Building above read-once polynomials: identity testing and hardness of representation

Meena Mahajan[1], B. V. Raghavendra Rao[2], and Karteek Sreenivasaiah[1]

[1] The Institute of Mathematical Sciences, Chennai, India.
{meena,karteek}@imsc.res.in
[2] Indian Institute of Technology Madras, Chennai, India. bvrr@cse.iitm.ac.in

Abstract. Polynomial Identity Testing (PIT) algorithms have focussed on polynomials computed either by small alternation-depth arithmetic circuits, or by read-restricted formulas. Read-once polynomials (ROPs) are computed by read-once formulas (ROFs) and are the simplest of read-restricted polynomials. Building structures above these, we show the following:

1. A deterministic polynomial-time non-black-box PIT algorithm for $\sum^{(2)} \cdot \prod \cdot \mathsf{ROF}$.
2. Weak hardness of representation theorems for sums of powers of constant-free ROPs and for 0-justified alternation-depth-3 ROPs.

1 Introduction

The Polynomial Identity Testing (PIT) problem is the most fundamental computational question that can be asked about polynomials: is the polynomial given by some implicit representation identically zero? The implicit representations of the polynomials can be arithmetic circuits, branching programs etc., or the polynomial could be presented as a black-box, where the black-box takes a query in the form of an assignment to the variables and outputs the evaluation of the polynomial on the assignment. PIT has a randomized polynomial time algorithm on almost all input representations, independently discovered by Schwartz and Zippel [Sch80,Zip79]. However, obtaining deterministic polynomial time algorithms for PIT remained open since then. In 2004, Impagliazzo and Kabanets [KI04] showed that a deterministic polynomial time algorithm for PIT implies lower bounds (either $\mathsf{NEXP} \not\subset \mathsf{P/poly}$ or permanent does not have polynomial size arithmetic circuits), thus making it one of the central problems in algebraic complexity. Following [KI04], intense efforts over the last decade have been directed towards de-randomizing PIT (see for instance [SY10,Sax14]). The attempts fall into two categories: considering special cases ([Sax14]), and optimizing the random bits used in the Schwartz-Zippel test [BHS08,BE11].

The recent progress on PIT mainly focusses on special cases where the polynomials are computed by restricted forms of arithmetic circuits. They can be seen as following one of the two main lines of restrictions: 1. Shallow circuits based on alternation depth of circuits computing the polynomial. 2. Restriction

on the number of times a variable is read by formulas (circuits with fanout 1) computing the polynomial.

The study of PIT on shallow circuits began with depth two circuits, where deterministic polynomial time algorithms are known even when the polynomial is given as a black-box [BOT88,KS01]. Further, there were several interesting approaches that lead to deterministic PIT algorithms on depth three circuits with bounded top fan-in [DS07,KS07]. However, progressing from bounded fan-in depth three circuits seemed to be a big challenge. In 2008, Agrawal and Vinay [AV08] explained this difficulty, showing that deterministic polynomial time algorithms for PIT on depth four circuits implies sub-exponential time deterministic algorithms for general circuits. There have been several interesting approaches towards obtaining black-box algorithms for PIT on restricted classes of depth three and four circuits, see [Sax14,SY10] for further details. Recently, Kamath, Kayal and Saptharishi [GKKS13] showed that, over infinite fields, deterministic polynomial time algorithms for PIT on depth three circuits would also imply lower bounds for the permanent.

A formula computing a polynomial that depends on all of its variables must read each variable at least once (count each leaf labeled x as reading the variable x). The simplest such formulas read each variable exactly once; these are Read-Once Formulas ROFs, and the polynomials computed by such formulas are known as read-once polynomials (ROP). In the case of an ROP f presented by a read-once formula computing it, a simple reachability algorithm on formulas can be applied to test if $f \equiv 0$. Shpilka and Volkovich [SV08] gave a deterministic polynomial time algorithm for PIT on ROPs given as a black-box. Generalizing this to formulas that read a variable more than once, they obtained a deterministic polynomial time algorithm for polynomials presented as a sum of $O(1)$ ROFs. Anderson et. al [AvMV11] showed that if a read-k formula, with $k \in O(1)$, is additionally restricted to compute multilinear polynomials at every gate, then PIT on such formulas can be done in deterministic polynomial time. The result by [AvMV11] subsumes the result in [SV08] since a k-sum of read-once formulas is read-k and computes multilinear polynomials at every gate. However, both [SV08] and [AvMV11] crucially exploit the multilinearity property of the polynomials computed under the respective models. In [MRS14], the authors explored eliminating the multilinear-at-each-gate restriction, and gave a non-blackbox deterministic polynomial time algorithm for read-3 formulas. However for the case of Read-k formulas for $k \geq 4$, even the non-blackbox version of the problem is open. Note that multilinearity checking itself is equivalent to PIT on general circuits [FMM12].

Our results: In this paper, we explore further structural properties of ROPs and polynomials that can be expressed as polynomial functions of a small number of ROPs. Our structural observations lead to efficient algorithms on special classes of bounded-read formulas.

