Blackbox Polynomial Identity Testing for Depth 3 Circuits

Neeraj Kayal[*]

Shubhangi Saraf[‡]

Abstract— We study $\Sigma\Pi\Sigma(k)$ circuits, i.e., depth three arithmetic circuits with top fanin k. We give the first *deterministic* polynomial time *blackbox* identity test for $\Sigma\Pi\Sigma(k)$ circuits over the field $\mathbb{Q}$ of rational numbers, thus resolving a question posed by Klivans and Spielman (STOC 2001).

Our main technical result is a structural theorem for $\Sigma\Pi\Sigma(k)$ circuits that compute the zero polynomial. In particular we show that if a $\Sigma\Pi\Sigma(k)$ circuit $C = \sum_{i \in [k]} A_i = \sum_{i \in [k]} \prod_{j \in [d]} \ell_{ij}$ computing the zero polynomial, where each A_i is a product of linear forms with coefficients in $\mathbb{R}$, is *simple* ($\gcd\{A_i \mid i \in [k]\} = 1$) and *minimal* (for all proper nonempty subsets $S \subset [k]$, $\sum_{i \in S} A_i \neq 0$), then the *rank* (dimension of the span of the linear forms $\{\ell_{ij} \mid i \in [k], j \in [d]\}$) of C can be upper bounded by a function only of k. This proves a weak form of a conjecture of Dvir and Shpilka (STOC 2005) on the structure of identically zero depth three arithmetic circuits. Our blackbox identity test follows from this structural theorem by combining it with a construction of Karnin and Shpilka (CCC 2008).

Our proof of the structure theorem exploits the geometry of finite point sets in $\mathbb{R}^n$. We identify the linear forms appearing in the circuit C with points in $\mathbb{R}^n$. We then show how to apply high dimensional versions of the Sylvester–Gallai Theorem, a theorem from incidence-geometry, to identify a special linear form appearing in C, such that on the subspace where the linear form vanishes, C restricts to a simpler circuit computing the zero polynomial. This allows us to build an inductive argument bounding the rank of our circuit. While the utility of such theorems from incidence geometry for identity testing has been hinted at before, our proof is the first to develop the connection fully and utilize it effectively.

Keywords-Arithmetic circuits, Derandomization, Sylvester–Gallai Theorem.

1. Introduction

Identity testing is the following problem: given an arithmetic circuit[1] computing a multivariate polynomial $f(X_1, \ldots, X_n)$ over a field $\mathbb{F}$, determine if the polynomial is identically zero. Algorithms for primality testing [2], [3], perfect matching [23] and some fundamental structural results in complexity such as the PCP Theorem and IP=PSPACE involve testing if a particular polynomial is zero.

Schwartz [25] and Zippel [28] observed that by evaluating a polynomial at randomly chosen points from a sufficiently

large domain, we can determine if the polynomial is nonzero with high probability. The correctness of their algorithm follows from the simple observation that any polynomial of total degree d cannot have many roots over a field whose size is much larger than d. The Schwartz–Zippel Lemma combined with a standard counting argument implies that for every integer s, there is a $poly(s)$-sized set of points P such that for every circuit C of size s, C computes the zero polynomial if and only if $C(\mathbf{a}) = 0$ for every $\mathbf{a} \in$ P. Blackbox Identity testing is the problem of giving an *explicit*[2] construction of such a test set P. Any explicit construction of such a set of points immediately gives, via interpolation, an explicit polynomial f which cannot be computed by circuits of size s [1].

A more surprising connection between identity testing and the task of proving arithmetic circuit lower bounds was discovered by Impagliazzo and Kabanets [15] who showed that *any* polynomial-time algorithm for identity testing (not necessarily a blackbox identity test[3]) would also imply certain arithmetic circuit lower bounds. More specifically, they showed that if identity testing has an efficient deterministic polynomial time algorithm then (almost) NEXP does not have polynomial size arithmetic circuits. For the pessimist, this indicates that derandomizing identity testing is a hopeless problem. For the optimist, this means on the contrary that to obtain an arithmetic circuit lower bound, we "simply" have to prove a good upper bound on identity testing.

Because of the difficulty of the general problem, research has focussed on bounded depth arithmetic circuits. Grigoriev and Karpinski [13] have shown that any depth three arithmetic circuit over a finite field computing the permanent or the determinant requires exponential size[4]. But progress in this direction stalled and very recently, an "explanation" for this was discovered by Agrawal and Vinay [4] who showed that there is chasm at depth four - proving exponential lower bounds for depth four arithmetic circuits already implies

---

[*]Microsoft Research. neeraka@microsoft.com.

[‡]MIT CSAIL. shibs@mit.edu. Research supported in part by NSF Award CCF 0829672.

[1]Arithmetic circuits are circuits with two types of internal nodes/gates: a $\times$ gate computes the product of its inputs whereas a $+$ gate is allowed to compute an arbitrary linear combination of its inputs, and the wires carry elements of a field $\mathbb{F}$.

[2]Over infinite fields such as the rationals, we require more so that the evaluation can be carried out efficiently - the bit-length of the coordinates of the points in P need to be polynomially bounded. Furthermore, if the degree of the polynomial computed is huge then we also require the construction to give a prime of small bit-length so that the computation can be carried out modulo p.

[3]A non-blackbox algorithm is given a full description of the circuit and it needs to decide whether it is identically 0.

[4]The size of the field is held constant and a lower bound is obtained on the size of the circuit as a function of the dimension of the matrix.

exponential lower bounds for arbitrary depth arithmetic circuits. They also showed that a complete blackbox derandomization of Identity Testing problem for depth four circuits with multiplication gates of small fanin implies a nearly complete derandomization of general Identity Testing. As most of these questions are fairly easy for depth two circuits, we see that depth three circuits stand between the relatively easy (depth-two) and the difficult, fairly general case (depth-four). Hence it is a worthwhile goal to get a good understanding of depth-three circuits.

Another important direction of research, pursued in the works of Chen and Kao [8], Lewin and Vadhan [22], Klivans and Spielman [21] and Agrawal and Biswas [2] on the identity testing problem has been the effort to take advantage of the structure of a polynomial to reduce the number of random bits needed for identity testing. In this process, Klivans and Spielman gave a blackbox identity testing algorithm for depth two arithmetic circuits and posed as a challenge the problem of devising blackbox identity testers for depth three circuits with bounded top fanin. Recall that a depth three arithmetic circuit, also called a $\Sigma\Pi\Sigma$-circuit, has an addition gate at the top (output) layer, followed by multiplication gates at the middle layer, followed by addition gates at the bottom layer, the gates being of arbitrary fanin[5]. In other words, a $\Sigma\Pi\Sigma$ circuit is a sum of terms, each of which is a product of a linear function of the input variables. We denote the set of n input, depth three circuits, where the top addition gate has fanin k, and the middle multiplication gates have fanin at most d, by $\Sigma\Pi\Sigma(k, d, n)$. The challenge posed by Klivans and Spielman was taken up by Dvir and Shpilka [9] and then by Kayal and Saxena [19] and a non-blackbox deterministic polynomial-time algorithm was devised (see also [5]). Recently Karnin and Shpilka [16] obtained a quasi-polynomial time *blackbox* identity test for $\Sigma\Pi\Sigma(k, d, n)$ circuits. Despite the progress made on this question, a deterministic polynomial-time blackbox test had remained elusive.

