Electronic Colloquium on Computational Complexity, Report No. 201 (2015)

Limitations of sum of products of Read-Once Polynomials

C. Ramya
Department of Computer Science and Engineering
IIT Madras, Chennai INDIA
ramya@cse.iitm.ac.in

B. V. Raghavendra Rao
Department of Computer Science and Engineering
IIT Madras, Chennai INDIA
bvrr@cse.iitm.ac.in

December 10, 2015

Abstract

We study limitations of polynomials computed by depth two circuits built over read-once polynomials (ROPs) and depth three syntactically multi-linear formulas. We prove an exponential lower bound for the size of the $\Sigma\Pi^{[N^{1/30}]}$ arithmetic circuits built over syntactically multi-linear $\Sigma\Pi\Sigma^{[N^{8/15}]}$ arithmetic circuits computing a product of variable disjoint linear forms on N variables. We extend the result to the case of $\Sigma\Pi^{[N^{1/30}]}$ arithmetic circuits built over ROPs of unbounded depth, where the number of variables with + gates as a parent in an proper sub formula is bounded by $N^{1/2+1/30}$. We show that the same lower bound holds for the permanent polynomial. Finally we obtain an exponential lower bound for the sum of ROPs computing a polynomial in VP defined by Raz and Yehudayoff [18].

Our results demonstrate a class of formulas of unbounded depth with exponential size lower bound against the permanent and can be seen as an exponential improvement over the multilinear formula size lower bounds given by Raz [14] for a sub-class of multi-linear and non-multi-linear formulas. Our proof techniques are built on the one developed by Raz [14] and later extended by Kumar et. al. [10] and are based on non-trivial analysis of ROPs under random partitions. Further, our results exhibit strengths and limitations of the lower bound techniques introduced by Raz [14].

ISSN 1433-8092

1 Introduction

More than three decades ago, Valiant [21] developed the theory of Algebraic Complexity classes based on arithmetic circuits as the model of algebraic computation. Valiant considered the permanent polynomial perm_n defined over an $n \times n$ matrix $X = (x_{i,j})_{1 \le i,j \le n}$ of variables:

$$\mathsf{perm}_n(X) = \sum_{\pi \in S_n} \prod_{i=1}^{n} x_{i,\pi(i)},$$

where S_n is the set of all permutations on n symbols. Valiant [21] showed that the polynomial family $(\mathsf{perm}_n)_{n \ge 0}$ is complete for the complexity class VNP. Further, Valiant [21] conjectured that perm_n does not have polynomial size arithmetic circuits. Since then, obtaining super polynomial size lower bounds for arithmetic circuits computing perm_n has been a pivotal problem in Algebraic Complexity Theory. However, for general classes of arithmetic circuits, the best known lower bound is quadratic in the number of variables [13].

Naturally, the focus has been on proving lower bound for perm_n against restricted classes of circuits. Grigoriev and Karpinski [3] proved an exponential size lower bound for depth three circuits of constant size over finite fields. Agrawal and Vinay [1] (See also [20, 9]) showed that proving exponential lower bounds against depth four arithmetic circuits is enough to resolve Valiant's conjecture, and hence explaining the lack of progress in extending the results in [3] to higher depth circuits. This was strengthened to depth three circuits over infinite fields by Gupta et. al. [4].

Recently, Gupta et. al. [5] obtained a $2^{\Omega(\sqrt{n}\log n)}$ size lower bound for homogeneous depth four circuits computing perm_n where the bottom fan-in is bounded by $O(\sqrt{n})$. The techniques introduced in [5, 6] have been generalized and applied to prove lower bounds against various classes of constant depth arithmetic circuits, regular arithmetic formulas and homogeneous arithmetic formulas. (See e.g., [7, 11, 8].) Exhibiting polynomials that have exponential lower bound against concrete classes of arithmetic circuits is an important research direction.

In 2004, Raz [14] showed that any multilinear formula computing perm_n requires size $n^{\Omega(\log n)}$, which was one of the first super polynomial lower bounds against formulas of unbounded depth. Further, in [15], Raz extended this to separate multilinear formulas from multilinear circuits. Raz's work lead to several lower bound results, most significant being an exponential separation of constant depth multilinear circuits [18]. More recently, Kumar et. al [10] extended the techniques developed in [14] to prove lower bounds against non-multilinear circuits and formulas.

Motivation and our Model : Depth three $\Sigma\Pi\Sigma$ circuits are in fact $\Sigma\Pi$ circuits built over linear forms. A linear form can be seen as the simplest form of read-once formulas (ROF): formulas where a variable appears at most once as a leaf label. Polynomials computed by ROFs are called read-once polynomials or ROPs. There are two natural generalizations of the $\Sigma\Pi\Sigma$ model: 1) Replace linear forms by sparse polynomials, this leads to the well studied $\Sigma\Pi\Sigma\Pi$ circuits; and 2) Replace linear forms with more general read-once formulae, this leads to the class of $\Sigma\Pi$ circuits over read-once formulas or $\Sigma\Pi$ROP for short.

In this paper, we consider the second extension, i.e., $\Sigma\Pi$ROP. Restricted forms of $\Sigma\Pi$ROP were already considered in the literature. For example, Shpilka and Volkovich [19] obtained identity testing algorithms for the sum of ROPs. Further [12] gives identity tests for $\Sigma\Pi$ROP when the top fan-in is restricted to two.

Apart from being a natural generalization of $\Sigma\Pi\Sigma$ circuits, the class $\Sigma\Pi$ROP can be seen as building non-multi-linear polynomials using the simplest possible multi-linear polynomials viz. ROPs.

Our Results : We study the limitations of the model $\Sigma\Pi\mathsf{ROP}$ for some restricted class of circuits. Firstly, we prove,

Theorem 1. *Let $f_{i,j}$ be N-variate $\Sigma\Pi\Sigma$ syntactic multi-linear formulas with bottom Σ-fan-in at most $N^{1/2+\lambda}$ where $\lambda \leq 1/30$, and top Σ-fan-in at most s' for $1 \leq i \leq s$ and $1 \leq j \leq t$. Also assume that $t \leq N^{1/30}$. There is a product of variable disjoint linear forms p_{lin} such that, if $\sum_i \prod_j f_{i,j} = p_{lin}$ then $s \cdot s' = 2^{\Omega(N^{1/4})}$.*

Our arguments do not directly generalize to the case of unbounded depth ROPs with small bottom Σ fan-in. Nevertheless, we obtain a generalization of Theorem 1, allowing ROPs of unbounded depth with a more stringent restriction than bottom Σ-fan-in. Let F be an ROF and for a gate v in F, let sum-fan-in(v) be the number of variables in the sub-formula rooted at v whose parents are labelled as $+$. Then s_F is the maximum value of sum-fan-in(v), where the maximum is taken over all $+$ gates in F excluding the top layer of $+$ gates. Note that, in the case of $\Sigma\Pi\Sigma$ ROPs, s_F is equivalent to the bottom fan-in. For an ROP f, s_f is the smallest value of s_F among all ROFs F computing f. We prove,

Theorem 2. *Let $f_{i,j}$ be ROPs with $s_{f_{i,j}} \leq N^{1/2+\lambda}$ for $\lambda \leq 1/30$, $1 \leq i \leq s$ and $1 \leq j \leq t$, where $t \leq N^{1/30}$. There is a product of linear forms p_{lin} such that, if $\sum_i \prod_j f_{i,j} = p_{lin}$ then $s = 2^{\Omega(N^{1/4})}$.*

As far as we know, this is the first exponential lower bound for a sub-class of non-multi-linear formulas of unbounded depth. It can be noted that our result above does not depend on the depth of the ROPs. Further, note that even though a product of linear forms is a simple linear projection of perm_n, Theorem 2 does not imply a lower bound for perm_n due to restrictions on s_F, since linear projections might change the bottom fan-in of the resulting ROPs. However, we prove,

Theorem 3. *Let $f_{i,j}$ be ROPs with $s_{f_{i,j}} \leq N^{1/2+\lambda}$ for $\lambda \leq 1/30$, $1 \leq i \leq s$ and $1 \leq j \leq t$, for $N = n^2$ and $t \leq N^{1/30}$. Then, if $\sum_i \prod_j f_{i,j} = \mathsf{perm}_n$ then $s = 2^{\Omega(N^{\epsilon})}$ for some $\epsilon > 0$.*

Finally, we show that the polynomial g defined by Raz-Yehudayoff [17] cannot be written as sum of sub-exponentially many ROPs:

Theorem 4. *There is a polynomial $g \in \mathsf{VP}$ such that for any ROPs $f_1, \ldots, f_s$, if $\sum_i f_i = g$, then we have $s = 2^{\Omega(n/\log n)}$.*

Related Results : Shpilka and Volkovich [19] proved a linear lower bound for a special class of ROPs to sum-represent the polynomial $x_1 \cdots x_n$ and used it crucially in their identity testing algorithm. Theorem 4 is an exponential lower bound against the same model as in [19], however against a polynomial in VP. It should be noted that the results in Raz [14] combined with [10] immediately implies a lower bound of $n^{\Omega(\log n)}$ for the sum of ROPs. Our results are an exponential improvement of bound given by [14].

Kayal [6] showed that at least $2^{n/d}$ many polynomials of degree d are required to represent the polynomial $x_1 \ldots x_n$ as sum of powers. Our model is significantly different from the one in [6] since it includes high degree monomials, though the powers are restricted to be sub-linear, whereas Kayal's argument works against arbitrary powers.

Our Techniques Our techniques are broadly based on the partial derivative matrix technique introduced by Raz [14] and later extended by Kumar et. al [10]. It can be noted that the lower bounds obtained in [14] are super polynomial and not exponential. Though Raz-Yehudayoff [18] proved exponential lower bounds, their argument works only against bounded depth multilinear circuits. Further, the arguments in [14, 18] do not work for the case of non-multilinear circuits, and fail even in the case of products of two multilinear formulas. This is because rank of the partial derivative matrix, a complexity measure used by [14, 18] (see Section 2 for a definition) is defined only for multi-linear polynomials. Even though this issue can be overcome by a generalization introduced by Kumar et. al [10], the limitation lies in the fact that the upper bound of $2^{n-n^{\epsilon}}$ for an n^2 or $2n$ variate polynomial, obtained in [14] or [18] on the measure for the underlying arithmetic formula model is insufficient to handle products of two ROPs.

