Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 62 (2021)

Improved Hitting Set for Orbit of ROABPs

Vishwas Bhargava* Sumanta Ghosh†

Abstract

The orbit of an n-variate polynomial $f(\mathbf{x})$ over a field $\mathbb{F}$ is the set $\{f(A\mathbf{x}+\mathbf{b}) \mid A \in \mathrm{GL}(n,\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n\}$, and the orbit of a polynomial class is the union of orbits of all the polynomials in it. In this paper, we give improved constructions of hitting-sets for the orbit of read-once oblivious algebraic branching programs (ROABPs) and a related model. Over field with characteristic zero or greater than d, we construct a hitting set of size $(ndw)^{O(w^2 \log n \cdot \min\{w^2, d \log w\})}$ for the orbit of ROABPs in unknown variable order where d is the individual degree and w is the width of ROABPs. We also give hitting set of size $(ndw)^{O(\min\{w^2, d \log w\})}$ for the orbit of polynomials computed by w-width ROABPs in any variable order. Our hitting sets improve upon the results of Saha and Thankey [ST21] who gave an $(ndw)^{O(d \log w)}$ size hitting set for the orbit of commutative ROABPs (a subclass of *any-order* ROABPs) and $(nw)^{O(w^6 \log n)}$ size hitting set for the orbit of multilinear ROABPs. Designing better hitting sets in large individual degree regime, for instance $d > n$, was asked as an open problem by [ST21] and this work solves it in small width setting.

We prove some new rank concentration results by establishing *low-cone concentration* for the polynomials over vector spaces, and they strengthen some previously known *low-support* based rank concentrations shown in [FSS14]. These new low-cone concentration results are crucial in our hitting set construction, and may be of independent interest. To the best of our knowledge, this is the first time when low-cone rank concentration has been used for designing hitting sets.

1 Introduction

Polynomial identity testing (PIT) problem is a fundamental problem in the area of algebraic circuit complexity. PIT is the problem of deciding whether a given multivariate polynomial is identically zero, where the input is given as an algebraic formula, circuit or other computational models like algebraic branching program. One way of testing zeroness of a polynomial is to check whether the coefficients of all the monomials are zero. However, the polynomial computed by a circuit or a branching program may have, in the worst-case, an exponential number of monomials compared to its size. Hence, by computing the explicit polynomial from the input, we cannot solve PIT problem in polynomial time. However, evaluating the polynomial at a point can be done in polynomial time of the input size. This helps us to get a polynomial time randomized algorithm for PIT by evaluating the input circuit at a random point, since any nonzero polynomial evaluated at a random point gives a nonzero value with high probability [DL78, Zip79, Sch80]. However, finding a deterministic polynomial time algorithm for PIT is a long-standing open question in algebraic complexity theory.

PIT captures several problems in algebra and combinatorics. For example, parallel algorithms for perfect matching [Tut47, Lov79, FGT16, ST17], primality testing [AKS04], multivariate polynomial factorization [KSS14], and many other problems [Sha90, DdOS14, GKS17]. PIT also has strong

*Department of Computer Science, Rutgers University, Piscataway, NJ 08854.1 Research supported in part by the Simons Collaboration on Algorithms and Geometry and NSF grant CCF-1909683. Email: vishwas1384@gmail.com.

†Department of Computer Science, IIT Bombay. Email: besusumanta@gmail.com.

ISSN 1433-8092

connection to circuit lower bounds [HS80, KI04, DSY09, CKS18, GKSS19]. See [Sax09, SY10, SS13] for surveys on PIT.

PIT problem is studied in two different settings: 1) *whitebox*, where we are allowed to access the internal structure of the circuit, and 2) *blackbox*, where only evaluation of the circuit at points is allowed. Deterministic blackbox PIT for an n-variate circuit class is equivalent to efficiently finding a set of points $\mathcal{H} \subseteq \mathbb{F}^n$, called a *hitting-set*, such that for any nonzero P in that circuit class, the set $\mathcal{H}$ contains a point at which $P \neq 0$ [1]. In this work, we only focus on the blackbox model.

Despite a lot of effort, little progress has been made on PIT problem in general. However, efficient deterministic PIT algorithms are known for many special circuit models. For example, blackbox PIT for depth-2 circuits (or sparse polynomials) [BT88, KS01, LV03], PIT algorithms for depth-3 circuits with bounded top fan-in [DS07, KS07, KS09, KS11, SS11, SS12, SS13], depth-3 diagonal circuits [Sax08, FS13a, FGS18] and various other subclasses of depth-3 circuits [SSS13, AGKS15, dOSV15], PIT for the subclasses of depth-4 circuits [ASSS12, BMS13, For15, KS17, PSS18] and certain types of symbolic determinants [FGT16, ST17, GT17].