We attempt to extend the class considered in [SV08] (namely, formulas of the form $\sum_i f_i$ where each f_i is an ROF) to the class of polynomials of the

form $\sum_{i=1}^{k} f_i g_i$ where the f_is and g_is are presented as ROFs and k is some constant. These are read-$2k$ polynomials, not necessarily multilinear. Over the ring of integers and the field of rationals, we can give an efficient deterministic non-blackbox PIT algorithm for the case $k = 2$; the polynomial is $f_1 f_2 + g_1 g_2$ where f_1, f_2, g_1, g_2 are all read-once polynomials presented by ROFs. This class can also be seen as a special case of read-4 polynomials. Our algorithm exploits the structural decomposition properties of ROPs and combines this with an algorithm that extracts greatest common divisors of the coefficients in an ROP. The algorithm easily generalises to polynomials of the form $f_1 f_2 f_3 \cdots f_m + g_1 g_2 \cdots g_s$ where f_is and g_is are presented as ROFs, but m, s can be unbounded; that is, the class $\sum^{(2)} \cdot \prod \cdot \mathsf{ROF}$. Note that this class of polynomials includes non-multilinear polynomials and also polynomials with no bound on the number of times variables are read. Thus it is incomparable with the classes considered in [SV08], [AvMV11] and [MRS14]. This result is presented in Section 3, Theorem 1.

Central to the PIT algorithm in [SV08] is a "hardness of representation" lemma showing that the polynomial $\mathcal{M}_n = x_1 x_2 \cdots x_n$, consisting of just a single monomial, cannot be represented as a sum of less than $n/3$ ROPs of a particular form (weakly 0-justified). More recently, a similar hardness of representation result appeared in [Kay12]: if $\mathcal{M}_n$ is represented as a sum of powers of low-degree (at most d) polynomials, then the number of summands is $\exp(\Omega(n/d))$. As is implicit in [Kay12], such a hardness of representation statement can be used to give a PIT algorithm. We analyze this connection explicitly, and show that the results in [Kay12] lead to a deterministic sub-exponential time algorithm for black-box PIT for sums of powers of polynomials with appropriate size and degree (Section 4, Theorem 2).

A minor drawback of both these statements is that they consider a model that cannot even individually compute all monomials. One would expect any reasonable model of representing polynomials to be able to compute $\mathcal{M}_n$. In Section 5, we consider the restriction of read-once formulas to *constant-free* formulas that are only allowed leaf labels ax, where x is a variable and a is a field element. This model can compute any single monomial. We show (Theorem 3) that the elementary symmetric polynomial $\mathsf{Sym}_{n,d}$ of degree d cannot be written as a sum of powers of such formulas unless the number of summands is $\Omega(\log(n/d))$. This appears weak compared to the $n/3$ bound from [SV08], but this is to be expected since unlike in [SV08] where the ROPs could only be added, we allow sums of powers. We also consider $0 - \mathsf{justified}$ read-once formulas with alternation depth (between + and $\times$) 3, and obtain a similar hardness-of-representation result for the polynomial $\mathcal{M}_n$ against sums of powers of polynomials computed by such formulas, showing that $n^{\frac{1}{2}-\epsilon}$ summands are needed (Theorem 4). Again, this appears weak compared to the $\exp(\Omega(n/d))$ bound from [Kay12], but unlike in [Kay12] where the degree of the inner functions is a parameter, our inner ROPs could have arbitrarily high degree.

2 Preliminaries

An arithmetic formula on n variables $X = \{x_1, \ldots, x_n\}$ is a rooted binary tree with leaves labeled from $\mathbb{F} \cup X$ and internal nodes labeled by $\circ \in \{+, \times\}$. Each node computes a polynomial in the obvious way, and the formula computes the polynomial computed at the root gate. An arithmetic formula is said to be read-once (ROF) if each $x \in X$ appears at most once at a leaf. Polynomials computed by ROFs are called read-once polynomials ROPs.

It is more convenient for us to allow leaves to be labeled by forms $ax + b$ for some $x \in X$ and some $a, b \in \mathbb{F}$. This does not change the class of polynomials computed, even when restricted to ROFs. Henceforth we assume that ROFs are of this form.

The alternation depth of the formula is the maximum number of maximal blocks of $+$ and $\times$ gates on any root-to-leaf path in the formula.

We say that an ROF is constant-free (denoted CF-ROF) if the labels at the leaves are of the form ax for $x \in X$ and $a \in \mathbb{F} \setminus \{0\}$. We call polynomials computed by such formulas constant-free ROPs, denoted CF-ROP.

For a polynomial $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$, a set $S \subseteq [n]$ and an assignment a, let $f_{S \to a_S}$ denote the polynomial on variables $\{x_i : i \notin S\}$ obtained from f by setting $x_j = a_j$ for $j \in S$. Using notation from [SV08], for a polynomial f, $\mathsf{var}(f)$ denotes the set of variables that f depends on non-trivially. We say that f is 0-justified if for all $S \subseteq \mathsf{var}(f)$, $\mathsf{var}(f|_{S \to 0}) = \mathsf{var}(f) \setminus S$.