Our approach to prove Theorems 2 and 3 lie in obtaining an exponentially stronger upper bounds (see Lemma 17) on the rank of the partial derivative matrix of an ROP F on N variables where $s_F \le N^{1/2+1/30}$. Our proof is a technically involved analysis of the structure of ROPs under random partitions of the variables. Even though the restriction on s_F might look un-natural, in Lemma 18, we show that a simple product of variable disjoint linear forms in N-variables, with $s_F \ge N^{2/3}$ achieve exponential rank with probability $1 - 2^{-\Omega(N^{1/3})}$. Thus our results highlight the strength and limitations of the techniques developed in [18, 10] to the case of non-multi-linear formulas.

Finally proof of Theorem 4 is based on an observation pointed out to the authors by an anonymous reviewer. We have included it here since the details have been worked out completely by the authors.

Due to space limitations, all the missing proofs can be found in Sections 5,6 and 7.

2 Preliminaries

Let $\mathbb{F}$ be an arbitrary field and $X = \{x_1, \ldots, x_N\}$ be a set of variables. An *arithmetic circuit* $\mathcal{C}$ over $\mathbb{F}$ is a directed acyclic graph with vertices of in-degree 0 or 2 and exactly one vertex of out-degree 0 called the output gate. The vertices of in-degree 0 are called *input gates* and are labeled by elements from $X \cup \mathbb{F}$. The vertices of in-degree more than 0 are labeled by either $+$ or $\times$. Thus every gate of the circuit naturally computes a polynomial. The polynomial f computed by $\mathcal{F}$ is the polynomial computed by the output gate of the circuit.

An *arithmetic formula* is a an arithmetic circuit $\mathcal{F}$ where every gate has out-degree bounded by 1, i.e., the underlying undirected graph $\mathcal{F}$ is a tree.

The *size* of an arithmetic circuit $\mathcal{F}$ is the number of gates in $\mathcal{F}$. For any gate v *depth* of v is the length of the longest path from an input gate to v gate in $\mathcal{F}$. Depth of $\mathcal{F}$ is defined as the depth of its output gate.

An *arithmetic read-once formula* (ROF for short) is an arithmetic formula $\mathcal{F}$ over X where every input variable $x \in X$ occurs as a label of at most once $\mathcal{F}$. The polynomial f computed by an ROF $\mathcal{F}$ is called a *read-once-polynomial* or ROP.

Let $f(y_1, \ldots, y_m, z_1, \ldots, z_m) \in \mathbb{F}[y_1, \ldots, y_m, z_1, \ldots, z_m]$ be a multilinear polynomial. The *partial derivative matrix of* f denoted by M_f [14] is a $2^m \times 2^m$ matrix defined as follows: The rows of M_f are labeled by all possible multilinear monomials in $\{y_1, \ldots, y_m\}$ and the columns of M_f be labeled by all possible multilinear monomials in $\{z_1, \ldots, z_m\}$. For any two multilinear monomials p and q, the entry $M_f[p, q]$ is the coefficient of $p \cdot q$ in f.

Lemma 1. [16]*(Sub-Additivity.) Let* $f = f_1 + f_2$ *where* f, f_1 *and* f_2 *are multilinear polynomials in* $\mathbb{F}[y_1, \ldots, y_m, z_1, \ldots, z_m]$*. Then,* $rank(M_f) \le rank(M_{f_1}) + rank(M_{f_2})$*. Moreover, if* $\mathsf{var(f_1)} \cap \mathsf{var(f_2)} = \emptyset$ *then* $rank(M_f) = rank(M_{f_1}) + rank(M_{f_2})$*.*

Lemma 2. [16]*(Sub-Multiplicativity.) Let* $f = f_1 \times f_2$*, where* f, f_1 *and* f_2 *are multilinear polynomials in* $\mathbb{F}[y_1, \ldots, y_m, z_1, \ldots, z_m]$*, and* $\mathsf{var(f_1)} \cap \mathsf{var(f_2)} = \emptyset$*. Then,* $rank(M_f) = rank(M_{f_1}) \cdot rank(M_{f_2})$*.*

Kumar et. al. [10] generalized the notion of partial derivative matrix to include polynomials that are not multilinear. Let $Y = \{y_1, \ldots, y_m\}$ and $Z = \{z_1, \ldots, z_m\}$. Let $f \in \mathbb{F}[Y, Z]$ be a polynomial.

The *polynomial coefficient matrix* of f denoted by $\widehat{M_f}$ is a $2^m \times 2^m$ matrix defined as follows. For multilinear monomials p and q in variables Y and Z respectively, the entry $\widehat{M_f}[p,q] = A$ if and only if f can be uniquely expressed as $f = pq \cdot A + B$ where $A, B \in \mathbb{F}[Y,Z]$ such that $\mathsf{var(A)} \subseteq \mathsf{var(p)} \cup \mathsf{var(q)}$ and B does not have any monomial that is divisible by $p \cdot q$ and contains only variables present in p and q.

Observation 1. *[10] For a multilinear polynomial $f \in \mathbb{F}[Y,Z]$, we have $\widehat{M_f} = M_f$.*

Observe that the matrix $\widehat{M_f}$ has polynomial entries. Therefore $\text{rank}(\widehat{M_f})$ is defined only under a substitution function that substitutes every variable in f to a field element.

For any substitution function $S : Y \cup Z \to \mathbb{F}$, let us denote by $\widehat{M_f}|_S$ the matrix obtained by substituting every variable in f at each entry of $\widehat{M_f}$ to the field element given by S. Define, $\text{maxrank}(\widehat{M_f}) \triangleq \max_{S: Y \cup Z \to \mathbb{F}} \text{rank}(\widehat{M_f}|_S)$. Having defined polynomial coefficient matrix $\widehat{M_f}$ and $\text{maxrank}(\widehat{M_f})$ we now look at properties of $\widehat{M_f}$ with respect to maxrank.

Lemma 3. [10]*(Sub-additivity.) Let $f, g \in \mathbb{F}[Y,Z]$. Then,* $\text{maxrank}(\widehat{M_{f+g}}) \leq \text{maxrank}(\widehat{M_f}) + \text{maxrank}(\widehat{M_g})$.

Lemma 4. [10]*(Sub-multiplicativity.) Let $Y_1, Y_2 \subseteq Y$ and $Z_1, Z_2 \subseteq Z$ such that $Y_1 \cap Y_2 = \emptyset$ and $Z_1 \cap Z_2 = \emptyset$. Then for any polynomials $f \in \mathbb{F}[Y_1, Z_1]$, $g \in \mathbb{F}[Y_2, Z_2]$ we have:* $\text{maxrank}(\widehat{M_{fg}}) = \text{maxrank}(\widehat{M_f}) \cdot \text{maxrank}(\widehat{M_g})$.

A partition of X is a function $\varphi : X \to Y \cup Z \cup \{0,1\}$ such that φ is an injection when restricted to $Y \cup Z$, i.e., $\forall x \neq x' \in X$, if $\varphi(x) \in Y \cup Z$ and $\varphi(x') \in Y \cup Z$ then $\varphi(x) \neq \varphi(x')$. Let F be an ROF and $\varphi : X \to Y \cup Z \cup \{0,1\}$ be a partition function. Define F^φ to be the formula obtained by replacing every variable x that appears as a leaf in F by $\varphi(x)$. Then the polynomial f^φ computed by F^φ is $f^\varphi = f(\varphi(x_1), \ldots, \varphi(x_n))$. Observe that $f^\varphi \in \mathbb{F}[Y,Z]$.

An arithmetic formula $\mathcal{F}$ is said to be a *constant-minimal formula* if no gate u in F has both its children to be constants. Observe that for any arithmetic formula F, if there exists a gate u in F such that $u = a \ \mathsf{op} \ b, a, b \in \mathbb{Z}$ then we can replace u in F by the constant $a \ \mathsf{op} \ b$, where $\mathsf{op} \in \{+, -\}$. Thus we assume without loss of generality that $\mathcal{F}$ is constant-minimal.

We need some observations on formulas that compute natural numbers. Recall that an arithmetic formula $\mathcal{F}$ is said to be monotone if $\mathcal{F}$ does not contain any negative constants.

Let G be a monotone arithmetic formula were the leaves are labeled numbers in $\mathbb{N}$. Then for any gate v in G, the value of v denoted by $\mathsf{value}(v)$ is defined as : If u is a leaf then $\mathsf{value}(u) = a$ where $a \in \mathbb{N}$ is the label of u and $u = u_1 \ \mathsf{op} \ u_2$ then $\mathsf{value}(u) = \mathsf{value}(u_1) \ \mathsf{op} \ \mathsf{value}(u_2)$, where $\mathsf{op} \in \{+, \times\}$. Finally, $\mathsf{value}(G)$ is the value of the output gate of G. Let G be a monotone arithmetic formula with leaves labelled by either 1 or 2. A node u a is called a *rank-*$(1,2)$*-separator* if u is a leaf and $\mathsf{value}(u) = 2$ or $u = u_1 + u_2$ with $\mathsf{value}(u) = 2$ and $\mathsf{value}(u_1) = \mathsf{value}(u_2) = 1$. The following is a simple upper bound on the value computed by a formula.

Lemma 5. *Let G be a binary monotone arithmetic formula with t leaves. If every leaf in G takes a value at most $N > 1$, then* $\mathsf{value}(G) \leq N^t$.

Proof. The proof is by induction on the size of the formula. Base Case : $s = 1$

- If G has a single $+$ gate then $G) \leq N + N \leq N^2$.
- If G has a single $\times$ gate then $G) \leq N \cdot N = N^2$.

Induction Step : Let u be the output gate of G with children u_1 and u_2. Let the number of leaves in the sub formula rooted at u_1 and u_2 be t_1 and t_2.

- If u is a $+$ gate. Then, $\mathsf{value}(u) = \mathsf{value}(u_1) + \mathsf{value}(u_2)$. By induction hypothesis, $\mathsf{value}(u) \leq N^{t_1} + N^{t_2} \leq N^{t_1+t_2} \leq N^t$.
- If u is a $\times$ gate. Then, $\mathsf{value}(u) = \mathsf{value}(u_1) \times \mathsf{value}(u_2)$. By induction hypothesis, $\mathsf{value}(u) \leq N^{t_1} \times N^{t_2} \leq N^{t_1+t_2} \leq N^t$.