The focus of this work is on the model of *read-once oblivious algebraic branching programs (ROABPs)*. An ROABP is a product of matrices

$$f = \mathbf{a}^T \cdot M_1(x_{\pi(1)}) M_2(x_{\pi(2)}) \cdots M_n(x_{\pi(n)}) \cdot \mathbf{c},$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{F}^{w \times 1}$ and for some permutation π on $[n]$ for each $i \in [n]$, $M_i(x_{\pi(i)}) \in \mathbb{F}^{w \times w}[x_{\pi(i)}]$ can be viewed as a polynomial over the matrix algebra. The permutation π is called the variable order of the ROABP. One reason to be interested in ROABP is that derandomizing blackbox PIT for ROABP can be viewed as an algebraic analogue of the RL vs. L question. Besides that, the ROABP model is surprisingly rich and powerful. It captures several other interesting circuit classes such as sparse polynomials or depth-two circuits, depth-three powering circuits (symmetric tensors), set-multilinear depth-three circuits (tensors), and semi-diagonal depth-3 circuits [FS13b]. Some notable polynomials such as the iterated matrix multiplication polynomial, the elementary and the power symmetric polynomials, and the sum-product polynomials can be computed by linear size ROABPs. Hitting sets for ROABPs have also led to the derandomization of an interesting case of the Noether Normalization Lemma [Mul12, FS13a], and to hitting sets for non-commutative algebraic branching programs [FS13b].

PIT question for ROABPs and its variants has been widely studied. There are three parameters associated with an ROABP: the number of variables n, the size of the matrices w called *width* and the individual degree d which is the maximum possible degree of any variable. First, [RS05] gave a polynomial time whitebox PIT algorithm for this model. [FS13b] first gave $(ndw)^{O(\log n)}$ size hitting set for ROABPs when the variable order is known. Later, [FSS14] gave an $(ndw)^{O(d \log w \cdot \log n)}$ size hitting for ROABPs with unknown variable order, and subsequently, [AGKS15] gave an improved hitting set of size $(ndw)^{O(\log n)}$ for this model. For zero or large characteristic fields, [GKS17] gave an $ndw^{\log n}$ size hitting sets for the known order ROABPs and the size becomes polynomially large when the width is constant. Better hitting set is known for a special class of ROABPs, called *any-order* ROABP. A polynomial f is computable by a w-width *any-order* ROABP, if for every permutation π on $[n]$, f is computable by a w-width ROABP. The notion of *any-order* ROABP subsumes the notion of commutative ROABP. An ROABP is called commutative ROABP if the polynomial computed by it remains unchanged under any permutation of the matrices involved in the product. [FSS14] gave two different constructions of hitting sets of size $(ndw)^{O(\log w)}$ and $d^{O(\log w)} \cdot (nw)^{O(\log \log w)}$ for *any-order* ROABPs [2]. Later, [GKS17] gives an improved hitting set of

[1] When $\mathbb{F}$ is a finite field, we are allowed to go some suitable extension $\mathbb{K}$ of $\mathbb{F}$ and pick points from $\mathbb{K}^n$.

[2] In [FSS14], *any-order* ROABPs are referred by "commutative ROABPs".

size $(ndw)^{O(\log\log w)}$ for this model. Recently, [GG20] gives improved hitting sets for both ROABPs and *any-order* ROABPs. Compared to the previous constructions, the size of hitting sets in [GG20] have finer dependence on the parameters of ROABPs. However, the construction of polynomial size hitting sets for ROABPs and its variants is still open.

In this work, we study the PIT question for the orbit of ROABPs. The *orbit* of an n-variate polynomial $f(\mathbf{x})$ over a field $\mathbb{F}$, denoted by $\mathrm{orbit}(f)$, is the set of polynomials obtained by applying invertible affine transformations on the variables of f , that is, $\mathrm{orbit}(f) = \{f(A\mathbf{x}+\mathbf{b}) \mid A \in \mathrm{GL}(n,\mathbb{F}), \text{ and } \mathbf{b} \in \mathbb{F}^n\}$. The orbit of a polynomial class $\mathcal{C}$, denoted by $\mathrm{orbit}(\mathcal{C})$, is the union of the orbits of the polynomials in the class. Apart from being a natural question to study the sturdiness of the known techniques (and improving them), designing hitting sets for the orbits of polynomial families and circuit classes is interesting for the following reasons:

