Improved Explicit Hitting-Sets for ROABPs

Zeyu Guo[1]
Department of Computer Science, University of Haifa, Israel
zguotcs@gmail.com

Rohit Gurjar
Department of Computer Science and Engineering, IIT Bombay, India
rohitgurjar0@gmail.com

Abstract

We give improved explicit constructions of hitting-sets for *read-once oblivious algebraic branching programs* (ROABPs) and related models. For ROABPs in an unknown variable order, our hitting-set has size polynomial in $(nr)^{\frac{\log n}{\max\{1,\log\log n-\log\log r\}}}d$ over a field whose characteristic is zero or large enough, where n is the number of variables, d is the individual degree, and r is the width of the ROABP. A similar improved construction works over fields of arbitrary characteristic with a weaker size bound.

Based on a result of Bisht and Saxena (2020), we also give an improved explicit construction of hitting-sets for *sum of several ROABPs*. In particular, when the characteristic of the field is zero or large enough, we give polynomial-size explicit hitting-sets for sum of constantly many log-variate ROABPs of width $r = 2^{O(\log d/\log\log d)}$.

Finally, we give improved explicit hitting-sets for polynomials computable by width-r ROABPs in any variable order, also known as *any-order ROABPs*. Our hitting-set has polynomial size for width r up to $2^{O(\log(nd)/\log\log(nd))}$ or $2^{O(\log^{1-\epsilon}(nd))}$, depending on the characteristic of the field. Previously, explicit hitting-sets of polynomial size are unknown for $r = \omega(1)$.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Theory of computation → Pseudorandomness and derandomization

Keywords and phrases polynomial identity testing, hitting-set, ROABP, arithmetic branching programs, derandomization

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2020.4

Category RANDOM

Acknowledgements We thank Nitin Saxena, Sumanta Ghosh, and Pranav Bisht for many helpful discussions about PIT for ROABPs and related models.

1 Introduction

Polynomial identity testing (PIT) is one of the fundamental problems in the area of derandomization. The problem asks whether a given multi-variate polynomial is identically zero. For example, the polynomial $(x+y)(x-y)-x^2-y^2$ is identically zero. The input to the problem can be given as an algebraic formula or circuit or other algebraic computation models like arithmetic branching programs or determinant of a symbolic matrix. The problem is not known to be polynomial-time solvable. One way to test zeroness could be to check whether the coefficient of each monomial is zero in the polynomial. However, for a given circuit or branching program, it might take exponential time (in the input size) to compute coefficients.

On the other hand, there is a simple (polynomial time) randomized algorithm to test zeroness of a given polynomial: just evaluate the input circuit at a random point and see if the evaluation is nonzero. It is known that a nonzero polynomial evaluated at a random

[1] Part of this work was done while the first author was a postdoc at IIT Kanpur.

point from gives a nonzero value with high probability [14, 6, 22, 20]. More precisely, for an n-variate polynomial of degree d, if you evaluate it at a random point from S^n for some subset $S \subseteq \mathbb{F}$, then the probability of the evaluation being zero is at most $d/|S|$. The polynomial identity testing question can be asked over any field, however as this randomized algorithm suggests, in case of finite characteristic we need to take a large enough field extension.

To obtain a deterministic polynomial time algorithm for the polynomial identity testing has been a long open question. Such an algorithm is known only for some special cases, for example, read-once oblivious arithmetic branching programs (ROABP) (for more such cases, see [21, 18, 19]). Deterministic identity testing for ROABPs has been widely studied in the last decade. One reason for such an interest in this special case is that it can be considered as an algebraic analogue of the RL vs. L question. An ROABP is a product of matrices $f = \beta^\top f_1 f_2 \cdots f_n \gamma$ where $\beta, \gamma \in \mathbb{F}^{r\times 1}$ and $f_i \in \mathbb{F}^{r\times r}[x_{\pi(i)}]$ is a matrix with entries being polynomials in the variable $x_{\pi(i)}$ for each $1 \leq i \leq n$ for some permutation $\pi\colon [n] \to [n]$. The permutation π is said to be the variable order of the ROABP.

Raz and Shpilka [16] gave the first polynomial time algorithm to test whether a given ROABP computes a nonzero polynomial. PIT is also studied in the so-called black-box model, where one does not have access to the circuit/ABP computing the polynomial. Instead, one has to construct an explicit hitting-set – a set of points with the guarantee that every nonzero polynomial in the class of interest gives a nonzero evaluation on at least one of the points in the set. Here, by *explicit* we mean that every point in the hitting-set should be computable in polynomial time. Forbes and Shpilka [9] first gave a quasi-polynomial size explicit hitting-set for ROABPs, when the variable order is known. In subsequent works [8, 1], a quasi-polynomial size explicit hitting-set was also constructed for the unknown order case. Constructing a polynomial-size explicit hitting-set for ROABPs remains a challenging open question. This situation is somewhat similar to that for pseudorandom generators (PRG) for log-space computation. There are no PRGs known with the optimal seed length, i.e. $O(\log n)$, but are known with close to optimal seed length i.e., $O(\log^2 n)$ [13, 12, 15].

There has been a sequence of work in last few years which improve the hitting-set construction for ROABPs with respect to various parameters. There are usually three parameters associated with ROABPs, its length or depth n, which is same as the number of variables, the individual degree d – maximum degree of any variable, and the width r – the size of the matrices involved in the product. The hitting-set of [9] and of [1] both had size $(ndr)^{O(\log n)}$, for the cases of known and unknown variable orders, respectively. For the known order case slightly better results are known. The first paper [9] also gave a bound of $(ndr)^{O(\log n/\max\{1,\log\log n - \log\log r\})}$, which is better when the width r is relatively small. For the small width case, another improved bound of $ndr^{\log n}$ was obtained by [10], when the field characteristic is zero or large enough.

A special class of polynomials, which is known to have better hitting-sets, is called any-order ROABPs. These are polynomials that have small-width ROABPs in every possible variable order. Any-order ROABPs generalize commutative ROABPs[2] and diagonal circuits [17]. Building upon the techniques of [8], an explicit hitting-set of size $(ndr)^{O(\log\log r)}$ for any-order ROABPs was obtained in [10].

A more general model, namely, sum of constantly many ROABPs was considered by [11]. As is known for ROABPs, they could give a polynomial time algorithm for sum of constantly many ROABPs in the white-box case and also a quasi-polynomial size explicit hitting-set. More precisely, for a sum of c ROABPs, their hitting-set size is $(ndr)^{O(c\cdot 2^c \log(ndr))}$.

[2] We say an ROABP is commutative if its output does not change under any permutation of the matrices involved in the product. The usage of "commutative ROABP" is slightly different in [8], which actually refers to any-order ROABPs in this paper.

Recently, Bisht and Saxena [3] considered PIT for ROABP and sum of ROABPs in the small variate regime. For a sum of c ROABPs, they gave a hitting-set of size $\text{poly}(r^{n3^c}, d^c)$, which also means a hitting-set of size $\text{poly}(r^n, d)$ for an ROABP. These results are better than those of [11] and [1] respectively, when $n = O(\log(rd))$ and $r = O(1)$.

In this work we give improved explicit hitting-sets for ROABPs (unknown order), sum of several ROABPs (small variate regime) and any-order ROABPs with respect to various parameters. Though, we are still away from a polynomial size hitting-set, one important feature of our results is a better dependence on the degree parameter d. In particular, for unknown order and any-order ROABPs, our dependence on d is only polynomial instead of quasi-polynomial (when field characteristic is zero/large). This is somewhat analogous to a recent result for read-once boolean branching programs [4], where they construct a hitting-set of size quasi-polynomial in length and width, but the dependence on the error parameter $1/\epsilon$ is nearly-polynomial.

1.1 Our Results

We now state our main theorems, which give improved explicit constructions of hitting-sets for ROABPs in an unknown order, sum of several ROABPs, and any-order ROABPs.

1.1.1 ROABPs in an Unknown Order

We have the following result for general ROABPs in an unknown order.

▶ **Theorem 1.** *Let $\mathcal{C}$ be the family of polynomials $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ computed by ROABPs of length n, width r and individual degree d in an unknown order. If $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d$, then there exists an explicit hitting-set for $\mathcal{C}$ of size polynomial in*

$$M(n, r, d) := d \cdot (nr)^{\frac{\log n}{\max\{1, \log\log n - \log\log r\}}}.$$

In arbitrary characteristic, there exists an explicit hitting-set for $\mathcal{C}$ of size polynomial in

$$M'(n, r, d) := \begin{cases} (nr)^{\log n} d & nd \leq r^2, \\ (nd)^{\frac{\log n}{\log\log(nd) - \log\log r}} & r^2 < nd < r^n, \\ nd & nd \geq r^n. \end{cases}$$

Comparison with Previous Work. In all cases, our bounds are strictly better than the previous best bound of $(ndr)^{O(\log n)}$ [1] for unknown order ROABPs. In particular, our dependence on the individual degree d is better. Our bounds are also better than known order case results of [9]. Recall that they had an explicit hitting-set of size $(ndr)^{O(\log n)}$, and for small r, they had an explicit hitting-set of size $(ndr)^{O(\log n/\max\{1, \log\log n - \log\log r\})}$ (not explicitly written, but follows from [9, Theorem 3.24]). These results are subsumed by Theorem 1. In fact, we follow the same idea in [9] of merging $k \geq 2$ parts of the ROABP at each level of the recursion. We note our construction has two advantages compared with [9]:

- Theorem 1 applies to ROABPs in an *unknown* order, while it is not clear how to achieve the same using the construction in [9]. The requirement that the hitting-set works in an unknown order is crucial for the model of the sum of several ROABPs which is discussed below.
- When $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d$, our size bound depends only polynomially on the individual degree bound d, which gives much smaller hitting-sets compared with [9] if $n, r \ll d$.