□

Any formula with a large value should have a large number of *rank*-$(1,2)$-*separator*s.

Lemma 6. *Let F be a binary monotone arithmetic formula with leaves labeled by either 1 or 2. If $\mathsf{value}(F) > 2^r$ then there exists at least $\frac{r}{\log N}$ nodes that are rank-$(1,2)$-separators.*

Proof. Let F be a binary monotone arithmetic formula with leaves labeled by either 1 or 2. First mark every node u such that u is a *rank*-$(1,2)$-*separator* and remove sub-formula rooted at u except u. Consider any leaf v that remains unmarked and along the path from v to root there is no node that is marked. Then $\mathsf{value}(v) = 1$. Consider the unique path from v to root in F. Let p the first node in the path such that $\mathsf{value}(p) \geq 2$. Let p_1 and p_2 be the children of p. Without loss of generality let p_1 be an ancestor of v. Then observe that there is atleast one marked node(say q) in the sub-formula rooted at p_2. Set $\mathsf{value}(q) = \mathsf{value}(q) + 1$. If p is a $+$ gate set $p_1 = 0$ else set $p_1 = 1$. Let $u_1, \ldots, u_t$ be the leaves of the resulting formula at the end of this process. For every $1 \leq i \leq t$, we have $2 \leq \mathsf{value}(u_i) \leq N$. Therefore by Lemma 5, $\mathsf{value}(F) \leq N^t$. Since $\mathsf{value}(F) > 2^r$, we have $2^r < N^t$. Therefore $t > \frac{r}{\log N}$ as required. □

Finally, we will use the following variants of Chernoff-Hoeffding bounds.

Theorem 5. [2]*(Chernoff-Hoeffding bound) Let $X_1, X_2, \ldots, X_n$ be independent random variables. Let $X = X_1 + X_2 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$. Then for any $\delta > 0$,*

(1) $\Pr[X > (1+\delta)\mu] < \left(\frac{e^\delta}{(1+\delta)^{(1+\delta)}}\right)^\mu$*; and*

(2) $\Pr[X \geq (1+\delta)\mu] \leq e^{\frac{-\delta^2\mu}{3}}$*; and*

(3) $\Pr[X \leq (1-\delta)\mu] \leq e^{\frac{-\delta^2\mu}{2}}$.

3 Hardness of representation for Sum of ROPs

Let $X = \{x_1, \ldots, x_{2n}\}, Y = \{y_1, \ldots, y_{2n}\}, Z = \{z_1, \ldots, z_{2n}\}$. Define $\mathcal{D}'$ as a distribution on the functions $\varphi : X \to Y \cup Z$ as follows : For $1 \leq i \leq 2n$,

$$\varphi(x_i) \in \begin{cases} Y & \text{with prob. } \frac{1}{2} \\ Z & \text{with prob. } \frac{1}{2} \end{cases}$$

Observe that $|\varphi(X) \cap Y| = |\varphi(X) \cap Z|$ is not necessarily true. Let F be a binary arithmetic formula computing a polynomial f on the variables $X = \{x_1, \ldots, x_{2n}\}$. Note that any gate with at least one variable as a child can be classified as:

(1) type-A gates : sum gates both of whose children are variables,

(2) type-B gates : product gates both of whose children are variables,

(3) type-C gates : sum gates exactly one child of which is a variable and the other an internal gate; and

(4) type- D gates: product gates exactly one child of which is a variable and the other an internal gate

Given any ROF F, let there be a type-A gates, b type-B, c type-C and d type-D gates in F. Note that $2a + 2b + c + d = 2n$. Let $\varphi \sim \mathcal{D}'$. Let there be a' gates of type-A that achieve rank-1 under φ and let a'' gates of type-A that achieve rank-2 under φ. Then, $a = a' + a''$.

Lemma 7. [1] *Let F be an* ROF *computing an* ROP *f and $\varphi : X \to Y \cup Z$. Then,* $\text{rank}(M_{f^\varphi}) \le 2^{a''+\frac{a'}{2}+b+\frac{c}{2}}$.

Proof. Observe that for any type-D gate $g = h \times x$, $\text{rank}(M_{g^\varphi}) = \text{rank}(M_{(x\cdot h)^\varphi}) = \text{rank}(M_{h^\varphi})$, and hence type-$D$ gates do not contribute to the rank.

The proof is by induction on the structure of F. Base case is when F is of depth 1. Let r be the root gate of F computing the polynomial f. Then

- r is an type-A gate with children x_1, x_2 : $f = x_1 + x_2$. For any φ, we have $\text{rank}(M_{f^\varphi}) \le 2$. Then $a = 1, b = 0, c = 0$. Therefore either $a' = 1$ or $a'' = 1$. In either case, $\text{rank}(M_{f^\varphi}) \le 2^{a''+\frac{a'}{2}+b}$.
- r is a type-B gate with children x_1, x_2 : $f = x_1 \cdot x_2$. For any φ we have $\text{rank}(M_{f^\varphi}) \le 1$. Then $a = 0, b = 1, c = 0$. Therefore $\text{rank}(M_{f^\varphi}) \le 2^{a''+\frac{a'}{2}+b+\frac{c}{2}}$.

For the induction step, we have the following cases based on the structure of f.

- r is a type-C gate with children x, h, i.e., $f = h + x$. For any φ, we have by sub-additivity $\text{rank}(M_{f^\varphi}) \le \text{rank}(M_{h^\varphi}) + \text{rank}(M_{x^\varphi})$. Let a'_h, a''_h be the number of type-A gates in the sub-formula rooted at h that achieve rank-1 and rank-2 under φ respectively. Let b_h, c_h be the number of type-B and c type-C gates in the sub-formula rooted at h. We now have $a' = a'_h, a'' = a''_h, b = b_h, c = c_h + 1$, and $\text{rank}(M_{f^\varphi}) \le \text{rank}(M_{h^\varphi}) + \text{rank}(M_{x^\varphi})$. By Induction hypothesis $\text{rank}(M_{h^\varphi}) \le 2^{a''_h+\frac{a'_h}{2}+b_h+\frac{c_h}{2}}$. First suppose the case when $a''_h + \frac{a'_h}{2} + b_h + \frac{c_h}{2} \ge 1.5$, then, $\text{rank}(M_{f^\varphi}) \le 2^{a''_h+\frac{a'_h}{2}+b_h+\frac{c_h}{2}} + \text{rank}(M_{x^\varphi}) = 2^{a''_h+\frac{a'_h}{2}+b_h+\frac{c_h}{2}} + 1 \le 2^{a''+\frac{a'}{2}+b+\frac{c}{2}}$. Now suppose $a''_h + \frac{a'_h}{2} + b_h + \frac{c_h}{2} < 1.5$ and hence $a''_h + \frac{a'_h}{2} + b_h + \frac{c_h}{2} \le 1$ (since a''_h, a_h, b_h and c_h are integers). If $a''_h = 1$, then $rank(M_{f^\varphi}) = 2 < 2^{a''+\frac{a'}{2}+\frac{b}{2}+\frac{c}{2}}$. Finally, if $a''_h = 0$, for all of the remaining possibilities, we have $\text{rank}(M_{f^\varphi}) \le 2 \le 2^{a''+\frac{a'}{2}+b+\frac{c}{2}}$.
- $r = g \times h$ be an internal gate. For $H \in \{g, h\}$, let a'_H, a''_H be the number of type-A gates that achieve rank-1 and rank-2 under φ respectively and b_H, c_H be the number of type-B and c type-C gates in the sub-formula rooted at H. Then $f = g * h$ where $* \in \{+, \times\}$. In either case, $\text{rank}(M_{f^\varphi}) \le \text{rank}(M_{g^\varphi}) \cdot \text{rank}(M_{h^\varphi})$, and from Induction hypothesis $\text{rank}(M_{f^\varphi}) \le \cdot 2^{a''_g+\frac{a'_g}{2}+b_g+\frac{c_g}{2}} 2^{a''_h+\frac{a'_h}{2}+b_h+\frac{c_h}{2}}$. Since $a' = a'_g + a'_h, a'' = a''_g + a''_h, b = b_h + b_g, c = c_g + c_h$ we have $\text{rank}(M_{f^\varphi}) \le 2^{a''+\frac{a'}{2}+b+\frac{c}{2}}$.

□

[1] A brief outline of the proof of Lemma 7 was suggested by an anonymous reviewer, the details included here for completeness and since the details were worked out completely by the authors.

Lemma 8. *Let F be a* ROF *and $\varphi \sim \mathcal{D}'$. Let a' be the number type-A gates that achieve* rank-1 *under φ. Then,* $\Pr_{\varphi\sim\mathcal{D}'}\left[\frac{2}{5}a \leq a' \leq \frac{3}{5}a\right] \geq 1 - 2^{-\Omega(a)}$.

Proof. Let v be a type-A gate in F. Then $f_v = x_i + x_j$ for some $i,j \in [N]$. Then $\Pr[\text{rank}(M_{f_v^{\varphi}}) = 1] = \Pr[(\varphi(x_i), \varphi(x_j) \in Z) \vee (\varphi(x_i), \varphi(x_j) \in Y)] = \frac{1}{2}$. Therefore, $\mathbb{E}[a'] = a/2$. Applying Theorem 5 (2) and (3) with $\delta = 1/2$, we get the required bounds for a'. □

Lemma 9. *Let F be a* ROF *computing and* ROP *f $2n$ variables, and $\varphi \sim \mathcal{D}'$. Then with probability at least $1 - 2^{-\Omega(n)}$,* $\text{rank}(M_{f^\varphi}) \leq 2^{n - \frac{n}{5\log n}}$.