- As observed by [ST21], the affine projections of "simple" polynomials have great expressive power. The set of affine projections of an n-variate polynomial $f(\mathbf{x})$ over a field $\mathbb{F}$ is $\mathrm{aproj}(f) := \{f(A\mathbf{x}+\mathbf{b}) \mid A \in \mathbb{F}^{n\times n} \text{ and } \mathbf{b} \in \mathbb{F}^n\}$. Formally, they show that if the characteristic of $\mathbb{F}$ is zero, the set of affine projections of an n-variate polynomial $f(\mathbf{x})$ over a field $\mathbb{F}$ lies inside the Zariski closure of the orbit of f (denoted by $\overline{\mathrm{orbit}(f)}$), that is $\mathrm{aproj}(f) \subseteq \overline{\mathrm{orbit}(f)}$. This observation has some interesting implications. For instance, using the above observation one can show that, the entire class of depth-3 circuits $\Sigma\Pi\Sigma$ with top fan-in s and degree d is contained in $\mathrm{aproj}(\mathsf{SP}_{s,d})$, where $\mathsf{SP}_{s,d} := \sum_{i\in[s]}\prod_{j\in[d]} x_{i,j}$ is a very structured s-sparse polynomial. The orbit closure of ROABPs is also very powerful, in fact they are as powerful as general ABPs. This can be seen by observing, the iterated matrix multiplication polynomial $\mathsf{IMM}_{w,d}$ is computable by a linear-size ROABP, yet every polynomial computable by a size-s general algebraic branching program is in $\mathrm{aproj}(\mathsf{IMM}_{s,s})$. For more polynomial families whose orbit closures contain interesting circuit classes see [MS21].
- For an n-variate polynomial f over a field $\mathbb{F}$, let $\mathbb{V}(f)$ denotes the variety (that is, zero locus) of f. Hitting set construction for an n-variate polynomial class $\mathcal{C}$ is the problem of picking a set of points $\mathcal{H}$ such that for each polynomial $f \in \mathcal{C}$, $\mathcal{H}$ is not entirely contained in $\mathbb{V}(f)$. On the other hand, Constructing hitting sets for the orbits of a polynomial class $\mathcal{C}$ is the task of finding a small set of points $\mathcal{H}$ such that for every $f \in \mathcal{C}$, $\mathcal{H}$ is not entirely contained in the set $\{A\mathbf{a}+\mathbf{b} \mid \mathbf{a} \in \mathbb{V}(f),\ A \in \mathrm{GL}(n,\mathbb{F}) \text{ and } \mathbf{b} \in \mathbb{F}^n\}$. This ensures that $\mathcal{H}$ will be independent to the choice of coordinate system making it mathematically and geometrically robust.

For a more detailed discussion on the reasons for studying hitting set of orbits see [ST21].

Hitting set construction for orbits of circuit classes is very recent, somewhat simultaneously Medini and Shpilka [MS21] and Saha and Thankey [ST21] started exploring PIT for the orbit of various polynomial classes. Medini and Shpilka [MS21] gave a quasi-polynomial size hitting set for the orbits of sparse polynomials ($\sum\prod$ circuits) and read-once formulas (ROFs). Saha and Thankey [ST21] gave hitting sets for the orbits of ROABPs and constant-read (more generally, constant-occur) formulas. Concretely, [ST21] gave an $(ndw)^{d\log w}$ size hitting set for the orbit of n-variate individual degree d width w commutative ROABPs. They also gave an $(nw)^{O(w^6\log n)}$ size hitting set for the orbit of n-variate multilinear polynomials computed by width w ROABPs. Building on this, they also gave quasi-polynomial size hitting set for constant-depth constant-occur formulas whose leaves are labeled by s-sparse polynomials with constant individual degree. In this work, we design hitting sets for the orbit of ROABPs and *any-order* ROABPs. Our results significantly improve the dependence on individual degree in the size of hitting sets in comparison to [ST21], from exponential to polynomial.

1.1 Our Results

First, we define the models studied in this paper. Algebraic branching programs (ABPs) were defined by Nisan in [NW97]. In this paper, we study a variant of ABPs known as read-once oblivious ABPs (ROABPs). While Nisan defined ABPs using directed graphs, we use a more conventional definition using product of matrices. Let $f(x_1, \ldots, x_n)$ be an n-variate individual degree d polynomial over a field $\mathbb{F}$. Let π be a permutation on $[n]$. We say f is computed by a width w ROABP with variable order π, if f can be written as

$$f = \mathbf{a}^T \cdot M_1(x_{\pi(1)}) M_2(x_{\pi(2)}) \cdots M_n(x_{\pi(n)}) \cdot \mathbf{c},$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{F}^{w \times 1}$ and for all $i \in [n]$, $M_i(x_{\pi(i)}) \in \mathbb{F}^{w \times w}[x_{\pi(i)}]$ can be viewed as a polynomial in $x_{\pi(i)}$ over the matrix algebra with degree at most d. We say f is computable by a w-width *any order* ROABP, if for every permutation π on $[n]$, f is computable by a width w ROABP. We say f is computed by a width w *commutative* ROABP, if all $M_i(x_{\pi(i)})$'s are polynomials over a commutative sub-algebra of the matrix algebra. For example, consider the coefficients of each M_i are diagonal matrices. One can observe that the set of polynomials computed by w-width commutative ROABPs are also computable by w-width *any-order* ROABPs. However, the converse direction is unkown to us. All PIT algorithms for ROABPs are designed by analyzing the coefficient space of $M_1(x_{\pi(1)}) M_2(x_{\pi(2)}) \cdots M_n(x_{\pi(n)})$.

In this paper, we design hitting sets for the orbits of ROABPs and *any-order* ROABPs. Let $f(\mathbf{x})$ be an n-variate polynomial over a field $\mathbb{F}$. The orbit of f, denoted by $\mathrm{orbit}(f)$, is the set $\{f(A\mathbf{x} + \mathbf{b}) \mid A \in \mathrm{GL}(n, \mathbb{F}) \text{ and } \mathbf{b} \in \mathbb{F}^n\}$. For a polynomial class $\mathcal{C}$, the orbit of $\mathcal{C}$, denoted by $\mathrm{orbit}(\mathcal{C})$, is the union of orbits of all the polynomials in $\mathcal{C}$. Now, we describe our result for the orbit of *any-order* ROABPs.

