THE COMBINATORIAL NULLSTELLENSÄTZE REVISITED

PETE L. CLARK

Abstract. We revisit and further explore the celebrated Combinatorial Nullstellensätze of N. Alon in several different directions.

Notation and Terminology: Let $\mathbb{N}$ be the non-negative integers. For $\mathbf{d} = (d_1, \ldots, d_n)$, $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{N}^n$, we write $\mathbf{d} \leq \mathbf{e}$ if $d_i \leq e_i$ for all $1 \leq i \leq n$. We write $\mathbf{d} < \mathbf{e}$ if $\mathbf{d} \leq \mathbf{e}$ and $\sum_{i=1}^n d_i < \sum_{i=1}^n e_i$. Our rings are commutative with multiplicative identity. A **domain** is a ring R in which $a, b \in \mathbb{R} \setminus \{0\} \implies ab \neq 0$. A ring R is **reduced** if for all $x \in R, n \in \mathbb{Z}^+$, we have $x^n = 0 \implies x = 0$. We abbreviate the polynomial ring $R[t_1, \ldots, t_n]$ by $R[\underline{t}]$.

1. Introduction

1.1. The Combinatorial Nullstellensätze.

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

Theorem 1.1. *Let F be a field, 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*

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

Let $f \in F[\underline{t}]$ 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) (Combinatorial Nullstellensatz I, or **CNI**) There are $q_1, \ldots, q_n \in F[\underline{t}]$ such that*

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

b) (Supplementary Relations) Let R be the subring of F generated by the coefficients of f and $\varphi_1, \ldots, \varphi_n$. Then the $q_1, \ldots, q_n$ may be chosen to lie in $R[\underline{t}]$ and satisfy

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

Theorem 1.2. *(Combinatorial Nullstellensatz II, or **CNII**) Let F be a field, $n \in \mathbb{Z}^+$, $d_1, \ldots, d_n \in \mathbb{N}$, and let $f \in F[\underline{t}] = F[t_1, \ldots, t_n]$. We suppose:*
(i) $\deg f \leq d_1 + \ldots + d_n$.
(ii) The coefficient of $t_1^{d_1} \cdots t_n^{d_n}$ in f is nonzero.
Then, for any subsets $X_1, \ldots, X_n$ of F with $\#X_i = d_i + 1$ 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 his Combinatorial Nullstellensätze 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 [Ta14], 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.

One easily deduces CNII from CNI and the Supplementary Relations, but (apparently) not conversely. For appplications in combinatorics and number theory, CNII seems more useful: [Al99] organizes its applications into seven different sections, and only in the last is CNI applied. Most later works simply refer to Theorem 1.2 as the Combinatorial Nullstellensatz. We find this trend somewhat unfortunate. On the one hand, CNI is stronger and does have some applications in its own right. On the other hand, it is CNI which is really a Nullstellensatz in the sense of algebraic geometry, and we find this geometric connection interesting and suggestive.

Recently attention has focused on the following sharpening of CNII due to Schauz, Lason and Karasev-Petrov [Sc08, Thm. 3.2], [La10, Thm. 3], [KP12, Thm. 4].

Theorem 1.3. *(Coefficient Formula) Let F be a field, and let $f \in F[\underline{t}]$. Let $d_1, \ldots, d_n \in \mathbb{N}$ be such that $\deg f \leq d_1 + \ldots + d_n$. For each $1 \leq i \leq n$, let $X_i \subset F$ with $\# X_i = d_i + 1$, and let $X = \prod_{i=1}^n X_i$. Let $\mathbf{d} = (d_1, \ldots, d_n)$, and let $c_{\mathbf{d}}$ be the coefficient of $t_1^{d_1} \cdots t_n^{d_n}$ in f. Then*

$$c_{\mathbf{d}} = \sum_{x=(x_1,\ldots,x_n)\in X} \frac{f(x)}{\prod_{i=1}^n \varphi_i'(x_i)}. \tag{4}$$

In this note we revisit and further explore these theorems, in three different ways.

• In §2 we improve CNI to a full Nullstellensatz for polynomial functions on arbitrary finite subsets $X \subset F^n$ over a field F (Theorem 2.4). When $F = \mathbb{F}_q$ and $X = \mathbb{F}_q^n$, we recover the **Finite Field Nullstellensatz** of G. Terjanian (Corollary 2.5).

• CNI and CNII hold with F replaced by any domain R. Schauz showed that Theorem 1.3 holds over any *ring* R so long as X satisfies "Condition (D)": no two distinct elements of any X_i differ by a zero-divisor. Moreover, one can view Alon's proof of CNI and CNII as a restricted variable analogue of Chevalley's proof of Chevalley's Theorem, and Schauz's work shows that one can do this over any ring with Condition (D) in hand. We do so in §3: following Chevalley, we establish versions of Theorems 1.1, 1.2 and 1.3 over any ring. It turns out that Condition (D) is necessary and sufficient for Theorem 1.1 to hold. On the other hand, if we clear denominators in (4) we get a formula which is meaningful even in the absence of Condition (D). This Integral Coefficient Formula (Theorem 3.9b)) follows by "the permanence of algebraic identities". We close up this circle of ideas by establishing a **Restricted Variable Chevalley-Warning Theorem** (Theorem 3.10), a refinement of the Restricted Variable Chevalley Theorem [Sc08], [Br11] which is complementary to the restricted variable version of Warning's Second Theorem [CFS14].

• In §4 we further analyze the evaluation map from polynomials to functions on an arbitrary subset $X \subset R^n$ for an arbitrary ring. We aim to show that the (perhaps rather arid-looking) formalism of a restricted variable Nullstellensatz leads to interesting open problems in polynomial interpolation over commutative rings.

