Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 42 (2007)

# Black Box Polynomial Identity Testing of Depth-3 Arithmetic Circuits with Bounded Top Fan-in

Zohar S. Karnin* Amir Shpilka*

**Abstract**

In this paper we consider the problem of determining whether an unknown arithmetic circuit, for which we have oracle access, computes the identically zero polynomial. Our focus is on depth-3 circuits with a bounded top fan-in. We obtain the following results.

1. A quasi-polynomial time deterministic black-box identity testing algorithm for $\Sigma\Pi\Sigma(k)$ circuits (depth-3 circuits with top fan-in equal $k$).
2. A randomized black-box algorithm for identity testing of $\Sigma\Pi\Sigma(k)$ circuits, that uses a poly-logarithmic number of random bits, and makes a single query to the black-box.
3. A polynomial time deterministic black-box identity testing algorithm for multilinear $\Sigma\Pi\Sigma(k)$ circuits (each multiplication gate computes a multilinear polynomial).

Another way of stating our results is in terms of *test sets* for the underlying circuit model. A test set is a set of points such that if two circuits give the same value on every point of the set then they compute the same polynomial. Thus, our first result gives an explicit test set, of quasi-polynomial size, for $\Sigma\Pi\Sigma(k)$ circuits. Our second result yields an explicit test set that any two different $\Sigma\Pi\Sigma(k)$ circuits are different on most points of the set. Our last result gives an explicit polynomial size test set for multilinear $\Sigma\Pi\Sigma(k)$ circuits.

Prior to our work, only depth-2 circuits (circuits computing sparse polynomials) had efficient deterministic black-box identity testing algorithms (in other words, polynomial size test sets). Depth-3 circuits were previously studied in the non black-box model (i.e. when the circuit is given as input), and a polynomial time deterministic algorithm for identity testing was found [KS06]. The question of giving efficient black-box polynomial identity testing algorithm for $\Sigma\Pi\Sigma(3)$ circuits was raised by Klivans and Spielman [KS01], and so, in particular, we answer this question.

The proof technique involves a construction of a family of affine subspaces that have a *rank-preserving* property, that is inspired by the construction of *linear seeded extractors for affine sources* of Gabizon and Raz [GR05], and a theorem regarding the structure of identically zero depth-3 circuits with bounded top fan-in of [DS06].

*Faculty of Computer Science, Technion, Haifa 32000, Israel. Email: {zkarnin,shpilka}@cs.technion.ac.il.
This research was supported by the Israel Science Foundation (grant number 439/06).

ISSN 1433-8092

# Contents

# 1 Introduction

Finding an algorithm for polynomial identity testing (PIT) is a widely pursued open problem: we are given as input a circuit that computes a multivariate polynomial, over some field, and we have to determine whether it computes the zero polynomial. The importance of the polynomial identity testing problem stems from its many applications: Algorithms for primality testing [AB03], for deciding if a graph contains a perfect matching [Lov79, MVV87, CRS95] and more, are based on reductions to the PIT problem (for more applications see the introduction of [LV98]). In this work we consider the problem of determining whether an arithmetic circuit for which we only have oracle access computes the identically zero polynomial. That is, the input is a black-box holding a circuit $C$ and we must find whether the polynomial computed by the circuit $C$ is the identically zero polynomial. In particular we can only ask the circuit for its value on points of our choice. It is clear that every such algorithm must produce a test set for the circuit. Namely, a set of points such that if the circuit vanishes on all the points then the circuit computes the zero polynomial. Note that the values of a circuit on the points in the test set completely determine the circuit, as if two circuits agree on all the points then their difference is zero on all points of the set and therefore their difference must be zero.

## 1.1 Known results

The complexity of the PIT problem is not well understood. It is one of a few problems for which we have coRP algorithms but no deterministic sub-exponential time algorithms. The first randomized black-box PIT algorithm was discovered independently by Schwartz [Sch80] and Zippel [Zip79]. In [LV98, AB03, CK00] randomized algorithms that use fewer random bits were given, however these algorithms need to get the circuit as input, whereas the Schwartz-Zippel algorithm is in the black-box model.

The problem of finding a deterministic algorithm is believed to be difficult. In particular, Kabanets and Impagliazzo [KI04] showed that efficient deterministic algorithms for PIT imply that NEXP does not have polynomial size arithmetic circuits, and vice versa. Namely, derandomization of the PIT problem (i.e. a deterministic sub-exponential time algorithm for PIT) will imply that NEXP $\not\subseteq$ P/poly, or that the Permanent is not computable by small arithmetic circuits. Conversely, [KI04] showed that from super-polynomial lower bounds on the size of arithmetic circuits one can construct a sub-exponential time deterministic algorithm for black-box PIT. However, known lower bounds are too weak and do not yield deterministic PIT algorithms, as suggested by [KI04].

Nevertheless, deterministic polynomial time algorithms for several restricted classes are known: for depth-2 arithmetic circuits (i.e. circuits computing sparse multivariate polynomials) there are many works giving black-box PIT algorithms over various fields [GK87, BOT88, GKS90, CDGK91, Wer94, SS96, KS96, KS01] and for non commutative arithmetic formulas there is a non black-box algorithm [RS05].

In [DS06] a PIT algorithm for depth-3 circuits was given. Their algorithm gets as an input a depth-3 arithmetic circuit with bounded top fan in, and determines whether the circuit computes the zero polynomial or not. The crux of their work is a theorem on the structure of depth-3 arithmetic circuits that compute the zero polynomial. Specifically, for every depth-3 arithmetic circuit with bounded top fan in, if the circuit is simple (i.e. no linear factor appears in all of the multiplication gates) and minimal (i.e. no subset of multiplication gates amounts to a circuit computing the zero polynomial), then the dimension of the linear space spanned by all the linear functions in the circuit is small. By small we mean constant in the multilinear case and polylogarithmic in the general case. The algorithm of [DS06] runs in quasi-polynomial time in the general case (and polynomial time

in the multilinear case). This result was later improved by Kayal and Saxena [KS06] who gave a polynomial time algorithm using a different approach. For our results however, we shall need the structural theorem of [DS06].

In this work we give a sub-exponential deterministic black-box algorithm for PIT of depth-3 circuits with bounded top fan-in. More precisely, the running time of our algorithm is similar to the running time of the non black-box algorithm of [DS06]. This is the first sub-exponential PIT algorithm in the black-box model for a class of circuits other than the widely studied class of depth-2 circuits. Before giving a formal statement of our results we need some definitions.

### 1.2 Some definitions and statement of our results

Let $f$ be a polynomial computed by a depth-3 circuit with $k$ multiplication gates (also known as $\Sigma\Pi\Sigma(k)$ circuit), over some field $\mathbb{F}$. Then $f$ has the following form:

$$f(\bar{x}) = \sum_{i=1}^{k} M_i = \sum_{i=1}^{k} \prod_{j=1}^{d_i} L_{i,j}(\bar{x}) \tag{1}$$

where the $L_{i,j}$'s are linear functions, over $\mathbb{F}$, in the variables $\bar{x} = (x_1, \ldots, x_n)$ and $M_1, \ldots, M_k$ are the multiplication gates of the circuit. Namely, $M_i = \prod_{j=1}^{d_i} L_{i,j}$. For a $\Sigma\Pi\Sigma(k)$ circuit $C$ we denote with $\deg(C)$ the maximal degree of its multiplication gates (i.e. $\max_{i=1}^{k}\{d_i\}$). The size of a $\Sigma\Pi\Sigma$ circuit is defined as the sum of degrees of the multiplication gates of the circuit (thus, the size of the circuit from Equation (1) is $\sum_{i=1}^{k} d_i$). We will denote the size of a circuit $C$ by $\text{size}(C)$. We denote with $\Sigma\Pi\Sigma(k,d)$ the family of $\Sigma\Pi\Sigma(k)$ circuits of degree $d$. The following theorems summarize our results for general $\Sigma\Pi\Sigma(k)$ arithmetic circuits:

**Theorem 1** (Deterministic algorithm for general circuits)**.** *Let $C$ be a $\Sigma\Pi\Sigma(k,d)$ circuit over a field $\mathbb{F}$, in $n$ indeterminates, for some constant $k$. Then there is a deterministic black-box algorithm that on input $k, d, n$ and black-box access to $C$ determines whether $C$ computes the zero polynomial. The running time of the algorithm is $\text{poly}(n,d) \cdot \exp\left((\log d)^{k-1}\right)$. If $|\mathbb{F}| \leq O(\deg(C)^3 \cdot n)$ then the algorithm is allowed to make queries to $C$ from an algebraic extension field of $\mathbb{F}$ of polynomial size.*

**Theorem 2** (Randomized algorithm for general circuits)**.** *Let $C$ be a $\Sigma\Pi\Sigma(k,d)$ circuit over a field $\mathbb{F}$, in $n$ indeterminates, for some constant $k$. Then there is a CoRP randomized black-box algorithm that on input $\epsilon, k, d, n$ makes a single query to (a black-box holding) $C$ and determines whether $C \equiv 0$. Namely, if $C \not\equiv 0$ then the algorithm outputs "non-zero circuit" with probability at least $1 - \epsilon$ and if $C \equiv 0$ then the algorithm always outputs "zero circuit". The number of random bits used by the algorithm is $O(\log 1/\epsilon \cdot (\log d)^{k-2} + \log n)$. If $|\mathbb{F}| \leq O(\deg(C)^3 \cdot n)$ then the algorithm is allowed to make queries to $C$ from an algebraic extension field of $\mathbb{F}$ of polynomial size.*