The hitting-set constructed in [3, Lemma 9] for $\mathcal{C}$ of size $\text{poly}(r^n, d)$ is also subsumed by our result. When $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d$, Theorem 1 improves this by giving an explicit hitting-set of size $M(n, r, d) \leq \text{poly}((nr)^{\log n}, d)$. In particular, in the log-variate case $n = O(\log(rd))$ considered in [3], they can achieve a $\text{poly}(n, r, d)$-size hitting-set only when $r = O(1)$, while we can achieve the same for r up to $2^{O(\log d/ \log\log d)}$. In arbitrary characteristic, we obtain a worse size bound $M'(n, r, d)$, which still subsumes [3, Lemma 9].[3]

Finally, in comparison with the hitting-set of [10, Theorem 3.6] of size $\text{poly}(n^{\log r}, d)$ for *known* order ROABPs, our bound of $M(n, r, d)$ is weaker. In particular, they give polynomial-size hitting-sets when the width r is constant. However, their result is not known to be extendible to ROABPs in an unknown order.

1.1.2 Sum of Several ROABPs

The paper [3] studied the problem of constructing hitting-sets for the sum of several (log-variate) ROABPs and established a reduction from this problem to constructing hitting-sets for ROABPs in an unknown order. Using this reduction, we obtain the following result for the model of sum of several ROABPs.

▶ **Theorem 2.** *Let $\mathcal{C}$ be the family of polynomials $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ computed by the sum of c ROABPs of length n, width $r \geq 2$ and individual degree d in unknown and possibly different orders.*

1. *If $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d$, there exists an explicit hitting-set for $\mathcal{C}$ of size polynomial in $2^{cn} \cdot M(n, (2r)^{3^c}, d)^c$ where $M(\cdot, \cdot, \cdot)$ is as in Theorem 1. In particular, the hitting-set has size $\text{poly}(d)$ when $c = O(1)$, $n = O(\log d)$ and $r = 2^{O(\log d/ \log\log d)}$.*
2. *In arbitrary characteristic, there exists an explicit hitting-set for $\mathcal{C}$ of size polynomial in $2^{cn} \cdot M'(n, (2r)^{3^c}, d)^c$ where $M'(\cdot, \cdot, \cdot)$ is as in Theorem 1.*

The paper [3] constructed an explicit hitting-set of size $\text{poly}(r^{n3^c}, d^c)$ for $\mathcal{C}$, which has size $\text{poly}(d)$ when $n = O(\log d)$ and c, r are constants. This result is subsumed by our Theorem 2 (2) since $M'(n, r, d)$ is bounded by $\text{poly}(n, r^n, d)$. Moreover, when $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d$, our Theorem 2 (1) yields a $\text{poly}(d)$-size hitting-set for $n = O(\log d)$, $c = O(1)$ and $r = 2^{O(\log d/ \log\log d)}$ (instead of constant r).

1.1.3 Any-Order ROABPs

Recall that any-order ROABPs are polynomials that have small-width ROABPs in every possible variable order. We obtain the following result for any-order ROABPs.

▶ **Theorem 3.** *Let $\mathcal{C}$ be the family of polynomials $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ computed by ROABPs of length n, width r and individual degree d in any order.*

1. *If $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > n^4(d+1)^2$, then there exists an explicit hitting-set for $\mathcal{C}$ of size $\text{poly}(n, r^{\log\log r}, d)$. In particular, the hitting-set has size $\text{poly}(n, d)$ for $r = 2^{O(\log(nd)/ \log\log(nd))}$.*
2. *In arbitrary characteristic, there exists an explicit hitting-set for $\mathcal{C}$ of size*

$$\text{poly}(r^{\log\log r}, (nd)^{1+\frac{\log\log r}{\max\{1, \log\log(nd) - \log\log r\}}}).$$

So the hitting-set has size $\text{poly}(n, d)$ for $r = 2^{O(\log^{1-\epsilon}(nd))}$ and any constant $0 < \epsilon < 1$.

---

[3] We note that [3, Lemma 9] is proved using ideas different from ours. To directly see that our bound subsumes the bound $\text{poly}(r^n, d)$ when $r^2 < nd < r^n$, write $nd = r^{n^{1/e}}$ with $1 < e < \log n$ and note $M'(n, r, d) = (nd)^{\frac{\log n}{\log\log(nd) - \log\log r}} = r^{en^{1/e}} = r^{O(n)}$.

The previous best explicit construction of hitting-sets for any-order ROABPs [10] has size $(ndr)^{O(\log\log r)}$, which is superpolynomial for width $r = \omega(1)$. Our hitting-set has polynomial size for r up to $2^{O(\log(nd)/\log\log(nd))}$ or $2^{O(\log^{1-\epsilon}(nd))}$ depending on the characteristic of $\mathbb{F}$.

1.2 Proof Techniques

We prove our results by combining the analyses in previous work [8, 1, 10, 11, 3] with the following ideas.

(1) Low-Degree Concentration via Random Shift. Randomly shifting a multivariate polynomial is an important and common technique in polynomial identity testing for ROABPs and related models. For example, it was used in [2, 8, 1, 10, 11, 7] to achieve rank concentration of polynomials. We use a simple version of this technique, applied only to univariate polynomials: View the layers of a width-r ROABP as univariate polynomials $f_1(x_1), f_2(x_2), \ldots, f_n(x_n)$ with matrix-valued coefficients. We preprocess these polynomials by performing the shift $f_i(x_i) \mapsto f_i(x_i + \alpha)$ simultaneously for $i = 1, 2, \ldots, n$ with randomly chosen $\alpha \in \mathbb{F}$.

Assuming $\mathrm{char}(\mathbb{F})$ is zero or large, a standard argument shows that with high probability, each of the new polynomials $f_i(x_i + \alpha)$ is *low-degree concentrated* in the sense that its coefficient span, which has dimension $\ell_i \leq r^2$, is spanned by the coefficients of the ℓ_i monomials with the lowest degrees. This is useful when the width r is much smaller than the degree bound d of the polynomials, as it allows us to reduce d to r^2 in the analysis.

We remark that a generalization of this technique was developed in [7], where it was shown that a (pseudo-)random shift achieves *low-cone concentration* for multivariate polynomials [7, Theorem 2]. We only need the special case for univariate polynomials, which is classical and uses the nonsingularity of the Wronskian matrix.

(2) Merging Multiple Parts at Each Level of the Recursion. Explicit hitting-sets for ROABPs of size $(ndr)^{O(\log n)}$ were constructed in [9, 1], which may be seen as analogues of the PRG constructions in [13] and [12] for read-once branching programs. Roughly speaking, these hitting-sets are recursively constructed as follows: Divide the ROABP into two parts, construct a hitting-set for each part recursively, and then merge them at the cost of increasing the size by a factor polynomial in ndr. The size of the final hitting-set is $(ndr)^{O(\log n)}$ as the recursion tree has depth $O(\log n)$.

A slightly better construction was also given in [9] for ROABPs of small width. The idea is to merge k parts of the ROABP at each level of the recursion, where k is possibly greater than two. We use the same idea in this paper but replace the construction in [9] by the one in [1], which has the advantage of working for ROABPs in an unknown order. The cost incurred at each level of the recursion is bounded by $\mathrm{poly}(n, d, r^k)$ while there are $O(\log n/\log k)$ levels. When $\mathrm{char}(\mathbb{F})$ is zero or large, the cost incurred at each level may be improved to $\mathrm{poly}(n, r^k)$ by using the idea (1) above. We then choose the optimal k according to the parameters n, r and d.

(3) Reducing the Number of Variables via Hashing. In [8, 10], hitting-sets for any-order ROABPs are constructed in two steps: The first step is to explicitly construct a small set $T \subseteq \mathbb{F}^n$ such that for some $s = (s_1, s_2, \ldots, s_n) \in T$, performing the shift $x_i \mapsto x_i + s_i$ achieves *low-support concentration* for any-order ROABPs. The second step is to convert an any-order ROABP with low-support concentration into a short ROABP.

In [8], the cost of the first step (i.e., the size of T) is polynomial in n and $d^{\log r}$. This was later improved to $(ndr)^{O(\log\log r)}$ in [10]. In this paper, we further improve the cost to $\mathrm{poly}(n, r^{\log\log r}, d)$ when $\mathrm{char}(\mathbb{F})$ is zero or large. In arbitrary characteristic, we obtain a worse bound which still improves those in [8, 10]. See Theorem 16 for details.

One crucial idea used in [8, 10] (which originates from [2]) is that for any-order ROABPs, low-support concentration is a "local" property. Namely, in order to achieve low-support concentration of n-variate any-order ROABPs, it suffices to achieve it when restricting to every subset of ℓ variables, where $\ell = O(\log r)$. In this paper, we use a construction similar to the one in [10] except that we further exploit the locality by using hash functions. This has the effect of reducing n to $\mathrm{poly}(\log r)$ in the analysis, which leads to the improvement.

Organization of the Paper. Preliminaries and notations are given in Section 2. Theorem 1 and 2 are proved in Section 3. Theorem 3 is proved in Section 4. Finally, some open problems are listed in Section 5.

2 Preliminaries

Notations. Let $\mathbb{N} := \{0, 1, 2, \dots\}$ and $\mathbb{N}^+ := \{1, 2, \dots\}$. Denote $\{1, 2, \dots, n\}$ by $[n]$. The cardinality of a set S is denoted by $|S|$. Denote by $\log a$ the logarithm of a with base two.