3 Identity testing for $\sum^{(2)} \cdot \prod \cdot$ROPs over $\mathbb{Z}$ or $\mathbb{Q}$

In this section we show that PIT can be solved efficiently for formulas presented in the form $f_1 f_2 \ldots f_m + g_1 g_2 \ldots g_s$, where each of the f_i, g_j is an ROF over the field of rationals.

Theorem 1. *Given Read-Once Formulas computing each of the polynomials $f_1, f_2, \cdots, f_r, g_1, g_2, \ldots, g_s \in \mathbb{Q}[x_1, \ldots, x_n]$, checking if $f_1 \cdot f_2 \cdots f_r \equiv g_1 \cdot g_2 \cdots g_s$ can be done in deterministic polynomial time.*

A crucial ingredient in our proof is the following structural characterization from [RS11,RS13] and its constructive version; this is a direct consequence of the characterisation of ROPs given in [SV08].

Lemma 1 ([RS13]). *Let f be an ROP. Then exactly one of the following holds:*

1. *$k \geq 1$, there exist ROPs $f_1, \ldots, f_k$, with $\mathsf{var}(f_i) \cap \mathsf{var}(f_j) = \emptyset$ for all distinct $i, j \in [k]$, such that $f = a + f_1 + \cdots + f_k$, for some $a \in \mathbb{F}$, and each f_i is either uni-variate or decomposes into variable-disjoint factors.*
2. *$k \geq 2$, there exist ROPs $f_1, \ldots, f_k$, with $\mathsf{var}(f_i) \cap \mathsf{var}(f_j) = \emptyset$ for all distinct $i, j \in [k]$, such that $f = a \times f_1 \times f_2 \times \cdots \times f_k$ for some $a \in \mathbb{F} \setminus \{0\}$, and none of the f_is can be factorised into variable-disjoint factors.*

Furthermore, ROFs computing such f_is can be constructed from an ROF computing f in polynomial time.

Given an ROF over $\mathbb{Q}$, we can clear all denominators to get an ROF over $\mathbb{Z}$, without changing the status of the $? \equiv 0?$ question. So we now assume that all the numbers a, b appearing in the ROF (recall, leaf labels are of the form $ax+b$) are integers. For a polynomial $p(X)$, let $\mathsf{content}(p(X))$ denote the greatest common divisor (gcd) of the non-zero coefficients of p. The next crucial ingredient in our proof is that for an ROF f, we can efficiently compute its content.

Lemma 2. *There is a polynomial-time algorithm that, given an ROF f in $\mathbb{Z}[X]$, computes $\mathsf{content}(f)$ and constructs an ROF f' in $\mathbb{Q}[X]$ such that $f = \mathsf{content}(f) \cdot f'$.*

Proof. It suffices to show how to compute $\mathsf{content}(f)$; then the ROF f' is just $\frac{1}{\mathsf{content}(f)} \times f$. We proceed bottom-up, or alternatively, we prove this by induction on the structure of f.

For a polynomial $p \in \mathbb{Z}[X]$, let $\hat{p} = p - p(0)$, where $p(0) = p(0, \ldots, 0)$, and let $\hat{p}'$ be the polynomial such that $\hat{p} = \mathsf{content}(\hat{p})\hat{p}'$.

If f is a single leaf node, then computing $\mathsf{content}(f)$ and $\mathsf{content}(\hat{f})$ is trivial. Otherwise, say $f = g \circ h$. Since f is an ROF, $\mathsf{var}(g) \cap \mathsf{var}(h) = \emptyset$.
Case $f = g + h$**:** Then $\hat{f} = \hat{g} + \hat{h}$, and $f(0) = g(0) + h(0)$. So

$$\mathsf{content}(f) := \gcd(\mathsf{content}(\hat{g}), \mathsf{content}(\hat{h}), g(0) + h(0)),$$
$$\mathsf{content}(\hat{f}) := \gcd(\mathsf{content}(\hat{g}), \mathsf{content}(\hat{h})).$$

Case $f = g \times h$**:** Then $\hat{f} = \hat{g}\hat{h} + h(0)\hat{g} + g(0)\hat{h}$, and $f(0) = g(0)h(0)$. We can show that

Claim. For any two variable-disjoint polynomials $p, q \in \mathbb{Z}[X]$, $\mathsf{content}(pq) = \mathsf{content}(p)\mathsf{content}(q)$.

