Higher-Dimensional Analogues of the Combinatorial Nullstellensatz

Jake Mundo

July 21, 2016

Abstract

The celebrated Combinatorial Nullstellensatz of Alon describes the form of a polynomial which vanishes entirely on a Cartesian product of one dimensional sets. We explore analogues of the Combinatorial Nullstellensatz in higher dimensions, that is, we describe the form of polynomials which vanish entirely on Cartesian products of arbitrary dimensional sets, giving two generalizations of the original theorem; for the special case where all the sets are two-dimensional, we also give another generalization. We also discuss possible applications of these results to similar generalizations of the famous Schwartz-Zippel lemma, which bounds the amount of intersection between a variety and a Cartesian product of one-dimensional sets.

1 Introduction

The well-known Schwartz-Zippel lemma (see [8]), which has numerous applications in areas including zero testing of polynomials, states that, for $F \in K[x_1, \cdots, x_n]$ a nonzero polynomial of degree d over a field K and S a finite subset of K,

$$|Z(F) \cap S^n| \leq d|S|^{n-1}.$$

The lack of any assumptions on the polynomial F in this lemma allows it to provide probabilistic zero testing algorithms which work without assuming anything about the polynomial being tested.

In this paper, we attempt to generalize this statement to intersections of zero sets of polynomials to Cartesian products of two-dimensional sets, and possibly higher dimensional sets. While the original Schwartz-Zippel lemma only bounds $|Z(F) \cap S^n|$ for $S \in K$, we would like to bound $|Z(F) \cap S^m|$ for $S \in K^2$ and F a polynomial in $2m$ variables, and possibly extend to higher dimensions as well. This work builds directly on work of Mojarrad et al. [4], who found that

$$|Z(F) \cap (P \times Q)| = O_{d,\epsilon}(|P|^{2/3}|Q|^{2/3+\epsilon} + |P| + |Q|)$$

for $P, Q \subset \mathbb{C}^2$ finite and F a polynomial in four variables over $\mathbb{C}$, unless F is of a particular form $G(x,y)H(x,y,s,t)+K(s,t)L(x,y,s,t)$. Polynomials of this form they call Cartesian, and we will generalize this definition to polynomials of dimension higher than 2 as well.

Related to the Schwartz-Zippel lemma is the also well-known Combinatorial Nullstellensatz of Alon [1], which gives conditions on a polynomial which must be met for the polynomial to vanish on a Cartesian product of sets S_i. The Combinatorial Nullstellensatz has diverse applications in areas from graph theory to number theory, many of which are included in Alon's original paper publishing the result. In this paper, we will provide two generalizations of the Combinatorial Nullstellensatz to Cartesian products of sets in more than one dimension as well.

A Word on Notation

Throughout this paper, we will often deal with a polynomial F in n variables $x_1, x_2, \cdots, x_n$ over a field K. Henceforth, we will always assume K is an field, and that we have fixed a particular arbitrary partition of n given by $n = n_1 + n_2 + n_3 + \cdots + n_k$. We will let x denote the vector $(x_1, \cdots, x_n)$, and denote the vector of the first n_1 variables $\overline{x_1}$, the vector of the next n_2 variables $\overline{x_2}$, and so on.

2 Preliminaries

2.1 Definitions

Alon's original Combinatorial Nullstellensatz [1] is the following two theorems:

Theorem 2.1. *Let $F \in K[x_1, \cdots, x_n]$, and let $S_1, \cdots, S_n \in K$ be nonempty. Define polynomials $G_i \in K[x_i]$ with $G_i(x_i) = \prod_{s_i \in S_i}(x_i - s_i)$ for each i. If F vanishes on $\prod_{1 \leq i \leq n} Z(G_i)$, then there are polynomials $H_1, \cdots, H_n \in K[x_1, \cdots, x_n]$, with $\deg(H_i) \leq \deg(F) - \deg(G_i)$, such that*