In this paper we fully resolve the Klivans–Spielman challenge for arithmetic circuits with rational coefficients by giving the first deterministic blackbox identity test for $\Sigma\Pi\Sigma(k, d, n)$ circuits whose running time, for every fixed value of k, is *polynomial* in d and n. Our main technical contribution towards the proof of this result is a structural theorem for such circuits that answers a weak form of a conjecture by Dvir and Shpilka. In particular we prove that the "rank" of bounded top fanin $\Sigma\Pi\Sigma$ circuits is a constant depending only on the size of the top fanin. Combined with a result from [16] which says that a good rank bound suffices for black-box identity testing, we obtain the full result. The proof of our structure theorem uses results from

[5]If the depth three circuit has a multiplication gate at the top then problems pertaining to identity testing and lower bounds boil down to the relatively easy case of depth two circuits.

the incidence geometry of $\mathbb{R}^n$. In particular we invoke a high dimensional version of the Sylvester–Gallai Theorem that enables us to identify certain configurations of linear forms appearing in any high rank circuit that prevent it from being identically zero. The survey by Borwein and Moser [7] contains a good introduction to the Sylvester–Gallai Theorem - its history, its proofs and its many generalizations. Before we state the conjecture and our main result, we introduce some terminology.

2. DEFINITIONS AND STATEMENT OF RESULTS

$[k]$ denotes the set $\{1, 2, \ldots, k\}$. $\mathbb{Q}$ denotes the field of rational numbers and $\mathbb{R}$ the field of real numbers.

Depth Three Arithmetic Circuits. We consider arithmetic circuits with coefficients in a field $\mathbb{F}$ (in this paper, $\mathbb{F}$ will always be either $\mathbb{Q}$ or $\mathbb{R}$) . A $\Sigma\Pi\Sigma$ circuit C is a formal expression of the form

$$\sum_{i \in [k]} A_i = \sum_{i \in [k]} \prod_{j \in [d]} \ell_{ij},$$

where the ℓ_{ij} are linear forms of the type $\ell_{ij} = \sum_{k \in [n]} a_k \cdot X_k = \mathbf{a} \cdot \mathbf{X}$, where $\mathbf{a} = (a_1, \ldots, a_n)$ is a fixed vector in $\mathbb{Q}^n$, and $\mathbf{X} = (X_1, \ldots, X_n)$ is the tuple of indeterminates. k is the fanin of the top gate of the circuit and d is the fanin of each multiplication gate A_i. The A_i's are referred to as the terms or the constituent $\Pi\Sigma$ subcircuits of C and the ℓ_{ij}'s as the set of linear forms that belong to the circuit. Recall that we denote the class of such circuits by $\Sigma\Pi\Sigma(k, d, n)$.

Remark   Note that the above definition only captured homogeneous circuits. For the purpose of (blackbox) identity testing, we can assume this without loss of generality. Indeed, notice that a polynomial $C(X_1, \ldots, X_n)$ of degree less than or equal to d is zero if and only if the corresponding homogeneous polynomial $Z^d \cdot C(\frac{X_1}{Z}, \ldots, \frac{X_n}{Z})$ is zero. This observation can be used to homogenize the input circuit C, i.e. given blackbox access to C, we can simulate blackbox access to the homogenization of C. Notice also that after the homogenization, all multiplication gates $\{A_i\}$ have the same fanin d. In the rest of the paper we will assume that the input circuit is homogeneous, i.e. the ℓ_{ij}'s are linear forms with zero constant term, and all the multiplication gates have the same fanin d.

When the context requires it, we will drop some of the parameters in talking about this class of circuits. $\Sigma\Pi\Sigma(k)$ will denote the set of $\Sigma\Pi\Sigma$ circuits with top fanin k and $\Sigma\Pi\Sigma(k, d)$ will be the set of $\Sigma\Pi\Sigma$ circuits with top fanin k and middle (multiplication gate) fanin d. Given such a circuit, we can naturally associate it with the polynomial computed by it. We say that C $\equiv 0$ if the polynomial computed by C is identically zero. We are now ready to state our main result which shows that for every fixed k,

there is a deterministic blackbox identity tester for the class of $\Sigma\Pi\Sigma(k,d,n)$ circuits over the field $\mathbb{Q}$ that runs in time polynomial in n and d.

Theorem 2.1: **[Blackbox PIT for $\Sigma\Pi\Sigma(k)$ circuits]** There is a deterministic algorithm that takes as input a triple (k,d,n) of natural numbers and in time $\mathrm{poly}(n)\cdot d^{2^{O(k\cdot\log k)}}$, outputs a set $P\subset\mathbb{Z}^n$ with the following properties:

1) Any $\Sigma\Pi\Sigma(k,d,n)$ circuit C with rational coefficients computes the zero polynomial if and only if $C(\mathbf{a})=0$ for every $\mathbf{a}\in P$.
2) The number of points in P is $\mathrm{poly}(n)\cdot d^{2^{O(k\cdot\log k)}}$.
3) For every $(a_1,\ldots,a_n)\in P$ and every $i\in[n]:|a_i|\leq \mathrm{poly}(2^{n^2}\cdot d)\cdot 2^{2^{O(k\log k)}}$. In particular, the bit-length of each point in P is $2^{O(k\log k)}\cdot O(n^3\cdot\log d)$.

Remark.

1) Notice that in the theorem above, the number of points in P and the bit-lengths of these points are both independent of the bit-lengths of the constants from $\mathbb{Q}$ used in the circuit. Hence we can allow arbitrary constants from $\mathbb{Q}$ to be used on the edges coming into addition gates in the circuit. We get this feature because the two main components of the proof, the structure theorem (Theorem 2.2) as well as the result from [16] (Lemma 2.3) are independent of the bit-lengths of the constants from $\mathbb{Q}$ used in the circuit.
2) For every fixed value of k, the algorithm for the construction of the set P alluded to in the above theorem can in fact be implemented in TC^0. Combined with the observation that a given depth three circuit can be evaluated at a given point in TC^0, we get a deterministic P-uniform TC^0-algorithm for identity testing of $\Sigma\Pi\Sigma(k,d,n)$ circuits. Previously no efficient deterministic algorithm, not even a non-blackbox one, for identity testing of $\Sigma\Pi\Sigma(k)$ was known which can be implemented in TC^0. We do not stress the constant depth computability because it is not the main point of our result. But the ability to do identity testing using small depth uniform circuits can potentially be useful at other places, such as in the context of the question [23]: Is BipartiteMatching $\in$ NC ?
3) For concreteness, we only state our results over $\mathbb{Q}$ but our theorem is valid over any field that can be embedded into the real numbers, in particular for any totally real extension of $\mathbb{Q}$. Over such fields, the same set of points as constructed above suffices for identity testing.
4) As noted in the introduction, a blackbox identity testing algorithm for any class of circuits can in general be used to construct explicit polynomials that are hard to compute by the corresponding class of circuits. It is known that $\Sigma\Pi\Sigma$ circuits with bounded top fanin cannot compute all polynomials - no matter how large their size. In particular such circuits cannot compute the determinant and the elementary symmetric polynomials. The best known lowerbound for the size of a general $\Sigma\Pi\Sigma$ circuit is quadratic, due to Shpilka and Wigderson [27].

After introducing the requisite terminology, we state the two main ingredients leading to this theorem - our proof of a conjecture by Dvir and Shpilka and a construction of rank preserving subspaces by Karnin and Shpilka.