Proof. Let $p = \mathsf{content}(p)(a_1M_1 + a_2M_2 + \cdots + a_kM_k)$ and $q = \mathsf{content}(q)(b_1N_1 + b_2N_2 + \cdots + b_\ell N_\ell)$, where M_i, N_j are monomials. By definition of content, $\gcd(\ldots, a_i, \ldots) = \gcd(\ldots, b_j, \ldots) = 1$. Since p and q are variable-disjoint, every monomial of the form $\mathsf{content}(p)\mathsf{content}(q)(a_ib_jM_iN_j)$ appears in the polynomial $p \times q$, and there are no other monomials. Hence $\mathsf{content}(p)\mathsf{content}(q) | \mathsf{content}(p \times q)$. For the converse, we need to show that $\gcd(S) = 1$, where $S = \{a_ib_j \mid i \in [k], j \in [\ell]\}$. Suppose not. Let c be the largest prime that divides all numbers in S. Then, $\forall i \in [k]$,

$$\begin{aligned} & c | a_ib_1 \text{ and } c | a_ib_2 \text{ and } \ldots \text{ and } c | a_ib_k. \\ \text{Hence } & c | a_i \text{ or } (c | b_1, c | b_2, \cdots, c | b_\ell). \\ \text{Hence } & c | a_i \text{ or } c = 1, \text{ since } \gcd(b_1, \ldots, b_\ell) = 1. \end{aligned}$$

Thus we conclude that c divides $\gcd(a_1, \ldots, a_k) = 1$, a contradiction. □

Using this claim, we see that

$$\mathsf{content}(f) := \mathsf{content}(g) \times \mathsf{content}(h),$$
$$\mathsf{content}(\hat{f}) := \gcd(\mathsf{content}(\hat{g})\mathsf{content}(\hat{h}), h(0)\mathsf{content}(\hat{g}), g(0)\mathsf{content}(\hat{h})).$$

□

Now we have all the ingredients for proving Theorem 1.

Proof (of Theorem 1). Let $f = f_1 \cdot f_2 \cdots f_r$ and $g = g_1 \cdot g_2 \cdots g_s$ As discussed above, without loss of generality, each f_i, g_i is in $\mathbb{Z}[X]$. Using Lemma 1 and 2, we can compute the irreducible variable-disjoint factors of each f_i and each g_i, and also pull out the content for each factor. That is, we express each f_i as $\alpha_i f_{i,1} \cdots f_{i,k_i}$, and each g_i as $\beta_i g_{i,1} \cdots g_{i,\ell_i}$ where the $f_{i,j}$s, $g_{i,j}$s are irreducible and have content 1. We obtain ROFs in $\mathbb{Q}[X]$ for each of the $f_{i,j}$s and $g_{i,j}$s. Note that if $\sum_i k_i \neq \sum_j \ell_j$, then there cannot be a component-wise matching between the factors of f and g, and hence we conclude $f \not\equiv g$. Otherwise, $\sum_i k_i = \sum_j \ell_j$. We now form multisets of the factors of f and of g, and we knock off equivalent factors one by one. (See Algorithm 1.) Detecting equivalent factors (the condition

Algorithm 1 Test if $\prod_{i=1}^{r} \alpha_i \prod_{j=1}^{k_i} f_{i,j} \equiv \prod_{i=1}^{s} \beta_i \prod_{j=1}^{\ell_i} g_{i,j}$

1: $S \leftarrow \{f_{1,1}, \cdots, f_{1,k_1}, f_{2,1}, \cdots, f_{2,k_2}, \ldots, f_{r,1}, \cdots, f_{r,k_r}\}$
2: $T \leftarrow \{g_{1,1}, \cdots, g_{1,\ell_1}, g_{2,1}, \cdots, g_{2,\ell_2}, \ldots, g_{s,1}, \cdots, g_{s,\ell_s}\}$
3: (Both S and T are multisets; repeated factors are retained with multiplicity.)
4: **for** $p \in S$ **do**
5: **for** $q \in T$ **do**
6: **if** $p \equiv q$ **then**
7: **if** S and T have unequal number of copies of p and q **then**
8: Return No
9: **else**
10: $S \leftarrow S \setminus \{p\}$. (Remove all copies).
11: $T \leftarrow T \setminus \{q\}$. (Remove all copies).
12: **end if**
13: **end if**
14: **end for**
15: **end for**
16: **if** $(\alpha_1\alpha_2\cdots\alpha_r = \beta_1\beta_2\cdots\beta_s) \wedge (S = T = \emptyset)$ **then**
17: Return Yes
18: **else**
19: Return No
20: **end if**

in Step 6) requires an identity test $p \equiv q$?, or $p - q \equiv 0$?, for ROFs in $\mathbb{Q}[X]$. Since we have explicit ROFs computing p and q, this can be done using [SV08]. □

4 PIT for sums of powers of low degree polynomials

In this section, we give a blackbox identity testing algorithm for multilinear sums of powers of low-degree polynomials.