2. A Nullstellensatz for Finitely Restricted Polynomial Functions

2.1. **Alon's Nullstellensatz versus Hilbert's Nullstellensatz.** The prospect of improving Theorem 1.1 *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 2.1. *(Hilbert's Nullstellensatz) Let F be an algebraically closed field, let $g_1, \ldots, g_m \in F[\underline{t}]$, and let $f \in F[\underline{t}]$ be a polynomial which vanishes on all the common zeros of $g_1, \ldots, g_m$. Then there is $k \in \mathbb{Z}^+$ and $q_1, \ldots, q_m \in F[\underline{t}]$ such that*

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

Let us compare Theorems 1.1 and 2.1. They differ in the following points:
• In Theorem 1.1, F can be any field. In Hilbert's Nullstellensatz, F must be algebraically closed. Really must: if not, there is a nonconstant polynomial $g(t_1)$ without roots in F; taking $m = 1$, $g_1 = g$ and $f = 1$, the conclusion fails.
• In CNI, the conclusion is that f itself is a linear combination of the φ_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 $f = t_1$.
• The Supplementary Relations give upper bounds on the degrees of the polynomials q_i: they make CNI **effective**. Hilbert's Nullstellensatz is not effective. Effective versions have been given by Brownawell [Br87], Kollár [Ko88] and others, but their bounds are much more complicated than the ones in Theorem 1.1.
• In Theorem 1.1 the φ_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 2.1 is a *full Nullstellensatz*, whereas Theorem 1.1 is a *partial Nullstellensatz*.

We will promote Theorem 1.1 to a full Nullstellensatz for all finite subsets.

2.2. **The Restricted Variable Formalism.**

For a set Z, let 2^Z be its power set. For a ring R, let $\mathcal{I}(R)$ be the set of ideals of R. For a subset J of a ring R, let $\langle J \rangle$ be the ideal of R generated by J and let $\operatorname{rad} J = \{f \in R \mid f^k \in \langle J \rangle \text{ for some } k \in \mathbb{Z}^+\}$. An ideal J is **radical** if $J = \operatorname{rad} J$.

Let R be a ring, and let $X \subset R^n$. For $x \in X,\ f \in R[\underline{t}]$, we put

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

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

When R is an algebraically closed field and $X \subset R^n$ is Zariski-closed (c.f. §4.2), this is the usual connection between subsets of an affine variety and its coordinate ring. We will see that the case of R any field and X finite is even better behaved. In §4 we return to the general case and find some new phenomena.

Put $V = V_{R^n}$. We may extend I and V_X to maps on power sets as follows:

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

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

In fact $I(2^X) \subset \mathcal{I}(R[\underline{t}])$ and $\forall J \subset R[\underline{t}],\ V(J) = V(\langle J \rangle)$. Moreover we have

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

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

hence also

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

$$J_1 \subset J_2 \subset R[\underline{t}] \implies I(V_X(J_1)) \subset I(V_X(J_2)).$$

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

$$\forall J \subset R[\underline{t}],\ I(V_X(J)) \supset I(V_X(0)) = I(X).$$

2.3. **The Finitesatz.**

Lemma 2.2. *a) Suppose R is a domain. For all ideals $J_1, \ldots, J_m$ of $R[\underline{t}]$, we have*

$$V_X(J_1 \cdots J_m) = \bigcup_{i=1}^{m} V_X(J_i).$$

b) Suppose R is reduced. Then for all $A \subset R^n$, $I(A)$ is a radical ideal.
c) If R is reduced, then for all $J \subset R[\underline{t}]$,

$$I(V_X(J)) \supset \operatorname{rad}(J + I(X)) \supset \operatorname{rad} J + I(X) \supset J + I(X). \tag{5}$$

Proof. a) 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 R is a domain, $f_1(x) f_2(x) \neq 0$, so $x \notin V_X(J_1 J_2)$.
b) If $f \in R[\underline{t}]$ and $f^k \in I(A)$ for some $k \in \mathbb{Z}^+$, then for all $x \in A$ we have $f(x)^k = 0$. Since R is reduced, this implies $f(x) = 0$ for all $x \in A$ and thus $f \in I(A)$.
c) $I(V_X(J)) = I(X \cap V(J))$ is a radical ideal containing both $I(X)$ and $I(V(J)) \supset J$, so it contains $\operatorname{rad}(J + I(X))$. The other inclusions are immediate. □

It is well known (see Theorem 3.3) that when F is infinite we have $I(F^n) = \{0\}$. This serves to motivate the following restatement of Hilbert's Nullstellensatz.

Theorem 2.3. *Let F be an algebraically closed field. For all $J \subset F[\underline{t}]$,*

$$I(V(J)) = \operatorname{rad} J.$$

In comparison, CNI says $I(V(\langle \varphi_1, \ldots, \varphi_n \rangle)) = \langle \varphi_1, \ldots, \varphi_n \rangle$.