2.1. Notions related to a $\Sigma\Pi\Sigma$ circuit

Let $C=\sum_{i\in[k]}A_i=\sum_{i\in[k]}\prod_{j\in[d]}\ell_{ij}$ be a $\Sigma\Pi\Sigma$ circuit. We give the following definitions:

minimal: We say that C is *minimal* if no strict nonempty subset of its constituent $\Pi\Sigma$ polynomials $\{A_1,\ldots,A_k\}$ sums to zero.

simple: We say that C is *simple* if the gcd of its constituent $\Pi\Sigma$ polynomials, $\gcd(A_1,A_2,\ldots,A_k)$ equals one. The simplification of a $\Sigma\Pi\Sigma$-circuit C, denoted $\mathrm{Sim}(C)$, is the $\Sigma\Pi\Sigma$ circuit obtained by dividing each term by the gcd of all the terms. i.e.,

$$\mathrm{Sim}(C)\overset{\text{def}}{=}\sum_{i\in[k]}\frac{A_i(\mathbf{X})}{g(\mathbf{X})},\quad\text{where }g(\mathbf{X})=\gcd(A_1,\ldots,A_k)$$

rank: Identifying each linear form $\ell=\sum_{i\in[k]}a_i\cdot X_i$ with the vector $(a_1,\ldots,a_n)\in R^n$, we define the *rank* of C to be the dimension of the vector space spanned by the set $\{\ell_{ij}\mid i\in[k],j\in[d]\}$.

pairwise-rank: For a $\Sigma\Pi\Sigma(k)$ circuit $C=\sum_{i\in[k]}A_i$, we define the *pairwise-rank* of C to be $\min_{1\leq i<j\leq k}\{\mathrm{rank}(\mathrm{Sim}(A_i+A_j))\}$, where A_i+A_j is the subcircuit of C containing just the two multiplication gates A_i and A_j. If C has only one multiplication gate, we say the pairwise-rank of C is ∞.

2.2. The Dvir–Shpilka conjecture and the main Structural Result

Very roughly, the conjecture of Dvir and Shpilka [9] asserts that for every k, there is a constant $c(k)$ such that if a depth three circuit C with top fanin k computes the zero polynomial then the rank of C is at most $c(k)$ (independent of the degree d of the intermediate polynomials computed at the different multiplication gates). As a step towards the conjecture, a $\mathrm{poly}(2^{k^2}\cdot\log d)$ upper bound on the rank was obtained by Dvir and Shpilka [9]. This was subsequently improved by Saxena and Seshadri [24] to $(\mathrm{poly}(k)\cdot\log d)$. Over *finite fields*, this conjecture was disproved by Kayal and Saxena [19] but the situation over fields of characteristic zero remained unclear. The conjecture soon revealed its fundamental nature - the weaker polylogarithmic upper bound was

used by Karnin and Shpilka[16] to give a quasipolynomial time deterministic blackbox identity test for $\Sigma\Pi\Sigma$ circuits with bounded top fanin. It was also used by Shpilka [26] and by Karnin and Shpilka [17] to give a quasipolynomial time algorithm for reconstruction of $\Sigma\Pi\Sigma$ circuits. In this paper, we prove the conjecture of Dvir and Shpilka over the field $\mathbb{R}$ of real numbers, and therefore also over all subfields of $\mathbb{R}$ such as $\mathbb{Q}$, the field of rational numbers. We then combine this result with ideas from [16] to get an efficient algorithm for blackbox identity testing of $\Sigma\Pi\Sigma$-circuits with bounded top fanin.

Theorem 2.2: [**Structure Theorem: Rank bound for** $\Sigma\Pi\Sigma(k)$ **circuits**] For every k, there exists a constant $c(k)$ (where $c(k) \leq 3^k((k+1)!)^2 = 2^{O(k \cdot \log k)}$) such that every $\Sigma\Pi\Sigma(k)$ circuit C with coefficients in $\mathbb{R}$ that is simple, minimal, and computes the zero polynomial has $\text{rank}(C) \leq c(k)$.

Remark.

1) Dvir and Shpilka conjectured that $c(k)$ is in fact a polynomially increasing function of k. We are able to only prove the weaker $\text{poly}(2^{k \cdot \log k})$ upper bound on $c(k)$. The best previously known bound was $(\text{poly}(k) \cdot \log d)$ [24] (note the dependence on d).

2) Our proof techniques also enable us to prove the structure theorem above (and hence blackbox identity testing) for the case $k = 3$ over complex numbers and over prime fields of very large characteristic. For more discussion about these results and why our proof does not go through for larger values of k over these fields, see Appendix A.

2.3. From the Rank Bound to Identity Testing

We give below the construction of Karnin and Shpilka [16] which used ideas from an earlier work of Gabizon and Raz [12] to show how the rank bound of Theorem 2.2 translates into the blackbox identity testing algorithm of Theorem 2.1.

Lemma 2.3: [**Translating rank bounds into a blackbox identity test.**] [16] Let $\mathbb{F}$ be a field and $R(k,d)$ be an integer such that every minimal and simple $\Sigma\Pi\Sigma(k,d,n)$ circuit over $\mathbb{F}$ computing the zero polynomial has rank at most $R(k,d)$. For $\alpha \in \mathbb{F}$ let A_α be the $n \times R(k,d)$ matrix for which $(A_\alpha)_{i,j} = \alpha^{i(j+1)}$. Let $b_\alpha \stackrel{\text{def}}{=} (\alpha, \alpha^2, \ldots, \alpha^n)$. Let S, T be subsets of $\mathbb{F}$ such that $|S| = n \cdot \left(\binom{kd}{2} + 2^k\right) \cdot \binom{R(k,d)+2}{2} + 1$ and $|T| = d+1$. Let $P \subset \mathbb{F}^n$ be the following set of points.

$$P \stackrel{\text{def}}{=} \left\{ A_\alpha \cdot \mathbf{x} + b_\alpha \ : \ \alpha \in S \quad \text{and} \quad \mathbf{x} \in T^{R(k,d)} \right\}.$$

Then for every $\Sigma\Pi\Sigma(k,d,n)$ circuit C, C is identically zero if and only if $C(\mathbf{a}) = 0$ for all $\mathbf{a} \in P$.

This lemma can be applied to our situation as follows.

Proof of Theorem 2.1 We set $\mathbb{F} = \mathbb{Q}$ and using Theorem 2.2, we get that $R(k,d) = c(k) = 2^{O(k \cdot \log k)}$ is independent of d. We choose S to be $\{1, 2, \ldots, m\}$ where

$$m = n \cdot \left(\binom{kd}{2} + 2^k \right) \cdot \binom{c(k)+2}{2} + 1$$

and T to be $\{1, 2, \ldots, d+1\}$. We apply the above lemma to these choices of $\mathbb{F}, R(k,d), S$ and T. We thus get a set P which satisfies property (1). The number of points in P is $|S| \cdot |T|$ so that $|P| = \text{poly}(n) \cdot d^{2^{O(k \log k)}}$. Thus P satisfies property (2). Every coordinate of a point in P is the dot product of two vectors of length $R(k,d) = c(k)$ whose entries have bit-length $2^{O(k \log k)} \cdot O(n^2 \cdot \log d)$. This means that the bit-length of each point in P is $2^{O(k \log k)} \cdot O(n^3 \cdot \log d)$. This proves property (3). Clearly, this set P is very explicit - in fact it is so explicit that for every fixed k, P can be computed in the complexity class P-uniform TC^0. This completes the proof of the theorem.

$\square$

The rest of this article is devoted to a proof of Theorem 2.2.

3. Organization

The rest of this paper is organized as follows. In Section 4, we give an overview of the techniques that we use in the proof of Theorem 2.2. In Section 5, we give the proof of Theorem 2.2 while deferring the proof of a key lemma used in the proof to the full version [18]. We give a sketch of the proof of this lemma and its connection to the Sylvester–Gallai Theorem and a related Hyperplane Decomposition Lemma in Section 6. The proof of the main technical (key) lemma, which we call the Fanin Reduction Lemma and the proof of the Hyperplane Decomposition Lemma which is used therein are in the full version [18]. We conclude with a discussion of open problems in Section 7. Finally, in Appendix A, we discuss some of the conjectures formulated in the conclusion.