Let $\mathbb{F}$ be a field. Throughout this paper, we always assume $|\mathbb{F}|$ is large enough. This can be guaranteed by replacing $\mathbb{F}$ with an extension field if necessary. We often write $\mathbf{x}$ as a shorthand for a list of variables $x_1, x_2, \dots, x_n$. For $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{N}^n$, write $\mathbf{x}^\mathbf{a}$ for the monomial $\prod_{i=1}^n x_i^{a_i}$. The *support* of $\mathbf{x}^\mathbf{a}$ is $\mathrm{supp}(\mathbf{x}^\mathbf{a}) := \{i \in [n] : a_i > 0\}$. The set of all monomials in $x_1, x_2, \dots, x_n$ is denoted by $\mathcal{M}(x_1, x_2, \dots, x_n)$ or $\mathcal{M}(\mathbf{x})$.

For an algebra $\mathbb{A}$ over $\mathbb{F}$, write $\mathbb{A}[\mathbf{x}]$ for the ring of polynomials in the variables $\mathbf{x}$ with coefficients in $\mathbb{A}$. For $f \in \mathbb{A}[\mathbf{x}]$ and a monomial $m = \mathbf{x}^\mathbf{a}$, denote by $\mathrm{coef}_f(m) \in \mathbb{A}$ the coefficient of m in f. The linear span of a set $T \subseteq \mathbb{A}$ over $\mathbb{F}$ is denoted by $\mathrm{span}\, T$. The *coefficient span* of $f \in \mathbb{A}[\mathbf{x}]$ is $\mathrm{span}(f) := \mathrm{span}\{\mathrm{coef}_f(m) : m \text{ is a monomial in } f\}$.

More generally, for an extension field $\mathbb{K}$ of $\mathbb{F}$, denote by $\mathbb{A} \otimes_\mathbb{F} \mathbb{K}$ the tensor product of $\mathbb{A}$ and $\mathbb{K}$ over $\mathbb{F}$, which is an algebra over $\mathbb{K}$, i.e., $\mathbb{A} \otimes_\mathbb{F} \mathbb{K}$ is obtained from $\mathbb{A}$ by extending the field of scalars from $\mathbb{F}$ to $\mathbb{K}$. For $f \in (\mathbb{A} \otimes_\mathbb{F} \mathbb{K})[\mathbf{x}]$ and a monomial $m = \mathbf{x}^\mathbf{a}$, again denote by $\mathrm{coef}_f(m) \in \mathbb{A} \otimes_\mathbb{F} \mathbb{K}$ the coefficient of m in f. The linear span of a set $T \subseteq \mathbb{A} \otimes_\mathbb{F} \mathbb{K}$ over $\mathbb{K}$ is denoted by $\mathrm{span}_\mathbb{K} T$. The coefficient span of $f \in (\mathbb{A} \otimes_\mathbb{F} \mathbb{K})[\mathbf{x}]$ over $\mathbb{K}$ is $\mathrm{span}_\mathbb{K}(f) := \mathrm{span}_\mathbb{K}\{\mathrm{coef}_f(m) : m \text{ is a monomial in } f\}$.

Let $r \in \mathbb{N}^+$ be a parameter. From now on, we fix $\mathbb{A}$ to be $M_{r\times r}(\mathbb{F})$, the algebra of $r \times r$ matrices over $\mathbb{F}$, even though statements in this paper often hold over other algebras as well. So $\mathbb{A} \otimes_\mathbb{F} \mathbb{K}$ is simply $M_{r\times r}(\mathbb{K})$, the algebra of $r \times r$ matrices over $\mathbb{K}$.

Rank Concentration. We need the following definitions about rank concentration.

▶ **Definition 4.** *Let $f \in \mathbb{A}[\mathbf{x}] = \mathbb{A}[x_1, x_2, \dots, x_n]$ be a polynomial over $\mathbb{A}$. For a set $S \subseteq \mathcal{M}(\mathbf{x})$ of monomials, we say f is* concentrated on S *if* $\mathrm{span}(f) = \mathrm{span}\{\mathrm{coef}_f(m) : m \in S\}$. *For $\ell \in \mathbb{N}$, we say f is* ℓ-support concentrated *if it is concentrated on $S = \{\mathbf{x}^\mathbf{a} : |\mathrm{supp}(\mathbf{x}^\mathbf{a})| < \ell\}$. Similarly, we say f is* ℓ-degree concentrated *if it is concentrated on $S = \{\mathbf{x}^\mathbf{a} : \deg(\mathbf{x}^\mathbf{a}) < \ell\}$.*

More generally, for an extension field $\mathbb{K}$ of $\mathbb{F}$, we say $f \in (\mathbb{A} \otimes_\mathbb{F} \mathbb{K})[\mathbf{x}]$ is concentrated on S over $\mathbb{K}$, ℓ-support concentrated *over $\mathbb{K}$, or* ℓ-degree concentrated *over $\mathbb{K}$ if f satisfies the corresponding property above with* $\mathrm{span}(f)$ *and* $\mathrm{span}\{\mathrm{coef}_f(m) : m \in S\}$ *replaced by* $\mathrm{span}_\mathbb{K}(f)$ *and* $\mathrm{span}_\mathbb{K}\{\mathrm{coef}_f(m) : m \in S\}$ *respectively.*

We use low-degree concentration of f only for univariate polynomials f in this paper.

Hitting-Sets. We say a set $\mathcal{H} \subseteq \mathbb{F}^n$ is a *hitting-set* for a nonzero polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ if there exists $\alpha \in \mathcal{H}$ such that $f(\alpha) \neq 0$. We say $\mathcal{H} \subseteq \mathbb{F}^n$ is a hitting-set for a class of polynomials $\mathcal{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ if $\mathcal{H}$ is a hitting-set for every nonzero polynomial in $\mathcal{C}$.

ROABPs. A *read-once oblivious arithmetic branching program* (ROABP) in the order $x_1, \ldots, x_n$ is a weighted directed graph $\mathcal{B}$ with $n+1$ layers of vertices $\{V_0, V_1, \ldots, V_n\}$ together with a start node s and an end node t. All the edges are from s to V_0, V_{i-1} to V_i for $i \in [n]$, or V_n to t.

For $i \in [n]$, the weight of an edge e from V_{i-1} to V_i is a univariate polynomial $w_e \in \mathbb{F}[x_i] \subseteq \mathbb{F}[\mathbf{x}]$. The weights of the edges e from s to V_0 and those from V_n to t are constants (i.e, $w_e \in \mathbb{F}$). We define the weight of a path in $\mathcal{B}$ from s to t to be the product of the weights of the edges on that path. The polynomial computed by $\mathcal{B}$ is the sum of the weights of the paths in $\mathcal{B}$ from s to t.

Let $r = \max\{|V_i| : i \in [n]\}$. We say $\mathcal{B}$ has *length*[4] n and *width* r. We say $\mathcal{B}$ has *individual degree* d if $\deg(w_e) \leq d$ for $e \in E(\mathcal{B})$. By adding dummy vertices, we may always assume each layer V_i of $\mathcal{B}$ has exactly r vertices. The polynomial f computed by $\mathcal{B}$ can be represented as a product of matrices $f = \beta^\top f_1 f_2 \cdots f_n \gamma$ where $\beta, \gamma \in \mathbb{F}^{r \times 1}$ and $f_i \in \mathbb{A}[x_i]$ for $i \in [n]$ with $\mathbb{A} = M_{r \times r}(\mathbb{F})$.

Let $c > 0$ be a large enough constant. Throughout the paper, we always assume the length n of an ROABP is at least c and the width r is at least two, which is fine since explicit hitting-sets of polynomial size for ROBAPs are easy to construct when $n < c$ or $r = 1$. These assumptions are made to avoid technicalities in boundary cases (e.g. $\log \log r$ is undefined when $r = 1$). Similarly, we always assume the individual degree bound d is at least c by replacing d with $\max\{d, c\}$ if necessary.

Unknown-Order and Any-Order ROABPs. The above definition of ROABPs is given with respect to the variable order $x_1, x_2, \ldots, x_n$. More generally, we say an ROABP has an *unknown order* or is an *unknown-order ROABP* if it has the variable order $x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}$ where π is an arbitrary permutation of $[n]$.

Let $\mathcal{C}$ be a class of unknown-order ROABPs. We say $f \in \mathbb{F}[\mathbf{x}]$ is computed by ROABPs in $\mathcal{C}$ *in any order* (or simply an *any-order ROABP* in $\mathcal{C}$) if for every permutation π of $[n]$, f is computed by an ROABP in $\mathcal{C}$ that has the variable order $x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}$. In this paper, $\mathcal{C}$ will be the class of unknown-order ROABPs of length n, width r and individual degree d for some n, r and d.

We also say a polynomial $f \in \mathbb{A}[\mathbf{x}]$ over $\mathbb{A}$ is computed by ROABPs of length n, width r and individual degree d in any order if for any permutation π of $[n]$, we can write $f = f_1 f_2 \cdots f_n$ such that $f_i \in \mathbb{A}[x_{\pi(i)}]$ is a univariate polynomial of degree at most d in $x_{\pi(i)}$ where $\mathbb{A} = M_{r \times r}(\mathbb{F})$.

3 Hitting-Sets for ROABPs

In this section, we give an explicit construction of hitting-sets for ROABPs in an unknown order. Then we prove Theorem 1 and Theorem 2.

[4] The length is also called the *depth* and equals the number of variables.

3.1 Low-Degree Concentration by Random Shift

We start with the following lemma, which states that random shift achieves low-degree concentration with high probability.