We say that a polynomial f has a sum-powers representation of degree d and size s if there are polynomials f_i each of degree at most d, and a set of positive integers e_i, such that $f = f_1^{e_1} + \ldots + f_s^{e_s}$. In [Kay12], it is shown that

computing the full multilinear monomial $\mathcal{M}_n = x_1 x_2 \cdots x_n$ using sums of powers of low-degree polynomials requires exponentially many summands:

Proposition 1. *[Kay12] There is a constant c such that for the polynomial $x_1 x_2 \cdots x_n$, any sum-powers representation of degree d requires size $s \geq 2^{\frac{cn}{d}}$.*

Shpilka and Volkovich [SV08] proved that sum of less than $n/3$ 0-justified ROPs cannot equal $\mathcal{M}_n$, and used it to obtain a black-box PIT algorithm for bounded sums of ROPs. Using these ideas along with Proposition 1, we note that such a hardness of representation for sums of powers of low-degree polynomials, where the final sum is multilinear, gives sub-exponential time algorithms for black-box PIT for this class.

Let $R = \{0, 1\} \subseteq \mathbb{F}$ be a finite set that contains 0. For any $k > 0$, define

$$W_k^n(R) \triangleq \{\boldsymbol{a} \in R^n | \ \boldsymbol{a} \text{ has at most } k \text{ non-zero coordinates}\}.$$

In Theorem 7.4 of [SV10], it is shown that for a certain kind of formula F (k-sum of degree-d 0-justified preprocessed ROP), and for any $R \subseteq \mathbb{F}$ containing 0 and of size at least $d + 1$, $F \equiv 0$ if and only if $F\ |_{W_{3k}^n(R)} \equiv 0$. The proof uses the Combinatorial Nullstellensatz [Alo99], see also Lemma 2.13 in [SV10]. We re-state it here for convenience:

Proposition 2 (Combinatorial Nullstellensatz, [Alo99]). *Let $P \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial where for every $i \in [n]$, the degree of x_i is bounded by t. Let $R \subseteq \mathbb{F}$ have size at least $t + 1$, and $S = R^n$. Then $P \equiv 0 \Leftrightarrow P|_S \equiv 0$.*

Along similar lines, using Propositions 1,2, we show that

Lemma 3. *Let $C(n, s, d)$ be the class of all n-variate multilinear polynomials that have a sum-powers representation of degree d and size s. Let c be the constant from Proposition 1. For $f \in C(n, s, d)$, $R = \{0, 1\}$, and $k = (d \log s)/c$, $f|_{W_k^n(R)} \equiv 0 \iff f \equiv 0$.*

Proof. The $\Leftarrow$ direction in the claim is trivial. To prove the $\Rightarrow$ direction, we proceed by induction on n.

Base case: $n \leq k$. Then $W_k^n(R) = R^n$. Using Proposition 2 (since f is multilinear, R is large enough), we conclude that $f \equiv 0$.

Induction Step: $n > k$. Suppose $f \not\equiv 0$. Consider any $i \in [n]$, and let $f' = f|_{x_i=0}$. Then $f' \in C(n-1, s, d)$. Since $f|_{W_k^n(R)} \equiv 0$, we have $f'|_{W_k^{n-1}(R)} \equiv 0$. So by the induction hypothesis, $f' \equiv 0$. Hence $x_i | f$. Since this holds for every $i \in [n]$, the monomial $x_1 \cdots x_n$ must divide f. Since f is multilinear, it must be that $f = x_1 \cdots x_n$. But $n > k = (d \log s)/c$, so $s < 2^{cn/d}$. This contradicts Proposition 1. Hence we conclude $f \equiv 0$. □

This gives the required black-box PIT algorithm, since for our choice of k in the above lemma, $|W_k^n(\{0, 1\})| \in n^{O(k)} \in 2^{O(d \log s \log n)}$. Thus

Theorem 2. *Let $C(n, s, d)$ be the class of all n-variate multilinear polynomials that have a sum-powers representation of degree d and size s. There is a deterministic black-box PIT algorithm for $C(n, s, d)$ running in time $2^{O(d \log n \log s)}$.*

Remark 1. Though f is multilinear in Lemma 3 (and hence Theorem 2), the polynomials f_i in the sum-powers representation of f need not be multilinear.

5 Hardness of representation for sum of powers of CF-ROPs

The hardness of representation result from [Kay12], stated in Proposition 1, and its precursor from [SV08],[SV10], are both for $\mathcal{M}_n$, the former using low-degree polynomials and the latter using a kind of ROPs called 0-justified ROPs. Note that ROPs, even when 0-justified, can have high degree, so these results are incomparable. Here we extend such a hardness result in two ways.

Our first hardness result is for elementary symmetric polynomials $\mathsf{Sym}_{n,d}$, not just for $d = n$. It works against another subclass of ROPs, CF-ROF; as is the case in [SV08,SV10], this class too can have high-degree polynomials. Recall that this class consists of polynomials computed by read-once formulas that have $+$ and $\times$ gates, and labels ax at leaves ($a \neq 0$). Hence for any f in this class, $f(0) = 0$. We show that powers of such polynomials cannot add up to elementary symmetric polynomials of arbitrary degree $d \leq n$ unless there are many such summands. First, we establish a useful property of this class.