Theorem 1.1. *Let $\mathbb{F}$ be a field of characteristic zero or greater than d. Let $\mathcal{C}$ be the set of n-variate polynomials over $\mathbb{F}$ with individual degree at most d and computable by a width w any-order ROABP. Then, there exists a hitting set for* $\mathrm{orbit}(\mathcal{C})$ *computable in time $(ndw)^{O(\ell)}$ where $\ell = \min\{w^2, 2d \log w\}$.*

Comparison with previous works: As far as we know, this is the first result addressing the orbit of *any-order* ROABPs, and it subsumes the commutative ROABP result of Saha and Thankey [ST21]. They gave an $(ndw)^{O(d \log w)}$ size hitting set for the orbit of commutative ROABPs. In fact, our result strengthens [ST21] in "low width" setting. Concretely, if the individual degree is $\mathrm{poly}(\log n)$, [ST21] gives quasi-polynomial time PIT for the orbit of commutative ROABPs. However, when $d \geq n$, their algorithm does not give any non-trivial PIT for the orbit of commutative ROABPs. On the other hand, our result gives quasi-polynomial time PIT for the orbit of *any-order* ROABPs when $\min\{d, w\} = \mathrm{poly}(\log n)$. Also, for constant width *any-order* ROABPs with unbounded individual degree, our result gives a polynomial time PIT for its orbit. However, [ST21] gives polynomial time PIT for the orbit commutative ROABPs when both d and w are constants. Thus, our result has much better dependence on the individual degree in comparison with [ST21].

Now, we describe our result regarding the orbit of ROABPs.

Theorem 1.2. *Let $\mathbb{F}$ be a field of characteristic zero or greater than d. Let $\mathcal{C}$ be the set of n-variate polynomials over $\mathbb{F}$ with individual degree at most d and computable by a width w ROABP. Then there exists a hitting set for* $\mathrm{orbit}(\mathcal{C})$ *computable in time $(ndw)^{O(\ell)}$ where $\ell = (w^2 \log n) \cdot \min\{w^2, 2d \log w\}$.*

Comparison with previous works: Saha and Thankey [ST21] gave an $(nw)^{O(w^6 \log n)}$ time PIT for the orbit of multilinear polynomials computed by ROABPs. Therefore, our result can be seen as the first one which gives PIT for the orbit of ROABPs with unbounded individual degree. Irrespective of the value of the individual degree, our result gives a quasi-polynomial time PIT for the orbit of ROABPs when the width $w = \mathrm{poly}(\log n)$. Also, the time complexity of our algorithm has better dependence on the width of ROABPs in comparison with [ST21].

Remark. Our results in this paper continue to hold even if we consider a more generalized definition for the orbit of an n-variate polynomial $f(\mathbf{x})$, that is $\mathrm{orbit}(f) = \{f(A\mathbf{y}+\mathbf{b}) \mid m \geq n,\ A \in \mathbb{F}^{n\times m}$ with rank n and $\mathbf{b} \in \mathbb{F}^n\}$ where $\mathbf{y} = (y_1, \ldots, y_m)$. However, we work with the conventional definition of the orbit of polynomials for the simplicity of exposition, and because the proofs of the results with the generalized definition of orbit is almost same as the proofs given in this paper.

1.2 Proof techniques

First, we briefly sketch the abstract framework followed by the proofs of our results. Let $\mathcal{C}$ be a set of n-variate polynomials in $\mathbf{y} = (y_1, \ldots, y_n)$ with individual degree at most d. Then $\mathrm{orbit}(\mathcal{C})$ is the set of n-variate polynomials in $\mathbf{x} = (x_1, \ldots, x_n)$ is defined as follows: for all $f(\mathbf{x}) \in \mathrm{orbit}(\mathcal{C})$ there exists a polynomial $h(\mathbf{y}) \in \mathcal{C}$, an invertible linear transformation $L(\mathbf{x}) = (\ell_1, \ldots, \ell_n)$ from $\mathbb{F}^n$ to $\mathbb{F}^n$ and a point $\mathbf{b} \in \mathbb{F}^n$ such that

$$f(\mathbf{x}) = h(L(\mathbf{x}) + \mathbf{b}).$$

In this paper, we design hitting sets for the orbits of ROABPs and *any-order* ROABPs. Hitting sets for ROABPs are constructed by designing a "smartly" chosen shift $\mathbf{g}(\mathbf{t})$ (a low variate polynomial map) such that when we shift any polynomial $h(\mathbf{y})$ computable by a small size ROABP, then there exists a "low-support" monomial (with nonzero coefficient) in $h(\mathbf{x}+\mathbf{g})$. Note that, it is straightforward to construct hitting sets when such a low-support monomial (with nonzero coefficient) exists. However, this approach does not *directly* work for a polynomial $f(\mathbf{x}) = h(L(\mathbf{x}) + \mathbf{b})$ in the orbit of ROABPs as shifting f has a slightly different effect. Note,

$$f(\mathbf{x}+\mathbf{g}) = h(L(\mathbf{x}+\mathbf{g}) + \mathbf{b}) = h(L(\mathbf{x}) + L\circ\mathbf{g} + \mathbf{b}).$$

That is, the shift gets composed with the affine transformation $L(\mathbf{x}) + \mathbf{b}$. The main idea in our construction is to choose a shift such that the transformed shift (for *any* affine transformation) is also "smart". That is, for any invertible linear transformation $L(\mathbf{x})$ and $\mathbf{b} \in \mathbb{F}^n$, there exists a "low-support" monomial (with nonzero coefficient) in $f(\mathbf{x}+\mathbf{g}) = h(L(\mathbf{x}) + L\circ\mathbf{g} + \mathbf{b})$.