A multilinear $\Sigma\Pi\Sigma(k)$ circuit is a circuit in which every multiplication gate computes a multilinear polynomial. For multilinear $\Sigma\Pi\Sigma(k)$ arithmetic circuits, we obtain the following result:

**Theorem 3** (Deterministic algorithm for multilinear circuits)**.** *Let $C$ be a multilinear $\Sigma\Pi\Sigma(k)$ circuit in $n$ indeterminates over a field $\mathbb{F}$ where $k$ is a constant. Then there is a deterministic polynomial time (in the number of variables) black-box algorithm that on input $k, n$ and black-box access to $C$ determines whether $C$ computes the zero polynomial. If $|\mathbb{F}| \leq O(n^3 \cdot k^2)$, then the algorithm is allowed to make queries to $C$ from an algebraic extension field of $\mathbb{F}$ of polynomial size.*

### 1.3 Our techniques

The idea behind our algorithm is the following: we consider several linear subspaces of $\mathbb{F}^n$ of "small" dimension, and for each subspace $V$ we verify that $C|_V \equiv 0$. Note, that the verification step requires $O(\deg(C)^{\dim(V)})$ time using simple (brute force) interpolation. Clearly if $C \equiv 0$ then we will get that $C|_V \equiv 0$. However, it is not clear why $C \equiv 0$ if all we know is that $C|_V \equiv 0$, for every subspace $V$ in our family. Indeed, for general circuits we cannot show that such a naive approach works, but in the case of $\Sigma\Pi\Sigma(k)$ circuits we have a structural theorem due to [DS06] that (roughly) says that if $C \equiv 0$ then it can be written as a sum of circuits, that are all identically zero, and such that each of the circuits essentially depends on a few linear functions (the complete statement of this theorem is given in Section 2.1). Thus, the structural theorem implies that for every subspace $V$, if $C|_V \equiv 0$ then it has the above structure. If we were guaranteed that for some $V$ the "structure" of $C$ remains (more or less) the same when restrict it to $V$, then the fact that $C|_V \equiv 0$ will imply that $C \equiv 0$.

The idea for finding the subspace on which we will evaluate the restriction of $C$ comes from the construction of *linear seeded extractors for affine sources* of [GR05]. In their work Gabizon and Raz constructed a set of linear transformations from $\mathbb{F}^n$ to $\mathbb{F}^r$ such that for every linear subspace of dimension $r$, at least one of the transformations (actually most of the transformations) maps it onto the entire space. It turns out that by applying the idea of [GR05] we can construct a family of subspaces that retains the structure of $\Sigma\Pi\Sigma(k)$ circuits, and therefore get a deterministic black-box PIT algorithm.

### 1.4 Organization

The paper is organized as follows. In section 2 we give some background on depth-3 arithmetic circuits. In section 3 we prove our results for general $\Sigma\Pi\Sigma(k)$ arithmetic circuits. Finally, in section 4 we give more efficient algorithms for the special case of multilinear $\Sigma\Pi\Sigma(k)$ circuits.

## 2 Preliminaries

For a positive integer $k$ we denote $[k] = \{1, \ldots, k\}$. Let $\mathbb{F}$ be a field. We denote with $\mathbb{F}^n$ the $n$'th dimensional vector space over $\mathbb{F}$. For a vector $v \in \mathbb{F}^n$ we denote with $|v|$ the number of non zero entries of $v$. We denote with $\{e_i\}_{i\in[n]}$, the natural basis for $\mathbb{F}^n$. That is, $e_i$ is an $n$-dimensional vector that has 1 in the $i$-th coordinate and zeroes elsewhere. We shall use the notation $\bar{x} = (x_1, \ldots, x_n)$ to denote the vector of $n$ indeterminates. For two linear functions $L_1, L_2$ we write $L_1 \sim L_2$ whenever $L_1$ and $L_2$ are linearly dependent. The same notations will be used for vectors. Let $V = V_0 + v_0 \subseteq \mathbb{F}^n$ be an affine subspace, where $v_0 \in \mathbb{F}^n$ and $V_0 \subseteq \mathbb{F}^n$ is a linear subspace. Let $L(\bar{x})$ be a linear function. We denote with $L|_V$ the restriction of $L$ to $V$. Assume the dimension of $V_0$ is $t$, then $L|_V$ can be viewed as a linear function of $t$ indeterminates in the following way: Let $\{v_i\}_{i\in[t]}$ be a basis for $V_0$. For $v \in V$ let $v = \sum_{i=1}^{t} y_i \cdot v_i + v_0$ be its representation according to the basis. We get that $L(v) = \sum_{i=1}^{t} y_i \cdot L(v_i) + L(v_0) \stackrel{\triangle}{=} L|_V(y_1, \ldots, y_t)$. We shall abuse notation and use both $L|_V(v)$ and $L|_V(y_1, \ldots, y_t)$ to denote the value of $L$ on $v \in V$.

A linear function $L$ will sometimes be viewed as a vector of $n+1$ entries. Namely, the function $L(x_1, \ldots, x_n) = \sum_{i=1}^{n} \alpha_i \cdot x_i + \alpha_0$ corresponds to the vector of coefficients $(\alpha_0, \alpha_1, \ldots, \alpha_n)$. Accordingly, we define the span of a set of linear functions of $n$ variables as the span of the corresponding vectors (i.e. as a subspace of $\mathbb{F}^{n+1}$). For an affine subspace $V = V_0 + v_0$ of dimension $t$, the linear function $L|_V$ can be viewed as a vector of $t+1$ entries. Thus, $V$, equipped with a basis $\{v_i\}_{i\in[t]}$ for $V_0$, defines a linear transformation from $\mathbb{F}^{n+1}$ to $\mathbb{F}^{t+1}$. We shall sometimes refer to this transformation as the linear transformation corresponding to the affine subspace $V$, and denote it with $T_V$.

### 2.1 Depth 3 Arithmetic circuits

The following notions will be used throughout this paper.

**Definition 4.** *Let $C$ be a $\Sigma\Pi\Sigma(k)$ arithmetic circuit that computes a polynomial as in Equation (1).*

1. *For each $A \subseteq [k]$, we define $C_A(\bar{x})$ to be a sub-circuit of $C$ as follows:*

$$C_A(\bar{x}) = \sum_{i \in A} M_i(\bar{x}).$$

2. *Define* $\gcd(C)$ *as the product of all the non-constant linear functions that belong to all the multiplication gates. i.e.* $\gcd(C) = \text{g.c.d.}(M_1, \ldots, M_k)$. *A circuit will be called simple if* $\gcd(C) = 1$.

3. *The simplification of* $C$, $\text{sim}(C)$ *is defined as* $\text{sim}(C) \stackrel{\Delta}{=} C/\gcd(C)$.

4. *We define* $\text{rank}(C)$ *as the dimension of the span of the linear functions in* $C$.

For a linear function $L$ and a $\Sigma\Pi\Sigma(k)$ arithmetic circuit $C$, we will use the term $L \in C$ as an indication that the linear function $L$ appears as a factor in one of the multiplication gates of $C$. We will sometimes denote a $\Sigma\Pi\Sigma(k)$ circuit as a $\Sigma\Pi\Sigma(k, d)$ circuit, where $d$ denotes the degree of $C$.

We use the notation $C \equiv 0$ to denote the fact that a $\Sigma\Pi\Sigma(k)$ circuit computes the identically zero polynomial. Notice that this is a syntactic definition, we are thinking of the circuit as computing a polynomial and not a function over the field. Let $C \equiv 0$ be a $\Sigma\Pi\Sigma(k)$ circuit. We say that $C$ is minimal if there is no $\emptyset \neq A \subsetneq [k]$ such that $C_A \equiv 0$. The following theorem of [DS06] gives a bound on the rank of $\Sigma\Pi\Sigma(k, d)$ identically zero arithmetic circuits:

**Theorem 5** (Lemma 5.2 of [DS06])**.** *Let $k \geq 3$ and $C \equiv 0$ be a simple and minimal $\Sigma\Pi\Sigma(k, d)$ circuit, of degree $d \geq 2$. Then* $\text{rank}(C) < 2^{O(k^2)} \log^{k-2}(d)$.

For convenience, we define $R(k, d) = 2^{O(k^2)} \log^{k-2}(d)$ as the bound on the rank given by Theorem 5. It follows that $R(k, d)$ is larger than the rank of any identically zero simple and minimal $\Sigma\Pi\Sigma(k, d)$ circuit. The following theorem gives a bound on the rank of multilinear $\Sigma\Pi\Sigma(k)$ circuits that are identically zero.

**Theorem 6** (Corollary 6.9 of [DS06])**.** *There exists a function $R_M(k) = 2^{O(k^2)}$ such that every multilinear $\Sigma\Pi\Sigma(k)$ circuit $C$ that is simple, minimal and equal to zero, satisfies* $\text{rank}(C) < R_M(k)$.

Specifically, $R_M(k)$ denotes the minimal integer larger than the rank of any identically zero simple and minimal multilinear $\Sigma\Pi\Sigma(k)$ circuit. This theorem will be used in section 4, where we discuss multilinear circuits.