Lemma 4. *For every* CF-ROP $f \in \mathbb{F}[x_1, \ldots, x_n]$*, there is a set* $S \subseteq [n]$ *with* $|S| \leq |\mathsf{var}(f)|/2$ *such that* $\deg(f|_{S\to 0}) \leq 1$.

Proof. Consider a CF-ROF F computing f. If F has a single node, then f is already linear, so $S = \emptyset$. Otherwise, $F = G_1 \circ G_2$, where G_1, G_2 are variable-disjoint CF-ROFs computing CF-ROPs g_1, g_2, respectively.
Case 1: $\circ = \times$**.** Without loss of generality, assume $|\mathsf{var}(g_1)| \leq |\mathsf{var}(f)|/2$. For $S = \{i : x_i \in \mathsf{var}(g_1)\}$, $g_1|_{S\to 0} \equiv f|_{S\to 0} \equiv 0$.
Case 2: $\circ = +$**.** Inductively, we can find sets S_i of at most half the variables of each g_i, such that $g_i|_{S_i\to 0}$ has degree at most 1. Define $S = S_1 \cup S_2$. Since G_1, G_2 are variable-disjoint, $|S| \leq |\mathsf{var}(f)|/2$, and $f|_{S\to 0}$ has degree at most 1. □

We use this to get our hardness-of-representation result for CF-ROPs, irrespective of degree.

Theorem 3. *Fix any* $d \in [n]$*. Suppose there are CF-ROPs* $f_1, \ldots, f_k$*, and positive integers* $e_1, \ldots, e_k$ *such that*

$$\sum_{i=1}^{k} f_i^{e_i} = \mathsf{Sym}_{n,d}.$$

Then $k \geq \min\{\log \frac{n}{d}, 2^{\Omega(d)}\}$.

Proof. Let $f = \mathsf{Sym}_{n,d}$.

We repeatedly apply Lemma 4 to restrictions of the f_i's obtain a formula of degree at most 1. Let $S_0 = T_0 = \emptyset$, and let S_{i+1} be the set obtained by applying the Lemma to $f_{i+1}|_{T_i\to 0}$, where each $T_i = S_1 \cup \ldots \cup S_i$. Define $S = T_k$. Since at least half the variables survive at each stage, we see that $r \triangleq |\mathsf{var}(f|_{S\to 0})| \geq |\mathsf{var}(f)|/2^k = n/2^k$.

– If $r \geq d$, then $f|_{S\to 0} = \mathsf{Sym}_{r,d} \not\equiv 0$. Add any $r-d$ surviving variables to the set S to obtain the expression $\mathsf{Sym}_{d,d} = f|_{S\to 0} = \sum_{i=1}^{k} (f_i|_{S\to 0})^{e_i}$ where each f_i is either linear or identically 0. Let k' be the number of non-zero polynomials $f_i|_{S\to 0}$. By Proposition 1, $k' \in 2^{\Omega(d)}$, and $k \geq k'$.
– If $r < d$, then $n/2^k \leq r < d$. So $k > \log(\frac{n}{d})$.

Thus if $k \leq \log \frac{n}{d}$, then $k \in 2^{\Omega(d)}$. □

What this tells us is that there is a threshold $r \sim \log\log n$ such that any sum-powers representation of $\mathsf{Sym}_{n,d}$ using CF-ROPs needs size $2^{\Omega(d)}$ for $d \leq r$, and size $\geq \log \frac{n}{d}$ for $d \geq r$.

Our second hardness result is for $\mathcal{M}_n$, but works against a different class of ROFs. These ROFs may not be constant-free, but they have bounded alternation-depth, and are also 0-justified. Again, first we establish a useful property of the class.

Lemma 5. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be computed by an ROF with alternation depth 3. For any degree bound $1 \leq d \leq n$, there is an $S \subseteq [n]$ of size at most $|\mathsf{var}(f)|/d$, and an assignment of values A_S to the variables x_i for $i \in S$, such that $\deg(f|_{S\to A}) \leq d$. Moreover, if f is 0-justified, then we can find an A_S with all non-zero values.*

Proof. Let f be computed by the ROF F with alternation depth 3, where no gate computes the 0 polynomial.

If the top gate in F is a $+$, then $F = \sum_{i=1}^{r} f_i$, where each summand f_i is of the form $\prod_{j=1}^{t_i} \ell_{i,j}$ and the factors $\ell_{i,j}$'s are linear forms on disjoint variable sets. We find a partial assignment that kills all summand of degree more than d. For each such summand f_i, identify the factor with fewest variables, and assign values to the variables in it to make it 0. We assign values to at most $|\mathsf{var}(f_i)|/d$ variables, so overall no more than $|\mathsf{var}(f)|/d$ variables are set.

Further, if f is 0-justified and read-once, then each f_i is also a 0-justified ROF. Hence no factor of f_i vanishes at 0; each factor $\ell_{i,j}$ is of the form $\sum_{k=1}^{p} a_{i,j,k} x_{i,j,k} - c_{i,j}$ where $c_{i,j} \neq 0$. We can kill such a factor with an assignment avoiding 0s (eg set $x_{i,j,k} = c_{i,j}/pa_{i,j,k}$.)