$$F = \sum_{i=1}^{n} G_i H_i.$$

Theorem 2.2. *Let $F \in K[x_1, \cdots, x_n]$, and suppose $\deg(F) = \sum_{i=1}^{n} t_i$, with each t_i a nonnegative integer. Suppose further that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in F is nonzero. Then, if $S_1, \cdots, S_n$ are subsets of F with $\#S_i > t_i$, there is $s \in \prod_{i=1}^{n} S_i$ such that*

$$f(s) \neq 0.$$

We generalize the special form of F appearing in the first theorem, extending a generalization of Mojarrad et al. [4] to F in 4 variables and G_i in 2 variables for each i to arbitrary partitions of the number of variables of F.

Definition Let $F \in K[x]$. We say F is $(n_1, \cdots, n_k)$-*Cartesian* if there exist polynomials $G_1, \cdots, G_k$, with $G_i \in K[\overline{x_i}]$ for each i, and polynomials $H_1, \cdots, H_k \in K[x]$, with $\deg(H_i) \leq \deg(F) - \deg(G_i)$ for each i, such that

$$F = \sum_{i=1}^{k} G_i H_i.$$

For any particular collection of polynomials $(G_1, \cdots, G_k)$ satisfying the above, we say F is $(G_1, \cdots, G_k)$-*Cartesian.*

We also define the algebraic degree of a set as follows.

Definition Let $S \in K^n$. Then the *algebraic degree* of S, denoted $d(S)$, is the minimal degree of a polynomial vanishing entirely on S.

To our knowledge, there is no standard name for this concept, so we call it algebraic degree; note that in one dimension, $d(S) = \#S$. It is impossible to give an upper bound on $\#S$ in terms of $d(S)$ in two or more dimensions, as hyperplanes, such as a line in two dimensional space, in more than one dimension can have infinite cardinality (if the field itself is infinite) and algebraic degree 1. The algebraic degree will effectively replace $\#S$ in the second Combinatorial Nullstellensatz's higher-dimensional analogue.

Finally, we give a definition of what we will call the $(n_1, \cdots, n_k)$-reduced support of F, recalling that ordinarily the support of a polynomial F is its set of exponent vectors.

Definition Let $F \in K[x]$. The $(n_1, \cdots, n_k)$-reduced support of F is the set of vectors of the form $(\deg_{\overline{x_1}}(M), \deg_{\overline{x_2}}(M), \cdots, \deg_{\overline{x_k}}(M))$ for M a monomial in F, where $\deg_{x_i}(M)$ is the degree of the monomial M in the variables of $\overline{x_i}$.

2.2 Statement of Results

We give our main two generalizations of the Combinatorial Nullstellensatz to higher dimensions.

Theorem 2.3. *Let $F \in K[x]$ for K algebraically closed, and let $G_i \in K[\overline{x_i}]$ be squarefree for each $i \in \{1, \cdots, k\}$. Suppose F vanishes on $\prod_{i=1}^{k} G_i$. Then F is $(G_1, \cdots, G_k)$-Cartesian (and hence also $(n_1, \cdots, n_k)$-Cartesian).*

This theorem is somewhat analogous to Alon's first Combinatorial Nullstellensatz [1], but we are in higher dimensions, so now requiring F to vanish on a zero set of a polynomial is no longer simply requiring F to vanish on a finite set of points. Hence, while Alon's first Combinatorial Nullstellensatz deals with a finite set of points, our theorem here deals with an infinite set.

We note also that K being algebraically closed is a necessary condition for this theorem, as if we take K to be $\mathbb{R}$, then we can have a polynomial vanishing on a product of zero sets in $\mathbb{R}$ of polynomials which is not Cartesian. Take, for example, the polynomial in four variables over $\mathbb{R}$ given by

$$F(x_1, x_2, y_1, y_2) = x_1y_1 + x_2 + y_2$$

,

with the partition fixed at $n_1 = n_2 = 3$. This polynomial vanishes on the product of the zero sets of $x_1^2+x_2^2$ and $y_1^2+y_2^2$ in $\mathbb{R}^2$, as these polynomials vanish only at $(0,0)$ over $\mathbb{R}$. It can be shown, however, that F is not $(2,2)$-Cartesian, for it does not vanish on the product of complex zero sets of two polynomials in 2 variables. This argument will be presented in more detail later on.