Theorem 2.4. *(Finitesatz) Let F be a field, and let $X \subset F^n$ be a finite subset.*
a) For all ideals J of $F[\underline{t}]$, 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) (CNI) Suppose $X = \prod_{i=1}^n X_i$ for finite nonempty subsets X_i of F. Define $\varphi_i(t_i) \in F[t_i]$ as in (1) above. Then

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

Proof. a) 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 $F[\underline{t}]/\mathfrak{m}_x \cong F$, so $\mathfrak{m}_x$ is maximal. On the other hand $\mathfrak{m}_x \subset I(x) \subsetneq F[\underline{t}]$, 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 $A = \{a_i\}_{i=1}^k \subset X$ with $a_i \neq a_j$ for $i \neq j$. Then

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

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

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

Let F^A be the set of all maps $f : A \to F$, so F^A is an F-algebra under pointwise addition and multiplication and $F^A \cong \prod_{i=1}^{\#A} F$. The **evaluation map**

$$E_A := F[\underline{t}] \to F^A, \; f \in F[\underline{t}] \mapsto (x \in A \mapsto f(x))$$

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

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

Thus ι is an injective F-linear map between F-vector spaces of equal finite dimension, hence it an is an isomorphism of rings. It follows that

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

Identifying $I(F[\underline{t}]/I(X))$ with $\{J \in I(F[\underline{t}]) \mid J \supset I(X)\}$ and restricting V_X to ideals containing $I(X)$, we get maps

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

For all $A \subset X$,

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

Since $\mathcal{I}(F[\underline{t}]/I(X))$ 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 $F[\underline{t}]$, using (5) we get

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

b) 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, we get $\Phi \subset \operatorname{Ker} E_X$, and thus there is an induced surjective F-algebra homomorphism

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

Since $F[\underline{t}]/\Phi$ and F^X are F-vector spaces of dimension $d_1 \cdots d_n$, $\tilde{E}_X$ is an isomorphism. Hence $F[\underline{t}]/\Phi \to F[\underline{t}]/\operatorname{Ker} E_X$ is injective, i.e., $\Phi = \operatorname{Ker} E_X = I(X)$. $\square$

Corollary 2.5. *(Finite Field Nullstellensatz* [Te66]*) 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 2.4 with $F = X_1 = \ldots = X_n = \mathbb{F}_q$. $\square$

3. Cartesian Reduction, the Atomic Formula, and the Nullstellensätze

3.1. Cartesian Reduction.

Lemma 3.1. *(Polynomial Division)*
Let R be a ring, and let $a(t_1), b(t_1) \in R[t_1]$ with b monic of degree d.
a) There are unique polynomials q and r with $a = qb + r$ and $\deg r < d$.
b) Suppose $R = A[t_2, \ldots, t_n]$ is itself a polynomial ring over a ring A, so $R[t_1] = A[t_1, \ldots, t_n] = A[\underline{t}]$ and that $b \in A[t_1]$. Then:
• If q has a monomial term of multidegree $(d_1, \ldots, d_n)$, then a has a monomial term of multidegree $(d_1 + d, d_2, \ldots, d_n)$. It follows that

$$\deg a \geq \deg q + d.$$

• If r has a monomial term of multidegree $(d_1, \ldots, d_n)$, then a has a monomial term of multidegree $(e_1, \ldots, e_n)$ with $d_i \leq e_i$ for all $1 \leq i \leq n$. It follows that

$$\deg r \leq \deg a.$$

Proof. a) Uniqueness: if $a = q_1 b + r_1 = q_2 b + r_2$, then since b is monic and $g_1 \neq g_2$ then we have $d \leq \deg((g_1 - g_2)b) = \deg(r_2 - r_1) < d$, a contradiction. Existence: when b is monic, the standard division algorithm involves no division of coefficients so works in any ring. Part b) follows by contemplating the division algorithm. $\square$

Proposition 3.2. *(Cartesian Reduction) Let R be a ring. For $1 \leq i \leq n$, let $\varphi_i(t_i) \in F[t_i]$ be monic of degree c_i. Put $\Phi = \langle \varphi_1, \ldots, \varphi_n \rangle$ and $\mathbf{c} = (c_1, \ldots, c_n)$. We say $f \in R[\underline{t}]$ is* **c-reduced** *if for all $1 \leq i \leq n$, $\deg_{t_i} f < c_i$. Then:*
a) The set $\mathcal{R}_{\mathbf{c}}$ of all $\mathbf{c}$-reduced polynomials is a free R-module of rank $c_1 \cdots c_n$.
b) For all $f \in R[\underline{t}]$, there are $q_1, \ldots, q_n \in R[\underline{t}]$ such that $\deg q_i \leq \deg f - \deg \varphi_i$ for all $1 \leq i \leq n$ and $f - \sum_{i=1}^n q_i \varphi_i$ is $\mathbf{c}$-reduced.
c) The composite map $\Psi : \mathcal{R}_{\mathbf{c}} \hookrightarrow R[\underline{t}] \to R[\underline{t}]/\Phi$ is an R-module isomorphism.
d) For all $f \in R[\underline{t}]$, there is a unique $r_{\mathbf{c}}(f) \in \mathcal{R}_{\mathbf{c}}$ such that $f - r_{\mathbf{c}}(f) \in \Phi$.

Proof. a) Indeed $\{t_1^{a_1} \cdots t_n^{a_n} \mid 0 \leq a_i < d_i\}$ is a basis for $\mathcal{R}_{\mathbf{c}}$.
b) Divide f by φ_1, then divide the remainder r_1 by φ_2, then divide the remainder r_2 by φ_n, and so forth, getting $f = \sum_{i=1}^n q_i \varphi_i + r_n$. Apply Lemma 3.1b).
c) Part b) implies that Ψ is surjective. For the injectivity: let $q_1, \ldots, q_n \in R[\underline{t}]$ be such that $f = \sum_{i=1}^n q_i \varphi_i \in \mathcal{R}_{\mathbf{c}}$. We must show that $f = 0$. For each i, by dividing q_i by φ_j for $i < j \leq n$ and absorbing the quotient into the coefficient q_j of φ_j, we may assume that $\deg_{t_j} q_i < d_j$ for all $j > i$. It follows inductively that for all $1 \leq m \leq n$, $\sum_{i=1}^m q_i \varphi_i$ is either 0 or has t_i-degree at least d_i for some $1 \leq i \leq m$. Applying this with $m = n$ shows $f = 0$. d) This follows from part c). $\square$

Let R be a ring and $X_1, \ldots, X_n \subset R$ be finite, nonempty subsets. Put $\varphi_i = \prod_{x_i \in X_i}(t_i - x_i)$, $\Phi = \langle \varphi_1, \ldots, \varphi_n \rangle$, $d_i = \#X_i - 1$, $\mathbf{d} = (d_1, \ldots, d_n)$ and $X = \prod_{i=1}^n X_i$. A polynomial $f \in R[\underline{t}]$ is **X-reduced** if it is $(\#X_1, \ldots, \#X_n)$-reduced. We write $\mathcal{R}_X$ for $\mathcal{R}_{\mathbf{d}}$, so $\dim \mathcal{R}_X = \prod_{i=1}^n (d_i + 1) = \#X$. The **$X$-reduced representative** of f is the unique polynomial $r_X(f)$ such that $f - r_X(f) \in \Phi$.