▶ **Lemma 5.** *Suppose* $\mathrm{char}(\mathbb{F}) = 0$ *or* $\mathrm{char}(\mathbb{F}) > d \in \mathbb{N}$. *Let* $f \in \mathbb{A}[x]$ *be a univariate polynomial of degree* d. *Let* $\ell = \dim_{\mathbb{F}}(\mathrm{span}(f)) \leq \dim_{\mathbb{F}} \mathbb{A} = r^2$. *Then for all but at most* $d\ell$ *choices of* $\alpha \in \mathbb{F}$, $f(x+\alpha)$ *is* ℓ*-degree concentrated.*

Proof. Using the fact that all the $\ell \times \ell$ minors of the Wronskian matrix $W = \left[\binom{i}{j}\right]_{0 \leq i \leq d, 0 \leq j < \ell}$ are nonzero when $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d$, it can be shown that $f(x+t)$ is ℓ-degree concentrated over $\mathbb{F}(t)$, where t is an indeterminate. We omit the proof of this claim but note it is a special case of [7, Theorem 2] applied to univariate polynomials.

View $\mathbb{A}$ as a vector space over $\mathbb{F}$. As $f(x+t)$ is ℓ-degree concentrated, the matrix formed by the ℓ vectors $\mathrm{coef}_{f(x+t)}(1), \mathrm{coef}_{f(x+t)}(x), \ldots, \mathrm{coef}_{f(x+t)}(x^{\ell-1}) \in \mathbb{A}$ has a nonzero $\ell \times \ell$ minor $g(t)$. Note $g(t)$ is a polynomial in t of degree at most $d\ell$. So for all but at most $d\ell$ choices of α, we have $g(\alpha) \neq 0$. For such α, the vectors $\mathrm{coef}_{f(x+\alpha)}(1), \mathrm{coef}_{f(x+\alpha)}(x), \ldots, \mathrm{coef}_{f(x+\alpha)}(x^{\ell-1})$ are linearly independent and hence span the space $\mathrm{span}(f) = \mathrm{span}(f(x+\alpha))$. So $f(x+\alpha)$ is ℓ-degree concentrated. ◀

We use Lemma 5 to preprocess the univariate polynomials f_i in an ROABP so that they are r^2-degree concentrated: Suppose $f_1 \in \mathbb{A}[x_1], f_2 \in \mathbb{A}[x_2] \ldots, f_n \in \mathbb{A}[x_n]$ are univariate polynomials of degree at most d. Let $S \subseteq \mathbb{F}$ such that $|S| > ndr^2$. By Lemma 5 and the union bound, there exists $\alpha \in S$ such that $f_i(x_i + a)$ is r^2-degree concentrated for $i \in [n]$.

▶ Remark. Lemma 5 may not hold if $0 < \mathrm{char}(\mathbb{F}) \leq d$. For example, let $a, b \in \mathbb{A}$ be linearly independent over a field $\mathbb{F}$ of characteristic $p > 0$. Let $f(x) = ax^d + b$ where $d \geq p$ is a power of p. Then $f(x+\alpha) = ax^d + \alpha^d a + b$ is not ℓ-degree concentrated for $\alpha \in \mathbb{F}$ and $\ell \leq d$.

3.2 Basis Isolation

A *weight assignment* of the variables $x_1, x_2, \ldots, x_n$ is a map $w : \{x_1, x_2, \ldots, x_n\} \to \mathbb{N}$. Extend w to a map $w : \mathcal{M}(\mathbf{x}) \to \mathbb{N}$ on the set $\mathcal{M}(\mathbf{x})$ of monomials by $w(\mathbf{x}^{\mathbf{a}}) := \sum_{i=1}^{n} w(x_i)a_i$ for $\mathbf{x}^{\mathbf{a}} = \prod_{i=1}^{n} x_i^{a_i} \in \mathcal{M}(\mathbf{x})$.

One basic tool we need is the following explicit construction of weight assignments that separate polynomially many monomials.

▶ **Lemma 6** ([1, Lemma 4, restated])**.** *For* $n, s, \ell \in \mathbb{N}^+$ *and* $0 < \epsilon < 1$, *there exist weight assignments* $w_1, w_2, \ldots, w_N : \{x_1, x_2, \ldots, x_n\} \to [N \log N]$, *where* $N = \mathrm{poly}(n, s, \log \ell, \epsilon^{-1})$, *such that for any* s *monomials* $m_1, m_2, \ldots, m_s \in \mathcal{M}(\mathbf{x})$ *of individual degree less than* ℓ, *all but at most* ϵ*-fraction of* w_i *among* $w_1, w_2, \ldots, w_N$ *separate these monomials, i.e.,* $w_i(m_j) \neq w_i(m_{j'})$ *for* $j, j' \in [s]$ *with* $m_j \neq m_{j'}$. *The weight assignments* $w_1, w_2, \ldots, w_N$ *can be computed in time polynomial in* N.

We are interested in weight assignments that have the property of *basis isolation*, introduced in [1].

▶ **Definition 7** (basis isolating weight assignment [1])**.** *For a polynomial* $f \in \mathbb{A}[\mathbf{x}]$, *we say* $w : \{x_1, x_2, \ldots, x_n\} \to \mathbb{N}$ *is a* basis isolating weight assignment *for* f *if there exists a set* $S \subseteq \mathcal{M}(\mathbf{x})$ *of monomials whose coefficients in* f *form a basis of* $\mathrm{span}(f)$, *such that*

1. $w(m) \neq w(m')$ *for distinct* $m, m' \in S$, *and*
2. $\mathrm{coef}_f(m) \in \mathrm{span}\{\mathrm{coef}_f(m') : m' \in S,\ w(m') < w(m)\}$ *for* $m \in \mathcal{M}(\mathbf{x}) \setminus S$.

The following lemma states that, if w is a basis isolating weight assignment, then the variable substitution map $x_i \mapsto y^{w(x_i)}$ preserves the nonzeroness of polynomials. This makes basis isolating weight assignments a very useful tool for PIT.

▶ **Lemma 8** ([1, Lemma 6]). *Let $f(\mathbf{x}) \in \mathbb{A}[\mathbf{x}]$, $\beta, \gamma \in \mathbb{F}^r$, and $g(\mathbf{x}) = \beta^\top f(\mathbf{x})\gamma \in \mathbb{F}[\mathbf{x}]$. Suppose $w : \{x_1, x_2, \ldots, x_n\} \to \mathbb{N}$ is a basis isolating weight assignment for $f \in \mathbb{A}[\mathbf{x}]$. Then $g(\mathbf{x}) = 0$ iff $g(y^{w(x_1)}, y^{w(x_2)}, \ldots, y^{w(x_n)}) = 0$.*

Explicit Construction. We use the following explicit construction of basis isolating weight assignments for ROABPs, which is a k-ary generalization of the one in [1].

Let $n, \ell \in \mathbb{N}^+$, $k \in \{2, \ldots n\}$ and $\epsilon \in (0, 1)$ where n is a power of k. Let $u = \log n / \log k \in \mathbb{N}$. Let $N = \text{poly}(n, s, \log \ell, \epsilon^{-1})$ and $w_1, w_2, \ldots, w_N$ be as in Lemma 6 with respect to the parameters n, s, ℓ, ϵ, where $s = \max\{\ell, r^{2k}\}$. Let $h = n\ell N \log N$. For $\mathbf{t} = (t_1, t_2, \ldots, t_u) \in [N]^u$, define the weight assignment $w_{\mathbf{t}} : \{x_1, x_2, \ldots, x_n\} \to [N \log N h^u]$ by

$$w_{\mathbf{t}}(x_i) = \sum_{j=1}^{u} w_{t_j}(x_i) h^{u-j}.$$

So $w_{\mathbf{t}}$ is a linear combination of $w_{t_1}, w_{t_2}, \ldots, w_{t_u}$, where w_{t_j} is multiplied by h^{u-j} for $j \in [u]$. If $u = 0$ (i.e., $n = 1$), define $w_{\mathbf{t}}(x_1) = 1$ instead for the unique element $\mathbf{t} \in [N]^u$.

▶ **Lemma 9.** *Let $\pi : [n] \to [n]$ be a permutation. Let $f = \prod_{i=1}^{n} f_i$ where $f_i \in \mathbb{A}[x_{\pi(i)}]$ is ℓ-degree concentrated for $i \in [n]$. Then for all but at most ϵ'-fraction of $\mathbf{t} \in [N]^u$, $w_{\mathbf{t}}$ is a basis isolating weight assignment for f, where $\epsilon' = \frac{(n-1)\epsilon}{k-1}$.*

Proof. We prove the lemma for the case $(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = (x_1, x_2, \ldots, x_n)$. The same proof works for arbitrary variable orders since the monomial separation property of w_i as asserted in Lemma 6 is closed under any permutation of the variables $x_1, x_2, \ldots, x_n$.

The proof is done by induction on $u = \log n / \log k$.

Base case: Suppose $u = 0$, i.e., $n = 1$. We want to prove that the weight assignment $w_{\mathbf{t}}$ defined by $w_{\mathbf{t}}(x_1) = 1$ is basis isolating for $f = f_1$. Choose the set of monomials $S \subseteq \mathbb{F}[x_1]$ in the following greedy way: Start with $S = \emptyset$ and enumerate $i = 0, 1, 2 \ldots$. For each i, add x^i to S whenever $\text{coef}_{f_1}(x_i) \notin \text{span}\{\text{coef}_{f_1}(m) : m \in S\}$. Continue this process until $\text{span}\{\text{coef}_{f_1}(m) : m \in S\} = \text{span}(f)$. Then $w_{\mathbf{t}}$ and S satisfy Definition 7. So $w_{\mathbf{t}}$ is a basis isolating weight assignment for $f = f_1$.