4. Overview of Proof of Rank Bound

In this section we give an overview of the proof of the structure theorem (Theorem 2.2). The proof proceeds by induction on the number of multiplication gates in the circuit. As induction hypothesis, we assume that any simple, minimal $\Sigma\Pi\Sigma$ circuit with fewer than k multiplication gates that is identically 0 cannot have high rank. Now if possible, let $C = \sum_{i=1}^{k} A_i = \sum_{i=1}^{k} \prod \ell_{ij}$ be a simple and minimal circuit in n variables that has high rank, and such that $C \equiv 0$. We will obtain a contradiction. For the sake of simplicity, we assume that each linear form ℓ_{ij} that appears in a gate of the circuit C, appears there with multiplicity one only.

In [18], when we give the full argument, we remove this assumption.

Looking at the circuit modulo a linear form. We will be looking at the circuit modulo an appropriately chosen linear form. If $\ell = a_1 \cdot X_1 + \cdots + a_n \cdot X_n$ is a linear form with $a_1 \neq 0$, then the image of a circuit C modulo ℓ is defined to be circuit obtained by replacing X_1 by $-\frac{1}{a_1} \cdot (a_2 \cdot X_2 + \ldots + a_n \cdot X_n)$ in C. i.e.

$$
\begin{aligned}
\mathrm{C}' &= \mathrm{C} \pmod{\ell} \\
&\stackrel{\text{def}}{=} \mathrm{C}(-\frac{1}{a_1}(a_2 X_2 + \ldots + a_n X_n), X_2, \ldots, X_n).
\end{aligned}
$$

(see [18] for a more accurate definition that avoids the degenerate case when $a_1 = 0$.) Observe that if A_i is a $\Pi\Sigma$ polynomial of rank r and ℓ is a linear form, then either A_i equals zero modulo ℓ (i.e. ℓ divides A_i) or the rank of A_i drops by at most one to $r - 1$. Now if we pick a linear form ℓ which occurs in one of the constituent $\Pi\Sigma$ polynomials, say in A_1, then A_1 equals zero modulo ℓ so that the resulting circuit $\mathrm{C}' = \mathrm{C} \pmod{\ell}$ would have at most $k - 1$ multiplication gates, each surviving gate having rank at most one less than what it had previously. Notice that if C computes the zero polynomial then so does the circuit C'. If this circuit C' was both simple and minimal we would be immediately done by the induction hypothesis.

However, in general it may not be possible to ensure C' is simple and minimal, and hence we use an intermediate notion, pairwise-rank, that very effectively captures and deals with the issues of simplicity and minimality. We first show that (1) any simple and minimal circuit computing the zero polynomial that has high rank must also have high pairwise-rank. We then show that (2) no circuit with high pairwise-rank can compute the zero polynomial.

Step (1) is the easier of the two steps. We show that if the circuit C has low pairwise-rank, then by setting some of the variables of the circuit to random values, we can obtain a new circuit that is still simple, minimal, has high rank, computes the zero polynomial, but has fewer multiplication gates (see Lemma 5.3). This contradicts the induction hypothesis.

Step (2) again uses the induction hypothesis. One of the key lemmas used here, which we refer to as the Fanin Reduction Lemma, roughly asserts that if C is a simple circuit with high pairwise-rank, then there exists a linear form ℓ in C such that if we go modulo ℓ, we get a circuit C' that still has high pairwise-rank, but with fewer multiplication gates. Also, if $\mathrm{C} \equiv 0$, then $\mathrm{C}' \equiv 0$. From C', we then show how to extract a subcircuit that is simple, minimal, computes the zero polynomial and has high rank. This will contradict the induction hypothesis. The bulk of the work goes into proving the Fanin Reduction Lemma, Lemma 5.5. The vital ingredient in the proof of Lemma 5.5

is a theorem from incidence geometry called the high dimensional Sylvester–Gallai Theorem. Before we state the Sylvester–Gallai Theorem, we first translate our problem into geometrical language.

4.1. A correspondence between $\Sigma\Pi\Sigma(k, d, n)$ circuits and k-colored points in $\mathbb{R}^n$

We identify the linear forms appearing in C with colored points in $\mathbb{R}^n$. A linear form $\ell = a_1 \cdot X_1 + \cdots + a_n \cdot X_n$ corresponds to the point $P_\ell = (1, \frac{a_2}{a_1}, \ldots, \frac{a_n}{a_1}) \in \mathbb{R}^n$ (see [18] for a more accurate definition of this correspondence which avoids the degenerate case when $a_1 = 0$). If the linear form $\ell \in A_i$ then we assign the color i to the point P_ℓ. Since a linear form could appear in multiple gates, in general a point could have many colors (see [18] for details). Our choice of the mapping of linear forms to points satisfies the property that 3 linear forms are linearly dependent iff they map to collinear points[6]. For two points $P \neq Q \in \mathbb{R}^n$ we will denote by $\lambda(P, Q)$ the line joining P and Q. For a point P and a color i we will denote by $\mathcal{L}_i^P$ the pencil of lines $\{\lambda(P, Q) : Q \text{ has color } i\}$.[7]

Translating the search for a suitable linear form into the search for a suitable point. Let the set of all points in the image of the set of linear forms in C be S. For a color $i \in [k]$, we will denote by S_i the set of points of color i. Now fix a linear form ℓ that occurs in C and consider two multiplication gates, say A_1 and A_2 occurring in C which do not contain ℓ. Consider the set $S_1 \Delta S_2$ which is the symmetric difference of the two sets of points of color 1 and 2 respectively (see [18] for a more accurate definition which takes care of degenerate cases when a linear forms occurs in a gate with a higher multiplicity). Then the dimension of the space spanned by points in $S_1 \Delta S_2$ corresponds to the rank of the simplification of the circuit $A_1 + A_2$. Now consider the two pencils of lines $\mathcal{L}_1^{P_\ell}$ and $\mathcal{L}_2^{P_\ell}$. Notice that $\mathcal{L}_1^{P_\ell} \bigcap \mathcal{L}_2^{P_\ell}$ is again a pencil of lines through P_ℓ. Now $\gcd(A_1 \pmod{\ell}, A_2 \pmod{\ell})$ is nontrivial ($\neq 1$) if and only if there exists a line common to these two pencils, i.e. $\mathcal{L}_1^{P_\ell} \bigcap \mathcal{L}_2^{P_\ell} \neq \phi$. In fact the degree of $\gcd(A_1 \pmod{\ell}, A_2 \pmod{\ell})$ is exactly the number of lines in the pencil $\mathcal{L}_1^{P_\ell} \bigcap \mathcal{L}_2^{P_\ell}$. Now let us consider the symmetric difference $\mathcal{L}_1^{P_\ell} \Delta \mathcal{L}_2^{P_\ell}$ which is again another pencil of lines through P_ℓ. The requirement that C modulo ℓ has high pairwise-rank, i.e. for all pairs of gates A_1, A_2 that do not contain ℓ, the simplification of $A_1 \pmod{\ell} + A_2 \pmod{\ell}$ should have high rank, then exactly translates into the requirement that the lines in this pencil $\mathcal{L}_1^{P_\ell} \Delta \mathcal{L}_2^{P_\ell}$ should span a high dimensional space.

---

[6]A set of points in $\mathbb{R}^n$ are said to be *collinear* if the points span a one dimensional affine space.

[7]A pencil of lines is just a set of lines through a common point.