Let $\mathbf{g}(\mathbf{t}) = (g_1, \ldots, g_n)$ be a polynomial map from $\mathbb{F}^m$ to $\mathbb{F}^n$ and $h'(\mathbf{y}) = h(\mathbf{y} + L\circ\mathbf{g} + \mathbf{b})$. Note that, $f'(\mathbf{x}) := f(\mathbf{x}+\mathbf{g}) = h'(L(\mathbf{x}))$. Our abstract format to design hitting sets for the orbits of ROABPs and *any-order* ROABPs has the following two steps.

Step 1: First we find some suitable low degree polynomial map $\mathbf{g}$ in few variables (compare to n) such that for *all* invertible linear transformation $L(\mathbf{x})$ and $\mathbf{b} \in \mathbb{F}^n$, after shifting $h(\mathbf{y}) \in \mathcal{C}$ by $L\circ\mathbf{g}+\mathbf{b}$, the new polynomial $h'(\mathbf{y}) = h(\mathbf{y} + L\circ\mathbf{g} + \mathbf{b})$ has the following property: for some small positive integer k, $\mathrm{hom}_{\leq k}(h'(\mathbf{y}))$ is a nonzero polynomial in $\mathbf{y}$ over the field $\mathbb{F}(\mathbf{t})$, where $\mathrm{hom}_{\leq k}(\cdot)$ denotes the degree up to k part of the input polynomial. This step, more specifically the construction of $\mathbf{g}(\mathbf{t})$, heavily relies on the structure of $\mathcal{C}$.

Step 2: Since $L(\mathbf{x})$ is an invertible linear transformation, all ℓ_i's are algebraically independent. Also, $\mathrm{hom}_{\leq k}(f') = \mathrm{hom}_{\leq k}(h')(L(\mathbf{x}))$. Therefore, $\mathrm{hom}_{\leq k}(f')$ is a nonzero polynomial in $\mathbf{x}$ over the field $\mathbb{F}(\mathbf{t})$. This implies that there exists a monomial $\mathbf{x}^{\mathbf{e}} = \prod_{i=1}^{n} x_i^{e_i}$ such that the support of $\mathbf{e}$ is at most k and the coefficient of $\mathbf{x}^{\mathbf{e}}$ in f' is a nonzero polynomial in $\mathbf{t}$. There are well known constructions of hitting sets for polynomials like $f'(\mathbf{x})$. For example, combining Lemma

2.12 and Observation 2.6 we get a hitting set for f' of size around $(nd)^{O(m+k)}$. Thus, we design a hitting set for orbit($\mathcal{C}$). This step is independent of the polynomial class $\mathcal{C}$.

For instance, assume that $\mathcal{C}$ is the set of n-variate polynomials with individual degree and sparsity are at most d and s, respectively. Then, from [For15], after shifting any polynomial $h(\mathbf{y}) \in \mathcal{C}$ by an $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ with all α_i's are nonzero the following holds: there exists a monomial $\mathbf{y}^{\mathbf{e}}$ such that the support of $\mathbf{e}$ is at most $\log s$ and its coefficient in $h(\mathbf{y} + \boldsymbol{\alpha})$ is nonzero. Let $\mathbf{g}(t)$ be the polynomial map from $\mathbb{F}$ to $\mathbb{F}^n$ defined as $(t, t^2, \ldots, t^n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$. Then, each $\ell_i(\mathbf{g}) + b_i$ is a nonzero polynomial. Therefore, there exists a monomial $\mathbf{y}^{\mathbf{e}}$ of support-size at most $\log s$ such that its coefficient in $h'(\mathbf{y})$ is a nonzero polynomial in t. Since the individual degree is at most d, the degree of $\mathbf{y}^{\mathbf{e}}$ is at most $\leq d \log s$. Now from the step 2, there exists a monomial in $\mathbf{x}$ of support-size at most $d \log s$ such that its coefficient in f' is a nonzero polynomial in t. Thus we have a hitting set for orbit($\mathcal{C}$) of size $(nd)^{O(d \log s)}$. This gives a different (and much simpler) hitting set construction than [ST21, Theorem 7] for the orbit of sparse polynomials with low individual degree.

Stronger rank concentration results: We describe some stronger rank concentration results which will be very useful in designing our hitting sets for the orbits of ROABPs and *any-order* ROABPs. Let $G(\mathbf{x})$ be an n-variate polynomial over the vector space $\mathbb{F}^k$. The *coefficient space* of G is the vector space spanned by the coefficient vectors in G. In general, the coefficient space of G can be spanned by the coefficients of any arbitrary set of monomials. In rank concentration, our goal is to construct a polynomial map $\mathbf{g}(\mathbf{t})$ such that after shifting $G(\mathbf{x})$ by $\mathbf{g}(\mathbf{t})$, the coefficient space of the new polynomial $G'(\mathbf{x}) = G(\mathbf{x} + \mathbf{g})$ is spanned the coefficients of a "small" set of monomials S. For example,

1. if S is the set monomials whose support-size is $\leq \ell$, we say G' has *ℓ-support concentration*. The support-size of a monomial is the number of variables appear in it.