## 3 Black-box PIT algorithm for general $\Sigma\Pi\Sigma(k)$ circuits

In this section we give PIT algorithms for general $\Sigma\Pi\Sigma(k)$ arithmetic circuits. As detailed in section 1.3, the algorithms are based on a construction of a small hitting set for $\Sigma\Pi\Sigma(k)$ circuits, that is composed from the union of several low dimensional subspaces. The section is organized as follows: In Section 3.1 we define the notion of a rank-preserving subspace for a $\Sigma\Pi\Sigma(k)$ circuit $C$. We then prove that if $V$ is rank-preserving for $C$ then $C|_V \equiv 0$ if and only if $C \equiv 0$. In Section 3.2 we find a small set of subspaces such that for each $\Sigma\Pi\Sigma(k)$ circuit $C$, there exist a subspace $V$ in the set that is rank-preserving for $C$. Finally in Section 3.3 we present our algorithms and give their analysis.

### 3.1 Rank-preserving affine subspaces

In this section we present the notion of a rank-preserving subspace for a $\Sigma\Pi\Sigma(k,d)$ circuit $C$. We then prove that in order to determine whether $C \equiv 0$ it suffices to check whether $C|_V \equiv 0$.

**Definition 7.** *Let $C$ be a $\Sigma\Pi\Sigma(k,d)$ arithmetic circuit and $V$ an affine subspace. We say that $V$ is rank-preserving for $C$ if the following properties hold:*

1. *For every two linear functions $L_1, L_2 \in C$ that are linearly independent, their restrictions $L_1|_V, L_2|_V$ are linearly independent. In other words, $L_1 \sim L_2$ if and only if $L_1|_V \sim L_2|_V$.*
2. *$\forall A \subseteq [k]$, $\text{rank}(\text{sim}(C_A)|_V) \geq \min\{\text{rank}(\text{sim}(C_A)), R(k,d)\}$.*

The following lemma lists some of the useful properties of rank-preserving subspaces.

**Lemma 8.** *Let $C$ be a $\Sigma\Pi\Sigma(k)$ circuit and $V$ be a rank-preserving affine subspace for $C$. Then we have the following:*

1. *For every $\emptyset \neq A \subset [k]$, $V$ is rank-preserving for $C|_A$.*
2. *$V$ is rank-preserving for $\text{sim}(C)$.*
3. *$\text{gcd}(C)|_V = \text{gcd}(C|_V)$.*
4. *$\text{sim}(C)|_V = \text{sim}(C|_V)$.*

*Proof.* The first and second claims follow immediately from the definition of $V$. The third claim is implied from the observation that no new linear functions are added to the g.c.d. (as otherwise there will be two linearly independent linear functions in $C$ that become dependent when restricted to $V$, in contradiction to Property 1 of Definition 7). The fourth claim is a direct consequence of the third claim and the definition of $\text{sim}(C)$. □

The main theorem of this section shows that if $V$ is rank-preserving for $C$ then $C|_V \equiv 0$ if and only if $C \equiv 0$.

**Theorem 9.** *Let $C$ be a $\Sigma\Pi\Sigma(k)$ arithmetic circuit and let $V$ be a rank-preserving affine linear subspace for $C$. If $C|_V \equiv 0$ then $C \equiv 0$.*

*Proof.* The proof is in three steps. We first prove the theorem for the case that $C|_V$ (which is identically zero) is simple and minimal. We then remove the simplicity assumption, and finally we remove the minimality assumption.

Assume that $C|_V$ is identically zero simple and minimal. As $C|_V$ is simple we get that $C$ is simple as well. By Theorem 5 we get that $\text{rank}(C|_V) < R(k,d)$. From the assumption that $V$ is rank-preserving for $C$ and from Property 2 of Definition 7 (applied for $A = [k]$) we get that $\text{rank}(C|_V) \geq \text{rank}(C)$, and thus

$$\text{rank}(C|_V) = \text{rank}(C).$$

Denote by $r$ the rank of the circuit $C$. Let $L_1, \ldots, L_r$ be linear functions forming a basis to the subspace spanned by the linear functions of $C$. In particular, there exist a polynomial $P$ such that

$$C \equiv P(L_1, \ldots, L_r).$$

Obviously,

$$C|_V \equiv P(L_1|_V, \ldots, L_r|_V).$$

The fact that $\text{rank}(C|_V) = \text{rank}(C)$ implies that $L_1|_V, \ldots, L_r|_V$ are linearly independent. Hence, for every $x \in \mathbb{F}^n$ there exists $y \in V$ such that $(L_1(x), \ldots, L_r(x)) = (L_1(y), \ldots, L_r(y)) = (L_1|_V(y), \ldots, L_r|_V(y))$. In particular, as $P(L_1|_V, \ldots, L_r|_V) \equiv 0$ it follows that $P(L_1, \ldots, L_r) \equiv 0$. Hence, $C \equiv 0$.

We now remove the simplicity assumption. Assume that $C|_V$ is identically zero minimal $\Sigma\Pi\Sigma(k)$ circuit. In a nutshell, the proof for this case has the following form:

$$C|_V \equiv 0 \overset{(1)}{\Rightarrow} \text{sim}(C|_V) \equiv 0 \overset{(2)}{\Rightarrow} \text{sim}(C)|_V \equiv 0 \overset{(3)}{\Rightarrow} \text{sim}(C) \equiv 0 \overset{(4)}{\Rightarrow} C \equiv 0 \tag{2}$$

We now explain each of the implications in Equation (2).

- Implication (1) follows if we prove that $\gcd(C)|_V \neq 0$. Indeed, Property 1 of Definition 7 guarantees that no two linearly independent linear functions become dependent when restricted to $V$. In particular no non-zero linear function was restricted to zero (we ignore the trivial case that $C$ contains only one linear function).

- This implication follows immediately from Lemma 8.

- Implication (3) follows from the fact that $\text{sim}(C)|_V$ is a simple and minimal identically zero $\Sigma\Pi\Sigma(k)$ circuit, for which we proved that $\text{sim}(C)|_V \equiv 0$ implies that $\text{sim}(C) \equiv 0$ (recall that if $V$ is rank-preserving for $C$ then it is also rank-preserving for $\text{sim}(C)$).

- Step (4) follows immediately from the definition of $\text{sim}(C)$.

We now prove the general case, that is we just assume that $C|_V \equiv 0$. Clearly there exists a partition $A_1, \ldots, A_s$ of $[k]$ such that for every $i \in [s]$ we have that $C_{A_i}|_V$ is an identically zero minimal $\Sigma\Pi\Sigma(k_i)$ circuit, for $k_i = |A_i|$. Recall that Definition 7 implies that $V$ is also rank-preserving for $C_{A_i}$. Hence, by what we just showed for minimal circuits, we get that $C_{A_i} \equiv 0$. It follows that $C = \sum_{i=1}^{s} C_{A_i} \equiv 0$. This completes the proof of the theorem. □

### 3.2 Construction of rank-preserving subspaces

So far we have proved that the restriction of a circuit to a rank-preserving subspace can be used to determine whether the original circuit computes the identically zero polynomial. Our next goal is to obtain such a subspace. In this section, we find a small set of affine subspaces that contains a rank-preserving subspace for every possible $\Sigma\Pi\Sigma(k, d)$ arithmetic circuit. Namely, if the restriction of a $\Sigma\Pi\Sigma(k, d)$ circuit to each of the subspaces in the set computes the zero polynomial, then so does the circuit itself.

Notice that the properties of rank-preserving subspaces refer to the linear transformation corresponding to the subspace (recall the definition from Section 2). It turns out that in [GR05] Gabizon and Raz make use of linear transformations with very similar properties. As a consequence, our construction is heavily based on the construction of [GR05].

The section will be organized as follows. We first present a lemma from [GR05], slightly modified to suit our notations and needs. We proceed by defining a subspace such that the transformation corresponding to the subspace is the same transformation defined in [GR05]. We finish the section with the a theorem that shows the equivalence between the rank preserving properties of the transformations of [GR05] and rank-preserving properties of the subspaces that we constructed.

Recall that the number of indeterminates of a circuit $C$ is denoted as $n$. Let $t \leq n$ denote some fixed integer whose exact value will be presented later.

**Lemma 10** (Lemma 6.1 of [GR05])**.** *Let $\alpha \in \mathbb{F}$ be some fixed element of the field. Denote $\varphi_\alpha : \mathbb{F}^{n+1} \to \mathbb{F}^{t+1}$ as the following linear transformation:*

$$\varphi_\alpha(a_0, \ldots, a_n) = \left( \sum_{i=0}^{n} a_i \alpha^i, \sum_{i=0}^{n} a_i \alpha^{2i}, \ldots, \sum_{i=0}^{n} a_i \alpha^{(t+1)i} \right).$$

*Fix any number of subspaces $W_1, \ldots, W_s \subseteq \mathbb{F}^{n+1}$ of dimension not larger than $t+1$. Then there are at most $s \cdot n \cdot \binom{t+2}{2}$ elements $\alpha \in \mathbb{F}$ for which there exists $i \in [s]$ such that $\dim(\varphi_\alpha(W_i)) < \dim(W_i)$. In other words, for all but $s \cdot n \cdot \binom{t+2}{2}$ elements of $\mathbb{F}$ we have that $\forall i \in [s]$, $\dim(\varphi_\alpha(W_i)) = \dim(W_i)$.*

For completeness we give the proof of the lemma in Appendix A. We now define, for each $\alpha \in \mathbb{F}$, an affine linear subspace $V_\alpha$ such that its corresponding linear transformation is $\varphi_\alpha$. That is, by the notations of Section 2, $T_{V_\alpha} = \varphi_\alpha$.