If the top gate in F is a $\times$, then $F = \prod_{i=1}^{r} F_i$, where the F_i have alternation depth 2 and are on disjoint variables. If f has degree more than d, it suffices to kill any one factor F_i to make the polynomial 0. Choosing the factor with fewest variables, and proceeding as above, we set no more than $|\mathsf{var}(f)|/d$ variables. Again, since F is an ROF, if F is 0-justified, then so are the F_i. So A_S can be chosen avoiding 0s. □

Using this, we get a hardness of representation result for 0-justified alternation-depth 3 ROPs.

Theorem 4. *Let $\epsilon \in (0, \frac{1}{2})$. If there are 0-justified, alternation-depth-3 ROPs $f_1, \ldots, f_s$, and non-negative integers $e_1, \ldots, e_s$ such that*

$$\sum_{i=1}^{s} f_i^{e_i} = x_1 \cdots x_n$$

then $s \geq n^{\frac{1}{2}-\epsilon}$.

Proof. Let d be a parameter to be chosen later. We identify a subset of variables S and an assignment A avoiding zeroes to variables of S, such that under this partial assignment, all the f_i's are reduced to degree at most d. We show that for any $d \in [n]$, this is possible with $|S| = t \leq \frac{s^2 n}{d}$. This gives a sum-powers representation of degree d and size s for $\prod_{x_i \notin S} x_i = M_{n-t}$. Invoking Kayal's result from Proposition 1, we see that $s \geq 2^{c(n-t)/d}$, and hence $\log s + \frac{cns^2}{d^2} \geq \frac{cn}{d}$. Choosing $d = 4n^{1-2\epsilon}$, we conclude that $s \geq n^{\frac{1}{2}-\epsilon}$.

The construction of S proceeds in stages. At the kth stage, polynomials $f_1, \ldots, f_{i-1}$ have already been reduced to low-degree polynomials, and we consider f_i. We want to use Lemma 5 at each stage. This requires that each polynomial f_i, **after all the substitutions from the previous stages**, is still a 0-justified ROF with alternation-depth 3. The alternation-depth-3 ROF is obvious; it is only maintaining 0-justified that is a bit tricky. We describe the construction for stage 1; the other stages are similar.

Applying Lemma 5 to f_1 with d as the parameter, we obtain a set R_1 of variables with $|R_1| \leq n/d$ and an assignment A_{R_1} avoiding 0, such that $\deg(f_1|_{R_1 \to A_{R_1}}) \leq d$. It may be the case that for some $i > 1$, the polynomial $f_i|_{R_1 \to A_{R_1}}$ is no longer 0-justified. We fix this by augmenting R_1 as follows.

Assume first that the ROFs for all the f_i's have top-gate $+$; we will discuss top-gate $\times$ later. So, as discussed in the proof of Lemma 5, each f_i has the form $\sum \prod \ell_{j,k}$ where each $\ell_{j,k}$ is a linear form. If $f_i|_{R_1 \to A_{R_1}}$ is not 0-justified, then some of the linear forms in it are homogeneous linear (no constant term). We identify such linear forms in each f_i, $i \geq 2$. Call this set L_1. That is,

$$L_1 = \left\{ \ell \mid \begin{array}{l} \ell \text{ is a linear form at level-2 of some } f_i; \\ \ell|_{R_1 \to A_{R_1}} \text{ is homogeneous linear but not} \\ \text{identically 0.} \end{array} \right\}$$

Since each f_i is a ROF, it contributes at most $|R_1|$ linear forms to L_1. Hence $|L_1| \leq (s-1)|R_1|$. Now pick a minimal set T_1 of variables from $X \setminus R_1$ that intersects each of the linear forms in L_1. By minimality, $|T_| \leq |L_1| \leq (s-1)|R_1|$. We want to assign non-zero values A_{T_1} to variables in T_1 in such a way that for all $i \geq 2$, the $f_i|_{R_1 \to A_{R_1}; T_1 \to A_{T_1}}$ are 0-justified. We must ensure that the linear forms in L_1 become homogeneous (or vanish altogether), and we must also ensure that previously non-homogeneous forms do not become homogeneous. To achieve this, consider

$$L_2 = \left\{ \ell \mid \begin{array}{l} \ell \text{ is a linear form at level-2 of some } f_i; \\ \ell|_{R_1 \to A_{R_1}} \not\equiv 0; \ell|_{R_1 \to A_{R_1}} \text{ contains a variable from } T_1. \end{array} \right\}$$

Clearly, $L_1 \subseteq L_2$. It suffices to find an assignment A_{T_1} to variables in T_1, avoiding zeroes, such that for each $\ell \in L_2$, either $\ell|_{R_1 \to A_{R_1}; T_1 \to A_{T_1}} \equiv 0$ or $\ell|_{R_1 \to A_{R_1}; T_1 \to A_{T_1}}(0) \neq 0$. For sufficiently large fields, such an assignment can always be found.