Inductive step: Suppose $u > 0$, and assume the claim holds for $u' = u-1$. Let $n' = n/k = k^{u'}$. Divide $[n]$ into k blocks $B_1, B_2, \ldots, B_k$, where $B_i = \{(i-1)n'+1, (i-1)n'+2, \ldots, in'\}$. For $i \in [k]$, let $f^{(i)} = \prod_{j \in B_i} f_j = \prod_{j=(i-1)n'+1}^{in'} f_j$. So $f = \prod_{i=1}^{k} f^{(i)}$.

Let $\epsilon'' = \frac{(n'-1)\epsilon}{k-1}$. By the induction hypothesis and the union bound, for all but at most $k\epsilon''$-fraction of $\mathbf{t} = (t_1, t_2, \ldots, t_{u-1}) \in [N]^{u-1}$, $w_{\mathbf{t}}$ is a basis isolating weight assignment for $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$. Fix such $\mathbf{t}$. For $i \in [k]$, let $S_i \subseteq \mathcal{M}(x_j : j \in B_i)$ be a set of monomials in the variables x_j with $j \in B_i$ such that $w_{\mathbf{t}}$, S_i and $f^{(i)}$ satisfy the conditions in Definition 7. Then $|S_i| \leq \dim_{\mathbb{F}} \text{span}(f^{(i)}) \leq \dim_{\mathbb{F}} \mathbb{A} = r^2$ for $i \in [k]$.

▷ Claim 10. The monomials in $S_1, S_2, \ldots, S_k$ have individual degree less than ℓ.

Proof of Claim 10. Assume to the contrary that some S_i contains a monomial m whose degree in some variable x_j is $d \geq \ell$. Write $m = x_j^d \bar{m}$ where $\bar{m}$ does not depend on x_j. As f_j is ℓ-degree concentrated, we have $\text{coef}_{f_j}(x_j^d) \in \text{span}\{\text{coef}_{f_j}(x_j^a) : 0 \leq a < \ell\}$. Using the fact $f^{(i)} = \prod_{j \in B_i} f_j$ and $f_j \in \mathbb{A}[x_j]$ for $j \in S_i$, we see

$$\text{coef}_{f^{(i)}}(m) \in \text{span}\{\text{coef}_{f^{(i)}}(x_j^a \bar{m}) : 0 \leq a < \ell\} \subseteq \text{span}\{\text{coef}_{f^{(i)}}(m') : w_{\mathbf{t}}(m') < w_{\mathbf{t}}(m)\}.$$

But, from (2) of Definition 7, we know that for any $m' \in \mathcal{M}(x_j : j \in B_i) \setminus S_i$,

$$\text{coef}_{f^{(i)}}(m') \in \text{span}\{\text{coef}_{f^{(i)}}(m'') : m'' \in S_i,\ w_{\mathbf{t}}(m'') < w_{\mathbf{t}}(m')\}.$$

From the above two containments we get that

$$\text{coef}_{f^{(i)}}(m) \in \text{span}\{\text{coef}_{f^{(i)}}(m'') : m'' \in S_i,\ w_{\mathbf{t}}(m'') < w_{\mathbf{t}}(m)\}.$$

This contradicts the fact that the coefficients of the monomials in S_i form a basis of $\text{span}(f_i)$ (Definition 7). ◁

Let $T := \{\prod_{i=1}^{k} m_i : m_i \in S_i \text{ for } i \in [k]\}$. Then $\text{span}\{\text{coef}_f(m) : m \in T\} = \text{span}(f)$. Note $|T| = \prod_{i=1}^{k} |S_i| \le r^{2k} \le s$, and T consists of monomials of individual degree less than ℓ. By Lemma 6, for all but at most ϵ-fraction of $t_u \in [N]$, w_{t_u} separates the monomials in T. Fix such t_u and let $\mathbf{t}' = (t_1, t_2, \ldots, t_u) = (\mathbf{t}, t_u)$.

For $m \in T$, as the individual degree of m is less than ℓ, we have $0 \le w_{t_u}(m) < n\ell N \log N = h$. By definition, $w_{\mathbf{t}'}(m) = w_{t_u}(m)$ if $u = 1$ and $w_{\mathbf{t}'}(m) = w_{\mathbf{t}}(m)h + w_{t_u}(m)$ if $u > 1$. In either case, we have $w_{\mathbf{t}'}(m) \neq w_{\mathbf{t}'}(m')$ whenever $w_{t_u}(m) \neq w_{t_u}(m')$ for $m, m' \in T$. Therefore, the weight assignment $w_{\mathbf{t}'}$ also separates the monomials in T.

Next, we choose a subset $S \subseteq T$ of monomials such that $w_{\mathbf{t}'}$, S, and f satisfy the conditions in Definition 7. Initially, let $S = \emptyset$. Choose $m \in T$ with the minimum weight $w_{\mathbf{t}'}(m)$ such that $\text{coef}_f(m) \notin \text{span}\{\text{coef}_f(m') : m' \in S\}$, and add m to S. Note m is unique as $w_{\mathbf{t}'}$ separates the monomials in T. Repeat this step until $\text{span}\{\text{coef}_f(m) : m \in S\}$ equals $\text{span}\{\text{coef}_f(m) : m \in T\} = \text{span}(f)$.

We check that $w_{\mathbf{t}'}$, S and f satisfy the conditions in Definition 7. The set $\{\text{coef}_f(m) : m \in S\}$ is a basis of $\text{span}(f)$ by our choice of S. As $w_{\mathbf{t}'}$ separates the monomials in $T \supseteq S$, Condition (1) of Definition 7 holds. We now prove that Condition (2) also holds.

▷ Claim 11. $\text{coef}_f(m) \in \text{span}\{\text{coef}_f(m') : m' \in S,\ w_{\mathbf{t}'}(m') < w_{\mathbf{t}'}(m)\}$ for $m \in \mathcal{M}(\mathbf{x}) \setminus S$.

Proof of Claim 11. We prove the claim by induction on $w := w_{\mathbf{t}'}(m)$. The claim is vacuously true for $w < 0$ (since this is impossible). Now suppose $w \ge 0$ and the claim holds for $w' < w$. If $m \in T$, the claim holds by our choice of S. So assume $m \notin T$. Write $m = \prod_{i=1}^{k} m_i$ where m_i is a monomial in the variables in B_i. As $m \notin T$, there exists $i \in [k]$ such that $m_i \notin S_i$. Assume $i = 1$ (the other cases are similar). By the choice of S_1, we have

$$\begin{aligned}\text{coef}_{f^{(1)}}(m_1) &\in \text{span}\{\text{coef}_{f^{(1)}}(m_1') : m_1' \in S_1,\ w_{\mathbf{t}}(m_1') < w_{\mathbf{t}}(m_1)\} \\ &\subseteq \text{span}\{\text{coef}_{f^{(1)}}(m_1') : m_1' \in S_1,\ w_{\mathbf{t}'}(m_1') < w_{\mathbf{t}'}(m_1)\}.\end{aligned}$$

where the second step holds since $w_{t_u}(m_1') < n\ell N \log N = h$ for $m_1' \in S_1$, which in turn holds by Claim 10. Therefore

$$\begin{aligned}\text{coef}_f(m) &\in \text{span}\{\text{coef}_f(m_1' m_2 \cdots m_k) : m_1' \in S_1,\ w_{\mathbf{t}'}(m_1') < w_{\mathbf{t}'}(m_1)\} \\ &\subseteq \text{span}\{\text{coef}_f(m') : m' \in \mathcal{M}(\mathbf{x}), w_{\mathbf{t}'}(m') < w_{\mathbf{t}'}(m)\}.\end{aligned}$$

Consider a monomial $m' \in \mathcal{M}(\mathbf{x})$ satisfying $w_{\mathbf{t}'}(m') < w_{\mathbf{t}'}(m)$. By the induction hypothesis, either $m' \in S$, or $\text{coef}_f(m')$ is in the span of the coefficients of those monomials in S with weight strictly less than $w_{\mathbf{t}'}(m') < w_{\mathbf{t}'}(m)$. It follows that $\text{coef}_f(m) \in \text{span}\{\text{coef}_f(m') : m' \in S, w_{\mathbf{t}'}(m') < w_{\mathbf{t}'}(m)\}$. ◁

By the union bound, for all but at most ϵ'-fraction of $\mathbf{t}' = (t_1, \ldots, t_u) \in [N]^u$, where $\epsilon' = k\epsilon'' + \epsilon = \frac{(n-1)\epsilon}{k-1}$, $w_{\mathbf{t}'}$ is a basis isolating weight assignment for f. This completes the proof for the inductive step. ◀

Let $\epsilon = 1/n$. Then the maximum values of the weight assignments $w_{\mathbf{t}}$ constructed above are polynomial in h^u with $h = \mathrm{poly}(n, \ell, r^k)$ and $u = \log n / \log k$, which suggests that we should choose $k = \Theta(\log(n\ell)/\log r)$. However, as $k \in \{2, \ldots, n\}$, we have to choose $k = 2$ (resp. $k = n$) when $\log(n\ell)/\log r$ is subconstant (resp. superlinear in n). This yields the following theorem.