**Definition 11.** *Let $\alpha \in \mathbb{F}$ be an element of the field and let $t = 2^k \cdot R(k,d)$.*

- *For $0 \le i \le t$ let $v_{i,\alpha} \in \mathbb{F}^n$ be the following vector*

$$v_{i,\alpha} = (\alpha^{i+1}, \ldots, \alpha^{n(i+1)}).$$

- *Let $P_\alpha$ be the matrix who's $j$-th column (for $1 \le j \le t$) is $v_{j,\alpha}$. Namely,*

$$P_\alpha = (v_{1,\alpha}, \ldots, v_{t,\alpha}) = \begin{pmatrix} \alpha^2 & \alpha^3 & \ldots & \alpha^{t+1} \\ \alpha^4 & \alpha^6 & \ldots & \alpha^{2(t+1)} \\ \vdots & \ddots & & \vdots \\ \alpha^{2n} & & \ldots & \alpha^{n(t+1)} \end{pmatrix}.$$

- *Let $V_{0,\alpha}$ be the linear subspace spanned by $\{v_i\}_{i \in [t]}$. Let $V_\alpha \subseteq \mathbb{F}^n$ be the affine subspace $V_\alpha = V_{0,\alpha} + v_{0,\alpha}$. In other words,*

$$V_\alpha = \left\{ P_\alpha \bar{y} + v_{0,\alpha} \ : \ \bar{y} \in \mathbb{F}^t \right\}.$$

**Claim 12.** *For every $\alpha \in \mathbb{F}$, $T_{V_\alpha} = \varphi_\alpha$, where $T$ is defined w.r.t. the basis $\{v_{i,\alpha}\}_{i \in [t]}$ of $V_{0,\alpha}$.*

*Proof.* Let $L$ be a linear function in $n$ variables, given by the equation $L(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{n} a_i x_i$. We need to show that the vector corresponding to $L|_{V_\alpha}$ is equal to $\varphi_\alpha(a_0, \ldots, a_n)$. Namely, we would like to show that the vector of coefficients of $L|_{V_0}$, with respect to the basis $\{v_{i,\alpha}\}_{i \in [t]}$ of $V_{0,\alpha}$, is

$$\left( \sum_{i=0}^{n} a_i \alpha^i, \sum_{i=0}^{n} a_i \alpha^{2i}, \ldots, \sum_{i=0}^{n} a_i \alpha^{(t+1)i} \right).$$

For convenience, we denote $L|_{V_\alpha}(y_1, \ldots, y_t) = \sum_{i=1}^{t} b_i y_i + b_0$. In other words, $b_i$ $(0 \le i \le t)$ is the $i$'th entry of the vector corresponding to $L|_{V_\alpha}$. Denote $\bar{a} = (a_1, \ldots, a_n)$. We get that

$$L|_{V_\alpha}(\bar{y}) = L\left( \sum_{i=1}^{t} y_i \cdot v_{i,\alpha} + v_{0,\alpha} \right) = \bar{a} \cdot (P_\alpha \cdot y) + \bar{a} \cdot v_{0,\alpha} + a_0 = (\bar{a} \cdot P_\alpha) \cdot y + \bar{a} \cdot v_{0,\alpha} + a_0.$$

The free term in this equation is

$$b_0 = \bar{a} \cdot v_{0,\alpha} + a_0 = \sum_{i=0}^{n} a_i \alpha^i.$$

For $1 \leq j \leq t$ we have that

$$b_j = (\bar{a} \cdot P_\alpha)_j = \sum_{i=0}^{n} a_i \alpha^{(j+1)i}$$

as required. □

We are now set to prove the main theorem of this section that shows that for a fixed $\Sigma\Pi\Sigma(k,d)$ circuit $C$, except of a small number of $\alpha \in \mathbb{F}$, we have that $V_\alpha$ is rank-preserving for $C$.

**Theorem 13.** *Let $C$ be a $\Sigma\Pi\Sigma(k,d)$ arithmetic circuit over a field $\mathbb{F}$. Let $t = 2^k \cdot R(k,d)$. There are at most $n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}$ different $\alpha \in \mathbb{F}$ such that $V_\alpha$ is not rank-preserving for $C$.*

*Proof.* The proof is in two steps. First we construct several subspaces (that are defined using linear functions from $C$) where each is of dimension $\leq t$, such that if $\varphi_\alpha$ preserves the rank of all of them then $V_\alpha$ is a rank-preserving subspace for $C$. We then use lemma 10 to prove that except a small number of $\alpha$-s, $\varphi_\alpha$ indeed preserves the rank of all those subspaces.

We first define a set of subspaces such that if $\varphi_\alpha$ preserves the rank of all them then $V_\alpha$ has Property 1 of Definition 7. Denote by $\{L_i\}_{i\in[l]}$ the linear functions appearing in $C$. For each pair of linearly independent linear functions $L_i, L_j$ denote with $W_{i,j}$ the subspace spanned by the vectors corresponding to $L_i$ and $L_j$. Assume that $\dim(\varphi_\alpha(W_{i,j})) = \dim(W_{i,j})$, for every $W_{i,j}$. It follows that if $L_i$ and $L_j$ are linearly independent then so are $L_i|_{V_\alpha}$ and $L_j|_{V_\alpha}$. Hence, $V_\alpha$ satisfies Property 1 of Definition 7.

We now construct a subspace that will ensure that $V_\alpha$ satisfies Property 2 of definition 7. Let $A_1, \ldots, A_{2^k-1}$ be all the nonempty subsets of $[k]$. Define $R_i = \operatorname{rank}(\operatorname{sim}(C_{A_i}))$, and $r_i = \min(R_i, R(k,d))$. For each $A_i$ let $\{L_{i,1}, \ldots, L_{i,r_i}\}$ be a set of $r_i$ linearly independent linear functions that appear in $\operatorname{sim}(C_{A_i})$. Let $v_{i,1}, \ldots, v_{i,r_i}$ be the corresponding set of vectors. Define $W_0$ as the span of all these vectors, i.e.

$$W_0 = \operatorname{span}\left\{v_{i,j} \mid i \in [2^k-1], j \in [r_i]\right\}.$$

Fact 12 shows that $L_{i,j}|_{V_\alpha}$ corresponds to $\varphi_\alpha(v_{i,j})$. Therefore, if $\dim(\varphi_\alpha(W_0)) = \dim(W_0)$ then, for every $i \in [2^k-1]$, we have that

$$\dim(\operatorname{span}\{v_{i,1}, \ldots, v_{i,r_i}\}) = \dim(\operatorname{span}\{\varphi_\alpha(v_{i,1}), \ldots, \varphi_\alpha(v_{i,r_i})\}).$$

Hence, if $\operatorname{rank}(\operatorname{sim}(C_{A_i})) = R_i \leq R(k,d)$ then $\operatorname{rank}(\operatorname{sim}(C_{A_i})) = \operatorname{rank}(\operatorname{sim}(C_{A_i})|_{V_\alpha})$. Otherwise, if $\operatorname{rank}(\operatorname{sim}(C_{A_i}) > R(k,d))$ then $r_i = R(k,d)$ and $\operatorname{rank}(\operatorname{sim}(C_{A_i})|_{V_\alpha}) \geq R(k,d)$. Namely, condition 2 of definition 7 is fulfilled when $\dim(\varphi_\alpha(W_0)) = \dim(W_0)$.

It is clear that we defined at most $\binom{l}{2}+1 \leq \binom{kd}{2}+1$ subspaces. Lemma 10 implies that there are at most $n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}$ possible values of $\alpha$ for which $\dim(\varphi_\alpha(W)) < \dim(W)$ for any of the our subspaces. Thus, except for $n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}$ many $\alpha$-s, all the $V_\alpha$-s are rank-preserving for $C$. □

The following corollary shows how to get a small set of subspaces such that for every $\Sigma\Pi\Sigma(k,d)$ circuit $C$, most of the subspaces are rank-preserving for $C$.

**Corollary 14.** *Let $t = 2^k \cdot R(k,d)$ and $S \subseteq \mathbb{F}$ be a set of $n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}/\epsilon$ different elements of the field[1]. Then, for every $\Sigma\Pi\Sigma(k,d)$ arithmetic circuit $C$ over $\mathbb{F}$ there are at least $(1-\epsilon)|S|$ elements $\alpha \in S$ such that $V_\alpha$ is a rank-preserving subspace for $C$.*

[1]Recall our assumption that if $|\mathbb{F}|$ is not large enough then we work over an algebraic extension field of $\mathbb{F}$.

### 3.3 The PIT algorithm for general $\Sigma\Pi\Sigma(k)$ circuits

We now present our algorithms for the general case and prove Theorems 1 and 2. Algorithm 1 gives a quasi-polynomial time deterministic algorithm for PIT of $\Sigma\Pi\Sigma(k)$ circuits and Algorithm 2 gives an efficient randomized algorithm that makes a single query to the black-box.

**Algorithm 1** Deterministic black-box PIT algorithm for depth-3 arithmetic circuits

Input: $k, n, d \in \mathbb{Z}$, and oracle access to a $\Sigma\Pi\Sigma(k,d)$ circuit $C$ in $n$ input variables.
Output: Determine whether $C \equiv 0$.