We give an analogue of Alon's second Combinatorial Nullstellensatz which deals with finite sets.

Theorem 2.4. *Let $F \in K[x]$, and let $(t_1, \cdots, t_k)$ be maximal in the $(n_1, \cdots, n_k)$-reduced support of F with respect to the ordering where $(a_1, \cdots, a_k) \geq (b_1, \cdots, b_k)$ iff $a_i \geq b_i$ for all i. Let $S_i \in K^{n_i}$ be finite sets, and suppose $d(S_i) > t_i$ for each i. Then there is $s \in \prod_{i=1}^k S_i$ such that*

$$f(s) \neq 0.$$

In the one dimensional case, this theorem is exactly the generalization of the Combinatorial Nullstellensatz given by Lasoń [3], which weakens the requirement on the vector $(t_1, \cdots, t_n)$ from the original theorem. The original theorem of Alon is a corollary of this theorem's one-dimensional case, as if $\deg(F) = \sum_{i=1}^k t_i$, then certainly $(t_1, \cdots, t_k)$ is maximal in the $(1, 1, \cdots, 1)$-support, which is just the support.

In the special case where $n_i = 2$ for all i, we have another theorem.

Theorem 2.5. *Suppose $n_i = 2$ for all i, and let $F \in K[x]$ for K algebraically closed. Suppose the degree of F in the two variables of $\overline{x_i}$ is d_i for each i. Then if $S_1, \cdots, S_k \subset K^2$ and $\#S_i > d_i$ for all i, there exists $s \in \prod_{i=1}^k S_i$ such that*

$$f(s) \neq 0$$

unless F is $(n_1, \cdots, n_k)$-Cartesian.

We note here that an exact analogue of this theorem in higher dimensions will not be feasible, as there exist polynomials in six variables which vanish on the product of two infinite sets in three dimensions, but which are not Cartesian. An example of such a polynomial is $F \in \mathbb{C}[x_1, x_2, x_3, y_1, y_2, y_3]$ defined by

$$F(x_1, x_2, x_3, y_1, y_2, y_3) = x_1y_1 + x_2 + y_2.$$

Clearly F vanishes on the product of infinite sets in three dimensions where x_1, y_1, x_2, and y_2 are all zero and x_3 and y_3 vary freely. But this polynomial can be shown to not be $(3,3)$-Cartesian, serving as a counterexample to the exact generalization of Theorem 2.5 to cases where the n_i exceed 2. This example will be discussed further later.

We hope this theorem will help us prove analogues of the Schwartz-Zippel lemma in higher dimensions in the $n_i = 2$ case. It is worth noting that this theorem does hold if some of the n_i are 1 as well, but we state this slightly weaker version for simplicity.

3 Proofs of Results

3.1 First Generalized Combinatorial Nullstellensatz

To prove Theorem 2.3, we will need the following lemma.

Lemma 3.1. *Let $R \in K[x]$, for K algebraically closed, and let $G_i \in K[\overline{x_i}]$ be squarefree for each $i \in \{1, \cdots, k\}$. Suppose R vanishes on $\prod_{i=1}^{k} G_i$. Suppose also that the leading monomial of each G_i, for some arbitrary but fixed monomial ordering, divides no monomial of R. Then R is identically zero.*

Proof. The proof will proceed by induction on k. For the base case, $k = 1$, we have a polynomial R vanishing on $Z(G_1)$, where the leading monomial of G_1 divides no monomial of R. As G_1 is squarefree and R vanishes on $Z(G_1)$, and K is algebraically closed, we must have that either G_1 divides R, or R is identically zero. But if G_1 divides R, then certainly the leading monomial of G_1 divides some monomial of R; this is a contradiction, so R is identically zero. This completes the base case.