Definition 1. *Let R be a ring and $n \in \mathbb{Z}^+$. A subset $S \subset R$ satisfies* ***Condition (F)*** *(resp.* ***Condition (D)****) if for all $x \neq y \in S$, $x - y \in R^\times$ (resp. $x - y$ is not a zero-divisor in R: i.e., $(x-y)z = 0$ implies that $z = 0$). We say $X = \prod_{i=1}^n X_i \subset R^n$ satisfies* ***Condition (F)*** *(resp.* ***Condition (D)****) if every X_i does.*

Condition (F) implies Condition (D). Conversely, Condition (D) implies Condition (F) with R replaced by its total fraction ring. A ring is a field (resp. a domain) iff every subset satisfies Condition (F) (resp. Condition (D)).

Theorem 3.3. *(**CATS Lemma** [Ch35] [AT92], [Sc08]) Let R be a ring. For $1 \leq i \leq n$, let $X_i \subset R$ be nonempty and finite. Put $X = \prod_{i=1}^n X_i$.*
a) (Schauz) The following are equivalent:
(i) X satisfies condition (D).
(ii) If $f \in \mathcal{R}_X$ and $f(x) = 0$ for all $x \in X$, then $f = 0$.
(iii) We have $\Phi = I(X)$.
b) (Chevalley-Alon-Tarsi) The above conditions hold when R is a domain.

Proof. a) (i) $\Longrightarrow$ (ii): By induction on n: suppose $n = 1$. Write $X = \{x_1, \ldots, x_{a_1}\}$, and let $f \in R[t_1]$ have degree less than $a_1 - 1$ such that $f(x_i) = 0$ for all $1 \leq i \leq a_1$. By Polynomial Division, we can write $f = (t_1 - x_1)f_2$ for $f_2 \in R[t_1]$. Since $x_2 - x_1$ is not a zero-divisor, $f_2(x_2) = 0$, so $f_2(t_1) = (t_1 - x_2)$. Proceeding in this manner we eventually get $f(t_1) = (t_1 - x_1) \cdots (t_1 - x_{a_1}) f_{a_1+1}(t_1)$, and comparing degrees shows $f = 0$. Suppose $n \geq 2$ and that the result holds in $n - 1$ variables. Write

$$f = \sum_{i=0}^{a_n - 1} f_i(t_1, \ldots, t_{n-1}) t_n^i$$

with $f_i \in R[t_1, \ldots, t_{n-1}]$. If $(x_1, \ldots, x_{n-1}) \in \prod_{i=1}^{n-1} X_i$, then $f(x_1, \ldots, x_{n-1}, t_n) \in R[t_n]$ has degree less than a_n and vanishes for all a_n elements $x_n \in X_n$, so it is the zero polynomial: $f_i(x_1, \ldots, x_{n-1}) = 0$ for all $0 \leq i \leq a_n$. By induction, each $f_i(t_1, \ldots, t_{n-1})$ is the zero polynomial and thus f is the zero polynomial.
(ii) $\Longrightarrow$ (iii): We have $\Phi \subset I(X)$. Let $f \in I(X)$. Since $f - r_X(f) \in \Phi \subset I(X)$, for all $x \in X$ we have $r_X(f)(x) = f(x) = 0$. Then (ii) gives $r_X(f) = 0$, so $f \in \Phi$.
(iii) $\Longrightarrow$ (i): We argue by contraposition: suppose X does not satisfy Condition (D). Then for some $1 \leq i \leq n$, we may write $X_i = \{x_1, x_2, \ldots, x_{a_i}\}$ such that there is $0 \neq z \in R$ with $(x_1 - x_2)z = 0$. Then $f = z(t_i - x_2)(t_i - x_3) \cdots (t_i - x_{a_i})$ is a nonzero element of $I(X) \cap \mathcal{R}_X$, hence $f \in I(X) \setminus \Phi$.
b) If R is a domain then Condition (D) holds for every X. □

3.2. **The Atomic Formula.**

Lemma 3.4. *Suppose Condition (F). Let $x = (x_1, \ldots, x_n) \in X$, and put*

$$\delta_{X,x} = \prod_{i=1}^n \prod_{y_i \in X_i \setminus \{x_i\}} \frac{t_i - y_i}{x_i - y_i} = \prod_{i=1}^n \frac{\varphi_i(t_i)}{(t_i - x_i)\varphi_i'(x_i)} \in F[\underline{t}].$$

a) We have $\delta_{X,x}(x) = 1$.
b) If $y \in X \setminus \{x\}$, then $\delta_{X,x}(y) = 0$.
c) For all $1 \leq i \leq n$, $\deg_{t_i} \delta_{X,x} = a_i - 1$. In particular, $\delta_{X,x}$ is X-reduced.

Proof. Left to the reader. □

The following is a result of U. Schauz [Sc08, Thm. 2.5].