Proof. Consider the following two cases:
Case 1 : $a + c \geq \frac{2n}{\log n}$**.** Then either $a \geq \frac{n}{\log n}$ or $c \geq \frac{n}{\log n}$.
Firstly, suppose $a \geq \frac{n}{\log n}$, then by Lemma 7, we have $\text{rank}(M_{f^\varphi}) \leq 2^{a''+a'/2+b+c/2}$. Since $2a' + 2a'' + 2b + c + d = 2n$, we have $a'/2 + a'' + b + c/2 \leq n - a'/2$. By Lemma 8, $a' \geq 2/5a \geq 2n/5\log n$. Therefore, $\text{rank}(M_{f_\varphi}) \leq 2^{a''+a'/2+b+c/2} \leq 2^{n-a'/2} \leq 2^{n-\frac{n}{5\log n}}$.
Now suppose $c \geq \frac{n}{5\log n}$. Since $2a'+2a''+2b+c \leq 2n$, we have $a''+a'+b+c/2 \leq n-c/2 \leq n-n/2\log n$. Therefore by Lemma 7, $\text{rank}(M_{f^\varphi}) \leq 2^{a''+a'/2+b+c/2} \leq 2^{a''+a'+b+c/2} \leq 2^{n-c/2} \leq 2^{n-\frac{n}{5\log n}}$.
Case 2 : $a + c < \frac{2n}{\log n}$**.** Observe that $b \leq n$. Since any type B gate achieves rank 1 under any φ, by a simple inductive argument we have $\text{rank}(M_{f^\varphi}) \leq 2^{a+c+b/2}$ for any φ. Therefore $\text{rank}(M_{f^\varphi}) \leq 2^{a+c+b/2} \leq 2^{n/2+2n/\log n} \leq 2^{n-n/5\log n}$. □

The following polynomial was introduced by Raz and Yehudayoff [17].

Definition 1. *Let $n \in \mathbb{N}$ be an integer. Let $X = \{x_1, \ldots, x_{2n}\}$ and $\mathcal{W} = \{w_{i,k,j}\}_{i,k,j\in[2n]}$. For any two integers $i, j \in \mathbb{N}$, we define an interval $[i,j] = \{k \in \mathbb{N}, i \leq k \leq j\}$. Let $|[i,j]|$ be the length of the interval $[i,j]$. Let $X_{i,j} = \{x_p \mid p \in [i,j]\}$ and $W_{i,j} = \{w_{i',k,j'} \mid i', k, j' \in [i,j]\}$. For every $[i,j]$ such that $|[i,j]|$ is even we define a polynomial $g_{i,j} \in \mathbb{F}[X, \mathcal{W}]$ as $g_{i,j} = 1$ when $|[i,j]| = 0$ and if $|[i,j]| > 0$ then, $g_{i,j} \triangleq (1+x_ix_j)g_{i+1,j-1} + \sum_k w_{i,k,j}g_{i,k}g_{k+1,j}$. where x_k, $w_{i,k,j}$ are distinct variables, $1 \leq k \leq j$ and the summation is over $k \in [i+1, j-2]$ such that the interval $[i,k]$ is of even length. Let $g \triangleq g_{1,2n}$.*

In the following, we view g as polynomial in $\{x_1, \ldots, x_{2n}\}$ with coefficients from the rational function field $\mathbb{G} \triangleq \mathbb{F}(\mathcal{W})$.

Lemma 10. *Let Let $X = \{x_1, \ldots, x_{2n}\}$, $Y = \{y_1, \ldots, y_{2n}\}$, $Z = \{z_1, \ldots, z_{2n}\}$ and $\mathcal{W} = \{w_{i,k,j}\}_{i,k,j\in[2n]}$ be sets of variables. Suppose $\varphi \sim \mathcal{D}'$ such that $||\varphi(X) \cap Y| - |\varphi(X) \cap Z|| = \ell$. Then for the polynomial g as in Definition 1 we have,* $\text{rank}(M_{g^\varphi}) \geq 2^{n-\ell/2}$.

Proof. Proof builds on Lemma 4.3 in [17] as a base case and is by induction on $n + \ell$.
Base case: Either $\ell = 0$ or $\ell = 2n$. For $\ell = 0$, the statement follows by Lemma 4.3 in [17]. When $\ell = 2n$, then $\text{rank}(M_{g^\varphi}) = 1 = 2^{n-\ell/2}$.
Induction step: Without loss of generality, assume that $|\varphi(X) \cap Y| = |\varphi(X) \cap Z| + \ell$. There are three possibilities:

Case 1 : Let $\varphi(x_1) \in Y$ and $\varphi(x_{2n}) \in Z$ or vice versa. In this case

$$\begin{aligned}\text{rank}(M_{g^\varphi}) &\geq \text{rank}(M_{(1+x_1x_{2n})^\varphi})\,\text{rank}(M_{g^\varphi_{2,2n-1}}) = 2 \cdot \text{rank}(M_{g^\varphi_{2,2n-1}}) \\ &\geq 2 \cdot 2^{n-1-\ell/2} = 2^{n-\ell/2} \qquad \text{[By Induction Hypothesis.]}\end{aligned}$$

Case 2 : $\varphi(x_1) \in Y$ and $\varphi(x_{2n}) \in Y$. Then

$$\begin{aligned}\text{rank}(M_{g^\varphi}) &\geq \text{rank}(M_{(1+x_1x_{2n})^\varphi})\,\text{rank}(M_{g^\varphi_{2,2n-1}}) = 1 \cdot \text{rank}(M_{g^\varphi_{2,2n-1}}) \\ &\geq 2^{(2n-2)/2-(\ell-2)/2} = 2^{n-\ell/2}. \qquad \text{[By Induction Hypothesis.]}\end{aligned}$$

For the penultimate inequality above, note that $g_{2,2n-1}$ is defined on $X' = \{x_2, \ldots, x_{2n-1}\}$ and $||\varphi(X') \cap Y| - |\varphi(X') \cap Z|| = \ell - 2$ and hence by Induction Hypothesis, $\text{rank}(M_{g^\varphi_{2,2n-1}}) \geq 2^{(2n-2)/2-(\ell-2)/2}$.

Case 3 $\varphi(x_1) \in Z$ and $\varphi(x_{2n}) \in Z$. Then there is an $i \in \{2, 2n-1\}$ such that $||\varphi(X_i) \cap Y| - |\varphi(X_i) \cap Z|| = 0$ and $||\varphi(X \setminus X_i) \cap Y| - |\varphi(X \setminus X_i) \cap Z|| = \ell$, where $X_i = \{x_1, \ldots, x_i\}$. Then by the definition of g, over $\mathbb{G}$, $\text{rank}(M_{g^\varphi}) \geq \text{rank}(M_{g^\varphi_{1,i}}) \cdot \text{rank}(M_{g^\varphi_{i+1,2n}}) \geq 2^{i/2} \cdot 2^{(2n-i)/2-\ell/2} = 2^{n-\ell/2}$, since $\text{rank}(M_{g^\varphi_{1,i}}) = 2^{i/2}$ by Lemma 4.3 in [17], and $\text{rank}(M_{g^\varphi_{i+1,2n}}) \geq 2^{(2n-i)/2-\ell/2}$ by Induction Hypothesis.

□

Lemma 11. $\Pr_{\varphi\sim\mathcal{D}'}[n - n^{2/3} \leq |\varphi(X) \cap Y| \leq n + n^{2/3}] \geq 1 - 2^{-\Omega(n^{1/3})}$.

Proof. Proof is a simple application of Chernoff's bound (Theorem 5) with $\delta = 1/n^{1/3}$. □

Corollary 1. $\Pr_{\varphi\sim\mathcal{D}'}[\text{rank}(M_{g^\varphi}) \geq 2^{n-n^{2/3}/2}] \geq 1 - 2^{-\Omega(n^{1/3})}$.

Proof. Apply Lemma 10 with $\ell = n/n^{1/3} = n^{2/3}$ and the probability bound follows from Lemma 11.

□

Proof of Theorem 4

Proof. Suppose $s < 2^{n/10\log n}$. Then by Lemma 9 and union bound, probability that there is an i such that $\text{rank}(M_{f_i^\varphi}) \geq 2^{n-n/5\log n}$ is $s2^{-\Omega(n)} = 2^{-\Omega(n)}$ and hence by Lemma 1, $\text{rank}(M_{g^\varphi}) \leq s2^{n-n/5\log n} \leq 2^{n-n/10\log n}$ with probability $1 - 2^{-\Omega(n)}$. However, by Corollary 1, $\text{rank}(M_{g^\varphi}) \geq 2^{n-n^{2/3}/2} > 2^{n-n/10\log n}$ with probability at least $1 - 2^{-\Omega(n^{1/3})}$, a contradiction. Therefore, $s = 2^{\Omega(n/\log n)}$. □

4 Sum of Products of ROPs

4.1 ROPs under random partition

Throughout the section, let $m \triangleq N^{1/3}$, $n \triangleq \sqrt{N}$ and $\kappa = 20\log n$. Let $\mathcal{D}$ denote the distribution on the functions $\varphi : X \to Y \cup Z \cup \{0, 1\}$ defined as follows

$$\varphi(x_{ij}) \in \begin{cases} Y & \text{with prob. } \frac{m}{N} \\ Z & \text{with prob. } \frac{m}{N} \\ 1 & \text{with prob. } \frac{\kappa n}{N} \\ 0 & \text{with prob. } 1 - \left(\frac{2m+\kappa n}{N}\right) \end{cases}$$

Lemma 12. *Let f be an* ROP *computed by an* ROF *F and $\varphi \sim \mathcal{D}$. Let X be a random variable that denotes the number of non-zero multiplication gates at depth 1. Then* $\Pr_{\varphi\sim D}\left[X > \mathcal{O}(N^{1/6}\log n)\right] \leq 2^{-\Omega(m)}$.

Proof. Consider a multiplication gate g at depth 1, with at least two variables as its input. Let m be the monomial (excluding the coefficient) computed by g, note that $d = \deg(m) \geq 2$. we have,

$$\Pr_{\varphi\sim D}[m^{\varphi} \neq 0] = \left(\frac{2m+\kappa n}{N}\right)^{d} \leq \left(\frac{2m+\kappa n}{N}\right)^{2} \leq \left(\frac{2\kappa n}{N}\right)^{2} \leq \left(\frac{2\kappa}{n}\right)^{2} \leq \mathcal{O}\left(\frac{\kappa^2}{N}\right).$$

In the above, we have used the fact that $2m < \kappa n$ for large enough n. Since F is an ROF in N variables , the ROP f computed by F has at most $N/2$ multiplication gates where both the inputs are variables. Then, $\mu \triangleq \mathrm{E}[X] \leq \frac{N}{2} \cdot \Pr_{\varphi\sim D}[m^{\varphi} \neq 0] \leq N \cdot c\left(\frac{\kappa^2}{N}\right) \leq c(\kappa^2)$, where c is a constant. By Theorem 5, let $\delta = \frac{N^{1/6}}{\log n} > 0$, we have

$$\Pr_{\varphi\sim D}\left[X > \left(1+\frac{N^{1/6}}{\log n}\right) c\log^2 n\right] \leq \mathrm{e}^{\frac{-cN^{2/6}}{3}} \leq 2^{-\frac{2cN^{1/3}}{3}} \leq 2^{-\Omega(m)}.$$

□

Lemma 13. *Let F be an* ROF *computing an* ROP *f and $\varphi \sim \mathcal{D}$. Then there exists an* ROF *F' such that every gate in F' at depth-1 is an addition gate, and* $\mathrm{rank}(M_{F^{\varphi}}) \leq \mathrm{rank}(M_{F'^{\varphi}}) \times 2^{\mathcal{O}(N^{1/6}\log n)}$ *with probability atleast* $1 - 2^{-\Omega(m)}$.