Applying the Sylvester–Gallai Theorem. At this point it is not a priori clear as to why there should exist even a single line in the pencil $\mathcal{L}_1^{P_\ell} \Delta \mathcal{L}_2^{P_\ell}$. In fact if we fix the point P_ℓ then such an assertion is easily seen to be false. We show that there indeed exists a linear form ℓ, and the corresponding point P_ℓ such that for every pair of colors i and j (P_ℓ has color neither i nor j), the lines in the pencil $\mathcal{L}_i^{P_\ell} \Delta \mathcal{L}_j^{P_\ell}$ span a space of large enough dimension. The proof of this fact forms the main substance of the proof of our Fanin Reduction Lemma, Lemma 5.5. In order to prove this result, we crucially use the Sylvester–Gallai Theorem, a result from incidence geometry. The basic Sylvester–Gallai Theorem roughly states that if S is a finite set of points in $\mathbb{R}^n$ that are not all collinear, then there exists a line passing through exactly 2 points of S. This kind of statement is already in the spirit of what we want to show. We use a high dimensional version of the Sylvester–Gallai Theorem along with some colorful combinatorics to obtain our final result[8].

5. The Rank Bound

In this section we the circuit rank bound, Theorem 2.2. The main technical result that we use is Lemma 5.5 (which we call the Fanin Reduction Lemma). A sketch of the proof of the Fanin Reduction Lemma is given in Section 6, and the full proof given in [18]. We first state some lemmas and definitions related to circuit transformations that will be useful in the proof of Theorem 2.2. We then state the Fanin Reduction Lemma (Lemma 5.5) and show how to combine the results on circuit transformations and the Fanin Reduction Lemma to give a proof of Theorem 2.2.

Remark For the rest of this paper, all $\Sigma\Pi\Sigma$ circuits will have coefficients in $\mathbb{R}$.

5.1. Circuit Transformations

In this section we discuss some operations on circuits that will be useful in the proof of the rank bound (Theorem 2.2).

Lemma 5.1: **[Invariance of circuit properties under invertible linear transformations of the variables.]** Let $\pi : \mathbb{R}^n \to \mathbb{R}^n$ be an invertible linear transformation. Let $C = \sum_{i \in [k]} A_i = \sum_{i \in [k]} \prod_{j \in d} \ell_{ij}$ be a $\Sigma\Pi\Sigma$ circuit, and let $\pi(C)$ be the circuit $\sum_{i \in [k]} \pi(A_i) = \sum_{i \in [k]} \prod_{j \in d} \pi(\ell_{ij})$, where for a linear form $\ell = \mathbf{a} \cdot \mathbf{X}$, $\pi(\ell) = \pi(\mathbf{a}) \cdot \mathbf{X}$. Then, $\pi(C)$ is simple $\iff$ C is simple, $\pi(C)$ is minimal

$\iff$ C is minimal, $\pi(C) \equiv 0 \iff C \equiv 0$, and $\mathrm{rank}(\pi(C)) = \mathrm{rank}(C)$.

The proof of this lemma is immediate from definitions, and we omit it. We say that two circuits C and C' are equivalent, denoted by $C \sim C'$, if there exists an invertible linear transformation $\pi : \mathbb{R}^n \to \mathbb{R}^n$ such that $C = \pi(C')$.

Lemma 5.2: **[Schwartz–Zippel Lemma]** Let $f(X_1, X_2, \ldots, X_n)$ be a nonzero n variate polynomial of degree d over $\mathbb{R}$. Then for $(a_1, a_2, \ldots, a_n)$ chosen uniformly at random in $[0,1]^n$, the probability that $f(a_1, a_2, \ldots, a_n) = 0$ is zero.

Lemma 5.3: **[Setting linear forms to random values.]** Let $C \equiv 0$ be a simple and minimal $\Sigma\Pi\Sigma$ circuit in the n indeterminates $X_1, X_2, \ldots, X_n$. Let $\mathrm{rank}(C) = r$. Let $t \in [n]$, and let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be real numbers picked independently and uniformly from $[0,1]$. Let Z be an indeterminate, and consider the new circuit C' formed by replacing X_i by $\alpha_i Z$ for all $i \in [t]$. Then with probability 1, C' is minimal and $\mathrm{rank}(\mathrm{Sim}(C')) \geq r - t$.

Definition 5.4: **[Setting a linear form to 0: $C|_{\ell=0}$]** Let $C = \sum_{i \in [k]} A_i = \sum_{i \in [k]} \prod_{j \in d} \ell_{ij}$ be a $\Sigma\Pi\Sigma$ circuit. Let ℓ be a linear form appearing in C. Let $\pi : \mathbb{R}^n \to \mathbb{R}^n$ is any linear map of rank $n-1$ such that $\mathrm{kernel}(\pi) = \mathrm{span}(\ell)$[9]. We let $C|_{\ell=0}$ denote the class of circuits obtained by applying such a transformation π to C, to get a circuit $\pi(C)$, where $\pi(C)$ is the circuit $\sum_{i \in [k]} \prod_{j \in d} \pi(\ell_{ij})$, where for a linear form $\ell = \mathbf{a} \cdot \mathbf{X}$, $\pi(\ell) = \pi(\mathbf{a}) \cdot \mathbf{X}$. Under such a transformation, all the constituent $\Pi\Sigma$ polynomials that contain ℓ get set to 0, and we remove all such gates from the circuit.

It is easy to see that if C_1 and C_2 are two circuits in $C|_{\ell=0}$, then $C_1 \sim C_2$, and we omit the proof. We abuse notation by using $C' = C|_{\ell=0}$ to refer to any circuit C' in the class $C|_{\ell=0}$. Note that if $C \equiv 0$, then for any circuit C' in the class $C|_{\ell=0}$, we have $C' \equiv 0$.

5.2. The Fanin Reduction Lemma

Lemma 5.5 is the main technical result of our paper that allows us to apply an induction argument to reason about the rank of $\Sigma\Pi\Sigma$ circuits computing the zero polynomial. We show that if a simple circuit C has high pairwise-rank, then by "setting a linear form to 0", we can transform it to a new circuit C' with fewer multiplication gates that still has high pairwise-rank. The proof of the lemma does not use the fact that $C \equiv 0$. However we get that if $C \equiv 0$, then $C' \equiv 0$.

Lemma 5.5: **[Fanin Reduction Lemma]** Let $k, A > 0$ be integers. Let $B = 3(A+1)k^2$. Let C be a simple $\Sigma\Pi\Sigma(k)$ circuit such that pairwise-rank$(C) \geq A$, and $\mathrm{rank}(C) \geq B$.

---

[8]Dvir and Shpilka [9] even observed that a certain colorful analog of the Sylvester–Gallai Theorem would imply the rank bound for the special case of $k = 3$. Such a result had in fact been proved much earlier by Edelstein and Kelly [10]. Unfortunately, such a direct approach does not generalize for higher values of k. For more discussion about these results, see Appendix A.

[9]Where for $\ell = \mathbf{a} \cdot \mathbf{X}$, $\mathrm{span}(\ell)$ denotes the one dimensional vector space spanned by the vector $\mathbf{a}$

Then there exists a linear form ℓ in the circuit C such that for $C' = C|_{\ell=0}$, pairwise-rank$(C') \geq A$.

A sketch of the proof of this lemma is given in Section 6 and the full proof is given in [18]. With these tools in hand, we are now ready to prove the main theorem of this paper.

5.3. Proof of Theorem 2.2: The Rank Bound

Theorem 2.2 [Rank bound for $\Sigma\Pi\Sigma(k)$ circuits]: *Let* $c(k) = 3^k((k+1)!)^2$. *Let* C *be a simple and minimal* $\Sigma\Pi\Sigma(k)$ *circuit that computes the zero polynomial. Then* rank$(C) \leq c(k)$.