2. if S is the set of monomials whose cone-size is $\leq \ell$, we say G' has *ℓ-cone concentration*. The cone-size of a monomial is the number of monomials divide it.

3. if S is the set of monomials which is closed under sub-monomials, we say G' has a *cone-closed basis*.

The notion of rank-concentration was introduced in [ASS13]. Subsequently, many PIT results are obtained based on "low-support" rank concentration [ASS13, FSS14, GKST15, GKS17, ST21]. Later, [FGS18] introduced the notion of cone concentration and cone-closed basis. Among the three notions of rank concentrations, cone-closed basis is stronger than the other two, then comes cone concentration and after that support concentration. More specifically, cone-closed basis of G' implies that it has also k-cone concentration , and k-concentration for G' implies it has also $\log k$-support concentration. For more details about the relation between these three notions of rank concentrations see Lemma 2.15. The notion of cone concentration is important for designing our improved hitting sets over [ST21]. To the best of our knowledge, this is the first time when the notion of cone concentration is used in designing PIT algorithms.

In this work, we strengthen some of the rank concentration results shown in [FSS14, FGS18]. [FSS14] showed that if $G(\mathbf{x})$ is shifted by $\mathbf{t} = (t_1, \ldots, t_n)$, the new polynomial $G(\mathbf{x} + \mathbf{t})$ has $\log k$-support concentration over the field $\mathbb{F}(\mathbf{t})$. Moreover, they showed that if G is shifted by a *n-wise independent monomial map* $\mathbf{g}'(\mathbf{s}, \mathbf{t})$, then the new shifted polynomial has $\log k$-support concentration. A polynomial map $\mathbf{g}'(\mathbf{s}, \mathbf{t})$ from $\mathbb{F}^m \times \mathbb{F}^{m'}$ to $\mathbb{F}^n$ is called ℓ-wise independent monomial map if for every $S \subseteq [n]$ of size $\leq \ell$ there exists an $\boldsymbol{\alpha} \in \mathbb{F}^m$ such that polynomials $\{\mathbf{g}'(\boldsymbol{\alpha}, \mathbf{t})^{\mathbf{e}}\}_{\mathrm{supp}(\mathbf{e}) \subseteq S}$ are distinct monomials in $\mathbf{t}$. Later, [FGS18] showed that $G(\mathbf{x} + \mathbf{t})$ has a cone-closed basis. Their result can also be extended to show that $G(\mathbf{x}+\mathbf{g}')$ has a cone-closed basis when $\mathbf{g}'$ is an n-wise independent monomial map. However, when we take composition of $\mathbf{g}'$ with an invertible affine transformation, that is $\mathbf{b} + L \circ \mathbf{g}'$ where $\mathbf{b} \in \mathbb{F}^n$ and $L(\mathbf{x})$ is an invertible linear transformation from $\mathbb{F}^n$ to $\mathbb{F}^n$, the n-wise independence property of $\mathbf{g}'$ breaks down. Therefore, the previous rank concentration results are not helpful in designing hitting sets for the orbits of circuit classes. We strengthen the rank concentration results of [FSS14, FGS18] in the following way: After shifting G by a polynomial map $\mathbf{g}' = (g_1, \dots, g_n)$ such that all g_i's are *algebraically independent*, the new polynomial has a cone-closed basis, hence k-cone concentration. Observe that the n-wise independence property implies the algebraic independence property needed in our hypothesis. Therefore, our hypothesis is weaker than the hypothesis used in [FSS14, FGS18]. Also, algebraic independence property of $\mathbf{g}'$ preserves even after composing it with invertible affine transformations. For details see Lemma 3.2. This rank concentration result will be helpful in designing the hitting sets for the orbit of *any-order* ROABPs.

We show one more rank concentration result which will help in designing PIT algorithms for the orbit of ROABPs. Assume that the coefficients of the monomials of total degree up to D spans the coefficient space of G. Let $\mathbf{g}'(\mathbf{s},\mathbf{t})$ be a *total degree D independent monomial map* from $\mathbb{F}^m \times \mathbb{F}^{m'}$ to $\mathbb{F}^n$, that is, there exists an $\boldsymbol{\alpha} \in \mathbb{F}^m$ such that the polynomials $\{\mathbf{g}'(\boldsymbol{\alpha},\mathbf{t})^{\mathbf{e}}\}_{|\mathbf{e}|_1 \le D}$ are distinct monomials in $\mathbf{t}$. Then [FSS14] showed that if $G(\mathbf{x})$ is shifted by $u\mathbf{g}'$, then the new shifted polynomial has $\log k$-support concentration over the field $\mathbb{F}(u,\mathbf{s},\mathbf{t})$. Our rank concentration result differs from [FSS14] in the following ways:

1. Our hypothesis is slightly stronger than [FSS14]. Instead of total degree D independent monomial map, we assume that $\mathbf{g}'(\mathbf{s},\mathbf{t})$ is a total degree Dk independent monomial map.