Proof. Given an arithmetic formula F we construct the formula F' by replacing every multiplication gate v at depth-1 in F by the constant 1. Let X of product gates of fan-in ≥1 in F^{φ}. Then, by the construction of F',

$$\mathrm{rank}(M_{F^{\varphi}}) \leq \mathrm{rank}(M_{F'^{\varphi}}) \times 2^{X}.$$

Now by Lemma 12, with probability atleast $1 - 2^{-\Omega(m)}$ we have,

$$\mathrm{rank}(M_{F^{\varphi}}) \leq \mathrm{rank}(M_{F'^{\varphi}}) \times 2^{\mathcal{O}(N^{1/6}\log n)}.$$

□

Recall that an arithmetic formula F over $\mathbb{Z}$ is said to be monotone if it does not have any node labelled by a negative constant.

Lemma 14. *Let F be an* ROF, *and $\varphi \sim \mathcal{D}$. Then there exists a monotone formula G such that* $\mathrm{rank}(M_{F^{\varphi}}) \leq \mathsf{value}(G^{\varphi})$.

Proof. Let F be an constant-minimal ROF, and $\varphi \sim \mathcal{D}$. Let G^{φ} be a monotone formula obtained from F^{φ} as follows:
By short circuiting the gates if necessary, every leaf node v labelled by a constant is replaced by 1. For every gate v in F^{φ} with at least one leaf as a child,

- If $v = \prod_{j=1}^{k} v_j$, with $v_1, \ldots, v_i$, $i \geq 1$ are non-constant leaf gates, then replace the gates $v_1 \times v_2 \times \ldots \times v_i$ by the rank of the polynomial computed by $\varphi(v_1 \times v_2 \times \ldots \times v_i)$.
- Similarly, if $v = \sum_{j=1}^{k} v_j$, with $v_1, \ldots, v_i$, $i \geq 1$ are non-constant leaf gates, then replace the gates $v_1 + v_2 + \ldots + v_i$ by the rank of the polynomial computed by $\varphi(v_1 + v_2 + \ldots + v_i)$.

Clearly, the formula constructed above is monotone, since negative constants (if any) in F^{φ} have been replaced by 1. Then, by Lemmas 1 and 2, we have for any φ, $\mathrm{rank}(M_{F^{\varphi}}) \leq \mathsf{value}(G^{\varphi})$. □

Observation 2. *Let F be an* ROF *and $\varphi \sim \mathcal{D}$. By Lemma 14, we have,* $\Pr[\mathrm{rank}(M_{F^{\varphi}}) > 2^r] \leq \Pr[\mathsf{value}(G^{\varphi}) > 2^r]$.

Definition 2. *Let F be an* ROF *and $\varphi \sim \mathcal{D}$. A gate u in F^φ is called a rank-$(1,2)$-separator, if either u is a leaf with* $\text{rank}(M_{u^\varphi}) = 2$*, or $u = u_1 + u_2$ with* $\text{rank}(M_{u_1^\varphi}) = \text{rank}(M_{u_2^\varphi}) = 1$ *and* $\text{rank}(M_{u^\varphi}) = 2$*.*

Corollary 2. *Let F be an* ROF*and $\varphi \sim \mathcal{D}$. Then by Lemma 6 we have*

$$\Pr[\text{rank}(M_{F^\varphi}) > 2^r] \le \Pr[\exists\ u_1, \ldots, u_{\frac{r}{\log N}} \in F^\varphi \ s.t.\ \forall 1 \le i \le \tfrac{r}{\log N}\ u_i \textit{ is a rank-}(1,2)\textit{-separator}]$$

Now all we need to do is to estimate the probability that a given set of nodes $u_1, \ldots, u_t$ where $t > \frac{r}{\log N}$ are a set of *rank*-$(1,2)$-*separator*s.

Let $u_i = u_{i,1} + u_{i,2}$ be a *rank*-$(1,2)$-*separator* in F^φ and $\text{rank}(M_{u_i^\varphi}) = 2$. Consider the sub-formula rooted at u_i. Note that $\text{rank}(M_{u_i^\varphi}) = 2$ only if $\mathsf{var}(\mathsf{u_i^\varphi}) \cap \mathsf{Y} \neq \emptyset$ and $\mathsf{var}(\mathsf{u_i^\varphi}) \cap \mathsf{Z} \neq \emptyset$. By simple applications of Chernoff's bound, we show that only a small number of $u_1, \ldots, u_t$ can achieve rank-2 under a random $\varphi \sim \mathcal{D}$. Let $\ell_{i_1}, \ldots, \ell_{i_r}$ be the addition gates at depth-1 in the sub-formula rooted at u_i. For $1 \le i \le t$ we define $S_i \triangleq \mathsf{var}(\ell_{\mathsf{i_1}}) \cup \cdots \cup \mathsf{var}(\ell_{\mathsf{i_r}})$. Let $v_1, \ldots, v_p$ be the addition gates at depth-1 in F^φ that are not contained in any of the sub-formulas rooted at $u_1, \ldots, u_t$. For $1 \le j \le p$, let $S_{t+j} = \mathsf{var}(\mathsf{v_j})$, also let $q = t + p$.

Note that $|S_i| \le s_F \le N^{1/2+\lambda}$. By merging sets in a greedy fashion whenever necessary, we assume that $|S_i| \in [N^{1/2+\lambda}, 2N^{1/2+\lambda}]$. Therefore $q \le N^{1/2-\lambda}$.

For $S \subseteq X$ and $\varphi \sim \mathcal{D}$ let $S^\varphi \triangleq \{\varphi(x) \mid x \in S\}$. Let $W = Y \cup Z$. We define the following random variables.

$$\begin{aligned}
X_2 &= \{S_i \mid 1 \le i \le q,\ |S_i^\varphi \cap W| = 2,\ |S_i^\varphi \cap Y| = 1,\ |S_i^\varphi \cap Z| = 1\}.\\
X_3 &= \{S_i \mid 1 \le i \le q,\ |S_i^\varphi \cap W| = 3,\ |S_i^\varphi \cap Y| \neq \phi,\ |S_i^\varphi \cap Z| \neq \phi\}.\\
X_4 &= \{S_i \mid 1 \le i \le q,\ |S_i^\varphi \cap W| = 4,\ |S_i^\varphi \cap Y| = 2,\ |S_i^\varphi \cap Z| = 2\}.\\
X_5 &= \{S_i \mid 1 \le i \le q,\ |S_i^\varphi \cap W| = 5,\ |S_i^\varphi \cap Y| = 3 \text{ and } |S_i^\varphi \cap Z| = 2 \text{ or vice versa}\}.\\
X_{\ge 6} &= \{S_i \mid 1 \le i \le q,\ |S_i^\varphi \cap W| \ge 6,\ |S_i^\varphi \cap Y| \ge 3,\ |S_i^\varphi \cap Z| \ge 3\}.
\end{aligned}$$

Then we have,

Lemma 15. *With the notations as above,*

(1) $\Pr[|X_2| + |X_3| + |X_4| + |X_5| \ge 4N^{4/15}] \le 2^{-\Omega(m)}$*; and*

(2) (2) $\Pr[|X_{\ge 6}| \ge 1] \le 2^{-\Omega(m)}$*.*

Proof. We argue that $\Pr[|X_2| \ge N^{1/5}] \le 2^{-\Omega(m)}$, the argument for the case of $\Pr[|X_3| \ge N^{1/5}]$, $\Pr[|X_4| \ge N^{1/5}]$ and $\Pr[|X_5| \ge N^{1/5}]$ are similar and the result follows by a simple union bound. Let $\mu_2 = \mathbb{E}[|X_2|] = \sum_{i=1}^{q} \frac{|S_i|(|S_i|-1)}{2} \left(\frac{m}{N}\right)^2 \left(1 - \frac{m}{N}\right)^{|S_i|-2}$. Since $\lambda \le \frac{1}{30}, q \le N^{1/2-\lambda}$ and $|S_i| \in [N^{1/2+\lambda}, 2N^{1/2+\lambda}]$, we have $\mu_2 = O(N^{1/5})$. Applying Theorem 5 with $\delta = \sqrt{\frac{m}{\mu_2}} - 1$ we get $\Pr[|X_2| \ge N^{4/15}] \le 2^{-\Omega(m)}$. With a similar argument we get $\Pr[|X_i| \ge N^{4/15}] \le 2^{-\Omega(m)}$ for $i \in \{3,4,5\}$ and (1) follows from union bound. For (2), we have

$$\mathbb{E}[|X_{\ge 6}] \le \sum_{i=1}^{q} |S_i|(|S_i|-1)(|S_i|-2)(|S_i|-3)(|S_i|-4)(|S_i|-5)(m/N)^6(1-m/N)^{|S_i|-6} \le 2^6 N^{-1/2+5\lambda}.$$

Then if $\lambda \le \frac{1}{30}$, setting $\delta = 1/\mu - 1$ in Theorem 5, we get $\Pr[|X_{\ge 6}| \ge 1] \le 2^{-\Omega(m)}$ as required. □

Lemma 16. *The number of rank-$(1,2)$-separator among $u_1, \ldots, u_t$ is at most $O(N^{4/15})$ with probability at least $1 - 2^{-\Omega(m)}$.*

Proof. Firstly, we show that with probability atleast $1 - 2^{-\Omega(m)}$ among $u_1, \ldots, u_t$ the number of *rank*-$(1,2)$-*separator*s is upper bounded by $|X_2| + |X_3| + 2(|X_4| + |X_5|)$, which proves the lemma as an immediate consequence. Note that the sets X_2, X_3, X_4, X_5 and $X_{\geq 6}$ are disjoint. Any $S_i \in X_2$ has exactly one variable each from Y and Z, and hence each such S_i can cause at most one of the u_j's to be a rank-(1,2)-separator. Similarly, $S_i \in X_3$ can also cause at most one of the u_j's to be a rank-(1,2)-separator. However, an $S_i \in X_4$, can result in at most two of the gates $u_1, \ldots, u_q$ being *rank*-$(1,2)$-*separator*s, since S_i could have been a result of merging two or more linear forms. Now the bound follows from Lemma 15. ☐

Lemma 17. *Let f be an* ROP*on N variables computed by an* ROF *F, with $s_F \leq N^{1/2+\lambda}$ for some $\lambda \leq 1/30$. Then,* $\Pr_{\varphi \sim \mathcal{D}}[\text{rank}(M_{f^\varphi}) \geq 2^{N^{4/15}}] \leq 2^{-\Omega(m)}$.