The proof proceeds by an induction on k, the number of multiplication gates in C. We first show that C must have high pairwise-rank. If it does not have high pairwise-rank, then we can use Lemma 5.3 to obtain a new circuit that is still simple and minimal and has high rank, but with fewer multiplication gates. This would contradict the induction hypothesis. We then use Lemma 5.5 to find a linear form ℓ such that the circuit $C' = C|_{\ell=0}$ also has high pairwise-rank, and is such that $C' \equiv 0$, but has fewer multiplication gates. Any minimal subset of the multiplication gates of C' that sums to 0 will give a circuit $C_{\min}$ that also has high pairwise-rank, is minimal, and still computes the zero polynomial. The simplification of $C_{\min}$ will then be simple, minimal, have high rank, and will have fewer than k multiplication gates, contradicting the induction hypothesis.

Proof: We will prove the above theorem by induction on k.

For $k = 1, 2$, the result is vacuously true. Let $k \geq 3$ and assume the theorem is true for $\Sigma\Pi\Sigma(m)$ circuits for all $m \leq k-1$.

If possible let

$$C = \sum_{i=1}^{k} A_i = \sum_{i=1}^{k} \prod_{j=1}^{d} \ell_{ij}$$

be simple and minimal such that $C \equiv 0$, and rank$(C) > c(k)$. Let the indeterminates appearing in C be $X_1, X_2, \ldots, X_n$.

Case 1: pairwise-rank$(C) < c(k) - c(k-1)$. Hence there exist $i, j \in [k]$ such that $i \neq j$ and rank$(\text{Sim}(A_i + A_j)) < c(k) - c(k-1)$. Let $A_i + A_j = \gcd(A_i, A_j) \cdot \text{Sim}(A_i + A_j)$. Without loss of generality, by Lemma 5.1 (equivalence up to linear transformations), let span$((\text{Sim}(A_i + A_j))$[10] be spanned by $X_1, X_2, \ldots, X_t$, where $t = \text{rank}(\text{Sim}(A_i + A_j))$. For each $i \in [t]$, let α_i be a uniformly random real number in $[0, 1]$. For $i \in [t]$, set $X_i = \alpha_i Z$. By Lemma 5.3, with probability 1 we get a (homogeneous) circuit C' such

---

[10]For $C = \sum_{i \in [k]} \prod_{j \in [d]} \ell_{ij}$, we let span$(C) = \text{span}(\{\ell_{ij} \mid i \in [k], j \in [d]\})$

that $C' \equiv 0$, it has at most $k-1$ gates (since after the random substitution, both A_i and A_j will have the same set of linear forms up to scalar multiples, and they can be merged into a single gate), is still minimal, and its gcd has rank at most 1. Also, since $t < c(k) - c(k-1)$ we get that rank of $\text{Sim}(C')$ is strictly greater than $c(k-1)$. Hence $\text{Sim}(C')$ is simple, minimal, computes the zero polynomial, has at most $k-1$ multiplication gates, and has rank strictly greater than $c(k-1)$, contradicting the induction hypothesis.

Case 2: pairwise-rank$(C) \geq c(k) - c(k-1)$. Hence for all $i, j \in [k]$ such that $i \neq j$, rank$(\text{Sim}(A_i + A_j)) \geq c(k) - c(k-1) > c(k)/2 > c(k-1) + 1$. Notice that by choice of the function c, $c(k) \geq 3k^2((c(k-1)+1)+1)$. By Lemma 5.5 (With $A = c(k-1) + 1$ and $B = c(k)$), there exists a linear form ℓ in C such that for $C' = C|_{\ell=0}$, pairwise-rank$(C') \geq c(k-1) + 1$.

Now, since the (multiplication) gates containing ℓ got set to 0, the number of (multiplication) gates in C' (which is the top fanin of C') is at most $k-1$. Also, pairwise-rank$(C') \geq c(k-1) + 1$ implies that for all subsets $S \subseteq [k]$ such that S indexes at least two nonzero gates of C, rank$(\text{Sim}(C'|_S)) \geq c(k-1) + 1$ (where $C'|_S$ is the subcircuit of C' obtained by restricting to only those multiplication gates of C' that are indexed by S). We know that $\sum_{i \in [k]} A_i' = 0$ (where at least one of the A_i' is set to 0). Now take the smallest nonempty such set S for which $\sum_{i \in S} A_i' = 0$. Then, $\sum_{i \in S} A_i'$ is a minimal circuit such that its simple part has rank at least $c(k-1) + 1$. This contradicts the induction hypothesis.

Thus we conclude that rank$(C) \leq c(k)$.

■

6. THE SYLVESTER–GALLAI THEOREM AND THE FANIN REDUCTION LEMMA

In this section we will sketch a proof of the Fanin Reduction Lemma (Lemma 5.5) and highlight the main ingredients in the proof. The full proof is given in [18]. Our proof of the Fanin Reduction Lemma first translates the problem from a question about circuits to a question purely about the incidence properties of colored points in $\mathbb{R}^n$. The main tools that we use in analyzing the points is the Sylvester–Gallai Theorem, and a related Hyperplane Decomposition Lemma. Before we state these results, we first introduce some terminology that we will use.

Affine spaces and hyperplanes. We say that $H \subseteq \mathbb{R}^n$ is an *affine space* if it is a translation of a linear space. In other words, there exists a linear vector space $H' \subseteq \mathbb{R}^n$ and a vector $v \in \mathbb{R}^n$ such that $H = v + H' = \{v + u \mid u \in H'\}$. The dimension $\dim(H)$ of the affine space is the dimension of the corresponding linear space $\dim(H')$. We will be using the term *hyperplane* interchangeably with affine space. In this terminology, a point is a hyperplane of dimension 0, a

line is a hyperplane of dimension 1 etc. For a set $S \subseteq \mathbb{R}^n$ of points, the *affine span* of S, denoted affine-span(S), is the intersection of all the affine spaces containing S. Note that the affine span of a set is also an affine space. Also note the difference between this notion of affine-span and the notion of vector space span[11].

The Sylvester–Gallai Theorem (see the survey by Borwein and Moser [7] for details) asserts the following:

Theorem 6.1: **[Sylvester–Gallai]** Let S be a finite set of points spanning an affine space $V \subseteq R^n$ such that $\dim(V) \geq 2$. Then there exists a line $L \subseteq V$ such that $|L \cap S| = 2$.

We state below the high dimensional Sylvester–Gallai Theorem. It was first proved in a slightly different form by Hansen [14]. The version below is a slightly refined version of Hansen's result, and was obtained by Bonnice and Edelstein [6, Theorem 2.1].

Theorem 6.2: **[Generalized Sylvester–Gallai for high dimensions]** ([14], [6]) Let S be a finite set of points spanning an affine space $V \subseteq \mathbb{R}^n$ such that $\dim(V) \geq 2t$. Then, there exists a t dimensional hyperplane H such that $|H \cap S| = t + 1$, and such that H is spanned by the points of S. i.e affine-span$(H \cap S) = H$.

Using the above result, we obtain the following 'decomposition' theorem. A similar decomposition procedure was carried out by Edelstein and Kelly [10] (to obtain a Sylvester–Gallai kind of theorem for colored points), and by Bonnice and Edelstein [6]. We defer the proof of the Hyperplane Decomposition Lemma (Lemma 6.3) to [18].

Lemma 6.3: **[Hyperplane Decomposition]** Let V be an m dimensional affine space over $\mathbb{R}$. Let $S \subset V$ be a finite set, such that affine-span$(S) = V$. Let $S_{\text{core}} \subseteq S$, and let $H_{\text{core}} = $ affine-span(S_{core}) be an affine space of dimension m_{core}. Then for some $r \geq \frac{m - m_{\text{core}}}{2}$, there exist hyperplanes $H_1, H_2, \ldots, H_r \subset V$, such that letting $H = $ affine-span$(\{H_i \mid i \in [r]\})$, we have the following properties.