Theorem 3.5. *(Atomic Formula) Suppose Condition (F). Then for all $f \in R[\underline{t}]$, we have*

$$r_X(f) = \sum_{x \in X} f(x)\delta_{X,x}. \tag{8}$$

Proof. Apply Theorem 3.3a) to $r_X(f) - \sum_{x \in X} f(x)\delta_{X,x}$. □

Let $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{N}^n$. We say a polynomial $f \in F[\underline{t}]$ is **c-topped** if for every $e = (e_1, \ldots, e_n)$ with $\mathbf{c} < \mathbf{e}$, the coefficient of $t^{\mathbf{e}} = t_1^{e_1} \cdots t_n^{e_n}$ in f is 0.

Remark 3.6. *Let $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{N}^n$. If $\deg f \leq c_1 + \ldots + c_n$, then f is $\mathbf{c}$-topped.*

Lemma 3.7. *Let $f \in R[\underline{t}]$ be $\mathbf{d}$-topped. Then the coefficient of $t^{\mathbf{d}} = t_1^{d_1} \cdots t_n^{d_n}$ in f is equal to the coefficient of $t^{\mathbf{d}}$ in $r_X(f)$.*

Proof. Write $\varphi_i(t_i) = t_i^{d_i+1} - \psi_i(t_i)$, $\deg(\psi_i) \leq d_i$. An **elementary reduction** of f consists of identifying a monomial which is divisible by $t_i^{d_i+1}$ and replacing $t_i^{d_i+1}$ by $\psi_i(t_i)$. Elementary reduction on a $\mathbf{d}$-topped polynomial yields a $\mathbf{d}$-topped polynomial with the same coefficient of $t^{\mathbf{d}}$. We obtain $r_X(f)$ from f by finitely many elementary reductions. □

3.3. Combinatorial Nullstellensätze Over Rings.

The following result sharpens [KMR12, Thm. 3].

Theorem 3.8. *Let R be a ring, let $X_1, \ldots, X_n \subset R$ be finite nonempty subsets, and define $\mathbf{d}$, X, $\varphi_1, \ldots, \varphi_n, \Phi$ as above. Suppose $f \in I(X)$: i.e., $f(x) = 0$ for all $x \in X$. Then:*
a) (Combinatorial Nullstellensatz I) The following are equivalent:
(i) X satisfies Condition (D).
(ii) We have $f \in \Phi$: there are $q_1, \ldots, q_n \in R[\underline{t}]$ such that $f(t) = \sum_{i=1}^n q_i(t)\varphi_i(t)$.
b) (Supplementary Relations) Suppose the equivalent conditions of part a) hold. Let $\mathfrak{r}$ be the subring of R generated by the coefficients of f and $\varphi_1, \ldots, \varphi_n$. We can take $q_1, \ldots, q_n \in \mathfrak{r}[t]$ satisfying $\deg q_i \leq \deg f - \deg \varphi_i$ for all $1 \leq i \leq n$.

Proof. If X satisfies Condition (D), replace R by $\mathfrak{r}$ and apply Proposition 3.2b) and Theorem 3.3. We get $q_1, \ldots, q_n \in \mathfrak{r}[t]$ such that $f = \sum_{i=1}^n q_i \varphi_i$ and $\deg q_i \leq \deg f - \deg \varphi_i$ for all $1 \leq i \leq r$. If X does not satisfy Condition (D), then by Theorem 3.3, there is a nonzero element $f \in \mathcal{R}_X \cap I(X)$, and then $f \notin \Phi$ by Proposition 3.2c). □

We put

$$M(X) = \prod_{i=1}^n \prod_{x_i \in X_i} \prod_{y_i \in X_i \setminus \{x_i\}} (x_i - y_i) = \prod_{i=1}^n \prod_{x_i \in X_i} \varphi_i'(x_i).$$

Thus $M(X)$ is *not* a zero-divisor in R iff X satisfies Condition (D). For all $x \in X$, $\prod_{i=1}^n \varphi_i'(x_i)$ is a "subproduct" of $M(X)$, and we denote by $\frac{M(X)}{\prod_{i=1}^n \varphi_i'(x_i)}$ the product $M(X)$ with the corresponding factors removed.

For a polynomial $g \in R[\underline{t}]$, let $c_{\mathbf{d}}(g)$ be the coefficient of $t^{\mathbf{d}} = t_1^{d_1} \cdots t_n^{d_n}$ in g.

Theorem 3.9. *Let R be a ring, let $X_1, \ldots, X_n \subset R$ be finite nonempty subsets, and define $\mathbf{d}$, X, $\varphi_1, \ldots, \varphi_n, \Phi$ as above. Let $f \in R[t_1, \ldots, t_n]$.*
a) ([Sc08, Thm. 2.9]*) Suppose X satisfies Condition (D). Then in the total fraction ring of R we have*

$$c_{\mathbf{d}}(r_X(f)) = \sum_{x=(x_1,\ldots,x_n)\in X} \frac{f(x)}{\prod_{i=1}^n \varphi_i'(x_i)}. \tag{9}$$

The right hand side of (9) lies in R if X satisfies Condition (F).
b) (Integral Coefficient Formula) In general, we have

$$M(X)c_{\mathbf{d}}(r_X(f)) = \sum_{x=(x_1,\ldots,x_n)\in X} \left(\frac{M(X)}{\prod_{i=1}^n \varphi_i'(x_i)}\right) f(x). \tag{10}$$

c) (CNII) Suppose X satisfies Condition (D). If $f \in I(X)$, then $c_{\mathbf{d}}(r_X(f)) = 0$.
d) If f is $\mathbf{d}$-topped – e.g. if $\deg f \leq \sum_{i=1}^n d_i$ – then $c_{\mathbf{d}}(f) = c_{\mathbf{d}}(r_X(f))$.