Proof. By Corollary 2 and, we have

$$\begin{aligned}
\Pr[\text{rank}(M_{f^\varphi}) \geq 2^{N^{4/15}}] &\leq \Pr[\exists\ \textit{rank}\text{-}(1,2)\text{-}\textit{separators}\ u_1, \ldots, u_{\frac{N^{1/4}}{\log N}}] \\
&\leq \binom{N}{\frac{N^{1/4}}{\log N}} 2^{-\Omega(m)} \leq 2^{-\Omega(m)}; \text{ by Lemma 6 and since } \binom{N}{\frac{N^{1/4}}{\log N}} = 2^{o(m)}.
\end{aligned}$$

☐

4.2 Polynomials with High Rank

In this section, we prove rank lower bounds for two polynomials under a random partition $\varphi \sim \mathcal{D}$. The first one is in VP and the other one is in VNP.

Lemma 18. *Let $p_{lin} = \ell_1 \cdots \ell_{m'}$ where $\ell_j = \left(\sum_{i=(j-1)(N/2m)+1}^{jN/2m} x_i\right) + 1$, where $m' = 2m$. Then,* $\text{rank}(M_{p_{lin}^\varphi}) = 2^{\Omega(m)}$ *with probability* $1 - 2^{-\Omega(m)}$.

Proof. Let $p_{lin} = \ell_1 \cdots \ell_{m'}$ where $\ell_j = \left(\sum_{(j-1)(N/2m)+1}^{jN/2m} x_i\right) + 1$ and $m' = 2m$.

Let us define indicator random variables $\rho_1, \rho_2, \ldots, \rho_{m'}$.

$$\rho_i = \begin{cases} 1 & \text{if rank}(M_{\ell_i^\varphi}) = 2 \\ 0 & \text{otherwise} \end{cases}$$

Observe that for any $1 \leq i \leq m', \text{rank}(M_{\ell_i^\varphi}) = 2$ iff $\ell_i^\varphi \cap Y \neq \emptyset$ and $\ell_i^\varphi \cap Z \neq \emptyset$. Therefore, $\Pr[\text{rank}(M_{\ell_i^\varphi}) = 2] = \Pr[\ell_i^\varphi \cap Y \neq \emptyset \text{ and } \ell_i^\varphi \cap Z \neq \emptyset]$. For any $1 \leq j \leq m'$, $\Pr[\ell_j^\varphi \cap Y \neq \emptyset \text{ and } \ell_j^\varphi \cap Z \neq \emptyset] \geq \frac{N}{2m}\left(\frac{N}{2m} - 1\right)\left(\frac{m}{N}\right)^2\left(1 - \frac{m}{N}\right)^{\frac{N}{2m}-2} \geq 1/16$ for large enough N. Let $\rho = \sum_{i=1}^{m'} \rho_i$. Then by linearity of expectation, $\mu \triangleq \mathbb{E}[\rho] = \sum_{i=1}^{m'} \mathbb{E}[\rho_i] \geq \frac{m}{8}$. By Theorem 5, $\Pr[\rho < (1-\delta)\mu] \leq e^{-\mu\delta^2/2} = 2^{-\Omega(m)}$. Since $\mu \geq m/8$, we have $\Pr[\rho < (1-\delta)m/8] \leq \Pr[\rho < (1-\delta)\mu] = 2^{-\Omega(m)}$. This concludes the proof, by setting $\delta = 1/4$, since $\text{rank}(M_{p_{lin}^\varphi}) = 2^\rho$. ☐

Throughout the section let φ denote a function of the form $\varphi : X \to Y \cup Z \cup \{0,1\}$. Let X_φ denote the matrix $(\varphi(x_{ij}))_{1 \leq i,j \leq n}$. If and when φ involved in a probability argument, we assume that φ is distributed according to $\mathcal{D}$.

Definition 3. *Let $1 \leq i, j \leq n$. (i,j) is said to be a* Y-special (*respectively* Z-special) *if $\varphi(x_{ij}) \in Y$ (respectively $\varphi(x_{ij}) \in Z$), $\forall i' \in [n], i' \neq i \;\; \varphi(x_{i'j}) \in \{0,1\}$ and $\forall j' \in [n], j' \neq j \;\; \varphi(x_{ij'}) \in \{0,1\}$.*

Lemma 19. *Let $\mathcal{Q} \in \{Y, Z\}$, φ as above and $\chi = |\varphi(X) \cap \mathcal{Q}|$ where $\varphi(X) = \{\varphi(x_{ij})\}_{i,j\in[n]}$. Then,* $\Pr_{\varphi\sim\mathcal{D}}\left[\frac{3m}{4} < \chi < \frac{5m}{4}\right] > 1 - 2^{-\Omega(m)}$.

Proof. Define indicator random variables χ_{ij} for $1 \leq i, j \leq n$:

$$\chi_{ij} = \begin{cases} 1 & \text{if } \varphi(x_{ij}) \in \mathcal{Q} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\chi = \sum_{i=1}^{n} \sum_{j=1}^{n} \chi_{ij}$ and $\mathbb{E}_{\varphi\sim\mathcal{D}}[\chi] = m$. Let $\delta = \frac{1}{4}$, then by Chernoff bounds in Theorem 5,

$$\Pr\left[\chi \geq \frac{5m}{4}\right] \leq \mathrm{e}^{-\frac{\delta^2\mu}{3}} \leq \mathrm{e}^{-\frac{m}{48}} = 2^{-\Omega(m)}; \text{ and} \Pr\left[\chi \leq \frac{3m}{4}\right] \leq \mathrm{e}^{-\frac{\delta^2\mu}{2}} \leq \mathrm{e}^{-\frac{m}{32}} = 2^{-\Omega(m)}.$$

Therefore, $\Pr_{\varphi\sim\mathcal{D}}\left[\frac{3m}{4} < \chi < \frac{5m}{4}\right] = 1 - 2^{-\Omega(m)}$. □

Let $C_1, \ldots, C_n$ denote the columns of X_φ and $R_1, \ldots, R_n$ denote the rows of X_φ.

Definition 4. *Let $\mathcal{Q} \in \{Y, Z\}$. A column C_j, $1 \leq j \leq n$ is said to be $\mathcal{Q}$-*good *if $\exists i \in [n]$, $\varphi(x_{ij}) \in \mathcal{Q}$; and $\forall i' \in [n], i' \neq i$ $\varphi(x_{i'j}) \in \{0, 1\}$. $\mathcal{Q}$-*good *rows are defined analogously.*

Observation 3. *Let C_i be a Y-good column in X_φ. Let $i, i' \in [n]$, R be the event that $\varphi(x_{ij}) \in Y$ and T be the event that $\varphi(x_{i'j}) \in Y$. The events R and T are mutually exclusive.*

By Observation 3 and union bound we have:

Lemma 20. *For $1 \leq i \leq n$, let C_i be a column in X_φ. Then for any $\mathcal{Q} \in \{Y, Z\}$, $\Pr_{\varphi\sim\mathcal{D}}[C_i \text{ is } \mathcal{Q}\text{-good}] = n \cdot \frac{m}{N}\left(1 - \frac{2m}{N}\right)^{n-1}$.*

For $\mathcal{Q} \in \{Y, Z\}$ let $\eta_\mathcal{Q} \triangleq |\{C_i \mid C_i \text{ is } \mathcal{Q}\text{-good}\}|$ and $\zeta_\mathcal{Q} \triangleq |\{R_j \mid R_j \text{ is } \mathcal{Q}\text{-good}\}$.

Lemma 21. *With notations as above, $\forall \mathcal{Q} \in \{Y, Z\}$, $\Pr_{\varphi\sim\mathcal{D}}[\eta_\mathcal{Q} \geq \frac{2m}{3}] \geq 1 - \frac{1}{2^{\Omega(m)}}$; and $\Pr_{\varphi\sim\mathcal{D}}[\zeta_\mathcal{Q} \geq \frac{2m}{3}] \geq 1 - \frac{1}{2^{\Omega(m)}}$.*

Proof. Proof is a simple application for Chernoff's bound. We argue for the case of η_Y, the rest are analogous. For $1 \leq i \leq n$, let

$$\eta_i = \begin{cases} 1 & \text{if } C_i \text{ is Y-good column} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\eta_Y = \eta_1 + \cdots + \eta_n$ and by Observation 3 and Lemma 20 $\mathbb{E}[\eta_i] = \Pr[C_i \text{ is Y-good}] = n \cdot \frac{m}{N}\left(1 - \frac{2m}{N}\right)^{n-1}$. By linearity of expectation, $\mathbb{E}[\eta_Y] = n^2 \cdot \frac{m}{N}\left(1 - \frac{2m}{N}\right)^{n-1} = m\left(1 - \frac{2m}{N}\right)^{n-1}$.