Now, suppose the statement holds for $k = l - 1$; we will show it holds for $k = l$. Write R as

$$R(x) = \sum_a R_a(x_1, x_2, \cdots, x_{n-n_l})\overline{x_l}^a$$

,

where a ranges over the exponent vectors of $\overline{x_l}$ in R. Fix some $q \in \prod_{i=1}^{l-1} Z(G_i)$, and let R_q be the polynomial given by setting the variables $x_1, \cdots, x_{n-n_l}$ to q in R; then $R_q = \sum_a R_a(q)\overline{x_l}^a$. Since R vanishes on $\prod_{i=1}^{l} Z(G_i)$, R_q must vanish on $Z(G_l)$.

Since R_q vanishes on $Z(G_l)$, and G_l is squarefree, we must have that either G_l divides R_q, or R_1 is identically zero. But if G_l divides R_q, then the leading monomial of G_l divides some monomial of R_q, and hence also some monomial of R. Hence, R_q is identically zero. But then $R_a(q) = 0$ for all a. Since this holds for any $q \in \prod_{i=1}^{l-1} Z(G_i)$, we must have that R_a vanishes on all of $\prod_{i=1}^{l-1} Z(G_i)$ for every a.

Furthermore, no leading monomial of any G_i for $1 \leq i \leq l-1$ can divide any monomial of R_a for any a, since then it would divide a monomial of R, which is a contradiction. Hence, by the inductive hypothesis, each R_a is identically zero. It follows that R is identically zero.

□

We are now ready to prove Theorem 2.3, which is restated here for convenience.

Theorem 3.2. *Let $F \in K[x]$ for K algebraically closed, and let $G_i \in K[\overline{x_i}]$ be squarefree for each $i \in \{1, \cdots, k\}$. Suppose F vanishes on $\prod_{i=1}^{k} G_i$. Then F is $(G_1, \cdots, G_k)$-Cartesian (and hence also $(n_1, \cdots, n_k)$-Cartesian).*

Proof. Fix a monomial ordering which agrees with the degree ordering, for example, the graded lexical ordering which orders first by degree and then lexically. By the multivariate division algorithm [2], we can write

$$F = \sum_{i=1}^{k} G_i H_i + R,$$

where each $H_i \in K[x]$ has $\text{multideg}(H_i) \leq \text{multideg}(F) - \text{multideg}(G_i)$, with respect to the monomial ordering, and the leading monomial of each G_i divides no monomial of $R \in K[x]$. Since we chose an ordering which agrees with the degree ordering, we have $\deg(H_i) \leq \deg(F) - \deg(G_i)$ as well. Hence, to show that F is $(G_1, \cdots, G_k)$-Cartesian, we need only show that R is identically zero.

Since F and $\sum_{i=1}^{k} G_i H_i$ both vanish completely on $\prod_{i=1}^{k} Z(G_i)$, we must have that R vanishes completely on $\prod_{i=1}^{k} Z(G_i)$ as well. Therefore, by Lemma 3.1, R is identically zero. Hence, F is $(G_1, \cdots, G_k)$-Cartesian.

□

As mentioned in the introduction, this theorem has a major weakness that the set $\prod_{i=1}^{k} Z(G_i)$ on which F must vanish to satisfy the conditions of the theorem is, in general, not finite, making it difficult to work with in application without a way to translate vanishing on a finite set into vanishing on a product of hypersurfaces.

Additionally, it was indicated in the comments above that the polynomial in four variables given by

$$F(x_1, x_2, y_1, y_2) = x_1 y_1 + x_2 + y_2$$

is not $(2, 2)$-Cartesian, serving to show that the above theorem does not hold over fields which are not algebraically closed. Here we explain in more detail why this polynomial is not $(2, 2)$-Cartesian.

