder $r_n$: thus

$$f = \sum_{i=1}^n h_i \varphi_i + r_n,$$

with $h_i \in F[t]$, and such that for all $1 \leq i \leq n$, we have

$$\deg h_i = \deg h_i \varphi_i - \deg \varphi_i = \deg(f - r_i) - \deg \varphi_i \leq \deg f - \deg \varphi_i$$

and

$$\deg_{t_i} r_n < \deg \varphi_i = d_i.$$

Thus $r_n = f - \sum_{i=1}^n h_i \varphi_i$ is $d$-reduced. c) By part b), $R$ is surjective. Since

$$\begin{aligned} F[t]/\Phi &\cong \left(F[t_1, \ldots, t_{n-1}]/\langle \varphi_1, \ldots, \varphi_{n-1} \rangle\right)[t_n]/\langle \varphi_n \rangle \\ &\cong F[t_1, \ldots, t_{n-1}]/\langle \varphi_1, \ldots, \varphi_{n-1} \rangle \otimes_F F[t_n]/\langle \varphi_n \rangle \cong \ldots \\ &\cong F[t_1]/\langle \varphi_1 \rangle \otimes_F \ldots \otimes_F F[t_n]/\langle \varphi_n \rangle \cong F^{d_1} \otimes_F \cdots \otimes_F F^{d_n} \cong F^{d_1 \cdots d_n}, \end{aligned}$$

$F[t]/\langle \varphi_1, \ldots, \varphi_n \rangle$ is a free $F$-module of rank $d_1 \cdots d_n$. Thus $R$ is a surjective $F$-map of free $F$-modules of equal, finite rank. Tensoring from $F$ to its fraction field and applying linear algebra, we see that $R$ is injective and thus an isomorphism.
d) This follows immediately from part c).
e) By part b) there are $h_1, \ldots, h_n \in F[t]$ with $\deg h_i \leq \deg f_i - \deg \varphi_i$ for all $i$ such that $\overline{f} = f - \sum_{i=1}^n h_i \varphi_i$ is $d$-reduced. Since $f \in \langle \varphi_1, \ldots, \varphi_n \rangle$, also $0 \in \mathcal{R}_d$ is such that $f - 0 \in \varphi_1, \ldots, \varphi_n$. Applying part d) we get $\overline{f} = 0$ and $f = \sum_{i=1}^n h_i \varphi_i$. □

When $\varphi_1, \ldots, \varphi_n$ are defined by (1), by (7) we have $\langle \varphi_1, \ldots, \varphi_n \rangle = I(X)$; combining with Proposition 10e), we get Alon's Combinatorial Nullstellensatz (Theorem 1).

## 2. Proof of the Finitely Restricted Nullstellensatz

### 2.1. **The proof of Theorem 8a).**

Let $F$ be a field, and let $X \subset F^n$ be finite. Let $x = (x_1, \ldots, x_n) \in X$. Let $\mathfrak{m}_x = \langle t_1 - x_1, \ldots, t_n - x_n \rangle$. Then $F[t]/\mathfrak{m}_x \cong F$, so $\mathfrak{m}_x$ is maximal. On the other hand $\mathfrak{m}_x \subset I(x) \subsetneq F[t]$, so $\mathfrak{m}_x = I(x)$. Moreover $V_X(\mathfrak{m}_x) = \{x\}$, hence

$$I(V_X(\mathfrak{m}_x)) = I(x) = \mathfrak{m}_x.$$

Now let $A = \{x_i\}_{i=1}^k \subset X$. Then

$$I(A) = I(\bigcup_i \{x_i\}) = \bigcap_i I(x_i) = \bigcap_i \mathfrak{m}_{x_i},$$

so by the Chinese Remainder Theorem [**?**, Cor. 2.2],

$$F[t]/I(A) = F[t]/\bigcap_i \mathfrak{m}_{x_i} \cong \prod_i F[t]/\mathfrak{m}_{x_i} \cong F^{\#X}.$$