Set $\rho = \left(1 - \frac{2m}{N}\right)^{n-1}$ so that $\mathbb{E}[\eta_Y] = \rho m$. For $\delta = \frac{1}{4}$, we have by Theorem 5,

$$\Pr\left[\eta_Y \leq \left(1 - \frac{1}{4}\right)\rho m\right] \leq \mathrm{e}^{\frac{-(1/4)^2\mu}{2}} \leq \mathrm{e}^{-\mu/32}.$$

As $m = o(n)$ and $N = n^2$, $\lim_{n\to\infty} \frac{2m}{N} = 0$. Thus for sufficiently large n, $\rho \geq 9/10$ and hence $\mu \geq 9m/10$. We conclude $Pr\left[\eta_Y \leq 27m/40\right] \leq 2^{-\Omega(m)}$. Since $27/40 > 2/3$ we have $\Pr[\eta_Y \geq \frac{2m}{3}] \geq 1 - \frac{1}{2^{\Omega(m)}}$ as required. □

Lemma 22. *For $\mathcal{Q} \in \{Y, Z\}$, let $\gamma_{\mathcal{Q}}$ denote the number of $\mathcal{Q}$-special positions in X_φ. Then $\forall \mathcal{Q} \in \{Y, Z\}$, $\Pr_{\varphi \sim \mathcal{D}}\left[\gamma_{\mathcal{Q}} \geq \frac{m}{12}\right] \geq 1 - 2^{-\Omega(m)}$.*

Proof. We argue for $\mathcal{Q} = Y$, the proof is analogous when $\mathcal{Q} = Z$. Let φ be distributed according to $\mathcal{D}$. Consider the following events on X_φ. E1 : $2m/3 \leq |X_\varphi \cap Y| \leq 5m/4$; E2 : The number of Y-good columns and Y-good rows is at least $r \triangleq 2m/3$.

By Lemmas 19 and 21, X_φ satisfies the events E1 and E2 with probability $1 - 2^{-\Omega(m)}$. Henceforth we assume that X_φ satisfies the events E1 and E2.

Without loss of generality, let $R_1, \ldots, R_r$ be the first r Y-good rows in X_φ. For every Y-good row R_i, $1 \leq i \leq r$ there exists a corresponding witness column $C_j, j \in [n]$ such that $\varphi(x_{ij}) \in Y$. Without loss of generality, assume $C_1, \ldots, C_r$ be columns that are witnesses for $R_1, \ldots, R_r$ being Y-good. Further, $X_\varphi(C_j)$ denote the set of values along the column C_j.

Suppose among $C_1, \ldots, C_r$, $t \geq 0$ columns are not Y-good, without loss of generality let them be $C_1, C_2, \ldots, C_t$.

Each of the column C_j has at least one variable from Y and hence the columns $C_1, \ldots, C_t$ contain at least t distinct variables from Y. By event E2, there are at least $\frac{2m}{3}$ Y-good columns that are distinct from $C_1, \ldots, C_t$, each containing exactly one distinct variable from Y. Since the total number of variables from Y in X_φ is at most $5m/4$ (by E1) we have, $t \leq \frac{5m}{4} - \frac{2m}{3} \leq \frac{7m}{12}$. That is, at most $7m/12$ of the columns among $C_1, \ldots, C_r$ are not Y-good. Therefore, at least $r - t$ of the columns among $C_1, \ldots, C_r$ are Y good and hence the number of Y-special positions in X_φ is atleast $r - t \geq (2/3 - 7/12)m = \frac{m}{12}$. We conclude, $\Pr_{\varphi \sim \mathcal{D}}\left[\gamma_Y \geq \frac{m}{12}\right] \geq 1 - 2^{-\Omega(m)}$. $\square$

A row R in the matrix $A \in (Y \cup Z \cup \{0,1\})^{n \times n}$ said to be 1-*good* if there is at least one 1 in R in a column other than Y-special and Z-special positions. The following observation is immediate :

Observation 4. *Let φ be distributed according to $\mathcal{D}$. Then for any row (column) R: $\Pr_{\varphi \sim \mathcal{D}}[R$ is 1-good$] \geq (1 - 1/n^3)$.*

Finally, we are ready to show that perm has high rank under a random $\varphi \sim \mathcal{D}$.

Theorem 6. $\Pr[\text{rank}(M_{\mathsf{perm}_n^\varphi}) \geq 2^{m/12}] \geq (1 - O(1/n^2))/2$.

We need a few notations and Lemmas before proving Theorem 6. Consider a $\varphi : X \to Y \cup Z \cup \{0,1\}$ and let the number of Y-special positions and the number of Z-special positions in X_φ are both be at least γ. Let $(i_1, j_1), (i_2, j_2), \ldots, (i_\gamma, j_\gamma)$ be a set of distinct Y- special positions that do not share any row or column and $(k_1, \ell_1), (k_2, \ell_2), \ldots, (k_\gamma, \ell_\gamma)$ be a set of distinct Z - special positions in X_φ that do not share any row or column.

Without loss of generality, suppose $i_1 < i_2 < \cdots < i_\gamma$ and $k_1 < k_2 < \cdots < k_\gamma$. Let $\mathcal{M}$ be the perfect matching $((i_1, j_1), (k_1, \ell_1)), \ldots, ((i_\gamma, j_\gamma), (k_\gamma, \ell_\gamma))$.
For an edge $\{(i_p, j_p), (k_p, \ell_p)\} \in \mathcal{M}$, $1 \leq p \leq \gamma$ consider the 2×2 matrix :

$$B_p = \begin{pmatrix} X_\varphi[i_p, j_p] & X_\varphi[i_p, \ell_p] \\ X_\varphi[k_p, j_p] & X_\varphi[k_p, \ell_p] \end{pmatrix}.$$

There exists a partition $\varphi : X \to Y \cup Z \cup \{0,1\}$ such that $\text{rank}(M_{B_p^\varphi}) = 2$. Let A be the matrix obtained by permuting the rows and columns in X_φ such that A can be written as in the Figure 1 below. Since (i_p, j_p) is a Y-special position, (k_p, ℓ_p) is a Z-special position we have $X_\varphi[i_p, j_p] \in Y$, $X_\varphi[k_p, \ell_p] \in Z$. Also $X_\varphi[i_p, \ell_p] \in \{0,1\}$ and $X_\varphi[k_p, j_p] \in \{0,1\}$. Further, $\text{rank}(M_{\mathsf{perm}(B_p)}) = 2$ if and only if $X_\varphi[k_p, j_p] = X_\varphi[i_p, \ell_p] = 1$. Consider the following events: F_1: $\gamma \geq m/12$; and F_2: Rows $i_1, \ldots, i_\gamma, k_1 \ldots, k_\gamma$ are 1-good.

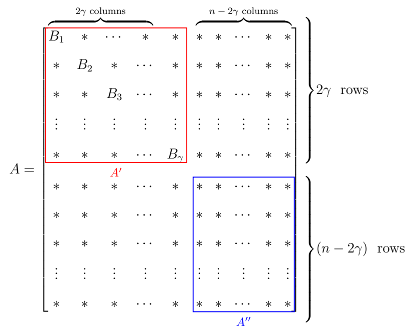

Figure 1: The matrix A after permuting the rows an columns. $*$ denotes unspecified entries.

Lemma 23. *Let A and A'' be matrices as above. Then* $\Pr_\varphi[\mathit{perm}(A'') \neq 0 \mid F_1, F_2] \geq 1 - \frac{1}{n^2}$.

Proof. Permanent of any matrix M with entries from $Y \cup Z \cup \{0,1\}$ is zero if and only if M has an all zero $s \times t$ sub matrix such that $s+t = n+1$.(See Theorem 12.1 in [22].) We begin with a bound on the probability that there is at least one column/row with all zero entries. Note that the event F_1 depends only on the entries of X_φ being in $Y \cup Z$, and the event F_2 is independent of the rows and columns of A''. Thus, for any position (i,j) in A'', we have $\Pr[\varphi(x_{i,j}) = 1] = \kappa n/N(1 - 2m/N) \approx \kappa n/N$, for large enough n. Thus,

$$\Pr[\forall j \in [n], \varphi(x_{ij}) = 0] \leq \left(1 - \frac{\kappa n}{N}\right)^{n-2\gamma} \text{ and hence,}$$

$$\Pr[\exists i\ \forall j \in [n], \varphi(x_{ij}) = 0] \leq n \cdot \left(1 - \frac{\kappa n}{N}\right)^{n-2\gamma} \quad \text{by union bound}$$

Since $\gamma = \mathcal{O}(m) = o(n)$ and $N = n^2$,

$$\Pr[\exists i\ \forall j \in [n], \varphi(x_{ij}) = 0] \leq n \frac{\left(1 - \frac{\kappa}{n}\right)^n}{\left(1 - \frac{\kappa}{n}\right)^{2\gamma}}$$

As $n \to \infty$, the denominator $\left(1 - \frac{\kappa}{n}\right)^{2\gamma} \to 1$. Now, consider $1 < c < n' - 1$, where $n' = n - 2\gamma$. We estimate the probability that there exists an $c \times (n' - c + 1)$ all zero sub-matrix of A''. For any $c \times (n' - c + 1)$ sub-matrix M of A'', $\Pr[M = 0] = (1 - \kappa/n)^{c(n'-c+1)}$.

As there are $\binom{n'}{c}^2$ many such sub-matrices M of A'', we get

$$\begin{aligned}\Pr[\exists M, M = 0] &\leq \binom{n'}{c}^2 (1 - \kappa/n)^{c(n'-c+1)} \\ &\leq (n'e/c)^c (1 - \kappa/n)^{c(n'-c+1)} \approx e^{2c\log((n+1)/c) - \kappa c(n'-c+1)/n} \leq e^{-4\log n}\end{aligned}$$

the last inequality follows since, $\kappa = 20\log n$, and hence $2c\log(n + 1/c) - \kappa(c-1)(n' - c + 1)/n \leq -2$ for large enough n.

$$\Pr[\mathit{perm}(\mathcal{A}'') = 0 \mid F_1, F_2] \leq n \cdot \left(1 - \frac{\kappa}{n}\right)^n + ne^{-4\log n} \leq n\left[\left(1 - \frac{\kappa}{n}\right)^{n/\kappa}\right]^\kappa + 1/n^3 \leq n \cdot \mathrm{e}^{-\kappa} \leq 1/n^2.$$

The penultimate inequality in the above is obtained by substituting $\kappa = 20\log n$. ☐

Let F_3 denote the event "$\mathsf{perm}(A'') \neq 0$". Define sets of matrices:

$$\mathcal{A} \triangleq \left\{ X_\varphi \mid \begin{array}{l} X_\varphi \in F_1 \cap F_2 \cap F_3 \text{ and } \exists i \leq \\ \gamma, \operatorname{rank}(M_{\mathsf{perm}(B_i)}) = 1 \end{array} \right\}; \qquad \mathcal{B} \triangleq \left\{ X_\varphi \mid \begin{array}{l} X_\varphi \in F_1 \cap F_2 \cap F_3 \text{ and } \forall i \leq \\ \gamma, \operatorname{rank}(M_{\mathsf{perm}(B_i)}) = 2. \end{array} \right\}$$