Proof. a) Replace R by its total fraction ring and apply (8).
b) There is a domain $\tilde{R}$ and a surjective ring homomorphism $q : \tilde{R} \to R$. For instance, let $\tilde{R}$ be a polynomial ring over $\mathbb{Z}$ in a set of indeterminates $\{T_r\}_{r\in R}$ indexed by the elements of R and let q be the unique homomorphism with $q(T_r) = r$. There is a unique extension of q to a ring homomorphism $q : \tilde{R}[t_1, \ldots, t_n] \to R[t_1, \ldots, t_n]$ with $\tilde{q}(t_i) = t_i$ for all $1 \leq i \leq n$. For $1 \leq i \leq n$, choose $\tilde{X}_i \subset \tilde{R}$ such that $q|_{\tilde{X}_i} : \tilde{X}_i \to X_i$ is a bijection, and put $\tilde{X} = \prod_{i=1}^n \tilde{X}_i$. Choose $\tilde{f} \in \tilde{R}[t_1, \ldots, t_n]$ such that $q(\tilde{f}) = f$. Applying part a) and multiplying through by $M(\tilde{X})$ gives

$$M(\tilde{X})c_{\mathbf{d}}(r_{\tilde{X}}(\tilde{f})) = \sum_{\tilde{x}\in\tilde{X}} \left(\frac{M(\tilde{X})}{\prod_{i=1}^n \varphi_i'(\tilde{x}_i)}\right) f(\tilde{x}). \tag{11}$$

Applying q to both sides of (11) gives

$$M(X)c_{\mathbf{d}}(q(r_{\tilde{X}}(\tilde{f}))) = \sum_{x\in X} \left(\frac{M(X)}{\prod_{i=1}^n \varphi_i'(x_i)}\right) f(x).$$

Applying q to $\tilde{f} - r_{\tilde{X}}(\tilde{f}) \in \tilde{\Phi}$ gives $f - q(r_{\tilde{X}}(\tilde{f})) \in \Phi$. Since $q(r_{\tilde{X}}(\tilde{f}))$ is X-reduced, Proposition 3.2d) implies

$$q(r_{\tilde{X}}(\tilde{f})) = r_X(f).$$

c) This follows from part a).
d) This is Lemma 3.7. □

3.4. **The Restricted Variable Chevalley-Warning Theorem.**

For a ring R and $x = (x_1, \ldots, x_n) \in R^n$, we put $w(x) = \#\{1 \leq i \leq n \mid x_i \neq 0\}$.

Theorem 3.10. *(Restricted Variable Chevalley-Warning Theorem) Let $P_1, \ldots, P_r \in \mathbb{F}_q[t] = \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1, \ldots, d_r$. For $1 \leq i \leq n$, let $\varnothing \neq X_i \subseteq \mathbb{F}_q$ be subsets, put $X = \prod_{i=1}^n X_i$ and also*

$$V_X = \{x = (x_1, \ldots, x_n) \in X \mid P_1(x) = \ldots = P_r(x) = 0\}.$$

Suppose that $(d_1 + \ldots + d_r)(q-1) < \sum_{i=1}^n (\#X_i - 1)$. *Then:*
a) As elements of $\mathbb{F}_q$, *we have*

$$\sum_{x \in V_X} \frac{1}{\prod_{i=1}^n \varphi_i'(x_i)} = 0 \tag{12}$$

and thus [Sc08] [Br11]

$$\#V_X \neq 1. \tag{13}$$

b) (Chevalley-Warning [Ch35], [Wa35]*) If* $\sum_{i=1}^r d_i < n$, *then* $p \mid \#V_{\mathbb{F}_q^n}$.
c) (Wilson [Wi06]*) If* $(d_1 + \ldots + d_r)(q-1) < n$, *then*

$$\#\{x \in V_{\{0,1\}^n} \mid w(x) \equiv 0 \pmod 2\} \equiv \#\{x \in V_{\{0,1\}^n} \mid w(x) \equiv 1 \pmod 2\} \pmod p.$$

d) If $(d_1 + \ldots + d_r)(q-1) < (q-2)n$, *then*

$$\sum_{x \in V_{\mathbb{F}_q^n}} x_1 \cdots x_n = 0.$$

Proof. a) We define

$$P(t) = \chi_{P_1,\ldots,P_r}(t) = \prod_{i=1}^r \left(1 - P_i(t)^{q-1}\right),$$

so

$$\deg P = (q-1)(d_1 + \ldots + d_r) < \sum_{i=1}^n (\#X_i - 1)$$

and thus the coefficient of $t_1^{\#X_1 - 1} \cdots t_n^{\#X_n - 1}$ in P is 0. Applying the Coefficient Formula (Theorem 1.3), we get

$$0 = \sum_{x \in X} \frac{P(x)}{\prod_{i=1}^n \varphi_i'(x_i)} = \sum_{x \in V_X} \frac{1}{\prod_{i=1}^n \varphi_i'(x_i)} \in \mathbb{F}_q.$$

Parts b) through d) follow from part a) by taking X to be, respectively, $\mathbb{F}_q^n$, $\{0,1\}^n$ and $(\mathbb{F}_q^\times)^n$, and computing the $\varphi_i'(t_i)'s$. The details are left to the reader. □

4. Further Analysis of the Evaluation Map

4.1. The Finitesatz holds only over a field.

If a ring R is not a field and $X \neq \varnothing$, the assertion of Theorem 2.4a) remains meaningful with R in place of F, but it is false. Let $x \in X$. Since $R[\underline{t}]/\mathfrak{m}_x \cong R$ is not a field, $\mathfrak{m}_x$ is not maximal. Let J be an ideal with $\mathfrak{m}_x \subsetneq J \subsetneq R[\underline{t}]$, and let $f \in J \setminus \mathfrak{m}_x$. Then $V_X(J) \subset V_X(\mathfrak{m}_x) = \{x\}$, and since $f \notin \mathfrak{m}_x$, $f(x) \neq 0$. Thus

$$I(V_X(J)) = I(\varnothing) = R[\underline{t}] \supsetneq J = J + I(X).$$

4.2. Towards an Infinitesatz.

We revisit the formalism of § 2.2: let R be a ring and let $X \subset R^n$.