Suppose F is $(2, 2)$-Cartesian. Then there exist polynomials G and H, each in two variables, of degree no more than 2 such that F vanishes on $Z(G) \times Z(H)$. Since $Z(H)$ must be infinite, this means at the very least that there are two distinct points (p_1, p_2) and (q_1, q_2) such that F vanishes on $Z(G) \times \{(p_1, p_2), (q_1, q_2)\}$. But then we have that G must vanish on the entire zero set of

$$x_1 p_1 + x_2 + p_2$$

and

$$x_1 q_1 + x_2 + q_2.$$

Since these are polynomials of degree 1, their zero sets can only have a shared curve if they are in fact identical; this can only happen if the two polynomials are multiples of each other, which can only happen if $p_1 = q_1$ and $p_2 = q_2$. But then the two points are not distinct, and it quickly follows that F is not $(2,2)$-Cartesian. As F vanishes on the product of the real zero sets of $x_1^2 + x_2^2$ and $y_1^2 + y_2^2$, that is, just $(0,0,0,0)$, it follows that Theorem 2.3 does not hold over $\mathbb{R}$.

3.2 Second Generalized Combinatorial Nullstellensatz

Our second generalized Combinatorial Nullstellensatz, Theorem 2.4, deals with finite sets, and is more closely related to Alon's second Combinatorial Nullstellensatz in that the restriction on the polynomial is in its support, not in its form as a sum of products of polynomials. The proof is a modification of a proof of Tao [8] to higher dimensions and with a slightly weaker condition, first suggested and proven in the one-dimensional case by Lasoń [3], on the support.

Theorem 2.4 is restated here for convenience.

Theorem 3.3. *Let $F \in K[x]$, and let $(t_1, \cdots, t_k)$ be maximal in the $(n_1, \cdots, n_k)$-reduced support of F with respect to the ordering where $(a_1, \cdots, a_k) \geq (b_1, \cdots, b_k)$ iff $a_i \geq b_i$ for all i. Let $S_i \in K^{n_i}$ be finite sets, and suppose $d(S_i) > t_i$ for each i. Then there is $s \in \prod_{i=1}^k S_i$ such that*

$$f(s) \neq 0.$$

Proof. Consider polynomials of the form

$$\sum_a c_a \overline{x_i}^a,$$

where a ranges across all vectors of nonnegative integers with sum of terms no more than t_i. This polynomial has degree no more than t_i. Hence, regardless of the choice of c_a, this polynomial cannot vanish on all of S_i, as $d(S_i) > t_i$, unless all the c_a are zero.

We will show that we can find functions $f_i : K^{n_i} \to K$ such that

$$\sum_{s \in S_i} f_i(s_i) s_i^a = 0$$

for all a with sum of terms less than t_i, and

$$\sum_{s \in S_i} f_i(s_i) s_i^a = 1$$

for all a with sum of terms exactly t_i.

To find such a function f_i for a particular fixed i, we need to solve the above linear system, which corresponds to a matrix with rows containing terms s_i^a for a fixed a, with s_i ranging all across S_i. Let the row of this matrix corresponding to a particular a be called r_a.

We will show that the rows of this matrix are linearly independent. Suppose that

$$\sum_a c_a r_a = (0, 0, \cdots, 0)$$

for some $c_a \in K$. We must show that all the c_a are zero to show that the r_a are linearly independent. But note that, if $\sum_a c_a r_a = 0$, since each row contains s_i^a for each $s_i \in S_i$, we have that

$$\sum_a c_a s^a = 0$$

for every $s \in S_i$; in other words, $\sum_a c_a x^a$ vanishes on all of S_i.

Since each a has sum of terms no greater than t_i, $\deg(\sum_a c_a x^a) \leq t_i$, so $\deg(\sum_a c_a x^a) < d(S_i)$; but $\sum_a c_a x^a$ vanishes on S_i, so the only possibility is that it is identically zero. Hence, the c_a are all zero, so the rows are linearly independent.