1) For all $i \in [r]$, $H_{\text{core}} \subseteq H_i$ and $\dim(H_i) = m_{\text{core}} + 1$.
2) $\dim(H) = m_{\text{core}} + r$. In particular, if $R \subseteq [r]$ is such that for each $i \in R$, P_i is a point in $H_i \setminus H_{\text{core}}$, then $\dim(\text{affine-span}(\{P_i \mid i \in R\})) = |R| - 1$.
3) For all $i \in [r]$, $(H_i \setminus H_{\text{core}}) \cap S \neq \phi$.
4) For every point $P \in S \cap H$, there exists $i \in [r]$ such that $P \in H_i$. Note that it is not necessary that every point in S lies on one of the H_i's but every point of S inside H certainly does lie on at least one of the H_i's.

[11]Informally, as sets, the vector space span of a set of points/vectors S would equal the affine span of $S \cup \{\mathbf{0}\}$, where $\{\mathbf{0}\}$ denotes the origin (or zero vector).

We present below a very informal outline of the proof of the Fanin Reduction Lemma (Lemma 5.5) to demonstrate how the Hyperplane Decomposition Lemma is used in its proof. For the full details of the proof, see [18].

Outline of proof of the Fanin Reduction Lemma: Lemma 5.5: In Section 4.1 we saw how to map the linear forms appearing in the circuit C to colored points in $\mathbb{R}^n$. We will assume the terminology used in Section 4.1. Recall that we want to show that there exists a linear form ℓ in C and the corresponding point P_ℓ such that for all pairs of colors i and j such that ℓ does not occur in A_i and A_j, the set of lines in the pencil $\mathcal{L}_i^{P_\ell} \Delta \mathcal{L}_j^{P_\ell}$ span a high dimensional space. We will use the Hyperplane Decomposition Lemma to accomplish this.

Let the set of points S corresponding to linear forms in C span the affine space V. We choose a (relatively low dimensional) subspace $H_{\text{core}} \subseteq V$ such that for every pair of colors i and j, the symmetric difference of the points of those colors, $S_i \Delta S_j$, contained within H_{core} spans a high dimensional subspace. We apply the Hyperplane Decomposition Lemma to V and H_{core} to get a large collection of hyperplanes $H_1, H_2, \ldots, H_r$ each containing H_{core} and satisfying the properties listed in Lemma 6.3. Let $H = $ affine-span$(H_1, H_2, \ldots, H_r)$. Observe that property (2) implies that if P_i and P_j are two points of S in $H_i \setminus H_{\text{core}}$ and $H_j \setminus H_{\text{core}}$ respectively, then the line through them does not contain any other point of S. This will be a very useful property.

For a pair of colors i, j, let $(S_i \Delta S_j)^H$ denote the set of points in $S_i \Delta S_j$ that lie in $H \setminus H_{\text{core}}$. We say a pair of colors (i, j) is *over-split* if a large subset of the hyperplanes $\{H_i\}$ contain an element of $(S_i \Delta S_j)^H$. Otherwise we say the pair is *under-split*. Since for each pair of under-split colors (i, j) the set $(S_i \Delta S_j)^H$ occurs in few hyperplanes, and since the total number of hyperplanes is large, the pigeon-hole principle implies that there exists a hyperplane H^* that does not contain any member of $(S_i \Delta S_j)^H$ for any under-split pair of colors $\{i, j\}$. By property (3), there exists a point P_ℓ contained in $H^* \setminus H_{\text{core}}$. Let the corresponding linear form be ℓ.

We will show that for all pairs of colors i and j such that ℓ does not occur in A_i and A_j, the set of lines in the pencil $\mathcal{L}_i^{P_\ell} \Delta \mathcal{L}_j^{P_\ell}$ span a high dimensional space. From now on we will only mention pairs of colors corresponding to multiplication gates in the circuit that do not contain ℓ. Now for any pair of colors $\{i, j\}$, since a line through P_ℓ and any point in $(S_i \Delta S_j)^H \setminus H^*$ does not contain any other point of S (by property (3)), the set of such lines is contained in the pencil $\mathcal{L}_i^{P_\ell} \Delta \mathcal{L}_j^{P_\ell}$.

If the pair of colors is over-split, then this pencil will span a high dimensional space, and hence this pair of colors

will not create any worry. If the pair of colors (i, j) is under-split, then recall that $H^* \setminus H_{\text{core}}$ does not contain any element of $(S_i \Delta S_j)^H$. Now consider the intersection of $(S_i \Delta S_j)$ with H_{core} and call it $(S_i \Delta S_j)^{\text{core}}$. Recall that by the choice of H_{core}, $(S_i \Delta S_j)^{\text{core}}$ spans a high dimensional space. Also, any line through P_ℓ and a point of $(S_i \Delta S_j)^{\text{core}}$ lies entirely within H^* and does not contain any other point of H_{core}. Since there are no points of $S_i \Delta S_j$ in $H^* \setminus H_{\text{core}}$, hence any such line is a line in the pencil $\mathcal{L}_i^{P_\ell} \Delta \mathcal{L}_j^{P_\ell}$. Since $(S_i \Delta S_j)^{\text{core}}$ spans a high dimensional space, so does the pencil $\mathcal{L}_i^{P_\ell} \Delta \mathcal{L}_j^{P_\ell}$. Hence under-split pairs of colors do not create a problem either, and we are done.

7. Conclusion

Our paper invites further work in several directions.

1) **Proving the high dimensional Sylvester–Gallai Theorem over the field of complex numbers.** Such a theorem would extend our results on the rank bound and identity testing to the complex numbers. We conjecture the following analogue of Lemma 6.2 over the field $\mathbb{C}$ of complex numbers: *There exists a constant $c \geq 2$ such that if S is a finite set of points spanning an affine space $V \subseteq \mathbb{C}^n$ with $\dim(V) \geq c \cdot t$ then there exists a t dimensional hyperplane $H \subseteq V$ such that $|H \cap S| = t + 1$ and H is spanned by the points of S. i.e* affine-span$(H \cap S) = H$.

2) **Conjecture for Sylvester–Gallai over finite fields.** Such a theorem would extend our results on the rank bound and identity testing to large finite fields. We conjecture that the following version of Sylvester–Gallai is true over finite fields: *There exists a constant $c \geq 2$ such that if p is a prime and S is a subset of points in the 3-dimensional projective space $\mathbb{P}^3(\mathbb{F}_p)$ and $p > |S|^c$, then there exists a pair of points in S such that the line through this pair of points contains no other point from S.*

3) **Devising a blackbox identity testing algorithm over finite fields.** As shown in [19], even the weaker form of the conjecture of Dvir and Shpilka is false over finite fields. Perhaps there is some other neat classification of the structure of depth three arithmetic circuits computing the zero polynomial over finite fields. We challenge the interested reader to devise a blackbox identity testing algorithm for $\Sigma\Pi\Sigma(k)$ circuits over finite fields.

4) **Resolving the stronger Dvir–Shpilka conjecture over fields of characteristic zero.** Prove or disprove that the rank $c(k)$ in Theorem 2.2 can be improved to a polynomially growing function of the top fanin k.

See Appendix A for a discussion on how the first two conjectures will affect our understanding of identity testing.

References

[1] M. Agrawal, "Proving lower bounds via pseudo-random generators," in *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science, 25th International Conference, Hyderabad, India, December 15-18, 2005, Proceedings*, ser. Lecture Notes in Computer Science, R. Ramanujam and S. Sen, Eds., vol. 3821. Springer, 2005, pp. 92–105.