For a subset $A \subset R^n$ we define the **Zariski closure** $\overline{A} = V(I(A))$. Thus $\overline{A}$ is the set of points at which any polynomial which vanishes at every point of A must also vanish. A subset A is **algebraic** if $A = \overline{A}$ and **Zariski-dense** if $\overline{A} = R^n$. When R is a domain the algebraic subsets are the closed sets of a topology, the **Zariski**

topology. Over an arbitrary ring this need not hold and some strange things can happen: for instance if $R = \mathbb{Z}/6\mathbb{Z}$ and $n = 1$ then $\overline{\{2,3\}} = \{0,2,3,5\}$. In fact for any composite positive integer $m \neq 4$, there is a subset $A \subset \mathbb{Z}/m\mathbb{Z}$ which is not algebraic [Si54], [Ch56]. Some partial results towards an explicit description of the operator $A \mapsto \overline{A}$ for subsets of $\mathbb{Z}/m\mathbb{Z}$ have recently been obtained by B. Bonsignore.

If F is an algebraically closed field and $X \subset F^n$ is algebraic, then using Hilbert's Nullstellensatz, for all ideals J of $F[\underline{t}]$,

$$I(V_X(J)) = I(V(J) \cap X) = I(V(J) \cap V(I(X)))$$
$$= I(V(J \cup I(X))) = I(V(J + I(X))) = \operatorname{rad}(J + I(X)).$$

When X is infinite, we CLAIM the "rad" cannot be removed in general.
PROOF OF CLAIM: Suppose $\operatorname{rad}(J + I(X)) = J + I(X)$ for all J. Equivalently, every ideal $J \supset I(X)$ is a radical ideal. Then for any element x in the quotient ring $F[\underline{t}]/I(X)$, since (x^2) is radical we must have $(x) = (x^2) = (x)^2$. It follows (e.g. [AM, p. 35, p. 44, p. 90]) that $F[\underline{t}]/I(X)$ is Noetherian and absolutely flat, hence is Artinian, hence has only finitely many maximal ideals. Since $x \mapsto \mathfrak{m}_x$ is an injection from X to the set of maximal ideals of $F[\underline{t}]/I(X)$, X is finite.

The case of an arbitrary subset over an arbitrary ring R is much more challenging. In fact, even determining whether the evaluation map $E_X : R[\underline{t}] \to R^X$ is surjective – **existence of interpolation polynomials** – or injective – **uniqueness of interpolation polynomials** – becomes nontrivial. In the next section we address these questions, but we are not able to resolve them completely.

4.3. Injectivity and Surjectivity of the Evaluation Map.

Lemma 4.1. *Let R be a ring. Let M_1 and M_2 be free R-modules, with bases $\mathcal{B}_1$ and $\mathcal{B}_2$. If $\iota : M_1 \to M_2$ is an injective R-module homomorphism, then $\#\mathcal{B}_1 \leq \#\mathcal{B}_2$.*

Proof. Combine [LMR, Cor. 1.38] and [EMR, Ex. 1.24]. □

Lemma 4.2. *Let R be a ring, and let X be an infinite set. Then R^X is* not *a countably generated R-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 R-linearly independent set: let $A_1, \ldots, A_n \in \mathcal{C}$ and $\alpha_1, \ldots, \alpha_n \in R$ 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: Suppose R^X is countably generated: thus there is a surjective R-module homomorphism $\Phi : \bigoplus_{i=1}^{\infty} R \to R^X$. For each $A \in \mathcal{C}$, choose $e_A \in \Phi^{-1}(1_A)$ and put $\mathcal{S} = \{e_A \mid A \in \mathcal{C}\}$. By Step 2, $\mathcal{S}$ is uncountable and R-linearly independent, so it spans a free R-module with an uncountable basis which is an R-submodule of $\bigoplus_{i=1}^{\infty} R$, contradicting Lemma 4.1. □

Theorem 4.3. *If $X \subset R^n$ is infinite, then $E_X : R[\underline{t}] \to R^X$ is* not *surjective.*

Proof. If $E_X : R[\underline{t}] \to R^X$ were surjective, then R^X would be a countably generated R-module, contradicting Lemma 4.2. $\square$

If $Y \subset X \subset R^n$, restricting functions from X to Y is a surjective R-algebra homomorphism $\mathfrak{r}_Y : R^X \to R^Y$. We have $E_Y = \mathfrak{r}_Y \circ E_X$, so if E_X is surjective, so is E_Y.

Let $\pi_i : R^n \to R$ be the ith projection map: $\pi_i : (x_1, \ldots, x_n) \mapsto x_i$. For a subset $X \subset R^n$, we define the **Cartesian hull** $\mathcal{C}(X)$ as $\prod_{i=1}^n \pi_i(X)$: it is the unique minimal Cartesian subset containing X, and it is finite iff X is.

Proposition 4.4. *Let $X \subset R^n$ be finite.*
a) If $\mathcal{C}(X)$ satisfies Condition (F), then E_X is surjective.
b) If there is a nonempty Cartesian subset $Y = \prod_{i=1}^n Y_i \subset X$ which does not satisfy Condition (F), then E_X is not surjective.