We denote by $F^A$ the set of all functions from $A$ to $F$; this is a commutative $F$-algebra under pointwise addition and multiplication (and is indeed just the product of copies of $F$ indexed by $X$). The **evaluation map**

$$E_A = F[t] \to F^A,\ f \in F[t] \mapsto (x \in A \mapsto f(x))$$

is a homomorphism of $F$-algebras. Moreover $\operatorname{Ker} E_A = I(A)$, so $E_A$ induces a map

$$\iota : F[t]/I(A) \hookrightarrow F^A.$$

Thus $\iota$ is an injective $F$-linear map between $F$-modules of equal finite dimension, hence – since $F$ is a field! – $\iota$ is an isomorphism. For a ring $R$, let $\mathcal{I}(R)$ be a set of ideals of $R$. Since $\iota$ is an isomorphism, we have

$$\#\mathcal{I}(F[t]/I(X)) = \#\mathcal{I}(F^X) = 2^{\#X}.$$

By restricting $V_X$ to ideals containing $I(X)$, we get maps

$$V_X : \mathcal{I}(F[t]/I(X)) \to 2^X,$$
$$I : 2^X \to \mathcal{I}(F[t]/I(X)).$$

For all $A \subset X$, we have

$$V_X(I(A)) = V_X(\prod_{i=1}^k \mathfrak{m}_{x_i}) = \bigcup_{i=1}^k V_X(\mathfrak{m}_{x_i}) = \bigcup_{i=1}^k \{x_i\} = A.$$

Since $\mathcal{I}(F[t]/I(X))$ and $2^X$ have the same finite cardinality, it follows that $V_X$ and $I$ are mutually inverse bijections! Thus for any ideal $J$ of $F[t]$, using (5) we get

$$J + I(X) \subset I(V_X(J)) \subset I(V_X(J + I(X))) = J + I(X).$$

### 2.2. **The proof of Theorem 8b).**

Let $d_i = \deg \varphi_i$ and put $\Phi = \langle \varphi_1, \ldots, \varphi_n \rangle$. Since $\varphi_i|_X \equiv 0$ for all $i$, $\Phi \subset \operatorname{Ker} E$, so there is an induced surjective $F$-algebra homomorphism

$$\tilde{E}_X : F[t]/\Phi \to F[t]/\operatorname{Ker} E_X \to F^X.$$

Both $F[t]/\Phi$ and $F^X$ are $F$-vector spaces of dimension $d_1 \cdots d_n$, so $\tilde{E}$ is an isomorphism. It follows that $F[t]/\Phi \to F[t]/\operatorname{Ker} E$ is injective, i.e., $\Phi = \operatorname{Ker} E = I(X)$.

2.3. **Supplement on Integral Domains.**

Let $F$ be a commutative ring which is not a field. Then the statement of Theorem 8a) is meaningful, but (except in the trivial case $X = \varnothing$) *false*: indeed, let $x \in X$. Since $F[t]/\mathfrak{m}_x \cong F$, $\mathfrak{m}_x$ is *not* maximal, so let $J$ be an ideal with $\mathfrak{m}_x \subsetneq J \subsetneq F[t]$. Then there is $f \in I$ such that $f(x) \neq 0$, so

$$I(V_X(J)) = I(\varnothing) = F[t] \supsetneq J + I(X) = J.$$

However, Theorem 8b) holds over any integral domain $F$. Most of the argument goes through verbatim; the one issue is that we used the surjectivity of $E_X : F[t] \to F^X$, and our proof of this in § 2.1 used that an injective $F$-linear mapping of $F$-vector spaces of equal finite dimension is an isomorphism. The analogous statement for free $F$-modules of finite rank is false over an integral domain which is not a field: indeed, let $a \in F$ be nonzero and not a unit, and consider the mapping $F^n \to F^n$ given by $x \mapsto ax$.

Nevertheless the evaluation map $E_X : F[t] \to F^X$ is surjective for any integral domain $F$, and the method of proof already exists in the literature: we reduce to the cylindrical case $X = \prod_{i=1}^n X_i$ and then *explicitly* write the characteristic function of each one element subset $\{x\} \subset X$ as a polynomial.