Set $t = 2^k \cdot R(k,d)$. For $\alpha \in \mathbb{F}$ let $P_\alpha$ be the $n \times t$ matrix for which $(P_\alpha)_{i,j} = \alpha^{i(j+1)}$. Let $v_{0,\alpha} = \left(\alpha, \alpha^2, \ldots, \alpha^n\right)$. Let $S, T \subseteq \mathbb{F}$ be subsets such that $|S| = n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}+1$ and $|T| = d+1$. Define

$$\mathcal{H} = \left\{P_\alpha \bar{y} + v_{0,\alpha} \ : \ \alpha \in S \ \text{ and } \ \bar{y} \in T^t\right\}.$$

If for every $p \in \mathcal{H}$, $C(p) = 0$, then return "zero circuit".
Else, return "non-zero circuit".

**Lemma 15.** *Let $C$ be a $\Sigma\Pi\Sigma(k,d)$ arithmetic circuit. Then Algorithm 1, when given $k, d, n$ as input and black-box access to $C$, return "zero circuit" if and only if $C \equiv 0$. The running time of the algorithm is $|S|(d+1)^t$ $(= \mathrm{poly}(n) \cdot \exp((\log d)^{k-1}))$.*

*Proof.* The claim regarding the running time is clear as the running time is equal to $|\mathcal{H}|$ and we have

$$|\mathcal{H}| = \left(n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}+1\right)\cdot(d+1)^t.$$

We now prove the correctness of the algorithm. For $\alpha \in S$ let $V_\alpha = \left\{P_\alpha \bar{y} + v_{0,\alpha} \ : \ \bar{y} \in \mathbb{F}^t\right\}$. Denote $\mathcal{H}_\alpha = \left\{P_\alpha \bar{y} + v_{0,\alpha} \ : \ \bar{y} \in T^t\right\}$. In other words, $\mathcal{H}_\alpha$ corresponds to a box isomorphic to $T^t$ inside $V_\alpha$. Theorem 13 implies that if $C \not\equiv 0$ then for some $\alpha \in S$, we have that $C|_{V_\alpha} \not\equiv 0$. Note that as $C|_{V_\alpha}$ is a polynomial of degree at most $d$ in $\{y_i\}_{i\in[t]}$ then by the Schwartz-Zippel lemma below (see [Sch80, Zip79]) we have that $C|_{V_\alpha} \equiv 0$ if and only if $C|_{\mathcal{H}_\alpha} = 0$. In particular $C \equiv 0$ if and only if $C|_{\mathcal{H}} = 0$. □

**Lemma 16** (Schwartz-Zippel)**.** *Let $f(x_1, ..., x_m)$ be a non-zero polynomial of degree $d$ in $m$ variables over a field $\mathbb{F}$. Let $S \subset \mathbb{F}$ be a subset of the field. Then the probability that $f$ vanishes on a randomly chosen input from $S^m$ is bounded by*

$$\Pr_{\bar{x}\in_R S^m}[f(x_1, ..., x_m) = 0] \leq \frac{d}{|S|}.$$

*In particular, if $|S| > d$ and $f \neq 0$ then $f|_{S^m} \neq 0$.*

Theorem 1 now follows easily.

*Proof of Theorem 1.* By Lemma 15 we have that Algorithm 1 decides correctly whether $C \equiv 0$ and runs in time $\left(n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}+1\right)\cdot(d+1)^t$ for $t = 2^k \cdot R(k,d)$. As $R(k,d) = O\left((\log d)^{k-2}\right)$ the theorem follows. □

From Lemma 16 it is clear that if we make the set $T$ large enough then if $C \not\equiv 0$ then a random input from $\mathcal{H}$ will be a non-zero of $C$ with high probability. This is formalized in Algorithm 2.

**Algorithm 2** Randomized black-box PIT algorithm for depth-3 arithmetic circuits

Input: $\epsilon, k, n, d \in \mathbb{Z}$, and oracle access to a $\Sigma\Pi\Sigma(k,d)$ circuit $C$ in $n$ input variables.
Output: Determine whether $C \equiv 0$.

Let $\epsilon > 0$ be a constant and $t = 2^k \cdot R(k,d)$. For $\alpha \in \mathbb{F}$ let $P_\alpha$ be the $n \times t$ matrix for which $(P_\alpha)_{i,j} = \alpha^{i(j+1)}$. Let $v_{0,\alpha} = \left(\alpha, \alpha^2, \ldots, \alpha^n\right)$. Let $S_\epsilon, T_\epsilon \subseteq \mathbb{F}$ be subsets such that $|S_\epsilon| = 2n\left(\binom{kd}{2}+1\right)\binom{t+2}{2}/\epsilon$ and $|T_\epsilon| = 2d/\epsilon$. Define

$$\mathcal{H}_\epsilon = \left\{P_\alpha \bar{y} + v_{0,\alpha} \ : \ \alpha \in S \ \text{ and } \ \bar{y} \in T^t\right\}.$$

Pick a random $p \in \mathcal{H}$. If $C(p) = 0$ then return "zero circuit".
Else, return "non-zero circuit".

**Lemma 17.** *Let $C$ be a $\Sigma\Pi\Sigma(k,d)$ arithmetic circuit. Let $\epsilon > 0$ be a constant. If $C \not\equiv 0$ then Algorithm 2, when given $\epsilon, k, d, n$ as input and black-box access to $C$, return "non-zero circuit" with probability at least $1-\epsilon$. If $C \equiv 0$ then the algorithm always answers "zero circuit". The number of random bits used by the algorithm is $\log|\mathcal{H}_\epsilon| = \log|S_\epsilon| + t\log|T_\epsilon| = O\left(t\log 1/\epsilon + t\log d + \log n\right)$.*

*Proof.* As before, for $\alpha \in S$ let $V_\alpha = \left\{P_\alpha \bar{y} + v_{0,\alpha} \ : \ \bar{y} \in \mathbb{F}^t\right\}$. Denote $\mathcal{H}_{\alpha,\epsilon} = \left\{P_\alpha \bar{y} + v_{0,\alpha} \ : \ \bar{y} \in T_\epsilon^t\right\}$. Corollary 14 implies that if $C \not\equiv 0$ then for $(1-\epsilon/2)$ of the elements $\alpha \in S$, we have that $C|_{V_\alpha} \not\equiv 0$. For such an $\alpha$ we have that $C|_{V_\alpha}$ is a polynomial of degree at most $d$ in $\{y_i\}_{i\in[t]}$ and by the Schwartz-Zippel lemma (Lemma 16) we have that

$$\Pr_{p \in_R \mathcal{H}_{\alpha,\epsilon}}[C(p) = 0] \leq \frac{d}{|T_\epsilon|} = \epsilon/2.$$

In particular, if $C \not\equiv 0$ then with probability at least $1-\epsilon$ the algorithm outputs "non-zero circuit". The claim regarding the number of random bits is clear. □

As before, Theorem 2 is an immediate corollary of Lemma 17.

We note that the set $\mathcal{H}$ defined in Algorithm 1, and the set $\mathcal{H}_\epsilon$ defined in Algorithm 2 give rise to test sets for $\Sigma\Pi\Sigma(k)$ circuits. More accurately, let $\mathcal{H}$ and $\mathcal{H}_\epsilon$ be the sets corresponding to $\Sigma\Pi\Sigma(2k)$ circuits. Then, as an immediate consequence of Theorem 1, we get that any two $\Sigma\Pi\Sigma(k)$ circuit that agree on all the points of $\mathcal{H}$ compute the same polynomial. Similarly we get that any two $\Sigma\Pi\Sigma(k)$ circuits that compute different polynomials get different values on $1-\epsilon$ of the points in $\mathcal{H}_\epsilon$.

# 4 Black-box PIT algorithm for multilinear $\Sigma\Pi\Sigma(k)$ circuits

In this section we present a PIT algorithm for the case of multilinear $\Sigma\Pi\Sigma(k)$ circuits as stated in Theorem 3. The proof of the Theorem follows the same scheme as the proof of the general case. However, we will have to slightly change the definition of rank-preserving subspaces so that if $C$ is multilinear then so is $C|_V$. As in section 3, we shall find a set of subspaces that for every multilinear $\Sigma\Pi\Sigma(k)$ circuit contains a rank-preserving subspace, and our algorithm will check whether the restriction of the given circuit to every subspace in the set computes the identically zero polynomial. If we manage to make sure that the restricted circuit is also multilinear then, in analogy to the proof of Theorem 1, we can take subspaces of dimension $R_M(k)$ (i.e., of constant dimension), and then the verification process will run in polynomial time.

### 4.1 Rank-preserving subspaces for multilinear circuits

In this section we define the notion of rank-reserving subspace for multilinear circuits and prove that if $V$ is rank-preserving for a multilinear $\Sigma\Pi\Sigma(k)$ circuit $C$ then $C|_V \equiv 0$ if and only if $C \equiv 0$.

**Definition 18.** *Let $C$ be a multilinear $\Sigma\Pi\Sigma(k)$ arithmetic multilinear circuit and $V$ an affine subspace. We say that $V$ is multilinear-rank-preserving for $C$ if the following properties hold:*

1. *Any two linear functions $L_1, L_2 \in C$ that are linearly independent are either restricted to constant functions on $V$ or they remain linearly independent when restricted to $V$.*
2. *$\forall A \subseteq [k]$, $\text{rank}(\text{sim}(C_A)|_V) \geq \min\{\text{rank}(\text{sim}(C_A)), R_M(k)\}$*
3. *No linear function $L \in C$ vanishes on $V$.*
4. *$C|_V$ is a multilinear circuit*

The following lemma is analogous to Lemma 8.