Proof. a) Since $X \subset \mathcal{C}(X)$, it suffices to show that $E_{\mathcal{C}(X)}$ is surjective, and we have essentially already done this: under Condition (F) we may *define* $r_X(f) = \sum_{x \in X} f(x)\delta_{X,x}(t)$, and as in § 3.3 we see that $E(r_X(f)) = f$.
b) There is $1 \leq i \leq n$ and $y_i \neq y_i' \in Y_i$ such that $y_1 - y_2 \notin R^\times$, hence a maximal ideal $\mathfrak{m}$ of R with $y_1 - y_2 \in \mathfrak{m}$. For all $j \neq i$, choose $y_j \in Y_j$; let $y = (y_1, \ldots, y_n)$; and let y' be obtained from y by changing the ith coordinate to y_i'. For any $f \in F[\underline{t}]$, $f(y) \equiv f(y') \pmod{\mathfrak{m}}$, so $f(y) - f(y') \in \mathfrak{m}$. Hence the function $\delta_{Y,y} : Y \to R$ which maps y to 1 and every other element of Y to 0 does not lie in the image of the evaluation map. Thus E_Y is not surjective, so E_X cannot be surjective. $\square$

Thus if X is itself Cartesian, the evaluation map is surjective iff X satisfies Condition (F): this result is due to Schauz. Proposition 4.4 is the mileage one gets from this in the general case. When every Cartesian subset of X satisfies condition (F) but $\mathcal{C}(X)$ does not, the question of the existence of interpolation polynomials is left open, to the best of my knowledge even e.g. over $\mathbb{Z}$.

We say that a ring R is **(F)-rich** (resp. **(D)-rich**) if for every $d \in \mathbb{Z}^+$ there is a d-element subset of R satisfying Condition (F) (resp. Condition (D)). If $\iota : R \hookrightarrow S$ is a ring embedding and R is (F)-rich, then S is (F)-rich, hence also (D)-rich.

Proposition 4.5. *Let R be a ring and $X \subset R^n$. Consider the following assertions:*
(i) E_X is injective.
(ii) X is infinite and Zariski-dense.
a) We always have (i) $\Longrightarrow$ (ii).
b) If R is (D)-rich – e.g. if it contains an (F)-rich subring – then (ii) $\Longrightarrow$ (i).
c) If R is finite, a domain, or an algebra over an infinite field, then (ii) $\Longrightarrow$ (i).
d) If R is an infinite Boolean ring – e.g. $R = \prod_{i=1}^\infty \mathbb{Z}/2\mathbb{Z}$ – and $X = R^n$, then (ii) holds and (i) does not.

Proof. a) By contraposition: suppose first that X is finite. Then F^X is a free F-module of finite rank $\#X$ and $F[\underline{t}]$ is a free F-module of infinite rank, so E cannot be injective. Now suppose X is not Zariski-dense: then there is $y \in F^n \setminus X$ and $f \in F[\underline{t}]$ such that $E(f)|_X \equiv 0$ and $E_X(f)(y) \neq 0$, hence $0 \neq f \in \operatorname{Ker} E$.
b) Let $f \in \operatorname{Ker} E_X = I(X)$, and let $d = \deg f$. Since X is Zariski-dense in F^n, $f(x) = 0$ for all $x \in F^n$. Since R is (D)-rich, there is a $S \subset R$ of cardinality $d+1$ satisfying Condition (D). Put $X = \prod_{i=1}^n S$. Then $f \in \mathcal{R}_X$ and $f(x) = 0$ for all $x \in X$, so $f = 0$ by Theorem 3.3. c) This is immediate from part b).

d) Since R is infinite, R^n is infinite and Zariski-dense. Since R is Boolean, the polynomial $t_1^2 - t_1$ evaluates to zero on every $x \in R^n$. $\square$

Acknowledgments. My interest in Combinatorial Nullstellensätze and connections to Chevalley's Theorem was kindled by correspondence with John R. Schmitt. The main idea for the proof of Lemma 4.2 is due to Carlo Pagano. I thank Emil Jeřábek for introducing me to the Finite Field Nullstellensatz. I am grateful to the referee for a careful and insightful reading.

References

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

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, Ont. 1969.

[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.

[Br11] D. Brink, *Chevalley's theorem with restricted variables.* Combinatorica 31 (2011), 127–130.

[CFS14] P.L. Clark, A. Forrow and J.R. Schmitt, *Warning's Second Theorem with Restricted Variables.* `http://arxiv.org/abs/1404.7793`

[Ch35] C. Chevalley, *Démonstration d'une hypothése de M. Artin.* Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[Ch56] M.M. Chojnacka-Pniewska, *Sur les congruences aux racines données.* Ann. Polon. Math 3 (1956), 9–12.

[EMR] T. Y. Lam, *Exercises in modules and rings.* Problem Books in Mathematics. Springer, New York, 2007.

[Ko88] J. Kollár, *Sharp effective Nullstellensatz.* J. Amer. Math. Soc. 1 (1988), 963–875.

[KMR12] G. Kós, T. Mészáros and L. Rónyai, *Some extensions of Alon's Nullstellensatz.* Publ. Math. Debrecen 79 (2011), 507-519.

[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.

[L] S. Lang, *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

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

[LMR] T. Y. Lam, *Lectures on modules and rings.* Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999.

[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.

[Si54] W. Sierpiński, *Remarques sur les racines d'une congruence.* Ann. Polon. Math. 1 (1954), 89-90.

[Ta14] T. Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory.* EMS Surv. Math. Sci. 1 (2014), 1–46.

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

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.* Abh. Math. Sem. Hamburg 11 (1935), 76–83.

[Wi06] R.M. Wilson, *Some applications of polynomials in combinatorics.* IPM Lectures, May, 2006.