In fact the evaluation map $E_X : F[t] \to F^X$ can be defined for *any* subset $X \subset F^n$, and it is natural to ask when it is injective and when it is surjective: indeed the former question is related to Cylindrical Reduction and thus work of Chevalley and Alon-Tarsi. The proofs for a general integral domain are a bit more technical, so we have held them back...until now.

**Lemma 11.** *Let $F$ be an integral domain, and let $X$ be an infinite set. Then $F^X$ is not a countably generated $F$-module.*

*Proof.* Step 1: For $x \in \mathbb{R}$, let $A_x = \{y \in \mathbb{Q} \mid y < x\}$, and let $\mathcal{C}_{\mathbb{Q}} = \{A_x\}_{x \in \mathbb{R}}$. Then $\mathcal{C}_{\mathbb{Q}} \subset 2^{\mathbb{Q}}$ is an uncountable linearly ordered family of nonempty subsets of $\mathbb{Q}$. Since $X$ is infinite, there is an injection $\iota : \mathbb{Q} \hookrightarrow X$; then $\mathcal{C} = \{\iota(A_x)\}_{x \in \mathbb{R}}$ is an uncountable linearly ordered family of nonempty subsets of $X$.

Step 2: For each $A \in \mathcal{C}$, let $1_A$ be the characteristic function of $A$. Then $\{1_A\}_{A \in \mathcal{C}}$ is an $F$-linearly independent set: let $A_1, \ldots, A_n \in \mathcal{C}$ and $\alpha_1, \ldots, \alpha_n \in F$ be such that $\alpha_1 1_{A_1} + \ldots + \alpha_n 1_{A_n} \equiv 0$. We may order the $A_i$'s such that $A_1 \subset \ldots \subset A_n$ and thus there is $x \in A_n \setminus \bigcup_{i=1}^{n-1} A_i$. Evaluating at $x$ gives $\alpha_n = 0$. In a similar manner we find that $\alpha_{n-1} = \ldots = \alpha_1 = 0$.

Step 3: Let $M = \bigoplus_{i=1}^{\infty} F$. If $F^X$ were countably generated as an $F$-module, there would be a surjective homomorphism of $F$-modules $\Phi : M \to F^X$. Under any homomorphism of $F$-modules, the preimage of a linearly independent set is a linearly independent set, so by Step 2, $\mathcal{S} = \Phi^{-1}(\{1_A\}_{A \in \mathcal{C}})$ is an uncountable $F$-linearly independent subset of $M$. Let $K$ be the field of fractions of $F$. Then $\{s \otimes 1 \mid s \in \mathcal{S}\}$ is an uncountable $K$-linearly independent subset of $M \otimes_F K = \bigoplus_{i=1}^{\infty} K$, a $K$-vector space of countably infinite dimension: contradiction. □

**Proposition 12.** *The following are equivalent:*
*(i) $E_X$ is surjective.*
*(ii) $X$ is finite.*

*Proof.* $\neg$ (ii) $\implies$ $\neg$ (i): If $E_X : F[t] \to F^X$ were surjective, then $F^X$ would be a countably generated $F$-module, contradicting Lemma 11.
(ii) $\implies$ (i): For $1 \leq i \leq n$, let $\pi_i : F^n \to F$ by $(x_1, \ldots, x_n) \mapsto x_i$, and let $X_i = \pi_i(X)$. Since for $X \subset Y \subset F^n$ the canonical restriction map $F^Y \to F^X$ is surjective, we may prove the result after replacing $X$ by the larger finite subset $\tilde{X} = \prod_{i=1}^n X_i$. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \tilde{X}$, let

$$\delta_\alpha(t) = \frac{\prod_{i=1}^n \prod_{x_i \in X_i \setminus \{\alpha_i\}} (t_i - x_i)}{\prod_{i=1}^n \prod_{x_i \in X_i \setminus \{\alpha_i\}} (\alpha_i - x_i)}. \tag{8}$$