From the fact that the rows are linearly independent, it follows that the above system of linear equations has a solution, that is, we can find f_i satisfying the above system for each i. Now, letting $s = (s_1, s_2, \cdots, s_k)$ and $S = S_1 \times S_2 \times \cdots \times S_k$, consider

$$\sum_{s \in S} \left(\prod_{i=1}^{k} f_i(s_i) \right) \left(\prod_{i=1}^{k} s_i^{a_i} \right).$$

This expression is 0 if any of the a_i have terms summing to less than t_i, and is exactly 1 if all of the a_i have terms summing to exactly t_i.

Now, we can separate F into monomials, and note that every $(d_1, \cdots, d_k)$ in the $(n_1, \cdots, n_k)$-reduced support of F has either some $d_i < t_i$ or all $d_i = t_i$, by the maximality of $(t_1, \cdots, t_k)$ in the $(n_1, \cdots, n_k)$-reduced support. Further, $(t_1, \cdots, t_k)$ must be somewhere in the support. Hence,

$$\sum_{s \in S} \left(\prod_{i=1}^{k} f_i(s_i) \right) F(x) \neq 0,$$

for all terms with some $d_i < t_i$ for some i contribute 0 to the sum and any term with $d_i = t_i$ for all i contributes 1, and at least one term of the latter type must exist. Therefore, F does not vanish on all of S.

$\square$

Like Alon's second Combinatorial Nullstellensatz, this result deals with finite sets; however, now we must require that the algebraic degrees of the sets be a certain size, rather than the somewhat easier to work with notion of the cardinalities.

3.3 Third Generalized Combinatorial Nullstellensatz

Our final generalized Combinatorial Nullstellensatz only applies to partitions $n = n_1 + \cdots + n_k$ with all $n_i \leq 2$, although we only state the weaker version where all $n_i = 2$ here for simplicity. It is difficult to generalize this result to higher dimensions, since the proof requires that if a set of polynomials of certain degree all vanish on some set of certain size, then they share a common factor. In higher dimensions, however, many curves can intersect in infinitely many points without sharing a common curve; take, for instance, many planes intersecting in a line. In two dimensions, however, we have the following lemma [4] [5].

Lemma 3.4. *Let $\mathcal{S}$ be a possibly infinite set of curves in K^2 of degree at most d, and suppose that their intersection $\cap_{C\in\mathcal{S}}C$ contains a set I of size $|I| > d^2$. Then there is a curve C_0 such that $C_0 \in \cap_{C\in\mathcal{S}}C$ and $|C_0 \cap I| \geq |I| - (d-1)^2$.*

A proof of this lemma can be found in [4], building on work from [5]. They only prove the result for $K = \mathbb{C}$, but the proof extends to any field K without any changes.

Finally, before proving the theorem, we will need a lemma which essentially says that we can translate vanishing on Cartesian products of finite sets of sufficient size to vanishing on Cartesian products of curves.

Lemma 3.5. *Let $F \in K[x]$, and let $n_i = 2$ for all i. Let d_i be the degree of F in the variables of $\overline{x_i}$ for each i. Suppose that, for some m, $1 \leq m \leq k$, there are sets $S_1, \cdots, S_m \in K^2$, with $\#S_i > d_i^2$ for each i, and polynomials $G_{m+1}, \cdots, G_k$ with $G_i \in K[\overline{x_i}]$ such that F vanishes on $\prod_{i=1}^m S_i \times \prod_{i=m+1}^k Z(G_i)$. Then there are polynomials $G_1, \cdots G_m$, with $|Z(G_i) \cap S_i| \geq |S_i| - (d_i-1)^2$ for each i, $1 \leq i \leq m$, such that F vanishes on $\prod_{i=1}^m Z(G_i)$.*

Proof. The proof will proceed by induction on m. For the base case $m = 0$, we already have the statement by hypothesis.

Now, suppose the statement holds for $m = l - 1$; we will show that it holds for $m = l$. Let $S_1, \cdots, S_l$ and $G_{l+1}, \cdots, G_k$ be as in the statement of the lemma. For each $q \in \prod_{i=1}^{l-1} S_i \times \prod_{i=l+1}^k Z(G_i)$, let F_q be the polynomial in $\overline{x_l}$ given by setting all the variables other than those in $\overline{x_l}$ to q.