▶ **Theorem 12.** *Let $\mathcal{C}$ be the family of polynomials $f = \beta^\top f_1 f_2 \cdots f_n \gamma$ computed by ROABPs of length n, width r and individual degree d in an unknown order, where each f_i is ℓ-degree concentrated. Then there exists an explicit hitting-set for $\mathcal{C}$ of size polynomial in $M_0(n, r, d, \ell)$, where*

$$M_0(n,r,d,\ell) := \begin{cases} (nr)^{\log n} d & n\ell \le r^2, \\ (n\ell)^{\frac{\log n}{\log\log(n\ell) - \log\log r}} d & r^2 < n\ell < r^n, \\ n\ell d & n\ell \ge r^n. \end{cases}$$

Proof. Choose

$$k = \begin{cases} 2 & n\ell \le r^2, \\ \log(n\ell)/\log r & r^2 < n\ell < r^n, \\ n & n\ell \ge r^n. \end{cases}$$

By adding dummy variables, we may assume n is a power of k. Let $\epsilon = 1/n$. Construct the weight assignment $w_{\mathbf{t}} : \{x_1, x_2, \ldots, x_n\} \to [N \log N h^u]$ for $\mathbf{t} \in [N]^u$ as above, where $N = \mathrm{poly}(n, s, \log \ell, \epsilon^{-1})$, $s = \max\{\ell, r^{2k}\}$, $h = n\ell N \log N$, and $u = \log n / \log k$.

Consider $0 \neq f = \beta^\top f_1 f_2 \cdots f_n \gamma \in \mathcal{C}$. By Lemma 9, there exists $\mathbf{t} \in [N]^u$ such that $w_{\mathbf{t}}$ is a basis isolating weight assignment for $f_1 f_2 \cdots f_n \in \mathbb{A}[\mathbf{x}]$, which implies that $g_{w_{\mathbf{t}}}(y) := f(y^{w_{\mathbf{t}}(x_1)}, \ldots, y^{w_{\mathbf{t}}(x_n)}) \neq 0$ by Lemma 8. As $g_{w_{\mathbf{t}}}(y)$ is univariate, any subset of $\mathbb{F}$ of size $\deg(g_{w_{\mathbf{t}}}) + 1 \le N \log N h^u n d + 1$ is a hitting-set for $g_{w_{\mathbf{t}}}$. Enumerating all $\mathbf{t} \in [N]^u$, we obtain an explicit hitting-set for $\mathcal{C}$ of size at most $N^u(N \log N h^u n d + 1)$, which is polynomial in $M_0(n, r, d, \ell)$. ◀

Theorem 1 follows easily from Theorem 12.

Proof of Theorem 1. Note degree-d polynomials are trivially $(d+1)$-degree concentrated. The second part of Theorem 1 (the claim for arbitrary characteristic) then follows from Theorem 12 with $\ell = d + 1$.

Moreover, when $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d$, we may preprocess the polynomials f_i using Lemma 5 so that they are r^2-degree concentrated. The first part of Theorem 1 then follows from Theorem 12 with $\ell = r^2$. ◀

3.3 Sum of Several ROABPs

Using the reduction in [3], we may extend Theorem 1 to the model of sum of several ROABPs and prove Theorem 2. Here we only sketch the proof as it is the same as the proof in [3] except for some small adjustments.

Proof sketch of Theorem 2. Choose a function $M^*(n, r, d) \ge \mathrm{poly}(n, r, d)$ such that we have explicit hitting-sets of size at most $M^*(n, r, d)$ for the family of polynomials computed by ROABPs of length n, width r and individual degree d in an unknown order. By Theorem 1, we may choose $M^*(n, r, d)$ to be polynomial in $M(n, r, d)$ when $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d$ and polynomial in $M'(n, r, d)$ in arbitrary characteristic.

Fix n and d. It was shown in the proof of [3, Lemma 14] (and the proof of [3, Lemma 12]) that for $c \geq 1$ and $r \geq 2$, one can explicitly construct a set $\mathcal{S}$ of ring homomorphisms $\Psi : \mathbb{F}[x_1, x_2, \ldots, x_n] \to \mathbb{F}[t]$ satisfying the following properties ($\mathcal{C}$ is the class of sum of c ROABPs):

- If $0 \neq f \in \mathcal{C}$, there exists $\Psi \in \mathcal{S}$ such that $\Psi(f) \neq 0$.
- For $f \in \mathcal{C}$ and $\Psi \in \mathcal{S}$, the degree of $\Psi(f)$ is at most $S(c, r)$, where $S(1, r) \leq M^*(n, r, d)$ and

$$S(c, r) \leq \text{poly}(M^*(n, r, d)) \cdot S(c - 1, 2r^3) \tag{1}$$

  for $c \geq 2$.
- The time complexity of computing $\mathcal{S}$ is at most $T(c, r)$, where $T(1, r) \leq \text{poly}(M^*(n, r, d))$ and

$$T(c, r) \leq n2^n \cdot \text{poly}(M^*(n, r, d)) \cdot T(c - 1, 2r^3) \tag{2}$$

  for $c \geq 2$. In particular, the size of $\mathcal{S}$ is bounded by $T(c, r)$.

Solving the recursive relations (1) and (2) above gives $S(c, r) \leq \text{poly}(M^*(n, (2r)^{3^c}, d)^c)$ and $T(c, r) \leq \text{poly}(2^{cn}, M^*(n, (2r)^{3^c}, d)^c)$.

For $f \in \mathcal{C}$ and $\Psi \in \mathcal{S}$, any subset of $\mathbb{F}$ of size $S(c, r)+1$ is a hitting-set for $\Psi(f)$ since $\Psi(f)$ is a univariate polynomial of degree at most $S(c, r)$. Enumerating all possible $\Psi \in \mathcal{S}$, we obtain an explicit hitting-set for $\mathcal{C}$ of size at most $T(c, r)(S(c, r) + 1)$, which is polynomial in $2^{cn} \cdot M(n, (2r)^{3^c}, d)^c$ when $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d$ and polynomial in $2^{cn} \cdot M'(n, (2r)^{3^c}, d)^c$ in arbitrary characteristic. ◀

4 Hitting-Sets for Any-Order ROABPs

In this section, we prove Theorem 3 by giving an explicit construction of hitting-sets for any-order ROABPs.

4.1 Low-Support Concentration

Following [8, 10], we first achieve low-support concentration by shifting the variables. The basic tool is the following lemma.

▶ **Lemma 13** ([11, Lemma 5.2]). *Suppose $w : \mathbf{x} \to \mathbb{N}$ is a basis isolating weight assignment for $f = \prod_{i=1}^{n} f_i \in \mathbb{A}[\mathbf{x}]$. Then $f(x_1 + y^{w(x_1)}, x_2 + y^{w(x_2)}, \ldots, x_n + y^{w(x_n)})$ is $\lceil \log(r^2 + 1) \rceil$-support concentrated over $\mathbb{F}(y)$.*

The next lemma states that low-support concentration is a "local" property for any-order ROABPs.

▶ **Lemma 14** ([2, 8, 10]). *Let $\ell < n$. Let $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in \mathbb{K}^n$ where $\mathbb{K}$ is an extension field of $\mathbb{F}$. Suppose for any distinct $i_1, i_2 \ldots, i_\ell \in [n]$ and $f_1 \in \mathbb{A}[x_{i_1}], f_2 \in \mathbb{A}[x_{i_2}], \ldots, f_\ell \in \mathbb{A}[x_{i_\ell}]$ of degree at most d, the product $f_1(x_{i_1} + s_{i_1}) f_2(x_{i_2} + s_{i_2}) \cdots f_\ell(x_{i_\ell} + s_{i_\ell})$ is ℓ-support concentrated over $\mathbb{K}$. Then for $f(\mathbf{x}) \in \mathbb{A}[\mathbf{x}]$ computed by ROABPs of length n, width r and individual degree d in any order, $f(\mathbf{x} + \mathbf{s})$ is ℓ-support concentrated over $\mathbb{K}$.*

Explicit Construction. Let $\mathbb{K} = \mathbb{F}(y, z, t)$, where y, z and t are indeterminates. We construct $\mathbf{s} \in \mathbb{F}[y, z, t]^n$ such that the shift $\mathbf{x} \mapsto \mathbf{x} + \mathbf{s}$ achieves low-support concentration over $\mathbb{K}$ for polynomials computed by any-order ROABPs. The construction is as follows.

- Let $\ell = r^2$ if $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d$. Otherwise let $\ell = d + 1$.
- Choose sufficiently large $\bar{n} = \mathrm{poly}(\log r)$ and let $\mathcal{H} = \{h : [n] \to [\bar{n}]\}$ be an explicit family of hash functions of size $\mathrm{poly}(n, \log r)$ such that for any $T \subseteq [n]$ of size $\lceil \log(r^2+1) \rceil$, there exists $h \in \mathcal{H}$ that maps T injectively to $[\bar{n}]$. Such an explicit family $\mathcal{H}$ can be constructed using pairwise independence [5].
- Using Lemma 9, construct a set $\mathcal{S}$ of weight assignments $w : \{u_1, u_2, \ldots, u_{\bar{n}}\} \to \mathbb{N}$ of the variables $u_1, u_2, \ldots, u_{\bar{n}}$ such that for any permutation $\pi : [\bar{n}] \to [\bar{n}]$ and polynomials $f_1 \in \mathbb{A}[u_1], f_2 \in \mathbb{A}[u_2], \ldots, f_{\bar{n}} \in \mathbb{A}[u_{\bar{n}}]$ of degree at most d that are ℓ-degree concentrated, there exists a basis isolating weight assignment in $\mathcal{S}$ for $\prod_{i=1}^{\bar{n}} f_{\pi(i)}$.
- Fix an injective map $\psi : \mathcal{S} \times \mathcal{H} \to \mathbb{F}$. For $(w, h) \in \mathcal{S} \times \mathcal{H}$, construct the polynomial $p_{w,h}(z) \in \mathbb{F}[z]$ of degree $|\mathcal{S} \times \mathcal{H}| - 1$ by interpolation such that for $(w', h') \in \mathcal{S} \times \mathcal{H}$,

$$p_{w,h}(\psi(w', h')) = \begin{cases} 1 & (w', h') = (w, h) \\ 0 & (w', h') \neq (w, h). \end{cases}$$

- Define $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in \mathbb{F}[y, z, t]^n$ by $s_i(y, z, t) = t + \sum_{(w,h) \in \mathcal{S} \times \mathcal{H}} y^{w(u_{h(i)})} p_{w,h}(z)$ for $i \in [n]$. So $s_i(y, \psi(w, h), t) = t + y^{w(u_{h(i)})}$ for $i \in [n]$ and $(w, h) \in \mathcal{S} \times \mathcal{H}$.