Then, as a function on $\tilde{X}$, $\delta_\alpha$ is the characteristic function of $\{\alpha\}$: $\delta_\alpha(\alpha) = 1$ and $\delta_\alpha(x) = 0$ for all $x \in \tilde{X} \setminus \{\alpha\}$. Then $\{\delta_\alpha\}_{\alpha \in \tilde{X}}$ is a basis for $F^{\tilde{X}}$, so every element of $F^{\tilde{X}}$ arises by evaluating a polynomial. □

As advertised above, this implies:

**Theorem 13.** *Theorem 8b) holds over any integral domain $F$.*

*Proof.* Following the argument given in § 2.2, we get that $\tilde{E}_X$ is a surjective $F$-linear map between free $F$-modules of equal finite rank. Tensoring to the fraction field and applying linear algebra, we get that $\tilde{E}_X$ is an isomorphism. □

**Proposition 14.** *The following are equivalent:*
*(i) $E_X$ is injective.*
*(ii) $X$ is infinite and **Zariski-dense** in $F^n$: for all $f \in F[t]$, if $f(x) = 0$ for all $x \in X$, then $f(x) = 0$ for all $x \in F^n$.*

*Proof.* b) $\neg$ (ii) $\implies$ $\neg$ (i): Suppose $X$ is finite. Then $F^X$ is a free $F$-module of finite rank $\#X$ and $F[t]$ is a free $F$-module of infinite rank, so $E$ cannot be injective. Next suppose that $X$ is not Zariski dense in $F^n$, i.e., $\overline{X} \subsetneq F^n$. Thus there is $y \in F^n \setminus X$ and $f \in F[t]$ such that $E(f)|_X \equiv 0$ and $E(f)(y) \neq 0$, hence $0 \neq f \in \operatorname{Ker} E$.
(ii) $\implies$ (i): Let $f \in \operatorname{Ker} E_X = I(X)$. Since $X$ is Zariski-dense in $F^n$, $f(x) = 0$ for all $x \in F^n$. Since $X$ is infinite, so is $F$, so we may choose $X_i \subset F$ such that $\deg_{t_i} f < \#X_i$. Put $X = \prod_{i=1}^n X_i$ and define $\varphi_1(t_1), \ldots, \varphi_n(t_n)$ as in (1). Then $f$ is $(\#X_1, \ldots, \#X_n)$-reduced. By Theorem 8b), $f \in \langle \varphi_1, \ldots, \varphi_n \rangle$. Using Proposition 10d) we conclude $f = 0$. □

## 3. Final Remarks

### 3.1. The Chevalley-Alon-Tarsi Lemma.

Our proof of the Finitely Restricted Nullstellensatz is set up so as to maximally exploit the following truly basic principle – for a map between two sets of equal finite cardinality, injectivity, surjectivity and bijectivity are all equivalent – as well as its analogue in linear algebra: for a linear map between two vector spaces of equal finite dimension, injectivity, surjectivity and bijectivity are all equivalent.

These principles guarantee the existence of multiple approaches to the Combinatorial Nullstellensatz and related topics. The traditional approach concentrates on injectivity by first establishing the following simple result.

**Lemma 15.** *(Chevalley-Alon-Tarsi) Let $F$ be a domain, $n \in \mathbb{Z}^+$, and $f(t) \in F[t] = k[t_1, \ldots, t_n]$; for $1 \leq i \leq n$, let $d_i$ be the $t_i$-degree of $f$, let $X_i$ be a subset of $F$ with $\#X_i > d_i$, and let $X = \prod_{i=1}^n X_i$. If $f(x) = 0$ for all $x \in X$, then $f = 0$.*

However in our approach Lemma 15 comes out last, by combining Proposition 10 with Theorem 8b). We structure things this way because Lemma 15 is particular to the cylindrical case $X = \prod_{i=1}^n X_i$ and we want to deal with a general finite subset.

3.2. **Multisets.**

Among the deluge of recent work on the Combinatorial Nullstellensatz, the ones which seem closest in spirit to the present note are [KMR11] and [KR12].