**Lemma 19.** *Let $C$ be a multilinear $\Sigma\Pi\Sigma(k)$ circuit and $V$ be a multilinear-rank-preserving affine subspace for $C$. Then we have the following:*

1. *For every $\emptyset \neq A \subset [k]$, $V$ is multilinear-rank-preserving for $C|_A$.*
2. *$V$ is multilinear-rank-preserving for $\text{sim}(C)$.*
3. *$\text{gcd}(C)|_V = \text{gcd}(C|_V)$.*
4. *$\text{sim}(C)|_V = \text{sim}(C|_V)$.*

*Proof.* Claims 1 and 2 are immediate from the definition. Claim 3 holds, as it is easy to see that no new linear function was added to the g.c.d. (as then we would have two linearly independent linear function that were restricted to non-constant independent linear functions). claim 4 follows from the definition of $\text{sim}(C)$ and the claim regarding $\text{gcd}(C)|_V$. □

The next theorem is analogous to Theorem 9.

**Theorem 20.** *Let $C$ be a multilinear $\Sigma\Pi\Sigma(k)$ arithmetic circuit and $V$ be a rank-preserving subspace for $C$. If $C|_V \equiv 0$ then $C \equiv 0$.*

*Proof.* The proof is almost identical to the proof of Theorem 9. The only difference is that now $C|_V$ is multilinear and so we can use Theorem 6 instead of Theorem 5. As in theorem 9 we prove our claim in three steps. We first prove the theorem for the case that $C|_V$ (which is identically zero) is simple and minimal. We then remove the simplicity assumption, and finally we remove the minimality assumption.

Assume that $C|_V$ is identically zero simple and minimal. As $C|_V$ is simple it follows that $C$ is simple as well. By Theorem 6 we get that $\text{rank}(C|_V) < R_M(k)$. From the assumption that $V$ is rank-preserving for $C$ and from Property 2 of Definition 18 (applied for $A = [k]$) we get that $\text{rank}(C|_V) \geq \text{rank}(C)$, and thus

$$\text{rank}(C|_V) = \text{rank}(C).$$

Denote by $r$ the rank of the circuit $C$. Let $L_1, \ldots, L_r$ be linear functions forming a basis to the subspace spanned by the linear functions of $C$. In particular, there exist a polynomial $P$ such that

$$C \equiv P(L_1, \ldots, L_r).$$

Obviously,

$$C|_V \equiv P(L_1|_V, \ldots, L_r|_V).$$

The fact that $\text{rank}(C|_V) = \text{rank}(C)$ implies that $L_1|_V, \ldots, L_r|_V$ are linearly independent. Hence, for every $x \in \mathbb{F}^n$ there exists $y \in V$ such that $(L_1(x), \ldots, L_r(x)) = (L_1(y), \ldots, L_r(y)) = (L_1|_V(y), \ldots, L_r|_V(y))$. It follows that as $P(L_1|_V, \ldots, L_r|_V) \equiv 0$ then also $P(L_1, \ldots, L_r) \equiv 0$. Hence, $C \equiv 0$.

We now remove the simplicity assumption. Assume that $C|_V$ is identically zero minimal $\Sigma\Pi\Sigma(k)$ circuit. Again, the proof has the following form:

$$C|_V \equiv 0 \overset{(1)}{\Rightarrow} \text{sim}(C|_V) \equiv 0 \overset{(2)}{\Rightarrow} \text{sim}(C)|_V \equiv 0 \overset{(3)}{\Rightarrow} \text{sim}(C) \equiv 0 \overset{(4)}{\Rightarrow} C \equiv 0 \tag{3}$$

We now explain each of the implications in Equation (3).

- Implication (1) follows if we prove that $\text{gcd}(C)|_V \neq 0$. Indeed, Property 3 of Definition 18 guarantees that no non-zero linear function is restricted to zero.
- The second implication follows as by Lemma 19 we have that $\text{sim}(C|_V) = \text{sim}(C)|_V$.
- Implication (3) follows from the fact that $\text{sim}(C)|_V$ is a simple and minimal identically zero $\Sigma\Pi\Sigma(k)$ circuit, for which we proved that $\text{sim}(C)|_V \equiv 0$ implies that $\text{sim}(C) \equiv 0$ (recall that if $V$ is rank-preserving for $C$ then it is also rank-preserving for $\text{sim}(C)$).
- Step (4) follows immediately from the definition of $\text{sim}(C)$.

We now prove the general case. That is, we just assume that $C|_V \equiv 0$. Clearly there exists a partition $A_1, \ldots, A_s$ of $[k]$ such that for every $i \in [s]$ we have that $C_{A_i}|_V$ is a multilinear identically zero minimal $\Sigma\Pi\Sigma(k_i)$ circuit, for $k_i = |A_i|$. Notice that Definition 18 implies that $V$ is also rank-preserving for $C_{A_i}$. Hence, by what we just showed for minimal circuits, we get that $C_{A_i} \equiv 0$. It follows that $C = \sum_{i=1}^{s} C_{A_i} \equiv 0$. This completes the proof of the theorem. □

### 4.2 Construction of Rank-preserving subspace for multilinear circuits

In this section we construct a set of subspaces that for every multilinear $\Sigma\Pi\Sigma(k)$ circuit contains a rank-preserving subspace. As we shall see, each subspace will be composed from a projection on a small set of coordinates and a shift. It is clear that the restriction of a multilinear circuit to such a subspace is again a multilinear circuit (setting a variable to a constant does not alter multilinearity). Thus, our task is to construct such subspaces that will have Properties 1-3 of Definition 18.

We now define a set of subspaces that are composed of a projection to a set of coordinates and an affine shift. The projections alone will satisfy Properties 2 and 4 of Definition 18 but not Properties 1 and 3. However, as we shall see, the shifted projections will have all the required properties.

**Definition 21.** *Let $B \subseteq [n]$ be a non-empty subset of the coordinates and $\alpha \in \mathbb{F}$ be a field element.*

- *Define $V_B$ as the following subspace:*

$$V_B = \text{span}\{e_i : \ i \in B\}.$$

- *Let $v_{0,\alpha}$ be, as before, the vector*

$$v_{0,\alpha} = \left(\alpha, \alpha^2, \ldots, \alpha^n\right).$$

- *Let $V_{B.\alpha} = V_B + v_{0,\alpha}$.*

Obviously, for a multilinear circuit $C$, the restricted circuit $C|_{V_{B,\alpha}}$ is also multilinear, for every $B$ and $\alpha$. The following theorem shows that if we just consider the set of all $V_B$-s for $|B| \leq 2^k \cdot R_M(k)$ then this set contains a subspace that has Properties 2 and 4 of Definition 18.

**Theorem 22.** *Let $C$ be a $\Sigma\Pi\Sigma(k)$ multilinear arithmetic circuit. There exists a subset $B \subseteq [n]$ such that $|B| \leq 2^k \cdot R_M(k)$ and $B$ has the following properties:*

1. $\forall A \subseteq [k],\ \mathrm{rank}(\mathrm{sim}(C_A)|_{V_B}) \geq \min\{\mathrm{rank}(\mathrm{sim}(C_A)), R_M(k)\}$.
2. *$C|_{V_B}$ is a multilinear $\Sigma\Pi\Sigma(k)$ circuit.*

*Proof.* It is clear that $C|_{V_B}$ is multilinear and so we turn to prove that the first claim of the theorem holds. Let $A_1, A_2, \ldots, A_{2^k-1}$ be the non-empty subsets of $[k]$. We first show that for each $A_i$, there exists a subset $B_i \subseteq [n]$ such that $|B_i| \leq R_M(k)$ and

$$\mathrm{rank}(\mathrm{sim}(C_{A_i})|_{V_{B_i}}) = \min\{\mathrm{rank}(\mathrm{sim}(C_{A_i})), R_M(k)\}.$$

Indeed, let $R_i = \mathrm{rank}(\mathrm{sim}(C_{A_i}))$, and let $L_1, \ldots, L_{R_i}$ be linearly independent linear functions from $\mathrm{sim}(C_{A_i})$. Denote by $Z$ the $R_i \times n+1$ matrix whose rows correspond to the vectors of coefficients of $\{L_j\}_{j\in[R_i]}$. Obviously, there are $R_i$ linearly independent column-vectors in $Z$. Let $B_i \subset [n]$ contain the indices of $\min\{R_i, R_M(k)\}$ columns that are linearly independent. We now observe that the matrix corresponding to the vectors of coefficients of the linear functions $\{L_j|_{V_B}\}_{j\in[R_i]}$ is equal to $Z$ on the columns of $B$ and has zeroes everywhere else. As the column rank of $Z$ is equal to its row rank (that is equal to $R_i$) we get that the rank of $\{L_j|_{V_B}\}_{j\in[R_i]}$ is exactly $\min\{R_i, R_M(k)\}$. Therefore,

$$\mathrm{rank}(\mathrm{sim}(C_{A_i})|_{V_{B_i}}) = \min\{\mathrm{rank}(\mathrm{sim}(C_{A_i})), R_M(k)\}.$$

Up till now we showed that for every $A_i$ there is a set $B_i$ satisfying $|B_i| = \min\{R_i, R_M(k)\}$ such that $V_{B_i}$ is good for $C_{A_i}$. However, it may be the case that different $A_i$-s need different $B_i$-s. Therefore we shall consider the following set

$$B = \bigcup_{i=1}^{2^k} B_i.$$

Clearly $|B| \leq 2^k \cdot R_M(k)$ and $C|_{V_B}$ is multilinear. Furthermore, for each $A_i \subseteq [k]$ we have that

$$\mathrm{rank}(\mathrm{sim}(C_{A_i})|_{V_B}) \geq \mathrm{rank}(\mathrm{sim}(C_{A_i})|_{V_{B_i}}) = \min\{\mathrm{rank}(\mathrm{sim}(C_{A_i})), R_M(k)\}.$$

This concludes the proof of the theorem. □

The following is an immediate corollary of Theorem 22.