The main difference between the above construction and the one in [10] is the use of hash functions, which has the effect of reducing the number of variables from n to $\bar{n} = \mathrm{poly}(\log r)$ in the analysis.

▶ **Lemma 15.** *Suppose $f \in \mathbb{A}[\mathbf{x}]$ is computed by ROABPs of length n, width r and individual degree d in any order. Then $f(\mathbf{x} + \mathbf{s})$ is $\lceil \log(r^2+1) \rceil$-support concentrated over $\mathbb{K} = \mathbb{F}(y, z, t)$.*

Proof. The lemma is trivial if $n < \lceil \log(r^2 + 1) \rceil$. So assume $n \geq \lceil \log(r^2 + 1) \rceil$. Let $n' = \lceil \log(r^2+1) \rceil$. Consider distinct $i_1, i_2 \ldots, i_{n'} \in [n]$ and $f_1 \in \mathbb{A}[x_{i_1}], f_2 \in \mathbb{A}[x_{i_2}], \ldots, f_{n'} \in \mathbb{A}[x_{i_{n'}}]$ of degree at most d. By Lemma 14, it suffices to prove that

$$g := \prod_{j=1}^{n'} f_j(x_{i_j} + s_{i_j}) \in (\mathbb{A}[y, z, t])[\mathbf{x}] \subseteq (\mathbb{A} \otimes_{\mathbb{F}} \mathbb{K})[\mathbf{x}]$$

is n'-support concentrated over $\mathbb{K}$.

Fix $h \in \mathcal{H}$ such that h maps $\{i_1, \ldots, i_{n'}\}$ injectively to $[\bar{n}]$. Note that there exists $\alpha \in \mathbb{F}$ such that for $j \in [n']$, $f_j(x_{i_j} + \alpha)$ is ℓ-degree concentrated: If $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d$, then $\ell = r^2$ and this claim follows from Lemma 5. Otherwise, $\ell = d + 1$ and this claim holds trivially. Fix such α.

Let $f^*(u_1, u_2, \ldots, u_{\bar{n}}) := \prod_{j=1}^{n'} f_j(u_{h(i_j)} + \alpha) \in \mathbb{A}[u_1, u_2, \ldots, u_{\bar{n}}]$. By the choice of $\mathcal{S}$, there exists a basis isolating weight assignment $w : \{u_1, u_2, \ldots, u_{\bar{n}}\} \to \mathbb{N}$ in $\mathcal{S}$ for f^*. Fix such w. By Lemma 13, $f^*(u_1 + y^{w(u_1)}, \ldots, u_{\bar{n}} + y^{w(u_{\bar{n}})}) = \prod_{j=1}^{n'} f_j(u_{h(i_j)} + y^{w(u_{h(i_j)})} + \alpha)$ is n'-support concentrated over $\mathbb{F}(y)$. Substituting $u_{h(i_j)}$ with x_{i_j} for $j \in [n']$, we see that

$$g^* := \prod_{j=1}^{n'} f_j(x_{i_j} + y^{w(u_{h(i_j)})} + \alpha) \in (\mathbb{A}[y])[\mathbf{x}] \subseteq (\mathbb{A} \otimes_{\mathbb{F}} \mathbb{F}(y))[\mathbf{x}]$$

is n'-support concentrated over $\mathbb{F}(y)$.

Let $g_0 = \prod_{j=1}^{n'} f_j(x_{i_j})$. As $g_0(\mathbf{x} + \alpha) = g^*|_{y=0}$, we have $\mathrm{span}_{\mathbb{F}(y)}(g_0) = \mathrm{span}_{\mathbb{F}(y)}(g_0(\mathbf{x} + \alpha)) \subseteq \mathrm{span}_{\mathbb{F}(y)}(g^*)$. On the other hand, note the coefficients of g^* can be written as linear combinations of those of g_0 over $\mathbb{F}(y)$. So $\mathrm{span}_{\mathbb{F}(y)}(g^*) \subseteq \mathrm{span}_{\mathbb{F}(y)}(g_0)$. It follows that $\mathrm{span}_{\mathbb{F}(y)}(g^*) = \mathrm{span}_{\mathbb{F}(y)}(g_0)$. Also note $\mathrm{span}_{\mathbb{K}}(g) = \mathrm{span}_{\mathbb{K}}(g_0)$ since $g(\mathbf{x}) = g_0(\mathbf{x} + \mathbf{s})$.

Let $D := \dim_{\mathbb{F}}(\mathrm{span}(g_0))$. We have $D = \dim_{\mathbb{F}(y)}(\mathrm{span}_{\mathbb{F}(y)}(g_0)) = \dim_{\mathbb{F}(y)}(\mathrm{span}_{\mathbb{F}(y)}(g^*))$ and $D = \dim_{\mathbb{K}}(\mathrm{span}_{\mathbb{K}}(g_0)) = \dim_{\mathbb{K}}(\mathrm{span}_{\mathbb{K}}(g))$. As g^* is n'-support concentrated over $\mathbb{F}(y)$, there exist $m_1, m_2, \ldots, m_D \in \mathcal{M}(\mathbf{x})$ of support size less than n' such that the coefficients $\mathrm{coef}_{g^*}(m_1), \mathrm{coef}_{g^*}(m_2), \ldots, \mathrm{coef}_{g^*}(m_D)$ are linearly independent. Also note $g^* = g|_{z=\psi(w,h),t=\alpha}$, which implies $\mathrm{coef}_{g^*}(m_i) = \mathrm{coef}_g(m_i)|_{z=\psi(w,h),t=\alpha}$ for $i \in [D]$. Therefore, the coefficients $\mathrm{coef}_g(m_1), \mathrm{coef}_g(m_2), \ldots, \mathrm{coef}_g(m_D)$ are also linearly independent. It follows that g is n'-support concentrated over $\mathbb{K}$, as desired. ◀

▶ **Theorem 16.** *Let $\mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{F}[y,z,t]^n$ be as above. Let $T \subseteq \mathbb{F}$ be a large enough set with*

$$|T| = \begin{cases} \mathrm{poly}(n, r^{\log\log r}, d) & \mathrm{char}(\mathbb{F}) = 0 \text{ or } \mathrm{char}(\mathbb{F}) > d \\ \mathrm{poly}(n, r^{\log\log r}, d^{1+\frac{\log\log r}{\max\{1, \log\log d - \log\log r\}}}) & \text{otherwise.} \end{cases}$$

Suppose $f \in \mathbb{A}[\mathbf{x}]$ is computed by ROABPs of length n, width r and individual degree d in any order. Then there exists $(a,b,c) \in T^3$ such that $f(\mathbf{x}+\mathbf{s}(a,b,c)) \in \mathbb{A}[\mathbf{x}]$ is $\lceil \log(r^2+1) \rceil$-support concentrated.

Proof. We know $|\mathcal{H}| = \mathrm{poly}(n, \log r)$. If $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d$, then $|\mathcal{S}|$ and the maximum value of every $w \in \mathcal{S}$ are bounded by $\mathrm{poly}(M(\bar{n}, r, d)) = \mathrm{poly}(r^{\log\log r}, d)$. Otherwise they are bounded by $\mathrm{poly}(M'(\bar{n}, r, d)) \leq \mathrm{poly}(r^{\log\log r}, d^{1+\frac{\log\log r}{\max\{1, \log\log d - \log\log r\}}})$. The degree of each $s_i \in \mathbb{F}[y,z,t]$ is polynomial in $|\mathcal{S}|$, $|\mathcal{H}|$ and $\max\{w(u_i) : w \in S, i \in [\bar{n}]\}$.

Let $D = \dim_{\mathbb{F}}(\mathrm{span}(f))$. By Lemma 15, $f(\mathbf{x}+\mathbf{s})$ is $\lceil \log(r^2+1) \rceil$-support concentrated over $\mathbb{K}$. So there exist monomials $m_1, m_2 \ldots, m_D \in \mathcal{M}(\mathbf{x})$ of support size less than $\lceil \log(r^2+1) \rceil$ and individual degree at most d such that $\mathrm{coef}_{f(\mathbf{x}+\mathbf{s})}(m_1), \mathrm{coef}_{f(\mathbf{x}+\mathbf{s})}(m_2), \ldots, \mathrm{coef}_{f(\mathbf{x}+\mathbf{s})}(m_D)$ are linearly independen over $\mathbb{K}$. Therefore, the matrix formed by these coefficients (viewed as vectors over $\mathbb{K}$) has a nonzero $D \times D$ minor $g \in \mathbb{K}$. Note g is a polynomial in y, z, t whose degree is polynomial in n, r, d and the degrees of the polynomials $s_i \in \mathbb{F}[y,z,t]$. By the Schwartz-Zippel-DeMillo-Lipton lemma, for large enough T whose size is as in Theorem 16, there exists $(a,b,c) \in T^3$ such that $g(a,b,c) \neq 0$. For such (a,b,c), the coefficients $\mathrm{coef}_{f(\mathbf{x}+\mathbf{s}(a,b,c))}(m_1), \mathrm{coef}_{f(\mathbf{x}+\mathbf{s}(a,b,c))}(m_2), \ldots, \mathrm{coef}_{f(\mathbf{x}+\mathbf{s}(a,b,c))}(m_D)$ span the coefficient span of f, which implies that $f(\mathbf{x}+\mathbf{s}(a,b,c))$ is $\lceil \log(r^2+1) \rceil$-support concentrated. ◀

4.2 Converting Low-Support Concentrated Any-Order ROABPs into Short ROABPs

Our next step follows that in [8, 10], which converts any-order ROABPs with low-support concentration into short ROABPs. In particular, we need the following lemma proved in [8].