[2] M. Agrawal and S. Biswas, "Primality and identity testing via chinese remaindering," *Journal of the ACM*, vol. 50, no. 4, pp. 429–443, 2003. [Online]. Available: http://doi.acm.org/10.1145/792538.792540

[3] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in p," *Annals of Mathematics*, vol. 160, no. 2, pp. 781–793, 2004.

[4] M. Agrawal and V. Vinay, "Arithmetic circuits: A chasm at depth four," in *FOCS*, 2008, pp. 67–75.

[5] V. Arvind and P. Mukhopadhyay, "The ideal membership problem and polynomial identity testing," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 14, no. 095, 2007.

[6] W. Bonnice and M. Edelstein, "Flats associated with finite sets in $\mathbf{P}^d$," *Niew. Arch. Wisk.*, vol. 15, pp. 11–14, 1967.

[7] P. Borwein and W. O. J. Moser, "A survey of sylvester's problem and its generalizations," *Aequationes Mathematicae*, vol. 40, no. 1, pp. 111–135, 1990.

[8] Z.-Z. Chen and M.-Y. Kao, "Reducing randomness via irrational numbers," *SIAM J. Comput.*, vol. 29, no. 4, pp. 1247–1256, 2000.

[9] Z. Dvir and A. Shpilka, "Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits." in *STOC*, 2005, pp. 592–601.

[10] M. Edelstein and L. M. Kelly, "Bisecants of finite collections of sets in linear spaces," *Canadanian Journal of Mathematics*, vol. 18, pp. 375–380, 1966.

[11] N. D. Elkies, L. M. Pretorius, and C. J. Swanepoel, "Sylvester-gallai theorems for complex numbers and quaternions," *Discrete & Computational Geometry*, vol. 35, no. 3, pp. 361–373, 2006.

[12] A. Gabizon and R. Raz, "Deterministic extractors for affine sources over large fields," in *FOCS*, 2005, pp. 407–418.

[13] D. Grigoriev and M. Karpinski, "An exponential lower bound for depth 3 arithmetic circuits," in *STOC*, 1998, pp. 577–582. [Online]. Available: http://doi.acm.org/10.1145/276698.276872

[14] S. Hansen, "A generalization of a theorem of sylvester on the lines determined by a finite point set," *Mathematica Scandinavia*, vol. 16, pp. 175–180, 1965.

[15] Impagliazzo and Kabanets, "Derandomizing polynomial identity tests means proving circuit lower bounds," in *STOC: ACM Symposium on Theory of Computing (STOC)*, 2003.

[16] Z. S. Karnin and A. Shpilka, "Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in," in *IEEE Conference on Computational Complexity*, 2008, pp. 280–291.

[17] ——, "Reconstruction of generalized depth-3 arithmetic circuits with bounded top fan-in," 2008, manuscript.

[18] N. Kayal and S. Saraf, "Blackbox polynomial identity testing for depth 3 circuits," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 16, no. 032, 2009. [Online]. Available: http://eccc.hpi-web.de/report/2009/032/

[19] N. Kayal and N. Saxena, "Polynomial identity testing for depth 3 circuits," in *Proceedings of the twenty-first Annual IEEE Conference on Computational Complexity (CCC)*, 2006.

[20] L. M. Kelly, "A resolution of the sylvester - gallai problem of j. -p. serre," *Discrete & Computational Geometry*, vol. 1, pp. 101–104, 1986.

[21] A. Klivans and D. A. Spielman, "Randomness efficient identity testing of multivariate polynomials," in *STOC*, 2001, pp. 216–223.

[22] D. Lewin and S. P. Vadhan, "Checking polynomial identities over any field: Towards a derandomization?" in *STOC*, 1998, pp. 438–447.

[23] K. Mulmuley, U. V. Vazirani, and V. V. Vazirani, "Matching is as easy as matrix inversion," *Combinatorica*, vol. 7, no. 1, pp. 105–113, 1987.

[24] N. Saxena and C. Seshadhri, "An almost optimal rank bound for depth-3 identities," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 15, no. 108, 2008.

[25] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *Journal of the ACM*, vol. 27, no. 4, pp. 701–717, 1980. [Online]. Available: http://doi.acm.org/10.1145/322217.322225

[26] A. Shpilka, "Interpolation of depth-3 arithmetic circuits with two multiplication gates," in *STOC*, 2007, pp. 284–293.

[27] A. Shpilka and A. Wigderson, "Depth-3 arithmetic circuits over fields of characteristic zero," *Computational Complexity*, vol. 10, no. 1, pp. 1–27, 2001.

[28] R. Zippel, "Interpolating polynomials from their values," *JSC*, vol. 9, no. 3, pp. 375–403, Mar. 1990.

APPENDIX

The following theorem was proved by Edelstein and Kelly [10].

Theorem A.1: Let A, B and C be 3 nonempty finite disjoint subsets of points in $\mathbb{R}^n$ such that affine-span$(A \cup B \cup C)$ has dimension at least 4 and $A \cap B \cap C = \phi$. Then there exists a line intersecting exactly 2 of the sets A, B, C.

The proof is a clever application of the Sylvester–Gallai Theorem, and uses a special case of the Hyperplane Decomposition Lemma (see the full version [18] for a proof). By the correspondence of linear forms appearing in the circuit with colored points in $\mathbb{R}^n$, this almost immediately gives a rank bound for simple and minimal $\Sigma\Pi\Sigma(3)$ circuits that compute the zero polynomial. For the case of $k = 3$, the connection of the structure theorem to Sylvester–Gallai type theorems was even observed in [9].

The above approach to proving the rank bound, however, does not directly generalize and additional ideas are needed for $k > 3$. One may hope that a suitable generalization of the Edelstein–Kelly result to a larger number of sets might be used to give a rank bound for $k > 3$. For $k = 3$, the linear forms in any *simple* ciruit are used to construct 3 disjoint sets of colors in $\mathbb{R}^n$. However, for $k > 3$, the sets of colors obtained need not be disjoint, and most natural generalizations of the Edelstein-Kelly result are false when the sets are allowed to have nonzero intersection.

Rank bound over other fields. Our proof of the rank bound, Theorem 2.2, uses high dimensional versions of the Sylvester–Gallai Theorem. If the high dimensional Sylvester–Gallai Theorem held over $\mathbb{C}$ or over any other field, then using the techniques of our paper, they would translate to rank bounds for $\Sigma\Pi\Sigma(k)$ circuits over the corresponding field. For $k = 3$, it suffices just to prove a Sylvester–Gallai Theorem for lines and fortunately this is known over $\mathbb{C}$ [20], [11]. The result by Edelstein and Kelly [10] essentially carries over for this case with a dimension bound of 5 instead of 4, and hence we get a rank bound of 6 for $\Sigma\Pi\Sigma(3)$ circuits over complex numbers. Furthermore proving a rank bound over complex numbers implies a rank bound over finite fields of characteristic significantly larger than the degree of the circuit.

In particular, the conjectures given in the conclusion would have the following implications.

Sylvester–Gallai over complex numbers, Conjecture (1): It will give a deterministic blackbox identity testing algorithm for $\Sigma\Pi\Sigma(k)$ circuits (k fixed) over *all* fields of characteristic zero.

Sylvester–Gallai over large finite fields, Conjecture (2): It will give a deterministic blackbox identity testing algorithm for $\Sigma\Pi\Sigma(3, d, n)$ circuits over fields of characteristic $p > \text{poly}(d)$.

Furthermore, using a standard argument involving the Hilbert Nullstellensatz, it can be shown that Conjecture (1) implies high dimensional Sylvester–Gallai over finite fields of characteristic $p > 2^{2^{O(d^2)}}$. Proving conjecture (2) will perhaps require a fundamentally new proof of the Sylvester–Gallai Theorem which somehow manages to avoid the well-ordered property of the real field.