If some of the f_i's have top-gate $\times$, we need only a minor modification. We use this fact:

Observation 1 *If $F = \prod F_r$ is a read-once formula, then F is* 0-justified *if and only if for each r, F_r is* 0-justified *and satisfies $F_r(0) \neq 0$.*

Treat each factor of the polynomials with top-gate $\times$ exactly as we dealt with the other polynomials. Add their level-2 linear factors to L_1. Note that each such f_i can have many factors, but since it is read-once, any one variable can occur in at most one of these factors. So f_i still contributes no more than R_1 linear forms to L_1. Also modify the definition of L_2 to include also all linear forms at level 3 of such f_i's, containing a variable of T_1. Finally, look for an assignment also satisfying the additional condition that the factors do not vanish at 0. Again, over sufficiently large fields, it is possible to find such an assignment.

Now we set $S_1 = R_1 \cup T_1$, and $A_1 = A_{R_1} \cup A_{T_1}$. We have ensured the following:

1. $\deg(f_1|_{S_1 \to A_1}) \leq d$; and
2. for $i \geq 2$, $f_i|_{S_1 \to A_1}$ is 0-justified.

Furthermore, $|S_1| = |R_1| + |T_1| \leq |R_1|(1 + (s-1)) \leq sn/d$.

Other stages are identical, working on the polynomials restricted by the already-chosen assignments. Finally, $S = S_1 \cup \ldots \cup S_s$, and so $|S| \leq s^2 n/d$, as required. □

6 Further Questions

- Can the results of [SV08] be extended to the case $\sum_{i=1}^{k} f_i^{r_i}$, where f_i's are ROFs?
- Can a hardness of representation for $\mathsf{Sym}_{n,d}$ be transformed into a polynomial identity test for a related model?
- Can the bound given by Theorem 3 be improved? We conjecture:

  Conjecture 1. There is a constant $\epsilon > 0$ such that if there are CF-ROPs $f_1, \ldots, f_k$, and integers $e_1, \ldots e_k \geq 0$ satisfying

  $$\sum_{i=1}^{k} f_i^{e_i} = \mathsf{Sym}_{n,n/2},$$

  then $k = \Omega(n^{\epsilon})$.

- Do the results of [AvMV11] extend to read-k-multilinear branching programs?

References

[Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Problem and Computing*, 8, 1999.

[AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *FOCS*, pages 67–75, 2008.

[AvMV11] Matthew Anderson, Dieter van Melkebeek, and Ilya Volkovich. Derandomizing polynomial identity testing for multilinear constant-read formulae. In *CCC*, pages 273–282, 2011.

[BE11] Markus Bläser and Christian Engels. Randomness efficient testing of sparse black box identities of unbounded degree over the reals. In *STACS*, pages 555–566, 2011.

[BHS08] Markus Bläser, Moritz Hardt, and David Steurer. Asymptotically optimal hitting sets against polynomials. In *ICALP (1)*, pages 345–356, 2008.

[BOT88] Michael Ben-Or and Prasoon Tiwari. A deterministic algorithm for sparse multivariate polynominal interpolation (extended abstract). In *STOC*, pages 301–309, 1988.

[DS07] Zeev Dvir and Amir Shpilka. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM J. Comput.*, 36(5):1404–1434, 2007.

[FMM12] Hervé Fournier, Guillaume Malod, and Stefan Mengel. Monomials in arithmetic circuits: Complete problems in the counting hierarchy. In *STACS*, pages 362–373, 2012.

[GKKS13] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *FOCS*, pages 578–587, 2013.

[Kay12] Neeraj Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *ECCC*, 19(TR12-081):81, 2012.

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

[KS01] Adam Klivans and Daniel A. Spielman. Randomness efficient identity testing of multivariate polynomials. In *STOC*, pages 216–223, 2001.

[KS07] Neeraj Kayal and Nitin Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity*, 16(2):115–138, 2007.

[MRS14] Meena Mahajan, B. V. Raghavendra Rao, and Karteek Sreenivasaiah. Monomials, multilinearity and identity testing in simple read-restricted circuits. *Theoretical Computer Science*, 524:90–102, 2014. preliminary version in MFCS 2012.

[RS11] B. V. Raghavendra Rao and Jayalal M. N. Sarma. Isomorphism testing of read-once functions and polynomials. In *FSTTCS*, pages 115–126, 2011.

[RS13] B. V. Raghavendra Rao and Jayalal M. N. Sarma. Isomorphism testing of read-once functions and polynomials. manuscript, 2013.

[Sax14] Nitin Saxena. Progress on polynomial identity testing - ii. *CoRR*, abs/1401.0976, 2014.

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

[SV08] Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. In *STOC*, pages 507–516, 2008. See also ECCC TR-2010-011.

[SV10] Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. *ECCC*, page 011, 2010. Preliminary version in STOC 2010.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Found. Trends Theor. Comput. Sci.*, 5(3):207–388, 2010.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM*, pages 216–226, 1979.