Since F vanishes on $\prod_{i=1}^l S_i \times \prod_{i=l+1}^k Z(G_i)$, we must have that F_q vanishes on S_l for any choice of q. As $\#S_l > d_l^2$, and $\deg(F_q) \leq d_l$ for every q, by Lemma 3.4, we have that the F_q must vanish on some common curve, and hence share a factor G_l, such that $|Z(G_l) \cap S_l| \geq |S_l| - (d_l - 1)^2$.

Since all the F_q vanish on $Z(G_l)$, we have that F vanishes on $\prod_{i=1}^{l-1} S_i \times \prod_{i=l}^k Z(G_i)$. The conditions for the inductive hypothesis are now satisfied, and thus we can find $G_1, \cdots, G_{l-1}$, with $|Z(G_i) \cap S_i| \geq |S_i| - (d_i - 1)^2$ for each i, such that F vanishes on $\prod_{i=1}^k Z(G_i)$, and the proof is complete.

□

Note that a lemma of this type is entirely unnecessary in the one-dimensional case, as it is easy to find a polynomial which vanishes exactly on any given finite set S, simply by taking $\prod_{s\in S}(x-s)$. In the higher-dimensional case, however, this lemma proves invaluable in linking a polynomial vanishing on a finite set to a polynomial vanishing on a product of curves. We are now ready to prove our final generalized Combinatorial Nullstellensatz, Theorem 2.5, which we restate here for convenience.

Theorem 3.6. *Suppose $n_i = 2$ for all i, and let $F \in K[x]$ for K algebraically closed. Suppose the degree of F in the two variables of $\overline{x_i}$ is d_i for each i. Then if $S_1, \cdots, S_k \subset K^2$ and $\#S_i > d_i$ for all i, there exists $s \in \prod_{i=1}^k S_i$ such that*

$$f(s) \neq 0$$

unless F is $(n_1, \cdots, n_k)$-Cartesian.

Proof. Suppose the contrary, that F vanishes on all of $\prod_{i=1}^k S_i$. Then, by Lemma 3.5, we can find $G_1, \cdots, G_k$, with $G_i \in K[\overline{x_i}]$ for each i such that F vanishes on $\prod_{i=1}^k Z(G_i)$; we can further select these G_i to be squarefree, as every polynomial in $K[x]$ shares its zero set with a squarefree polynomial. By Theorem 2.3, it follows that F is $(n_1, \cdots, n_k)$-Cartesian. This completes the proof.

□

It was indicated earlier that this theorem does not hold in higher dimensions, at least not in the $n_1 = n_2 = 3$ case, because the polynomial in six variables defined by

$$F(x_1, x_2, x_3, y_1, y_2, y_3) = x_1y_1 + x_2 + y_2$$

is not $(3,3)$-Cartesian but vanishes on a product of infinite sets in three dimensions, namely, the sets defined by $x_1 = x_2 = 0$ and $y_1 = y_2 = 0$. To see that this polynomial is not Cartesian, note that it is essentially the same polynomial as the polynomial discussed just after Theorem 2.3, but now in six variables; unsurprisingly, the argument that the polynomial is not Cartesian is almost identical. Suppose F is $(3,3)$-Cartesian, so it vanishes on the product of zero sets of polynomials in three variables G and H. Then, since each $Z(H)$ is two dimensional, there are at the very least two distinct pairs (p_1, p_2) and (q_1, q_2) such that

$$x_1p_1 + x_2 + p_2$$

and

$$x_1q_1 + x_2 + q_2,$$

now as polynomials in 3 variables x_1, x_2, and x_3, share a common factor. As they are degree 1 polynomials, this could only happen if they are multiples of each other, which just as above implies $(p_1, p_2) = (q_1, q_2)$, contradicting the assumption that the two pairs are distinct. Hence, F is not $(3,3)$-Cartesian, demonstrating the failure of an exact generalization of Theorem 2.5. Should such a generalization be sought, the condition on the sets S_i must be stronger than cardinality alone (such as the algebraic degree condition in Theorem 2.4).