**Corollary 23.** *For every $\Sigma\Pi\Sigma(k)$ multilinear arithmetic circuit $C$, there exists a subset $B \subset [n]$, of size $|B| = 2^k \cdot R_M(k)$, such that $V_B$ satisfies Properties 2 and 4 of Definition 18.*

*Proof.* Let $C$ be a multilinear $\Sigma\Pi\Sigma(k)$ circuit and let $B' \subseteq [n]$ be a subset guaranteed by Theorem 22. Let $B \subset [n]$ be such that $B' \subseteq B$ and $|B| = 2^k \cdot R_M(k)$. It is clear that $B$ also satisfies the requirements of Theorem 22. □

We also note that if $V_B$ satisfies Theorem 22 for some circuit $C$, then so does $V_{B,\alpha}$ for any $\alpha \in \mathbb{F}$. The reason is that restricting to an affine shift of $V_B$ does not decrease the rank of the restricted linear functions.

The following theorem shows that for every $\Sigma\Pi\Sigma(k)$ circuit $C$ there are at most $\mathrm{poly}(n)$ many $\alpha$-s such that $V_{B,\alpha}$ is not rank preserving for the $B$ guaranteed by Corollary 23.

**Theorem 24.** *Let $C$ be a $\Sigma\Pi\Sigma(k)$ multilinear arithmetic circuit over a field $\mathbb{F}$. Let $B$ be the set guaranteed by Corollary 23. Then there are less than $n^3k^2$ many $\alpha \in \mathbb{F}$ such that $V_{B,\alpha}$ is not rank preserving for $C$.*

*Proof.* We first bound the number of $\alpha$-s for which $V_{B,\alpha}$ does not satisfy Property 3. Consider a linear function $L \in C$ given by $L(x_1, \ldots, x_n) = a_0 + a_1x_1 + \ldots + a_nx_n$, and the subspace $V_{B,\alpha}$ for some $\alpha$. Then the restriction of $L$ to $V_{B,\alpha}$ is given by $\sum_{i\in B} a_ix_i + L(v_{0,\alpha}) = \sum_{i\in B} a_ix_i + \sum_{i=0}^{n} a_i\alpha^i$. It follows that $L|_{V_{B,\alpha}} = 0$ if and only if $L$ is supported on $[n] \setminus B$ (that is, $a_i = 0$ for $i \in B$) and $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. In particular $\alpha$ must be a zero of the polynomial

$$p_L(x) \triangleq a_0 + a_1x + \ldots a_nx^n$$

(notice that this polynomial does not depend on the set $B$). As $p_L(x)$ is a non-zero polynomial of degree $n$ it has at most $n$ distinct roots. Going over all $L \in C$ we see that there are at most $n \cdot size(C)$ bad $\alpha$-s for $C$. As $C$ is a multilinear $\Sigma\Pi\Sigma(k)$ circuit we have that $size(C) \leq nk$ and so the number of $\alpha$-s for which Property 3 is violated is at most $n^2k$.

We now bound the number of $\alpha$-s for which $V_{B,\alpha}$ violates Property 1. For simplicity we shall only consider those $\alpha$-s for which Property 3 is satisfied. Let $L, \tilde{L} \in C$ be two linearly independent linear functions. We have three cases. The first case is that both $L$ and $\tilde{L}$ are supported on $[n] \setminus B$. In this case it is clear that the restriction of both functions to $V_{B,\alpha}$ is constant, for any $\alpha$ (which is ok). The second case is that exactly one of the functions is supported on $[n] \setminus B$, say $L$. In this case $L$ is restricted to a constant non-zero function and $\tilde{L}$ is restricted to a non-constant function (no matter what $\alpha$ is) and so they remain linearly independent. The third, and more interesting, case is when both functions are restricted to non constants. Denote $L(\bar{x}) = a_0 + a_1x_1 + \ldots a_nx_n$ and $\tilde{L} = \tilde{a}_0 + \tilde{a}_1x_1 + \ldots \tilde{a}_nx_n$. For $L|_{V_{B,\alpha}}$ and $\tilde{L}|_{V_{B,\alpha}}$ to be linearly dependent there must be a constant $\gamma \in \mathbb{F}$, independent of $\alpha$, such that $L|_{V_B} = \gamma \cdot \tilde{L}|_{V_B}$. For this $\gamma$ we have that $\alpha$ must satisfy that $L(v_{0,\alpha}) = \gamma \cdot \tilde{L}(v_{0,\alpha})$ or, equivalently, that $(L - \gamma \cdot \tilde{L})(v_{0,\alpha}) = 0$. As we assume that $L$ and $\tilde{L}$ are linearly independent we have that $L - \gamma \cdot \tilde{L} \neq 0$. Define the polynomial $p_{L-\gamma\cdot\tilde{L}}(x)$ as before. We see that it must be the case that $p_{L-\gamma\cdot\tilde{L}}(\alpha) = 0$. Thus, $\alpha$ is a root of a degree $n$ polynomial that depends only on $L, \tilde{L}$ and $B$. Thus, for our $B$ there are at most $n \cdot \binom{size(C)}{2} < n^3k^2/2$ $\alpha$-s such that $V_{B,\alpha}$ violates Property 1.

Concluding, we see that for our $B$ there are less than $n^2k + n^3k^2/2 < n^3k^2$ $\alpha$-s for which $V_{B,\alpha}$ is not rank-preserving for $C$. This concludes the proof of the theorem. □

**Corollary 25.** *Let $T \subset \mathbb{F}$ be of size $n^3k^2$. Let $C$ be a $\Sigma\Pi\Sigma(k)$ multilinear circuit. Then there exist $B \subset [n]$ of size $|B| = 2^k \cdot R_M(k)$ and $\alpha \in T$ such that $V_{B,\alpha}$ is rank-preserving for $C$.*

*Proof.* Follows immediately from Corollary 23 and Theorem 24. □

### 4.3 The PIT algorithm for multilinear $\Sigma\Pi\Sigma(k)$ circuits

In this section we give a polynomial time deterministic algorithm (Algorithm 3) for identity testing of multilinear $\Sigma\Pi\Sigma(k)$ circuits, which proves Theorem 3. The algorithm is completely analogous to Algorithm 1, with the exception that the hitting set is the one implied by Corollary 25.

The following lemma shows that Algorithm 3 is correct, and gives a trivial upper bound on its running time. This immediately imply Theorem 3.

**Algorithm 3** Deterministic PIT for multilinear $\Sigma\Pi\Sigma(k)$ arithmetic circuits

Input: $k, n \in \mathbb{Z}$, and oracle access to a $\Sigma\Pi\Sigma(k)$ multilinear circuit $C$ in $n$ input variables.
Output: Determine whether $C \equiv 0$.

Let $T \subset \mathbb{F}$ be a subset of size $n^3k^3$ field elements. For $\alpha \in \mathbb{F}$ let $v_{0,\alpha} = (\alpha, \ldots, \alpha^n) \in \mathbb{F}^n$. Define $\mathcal{H}_M$ as

$$\mathcal{H}_M = \left\{ v + v_{0,\alpha} \ : \ v \in \{0,1\}^n,\ |v| \leq 2^k \cdot R_M(k),\ \alpha \in T \right\}.$$

If for every $p \in \mathcal{H}_M$, $C(p) = 0$ then output zero-circuit.
Else, return non-zero circuit.

**Lemma 26.** *Let $C$ be a multilinear $\Sigma\Pi\Sigma(k)$ circuit. Then Algorithm 3, when given $k, n$ as input and oracle access to $C$, determines whether $C \equiv 0$. the running time of the algorithm is*

$$n^3k^2 \cdot \sum_{t=0}^{2^k \cdot R_M(k)} \binom{n}{t} = \Theta\left(n^{2^k \cdot R_M(k)+3}\right).$$

*Proof.* Certainly if $C \equiv 0$ then the algorithm returns zero-circuit. So assume that $C \not\equiv 0$. By Corollary 25 we see that there exist a set $B \subset [n]$ of size $2^k \cdot R_M(k)$ and $\alpha \in T$ such that $V_{B,\alpha}$ is rank-preserving for $C$. Theorem 20 assures us that $C|_{V_{B,\alpha}}$, which computes a multilinear polynomial, is not the zero polynomial. Let $\bar{x}_B$ be the vector of indeterminates that is supported on $B$, namely, replace $x_i$ with 0 for $i \notin B$. It is easy to see that $C|_{V_{B,\alpha}}$can be represented as $C(\bar{x}_B + v_{0,\alpha})$. Since $C(\bar{x}_B + v_{0,\alpha})$ is a multilinear polynomial in $\bar{x}_B$, we get that there is some 0/1 assignment to $\bar{x}_B$, which we denote with $\rho_B$, such that $C(\rho_B + \alpha) \neq 0$. Notice that $\rho_B \in \{0,1\}^n$ is a vector of weight $|\rho_B| \leq |B| = 2^k \cdot R_M(k)$. Therefore $\rho_B + \alpha \in \mathcal{H}_M$ and so the algorithm will output "non-zero circuit". The claim regarding the running time is trivial, as all we have to do is to bound the size of $\mathcal{H}_M$. □

As in the general case we get that the set $\mathcal{H}_M$, as defined in Algorithm 3 for $\Sigma\Pi\Sigma(2k)$ circuits, is a test set for multilinear $\Sigma\Pi\Sigma(k)$ circuits. Namely, any two multilinear $\Sigma\Pi\Sigma(k)$ circuits that agree on all the points of $\mathcal{H}_M$, compute the same polynomial.