2. On the other hand, we strengthen the conclusion as follows: for every invertible linear transformation $L(\mathbf{x})$ from $\mathbb{F}^n$ to $\mathbb{F}^n$, if we shift G by $uL \circ \mathbf{g}'$, then the new shifted polynomial has a cone-closed basis over the field $\mathbb{F}(u,\mathbf{s},\mathbf{t})$.

For details see Lemma 3.3.

Proof idea of Theorem 1.1: Suppose that $\mathcal{C}$ is the set of all n-variate polynomials in $\mathbf{y}$ with individual degree at most d and computed by width w *any-order* ROABPs. Let $f(\mathbf{x})$ be an n-variate polynomial in orbit$(\mathcal{C})$. Then there exists a polynomial $h(\mathbf{y}) \in \mathcal{C}$, an invertible linear transformation $L(\mathbf{x})$ and a point $\mathbf{b} \in \mathbb{F}^n$ such that

$$f(\mathbf{x}) = h(L(\mathbf{x}) + \mathbf{b}).$$

Since $h(\mathbf{y}) \in \mathcal{C}$, there exists a polynomial $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{w \times w}$ with individual degree at most d and computed by a width w *any-order* ROABP such that

$$h(\mathbf{y}) = \mathbf{a}^T \cdot G(\mathbf{y}) \cdot \mathbf{c},$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{F}^w$.

Now we will describe the first step of aforementioned abstract format. First, we show how to achieve w^2-cone concentration in $G(\mathbf{y})$. Let $\mathbf{g}(\mathbf{t}) = (g_1, \dots, g_n)$ be a polynomial map from $\mathbb{F}^m$ to $\mathbb{F}^n$ such that for any $S \subseteq [n]$ of size $k := \lceil 2\log w + 1 \rceil$, the set of polynomials $\{g_i \mid i \in S\}$ are algebraically independent. Then, in Lemma 4.1, we prove that $G(\mathbf{y}+\mathbf{g})$ has w^2-cone concentration over the field $F(\mathbf{t})$. It strengthens the rank-concentration result for *any-order* ROABPs shown in [FSS13, Theorem 4.1]. They showed that if we shift G by a k-wise independent monomial map, then the new polynomial has $2\log w$-support concentration. Next, in Lemma 4.2, we show that for any invertible linear transformation $L(\mathbf{x})$ and $\mathbf{b} \in \mathbb{F}^n$, the polynomial map defined as the composition of $L(\mathbf{x}) + \mathbf{b}$ and Shpilka-Volkovich generator $\mathcal{G}^{SV}_{n,k}$ (see Definition 2.10, or [SV09]), that is $L \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b}$, satisfies the property required for achieving w^2-cone concentration in $G(\mathbf{y})$. Therefore, $G(\mathbf{y} + L \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b})$ has w^2-cone concentration. This implies that there exists a monomial $\mathbf{y}^{\mathbf{e}}$ of cone-size $\leq w^2$ such that the coefficient of $\mathbf{y}^{\mathbf{e}}$ in $h'(\mathbf{y}) = h(\mathbf{y} + L \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b})$ is nonzero. For any monomial of cone-size $\leq w^2$, its degree is less than w^2 and the support set is of size at most $2 \log w$. Since the individual degree is at most d, the degree of $\mathbf{y}^{\mathbf{e}}$ is at most ℓ where $\ell := \min\{w^2, d \log w\}$. Therefore, $\hom_{\leq \ell}(h')$ is nonzero. Now we apply the step two of the abstract format, which is independent of $\mathcal{C}$, and get our desired hitting set for orbit($\mathcal{C}$).

Proof idea of Theorem 1.2: Suppose that $\mathcal{C}$ is the set of all n-variate polynomials in $\mathbf{y}$ with individual degree at most d and computed by width w ROABPs. Let $f(\mathbf{x})$ be an n-variate polynomial in orbit($\mathcal{C}$). Then there exists a polynomial $h(\mathbf{y}) \in \mathcal{C}$, an invertible linear transformation $L(\mathbf{x})$ and $\mathbf{b} \in \mathbb{F}^n$ such that

$$f(\mathbf{x}) = h(L(\mathbf{x}) + \mathbf{b}).$$

Since $h(\mathbf{y}) \in \mathcal{C}$, there exists a polynomial $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{w \times w}$ and a permutation π on $[n]$ such that

$$h(\mathbf{y}) = \mathbf{a}^T \cdot G(\mathbf{y}) \cdot \mathbf{c} \text{ and } G(\mathbf{y}) = \prod_{i=1}^{n} M_i(x_{\pi(i)})$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{F}^w$ and for all $i \in [n]$, $M_i(x_{\pi(i)})$ is a polynomial in $\mathbb{F}[x_{\pi(i)}]^{w \times w}$.

Now like *any-order* ROABPs, we want to achieve w^2-cone concentration in $G(\mathbf{y})$. However, our approach here will be different from *any-order* ROABPs. Here, we strengthen the "merge-and-reduce" approach of [FSS14] in the following ways:

1. In [FSS14], the polynomial maps $\mathbf{h}_j$ (for $j = 0, 1, \ldots, \lceil \log n \rceil$) were inductively constructed such that after shifting G by $\mathbf{h}_j$, in the new polynomial $G(\mathbf{x} + \mathbf{h}_j)$, product of any 2^j consecutive matrices have $2 \log w$-support concentration. We strengthen this result by showing w^2-cone concentration at each inductive step.