In [KMR11] it is shown that Corollary 2 and portions of Proposition 10 can be appropriately generalized so as to work over any commutative ring $F$. We have not pursued that direction here because it seems that we would be leaving behind all connections with geometry: $V_A(J)$ need no longer be a radical ideal, the map $A \subset X \mapsto V_X(I(A))$ need not be a Kuratowski closure operator (i.e., need not induce a topology on $X$), and there seems little hope of attaining a Nullstellensatz.

More pertinently, [KMR11] and [KR12] also treat nonsquarefree polynomials

$$\varphi_i(t_i) = \prod_{x_i \in X_i} (t_i - x_i)^{m_i}.$$

When $\max m_i > 1$, $\Phi = \langle \varphi_1, \ldots, \varphi_n \rangle$ is no longer a radical ideal; equivalently

$$F[t]/\Phi \cong \bigotimes_{i=1}^n F[t_1]/\langle t_1^{m_i} \rangle$$

is a non-reduced ring. Proposition 10 on Cylindrical Reduction still applies, but $\Phi$ is no longer the ideal of functions vanishing on a finite subset, so the problem is to usefully interpret the hypothesis $f \in \Phi$ in this context. The authors solve this problem very nicely by giving an interpretation in terms of vanishing coefficients of the Taylor series expansion of $f$ at $(x_1, \ldots, x_n)$. Their approach is especially appealing and useful from the perspective of combinatorial applications.

It would be interesting to explore simultaneous generalizations of these works and the present work, e.g. by considering the ideals corresponding to non-cylindrical multisets, in particular products of not necessarily distinct maximal ideals $\mathfrak{m}_x$ of points $x \in F^n$. It is also an interesting challenge to fashion a Nullstellensatz here: the usual Nullstellensatz setup inherently ignores multiplicities, but "Nullstellensätze with nilpotents" are not absolutely unheard of: e.g. [EH79].

**Acknowledgments**: My interest in the Combinatorial Nullstellensatz and its connections to Chevalley's Theorem was kindled by correspondence with John R. Schmitt. The main idea for the proof of Lemma 11 is due to Carlo Pagano. I thank Emil Jeřábek for introducing me to the Finite Field Nullstellensatz.

## References


[AF93] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*. Eur. J. Comb. 14 (1993), 79-83.

[Al99] N. Alon, *Combinatorial Nullstellensatz*. Recent trends in combinatorics (Mátraháza, 1995). Combin. Probab. Comput. 8 (1999), 7-29.

[AT92] N. Alon and M. Tarsi *Colorings and orientations of graphs*. Combinatorica 12 (1992), 125–134.

[Br87] W.D. Brownawell, *Bounds for the degrees in the Nullstellensatz.* Ann. of Math. (2) 126 (1987), 577-591.

[Ch35] C. Chevalley, *Démonstration dune hypothèse de M. Artin.* Abh. Math. Sem. Univ. Hamburg 11 (1935), 73-75.

[EH79] D. Eisenbud and M. Hochster, *A Nullstellensatz with nilpotents and Zariski's main lemma on holomorphic functions*. J. Algebra 58 (1979), 157-161.

[KMR11] G. Kós, T. Mészáros and L. Rónyai, *Some extensions of Alon's Nullstellensatz*. Publ. Math. Debrecen 79 (2011), no. 3-4, 507-519.

[Ko88] J. Kollár, *Sharp effective Nullstellensatz*. J. Amer. Math. Soc. 1 (1988), 963-975.

[KP12] R.N. Karasev and F.V. Petrov, *Partitions of nonzero elements of a finite field into pairs*. Israel J. Math. 192 (2012), 143-156.

[KR12] G. Kós and L. Rónyai, *Alon's Nullstellensatz for multisets*. Combinatorica 32 (2012) 589-605.

[La10] M. Lasoń, *A generalization of combinatorial Nullstellensatz*. Electron. J. Combin. 17 (2010), Note 32, 6 pp.

[Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. Electron. J. Combin. 15 (2008), no. 1, Research Paper 10, 35 pp.

[Ta13] T. Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, preprint.

[Te66] G. Terjanian, *Sur les corps finis*. C. R. Acad. Sci. Paris Sér. A-B 262 (1966), A167-A169.