Observation 5. *$\forall A \in \mathcal{A}$, $\text{rank}(\mathsf{perm}(A')) < 2^\gamma$ and $\forall B \in \mathcal{B}, \text{rank}(\mathsf{perm}(B)) \geq 2^\gamma$.*

Lemma 24. *Let $\mathcal{A}$ and $\mathcal{B}$ as defined above. Then (a) $\Pr_{\varphi\sim\mathcal{D}}[\text{rank}(M_{\mathsf{perm}(X_\varphi)}) \geq 2^\gamma)] \geq \mathcal{D}(\mathcal{B})$; and (b) $\mathcal{D}(B) \geq \mathcal{D}(\mathcal{A})$, where $\mathcal{D}(S) = \Pr_{\varphi\sim\mathcal{D}}[X_\varphi \in S]$ for $S \in \{\mathcal{A}, \mathcal{B}\}$.*

Proof. (a) follows from Observation 5. For (b), we establish a one-one mapping $\pi : \mathcal{A} \to \mathcal{B}$ defined as follows. Let φ be such that $X_\varphi \in \mathcal{A}$. Consider $1 \leq p \leq \gamma$ such that $\text{rank}(M_{\mathsf{perm}(B_p)}) = 1$. Then either $X_\varphi[k_p, j_p] = 0$ or $X_\varphi[i_p, \ell_p] = 0$ or both. If $X_\varphi[k_p, j_p] = 0$, then set $X_{\varphi'}[k_p, j_p] = 1$, and $X_{\varphi'}[k_p, \iota_p] = 0$ where $\iota_p \in [n] \setminus \{j_1 \ldots, j_\gamma, \ell_1 \ldots, \ell_\gamma\}$ is the first index from left such that $X_\varphi[k_p, \iota_p] = 1$. Similarly, if $X_\varphi[i_p, \ell_p] = 0$, then set $X_{\varphi'}[i_p, \ell_p] = 1$, and $X_{\varphi'}[i_p, \lambda_p] = 0$ where $\lambda_p \in [n] \setminus \{j_1 \ldots, j_\gamma, \ell_1 \ldots, \ell_\gamma\}$ is the first index from left such that $X_\varphi[k_p, \lambda_p] = 1$. Let φ' be the partition obtained from φ by applying the above mentioned swap operation for every $1 \leq p \leq \gamma$ with $\text{rank}(M_{\mathsf{perm}(B_p)}) = 1$, keeping other values of φ untouched. Clearly $X_{\varphi'} \in \mathcal{B}$. Set $\pi(X_\varphi) \mapsto X_{\varphi'}$. It can be seen that π is an one-one map. Further, for any fixed $A \in \mathcal{A}$, $\Pr_\varphi[X_\varphi = A] = \Pr_\varphi[X_\varphi = \pi(A)]$ since φ is independently and identically distributed for any position in the matrix. Thus we have $\mathcal{D}(\mathcal{A}) \leq \mathcal{D}(\mathcal{B})$. □

Proof of Theorem 6. It is enough to argue that $\Pr_{\varphi\sim\mathcal{D}}[X\varphi \in \mathcal{A}\cup\mathcal{B}] = 1 - O(\frac{1}{n^2})$, as $\mathcal{A}\cap\mathcal{B} = \emptyset$. Now, $\Pr_{\varphi\sim\mathcal{D}}[X_\varphi \in \mathcal{A}\cup\mathcal{B}] = \Pr_{\varphi\sim\mathcal{D}}[F_1 \cap F_2 \cap F_3]$. By Lemma 19, $Pr_{\varphi\sim\mathcal{D}}[F_1] = 1 - 2^{-\Omega(m)}$, by Lemma 4 combined with union bound we have $Pr_{\varphi\sim\mathcal{D}}[F_2] \geq 1 - \gamma/n^3$ and by Lemma 23 $Pr_{\varphi\sim\mathcal{D}}[F_3|F_1, F_2] \geq 1 - 2/n^2$. Thus we conclude $\Pr_{\varphi\sim\mathcal{D}}[F_1 \cap F_2 \cap F_3] = 1 - O(\frac{1}{n^2})$. As $\mathcal{D}(\mathcal{B}\cap\mathcal{A}) = \mathcal{D}(\mathcal{A}) + \mathcal{D}(\mathcal{B})$, by Lemma 24 we have $\Pr_{\varphi\sim\mathcal{D}}[\text{rank}(M_{\mathsf{perm}(X_\varphi)}) \geq 2^\gamma] \geq 1/2(1 - O(\frac{1}{n^2}))$. □

4.3 Putting them all together

Proof of Theorem 1

Proof. Suppose $p_{lin} = \sum_{i=1}^{s}\prod_{j=1}^{t} f_{i,j}$ where $f_{i,j}$ are syntactically multi-linear $\Sigma\Pi\Sigma$ formula, with $s < 2^{N^{1/4}}$, Let $f_{i,j} = \sum_{k=1}^{s'} T_{i,j,k}$, and $T_{i,j,k}$ are products of variable disjoint linear forms, and hence ROPs. Further, since the bottom fan-in of each $f_{i,j}$ is bounded by $N^{1/2+\lambda}$, we have $s_{T_{i,j,k}} \leq 2^{N^{1/2+\lambda}}$. Then by Lemma 17 and union bound there is an i, j, k such that $\text{rank}(M_{T^{\varphi}_{i,j,k}}) \geq 2^{N^{4/15}}$ with probability at most $sts'2^{-\Omega(m)}$. By Lemma 3 and 4, we have $\text{maxrank}(\widehat{M}_{p^{\varphi}_{lin}}) \leq 2^{N^{4/15}}$ with probability $1 - o(1)$. However by Lemma 18, $\text{maxrank}(\widehat{M}_{p^{\varphi}_{lin}}) = \text{rank}(M_{p^{\varphi}_{lin}}) = 2^{\Omega(m)}$ with probability at least $1 - 2^{-\Omega(m)}$, a contradiction. Hence $ss' = 2^{\Omega(N^{1/4})}$. □

Proof of Theorem 2

Proof. Suppose $s < 2^{N^{1/4}}$. Then by Lemma 17, the probability that there is an $f_{i,j}$ with $\text{rank}(M_{f^{\varphi}_{i,j}}) \geq 2^{N^{4/15}}$ is at most $2^{-\Omega(m)}s \cdot t = o(1)$. By Lemma 3 and 4, we have $\text{maxrank}(\widehat{M}_{p^{\varphi}_{lin}}) \leq 2^{N^{4/15}}$ with probability $1-o(1)$. However by Lemma 18, $\text{maxrank}(\widehat{M}_{p^{\varphi}_{lin}}) = \text{rank}(M_{p^{\varphi}_{lin}}) = 2^{\Omega(m)}$ with probability $1 - 2^{-\Omega(m)}$, a contradiction. Hence $s \geq 2^{N^{1/4}}$. □

Proof of Theorem 3

Proof. Suppose $s < 2^{N^{1/4}}$. Then by Lemma 17, Probability that there is an $f_{i,j}$ with $\text{rank}(M_{f^{\varphi}_{i,j}}) \geq 2^{N^{4/15}}$ is at most $2^{-\Omega(m)}s \cdot t = o(1)$. By Lemma 3 and 4, we have $\text{maxrank}(\widehat{M}_{\mathsf{perm}^{\varphi}_n}) \leq 2^{N^{4/15}}$ with probability $1 - o(1)$. However, by Theorem 6, $\text{maxrank}(\widehat{M}_{\mathsf{perm}^{\varphi}_n}) = \text{rank}(\mathsf{perm}^{\varphi}_n) = 2^{\Omega(m)}$ with probability $(1 - 1/n^2)/2$, a contradiction. Hence $s \geq 2^{N^{1/4}}$. □

Acknowledgements

We thank anonymous reviewers of an earlier version of the paper for suggestions which improved the presentation. Further, we thank one of the anonymous reviewers for pointing out an outline of argument for Lemma 7.

References

[1] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *FOCS*, pages 67–75, 2008.

[2] Devdatt Dubhashi and Alessandro Panconesi. *Concentration of Measure for the Analysis of Randomized Algorithms*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[3] Dima Grigoriev and Marek Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *STOC*, pages 577–582, 1998.

[4] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *FOCS*, pages 578–587, 2013.

[5] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. *J. ACM*, 61(6):33:1–33:16, 2014.

[6] Neeraj Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:81, 2012.

[7] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. STOC. pages 119–127, 2014.

[8] Neeraj Kayal and Chandan Saha. Multi-k-ic depth three circuit lower bound. In *STACS*, pages 527–539, 2015.

[9] Pascal Koiran. Arithmetic circuits: The chasm at depth four gets wider. *Theor. Comput. Sci.*, 448:56–65, 2012.

[10] Mrinal Kumar, Gaurav Maheshwari, and Jayalal Sarma. Arithmetic circuit lower bounds via maxrank. In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*, pages 661–672, 2013.

[11] Mrinal Kumar and Shubhangi Saraf. On the power of homogeneous depth 4 arithmetic circuits. In *FOCS*, pages 364–373, 2014.

[12] Meena Mahajan, B. V. Raghavendra Rao, and Karteek Sreenivasaiah. Building above read-once polynomials: Identity testing and hardness of representation. In *COCOON*, pages 1–12, 2014.

[13] Thierry Mignon and Nicolas Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notices*, 2004(79):4241–4253, 2004.

[14] Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, June 13-16, 2004*, pages 633–641, 2004.

[15] Ran Raz. Multilinear-nc neq multilinear-nc. In *FOCS*, pages 344–351, 2004.

[16] Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. *J. ACM*, 56(2), 2009.

[17] Ran Raz and Amir Yehudayoff. Balancing syntactically multilinear arithmetic circuits. *Computational Complexity*, 17(4):515–535, 2008.

[18] Ran Raz and Amir Yehudayoff. Lower bounds and separations for constant depth multilinear circuits. *Computational Complexity*, 18(2):171–207, 2009.

[19] Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. In *STOC*, pages 507–516, 2008.

[20] Sébastien Tavenas. Improved bounds for reduction to depth 4 and depth 3. In *MFCS*, pages 813–824, 2013.

[21] Leslie G. Valiant. Completeness classes in algebra. In *STOC*, pages 249–261, 1979.

[22] J. H. van Lint and R. M. Wilson. *A Course In Combinatorics*. Cambridge University Press, 2nd edition, 2001.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de