## Acknowledgements

AS would like to thank Zeev Dvir for many helpful conversations.

## References

[AB03] M. Agrawal and S. Biswas. Primality and identity testing via chinese remaindering. *JACM*, 50(4):429–443, 2003.

[BOT88] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynominal interpolation. In *Proceedings of the 20th Annual STOC*, pages 301–309, 1988.

[CDGK91] M. Clausen, A. W. M. Dress, J. Grabmeier, and M. Karpinski. On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields. *Theor. Comput. Sci.*, 84(2):151–164, 1991.

[CK00] Z. Chen and M. Kao. Reducing randomness via irrational numbers. *SIAM J. on Computing*, 29(4):1247–1256, 2000.

[CRS95] S. Chari, P. Rohatgi, and A. Srinivasan. Randomness-optimal unique element isolation with applications to perfect matching and related problems. *SIAM J. on Computing*, 24(5):1036–1050, 1995.

[DS06] Z. Dvir and A. Shpilka. Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM J. on Computing*, 36(5):1404–1434, 2006.

[GK87] D. Grigoriev and M. Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in nc (extended abstract). In *28th Annual Symposium on Foundations of Computer Science*, pages 166–172, 1987.

[GKS90] D. Grigoriev, M. Karpinski, and M. F. Singer. Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields. *SIAM J. on Computing*, 19(6):1059–1063, 1990.

[GR05] A. Gabizon and R. Raz. Deterministic extractors for affine sources over large fields. In *46th Annual FOCS*, pages 407–418, 2005.

[KI04] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[KS96] M. Karpinski and I. Shparlinski. On some approximation problems concerning sparse polynomials over finite fields. *Theoretical Computer Science*, 157(2):259–266, 1996.

[KS01] A. Klivans and D. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the 33rd Annual STOC*, pages 216–223, 2001.

[KS06] N. Kayal and N. Saxena. Polynomial identity testing for depth 3 circuits. In *Proceedingds of the 21st Annual IEEE Conference on Computational Complexity*, pages 9–17, 2006.

[Lov79] L. Lovasz. On determinants, matchings, and random algorithms. In L. Budach, editor, *Fundamentals of Computing Theory*. Akademia-Verlag, 1979.

[LV98] D. Lewin and S. Vadhan. Checking polynomial identities over any field: Towards a derandomization? In *Proceedings of the 30th Annual STOC*, pages 428–437, 1998.

[MVV87] K. Mulmuley, U. Vazirani, and V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987.

[RS05] R. Raz and A. Shpilka. Deterministic polynomial identity testing in non commutative models. *J. of Computational Complexity*, 14(1):1–19, 2005.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *JACM*, 27(4):701–717, 1980.

[SS96] R. E. Schapire and L. M. Sellie. Learning sparse multivariate polynomials over a field with queries and counterexamples. *J. of Computer and System Sciences*, 52(2):201–213, 1996.

[Wer94] K. Werther. The complexity of sparse polynomial interpolation over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 5:91–103, 1994.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation*, pages 216–226. 1979.

# A Proof of Lemma 10

Notice that by the union bound it is enough to proof the theorem for the case that $s = 1$. Hence, we assume w.l.o.g. that $s = 1$ and that we have only one subspace, $W$. We shall also assume that $\dim(W) = t + 1$, as any subspace $W$ such that $\dim(W) < t + 1$, is contained in a subspace $W \subseteq W'$ of dimension $t + 1$, and the equality $\dim(\varphi_\alpha(W')) = \dim(W')$ implies that $\dim(\varphi_\alpha(W)) = \dim(W)$.

Let $\tilde{w}^{(1)}, \ldots, \tilde{w}^{(t+1)}$ be a basis of $W$. For convenience we denote $\tilde{w}^{(l)} = (\tilde{w}_0^{(l)}, \ldots, \tilde{w}_n^{(l)})$. For $j \in [t + 1]$, let $j_{max}$ to be the maximal $i \in \{0, \ldots, n\}$ such that $\tilde{w}_i^{(j)}$ is non-zero. Note that (e.g. by using Gaussian elimination) there exists a basis $w^{(1)}, \ldots, w^{(t+1)}$ of $W$ such that

$$0 \leq 1_{max} < 2_{max} < \ldots < (t + 1)_{max}.$$

Denote with $B$ the $(n + 1) \times (t + 1)$ matrix who's $j$-th column is $w^{(j)}$. That is,

$$B = (w^{(1)}, \ldots, w^{(t+1)}).$$

Let $P_{\varphi_\alpha}$ be the matrix corresponding to the linear transformation $\varphi_\alpha$ (with respect to the basis $\{e_1\}_{i\in[n]}$). As $W = B(\mathbb{F}^{t+1})$ we have that

$$\varphi_\alpha(W) = P_{\varphi_\alpha} \cdot B(\mathbb{F}^{t+1}).$$

Let $C_\alpha$ the $(t + 1) \times (t + 1)$ matrix $P_{\varphi_\alpha} \cdot B$. That is,

$$(C_\alpha)_{j,l} = \sum_{i=0}^{n} \alpha^{ji} \cdot w_i^{(l)}.$$

Recall that $C_\alpha(\mathbb{F}^{t+1}) = \mathbb{F}^{t+1}$ if and only if $Det(C_\alpha) \neq 0$. Thus, our result will follow if we show that for most $\alpha$-s the determinant of $C_\alpha$ is non zero. Let $f(\alpha) = Det(C_\alpha)$. We will show that $f(\alpha)$ is a non-zero polynomial of degree not larger than $n \cdot \binom{t+2}{2}$ in $\alpha$. Hence, $Det(C_\alpha) = 0$ for at most $n \cdot \binom{t+2}{2}$ values of $\alpha$ and the lemma follows. Consider the following representation of $f$

$$f(\alpha) = Det(C_\alpha) = \sum_{\sigma \in S_{t+1}} sgn(\sigma) \cdot f_\sigma(\alpha),$$

where $S_{t+1}$ is the group of all permutations of $t + 1$ elements and

$$f_\sigma(\alpha) = \prod_{j=1}^{t+1} (C_\alpha)_{j,\sigma(j)}.$$

Let $\mathrm{Id} \in S_{t+1}$ be the identity permutation. We will show that for every $\sigma \neq \mathrm{Id}$ in $S_{t+1}$, we have that $\deg(f_\sigma) < \deg(f_{\mathrm{Id}})$. Assume for a contradiction that there exists $\sigma \neq \mathrm{Id}$ such that $\deg(f_\sigma) \geq \deg(f_{\mathrm{Id}})$. Fix a permutation $\sigma \neq \mathrm{Id}$ that maximizes $\deg(f_\sigma)$. That is, $\deg(f_\sigma) \geq \deg(f_{\sigma'})$ for every $\sigma' \in S_{t+1}$. By definition, $(C_\alpha)_{j,\sigma(j)}$ is a polynomial of degree $j \cdot \sigma(j)_{max}$ in $\alpha$ (as $w_i^{(\sigma(j))} = 0$ for $i > \sigma(j)_{\max}$). Therefore, $f_\sigma$ has degree

$$\deg(f_\sigma) = \sum_{j=1}^{t+1} j \cdot \sigma(j)_{max}. \tag{4}$$

By our assumption, $\sigma \neq \mathrm{Id}$, and so there exist $j_1 < j_2$ such that $\sigma(j_1) > \sigma(j_2)$. Let $\tau = (\sigma(j_1), \sigma(j_2)) \cdot \sigma$, i.e. the permutation $\tau$ consists of applying $\sigma$ and then "switching" between $\sigma(j_1)$ and $\sigma(j_2)$. By Equation (4) we get that

$$\begin{aligned}\deg(f_\tau) - \deg(f_\sigma) &= j_2\tau(j_2)_{max} + j_1\tau(j_1)_{max} - j_2\sigma(j_2)_{max} - j_1\sigma(j_1)_{max} \\ &= j_2\sigma(j_1)_{max} + j_1\sigma(j_2)_{max} - j_2\sigma(j_2)_{max} - j_1\sigma(j_1)_{max} \\ &= (j_2 - j_1)(\sigma(j_1)_{max} - \sigma(j_2)_{max}) > 0\end{aligned}$$

which contradicts the maximality of $\deg(f_\sigma)$.

Hence, for any $\sigma \neq \mathrm{Id}$, $\deg(f_\sigma) < \deg(f_{\mathrm{Id}})$. Thus, the highest degree monomial in $f_{\mathrm{Id}}$ cannot be cancelled out by the other summands in $f(\alpha)$, and therefore $f(\alpha)$ is a non-zero polynomial of degree

$$\deg(f) = \deg(f_{\mathrm{Id}}) = \sum_{j=1}^{t+1} j \cdot j_{max} \leq n \cdot \sum_{j=1}^{t+1} j = n \cdot \frac{(t+1)(t+2)}{2} = n\binom{t+2}{2}.$$

This completes the proof of the lemma. □



ECCC ISSN 1433-8092
http://eccc.hpi-web.de/