4 Future Directions

In future work, we hope to generalize the Schwartz-Zippel to higher dimensions as well. As mentioned in the introduction, the Schwartz-Zippel lemma asserts that, for $F \in K[x_1, \cdots, x_n]$ a nonzero polynomial of degree d over a field K and S a finite subset of K,

$$|Z(F) \cap S^n| \leq d|S|^{n-1}.$$

As mentioned in the introduction, Mojarrad et al. provide something like a higher-dimensional analogue of this lemma for two sets P and Q of dimension 2 intersecting a variety in $\mathbb{C}^4$ [4]. They show that, if X is a variety in $\mathbb{C}^4$ of degree d and dimension three, and $P, Q \in \mathbb{C}^2$ are finite, then

$$|X \cap (P \times Q)| = O_{d,\epsilon}(|P|^{2/3}|Q|^{2/3+\epsilon} + |P| + |Q|).$$

We hope to generalize this to arbitrarily many two-dimensional sets in $\mathbb{C}^{2k}$, and further to make the dependence on d explicit, as in the original Schwartz-Zippel lemma. In their proof, Mojarrad et al. make use of the following incidence bound, proven by Sheffer and Zahl [6]:

Theorem 4.1. *Let $\mathcal{P} \subset \mathbb{C}^2$ and let $\mathcal{C}$ be a set of algebraic curves of degree at most d. If the incidence graph of $\mathcal{P}$ and $\mathcal{C}$ contains no $K_{2,M}$ or $K_{M,2}$, then*

$$I(\mathcal{P}, \mathcal{C}) = O_{d,M,\epsilon}(|\mathcal{P}|^{2/3+\epsilon}|\mathcal{C}|^{2/3} + |\mathcal{P}| + |\mathcal{C}|).$$

Here, the incidence graph refers to the bipartite graph with vertex sets $\mathcal{P}$ and $\mathcal{C}$, where there is an edge between $p \in \mathcal{P}$ and $C \in \mathcal{C}$ exactly when $p \in C$. $I(\mathcal{P}, \mathcal{C})$ refers to the number of edges in this graph, that is, the number of incidences. In future work, we hope to make use of incidence bounds due to Solymosi and Tao [7] to further generalize the Schwartz-Zippel Lemma in a similar way.

5 Acknolwedgments

I would like to firstly thank my mentor and research collaborator, Alperen Ergur, for introducing me to this project and working closely with me throughout the research process, and my research advisor, J. Maurice Rojas, for giving me this opportunity to do mathematical research and guiding me through the process. I would also like to thank the NSF for providing funding for this research experience.

References

[1] N. Alon. Combinatorial Nullstellensatz. *Comp. Prob. Comput.*, 8:7–29, 1999.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer Science+Business Media, LLC, New York, USA, 2007.

[3] M. Lasoń. A generalization of Combinatorial Nullstellensatz. *Electronic Journal of Combinatorics*, 17:1–6, 2010.

[4] H. Mojarrad, T. Pham, C. Valculescu, and F. de Zeeuw. Schwartz-Zippel bounds for two-dimensional products. 2015, arXiv:1507.08083.

[5] O. Raz, M. Sharir, and F. de Zeeuw. Polynomials vanishing on Cartesian products: The Elekes-Szabó Theorem revisited. In *31st Annual Symposium on Computational Geometry*, pages 522–536, 2015.

[6] A. Sheffer and J. Zahl. Point-curve incidences in the complex plane, 2015, arXiv:1502.07003.

[7] J. Solymosi and T. Tao. An incidence theorem in higher dimensions, 2012, arXiv:1103.2926.

[8] T. Tao. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory, 2014, arXiv:1310.6482.