▶ **Lemma 17** ([8, Lemma 7.6, restated]). *Let $\mathcal{C}$ be the set of polynomials $f \in \mathbb{F}[\mathbf{x}]$ computed by ROABPs of length n, width r and individual degree d in any order such that f has a monomial m with a nonzero coefficient and $|\mathrm{supp}(m)| < \ell$. Then for some $n' = O(\ell^2)$, there exists an explicit set $S \subseteq (\mathbb{F}[y_1, y_2, \ldots, y_{n'}])^n$ of size $\mathrm{poly}(n,r,d)$ satisfying the following condition: For any $f \in \mathcal{C}$, there exists $(\phi_1, \phi_2, \ldots, \phi_n) \in S$ such that $f(\phi_1, \phi_2, \ldots, \phi_n) \in \mathbb{F}[y_1, y_2, \ldots, y_{n'}]$ is a nonzero polynomial computed by ROABPs of length n', width r and individual degree $n^4(d+1)^2$ in any order.*

Now we are ready to prove Theorem 3.

Proof of Theorem 3. Consider $0 \neq f \in \mathcal{C}$. Regard $f \in \mathbb{F}[\mathbf{x}]$ as an element of $\mathbb{A}[\mathbf{x}] \cong M_{r\times r}(\mathbb{F}[\mathbf{x}])$ such that the $(1,1)$-th entry of the corresponding matrix is f and the other entries are zero. Then f, regarded as an element of $\mathbb{A}[\mathbf{x}]$ this way, is also computed by ROABPs of length n, width r and individual degree d in any order. Let $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in \mathbb{F}[y,z,t]^n$

and $T \subseteq \mathbb{F}$ be as in Theorem 16. By Theorem 16, there exists $(a,b,c) \in T^3$ such that $f^*(\mathbf{x}) := f(\mathbf{x}+\mathbf{s}(a,b,c))$ is $\lceil \log(r^2+1) \rceil$-concentrated. As $f \neq 0$, this implies that $f^*(\mathbf{x})$ has a monomial m with a nonzero coefficient and $|\mathrm{supp}(m)| < \lceil \log(r^2+1) \rceil$.

Let $S \subseteq (\mathbb{F}[y_1, y_2, \ldots, y_{n'}])^n$ be the set in Lemma 17 with $\ell = \lceil \log(r^2+1) \rceil$. By Lemma 17, there exists $\phi = (\phi_1, \phi_2, \ldots, \phi_n) \in S$ such that $f^*(\phi_1, \phi_2, \ldots, \phi_n)$ is a nonzero polynomial computed by ROABPs of length n', width r and individual degree $n^4(d+1)^2$, where $n' = O((\log r)^2)$.

Finally, use Theorem 1 to construct an explicit hitting-set $\mathcal{H}$ for

$$f^*(\phi_1, \phi_2, \ldots, \phi_n) = f(\phi_1 + s_1(a,b,c), \phi_2 + s_2(a,b,c), \ldots, \phi_n + s_n(a,b,c)).$$

Then $\mathcal{H}_{a,b,c,\phi} := \{(\phi_1(\alpha) + s_1(a,b,c), \phi_2(\alpha) + s_2(a,b,c), \ldots, \phi_n(\alpha) + s_n(a,b,c)) : \alpha \in \mathcal{H}\}$ is a hitting-set for f. We do not know the correct $(a,b,c) \in T^3$ and $\phi \in S$ but may just enumerate all the possible choices and then take the union of $\mathcal{H}_{a,b,c,\phi}$. When $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > n^4(d+1)^2$, the size of the final hitting-set we obtain is polynomial in

$$\begin{aligned} |T|^3 \cdot |S| \cdot M(n', r, n^4(d+1)^2) &= \mathrm{poly}(n, r^{\log\log r}, d) \cdot \mathrm{poly}(n, r, d) \cdot M(n', r, n^4(d+1)^2) \\ &= \mathrm{poly}(n, r^{\log\log r}, d). \end{aligned}$$

In arbitrary characteristic, the size of the final hitting-set is polynomial in

$$\begin{aligned} &|T|^3 \cdot |S| \cdot M'(n', r, n^4(d+1)^2) \\ &= \mathrm{poly}(n, r^{\log\log r}, d^{1+\frac{\log\log r}{\max\{1, \log\log d - \log\log r\}}}) \cdot \mathrm{poly}(n, r, d) \cdot M'(n', r, n^4(d+1)^2) \\ &= \mathrm{poly}(r^{\log\log r}, (nd)^{1+\frac{\log\log r}{\max\{1, \log\log(nd) - \log\log r\}}}). \end{aligned}$$

◀

5 Open Problems

We list some open problems.

- The results we have obtained in positive characteristics are worse than those in characteristic zero, due to the issue that random shift may fail to achieve low-degree concentration in positive characteristics. Is it possible to close the gaps between characteristic zero and characteristic $p > 0$?
- In characteristic $p > 0$, are there explicit hitting-sets of polynomial size for any-order ROABPs of length n, width r and individual degree d when $r, d = 2^{O(\log n / \log\log n)}$? The following issue prevents us from obtaining such a result: In Lemma 17, the substitution map $f \mapsto f(\phi_1, \phi_2, \ldots, \phi_n)$ increases the individual degree from d to $n^4(d+1)^2$. Thus an application of Lemma 17 forces the new individual degree to be at least $\mathrm{poly}(n)$ even if we start with $d = n^{o(1)}$.
- It was shown in [7] that in characteristic zero, explicit hitting-sets of size $\mathrm{poly}(s)$ exist for log-variate diagonal circuits of size s. It is a natural question to ask if this result can be extended to commutative or any-order log-variate ROABPs of width $\mathrm{poly}(s)$ and individual degree $\mathrm{poly}(s)$.

References

1 Manindra Agrawal, Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Hitting-sets for ROABP and sum of set-multilinear circuits. *SIAM Journal on Computing*, 44(3):669–697, 2015. doi:10.1137/140975103.

2 Manindra Agrawal, Chandan Saha, and Nitin Saxena. Quasi-polynomial hitting-set for set-depth-Δ formulas. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC 2013)*, pages 321–330, 2013. doi:10.1145/2488608.2488649.

3 Pranav Bisht and Nitin Saxena. Poly-time blackbox identity testing for sum of log-variate constant-width ROABPs. *Electronic Colloquium on Computational Complexity (ECCC)*, 2020. URL: https://eccc.weizmann.ac.il/report/2020/042.

4 Mark Braverman, Gil Cohen, and Sumegha Garg. Hitting sets with near-optimal error for read-once branching programs. In *Proceedings of the 50th Annual ACM Symposium on Theory of Computing (STOC 2018)*, page 353–362, 2018. doi:10.1145/3188745.3188780.

5 J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979. doi:10.1016/0022-0000(79)90044-8.

6 Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978. doi:10.1016/0020-0190(78)90067-4.

7 Michael A. Forbes, Sumanta Ghosh, and Nitin Saxena. Towards blackbox identity testing of log-variate circuits. In *Proceedings of the 45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, pages 54:1–54:16, 2018. doi:10.4230/LIPIcs.ICALP.2018.54.

8 Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC 2014)*, pages 867–875, 2014. doi:10.1145/2591796.2591816.

9 Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *Proceedings of the 54th Annual Symposium on Foundations of Computer Science (FOCS 2013)*, pages 243–252, 2013. doi:10.1109/FOCS.2013.34.

10 Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Identity testing for constant-width, and any-order, read-once oblivious arithmetic branching programs. *Theory of Computing*, 13(2):1–21, 2017. doi:10.4086/toc.2017.v013a002.

11 Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf. Deterministic identity testing for sum of read-once oblivious arithmetic branching programs. *Computational Complexity*, 26(4):835–880, 2017. doi:10.1007/s00037-016-0141-z.

12 Russell Impagliazzo, Noam Nisan, and Avi Wigderson. Pseudorandomness for network algorithms. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC 1994)*, pages 356–364, 1994. doi:10.1145/195058.195190.

13 Noam Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992. doi:10.1007/BF01305237.

14 Øystein Ore. Über höhere Kongruenzen. *Norsk Mat. Forenings Skrifter Ser. I*, 7(15):27, 1922.

15 Ran Raz and Omer Reingold. On recycling the randomness of states in space bounded computation. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC 1999)*, pages 159–168, 1999. doi:10.1145/301250.301294.

16 Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005. doi:10.1007/s00037-005-0188-8.

17 Nitin Saxena. Diagonal circuit identity testing and lower bounds. In *Proceedings of the 35th International Colloquium on Automata, Languages, and Programming (ICALP 2008)*, pages 60–71, 2008. doi:10.1007/978-3-540-70575-8_6.

18 Nitin Saxena. Progress on polynomial identity testing. *Bulletin of the EATCS*, 99:49–79, 2009.

19 Nitin Saxena. Progress on polynomial identity testing- II. In *Perspectives in Computational Complexity*, volume 26 of *Progress in Computer Science and Applied Logic*, pages 131–146. Springer, 2014. doi:10.1007/978-3-319-05446-9_7.

20 Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980. doi:10.1145/322217.322225.

21 Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010. doi:10.1561/0400000039.

22 Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, 1979. doi:10.1007/3-540-09519-5_73.