2. At each induction step, since we are dealing with polynomials in orbit (of ROABPs), we not only need construct a polynomial map which helps to achieve w^2-cone concentration, but its composition with any invertible affine transformation also helps to achieve the same property.

In [FSS14], $\mathbf{h}_j$ was constructed as follows: $\mathbf{h}_0 = \mathbf{0}$ and for all $j \in [\lceil \log n \rceil]$, $\mathbf{h}_j = \mathbf{h}_{j-1} + u_j \mathbf{g}(\mathbf{s}_j, \mathbf{t}_j)$ where $\mathbf{g}(\mathbf{s}_j, \mathbf{t}_j)$ is a total degree $4d \log w$ independent monomial map from $\mathbb{F}^m \times \mathbb{F}^{m'}$ to $\mathbb{F}^n$. They showed that the product of any 2^j consecutive matrices in $G(\mathbf{y} + \mathbf{h}_j)$ has $2 \log w$-support concnetration over the field $\mathbb{F}((u_k, \mathbf{s}_k, \mathbf{t}_k)_{k \in [j]})$.

Our definition of $\mathbf{h}_j$ is very close to the definition used in [FSS14]. For $j = 0$, $\mathbf{h}_j = (t, t^2, \ldots, t^n)$ and for all $j \in [\lceil \log n \rceil]$, $\mathbf{h}_j = \mathbf{h}_{j-1} + u_j \mathbf{g}(\mathbf{s}_j, \mathbf{t}_j)$ where $\mathbf{g}(\mathbf{s}_j, \mathbf{t}_j)$ is a total degree D independent monomial map from $\mathbb{F}^m \times \mathbb{F}^{m'}$ to $\mathbb{F}^n$ where $D = 2w^2 \cdot \min\{w^2, 2d \log w\}$. We show that for every invertible linear transformation $L(\mathbf{x})$ from $\mathbb{F}^n$ to $\mathbb{F}^n$ and $\mathbf{b} \in \mathbb{F}^n$, the product of any 2^j consecutive matrices in $G(\mathbf{y} + L \circ \mathbf{h}_j + \mathbf{b})$ has a cone-closed basis, hence has w^2-cone concentration, over the field $\mathbb{F}(t, (u_k, \mathbf{s}_k, \mathbf{t}_k)_{k \in [j]})$. Our rank concentration results play an important role in proving this property of $\mathbf{h}_j$. For more details see Lemma 5.1 and 5.2. There are many known constructions of total degree D independent monomial map with $m = m' = O(D)$. For example see Lemma 2.9. After constructing a polynomial map which gives w^2-cone concentration in $G(\mathbf{y})$, the rest of the proof will be similar to what we did for the *any-order* ROABP case.

1.3 Organization of the paper

In Section 2, we discuss all the preliminaries and necessary notations. Section 3 describes our rank concentration results. In Section 4 and 5, we give the construction of our hitting sets for the orbits of *any-order* ROABPs and ROABPs, respectively.

2 Notations and Preliminaries

By $\mathbb{N}$ we denote the set of natural numbers. For any positive integer n, $[n]$ denotes the set $\{1, 2, \ldots, n\}$. For a variable tuple $\mathbf{x} = (x_1, \ldots, x_n)$ and a tuple $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{N}^n$, $\mathbf{x}^{\mathbf{e}}$ denotes the monomial $\prod_{i=1}^{n} x_i^{e_i}$. The *degree*, or *total degree*, of $\mathbf{x}^{\mathbf{e}}$ is $|\mathbf{e}|_1 = \sum_{i=1}^{n} e_i$ and the *individual degree* of $\mathbf{x}^{\mathbf{e}}$ is $|\mathbf{e}|_\infty = \max i \in [n] e_i$. The *support* of $\mathbf{x}^{\mathbf{e}}$ is the subset S of $[n]$ such that $i \in S$ if and only if $e_i > 0$, and the *support-size* denotes the cardinality of S. The *cone* of $\mathbf{x}^{\mathbf{e}}$ is the set of monomials which divide it and the *cone-size* is the cardinality of that set , that is $\prod_{i=1}^{n}(e_i + 1)$. A monomial $\mathbf{x}^{\mathbf{f}}$ is called a *sub-monomial* of $\mathbf{x}^{\mathbf{e}}$, if $\mathbf{x}^{\mathbf{e}}$ divides $\mathbf{x}^{\mathbf{f}}$, that is $e_i \leq f_i$ for all $i \in [n]$. A set of monomials B is called *cone-closed* if for every monomial in B all its sub-monomials are also in B. For a polynomial f in $\mathbf{x}$ and a monomial $\mathbf{x}^{\mathbf{e}}$, $\mathrm{coef}_f(\mathbf{x}^{\mathbf{e}})$ denotes the coefficient of $\mathbf{x}^{\mathbf{e}}$ in f.

Observation 2.1. *For a monomial of cone-size at most k, its degree is less that k and the support-size is at most $\log k$.*

A *monomial ordering* is a total ordering on the set of all monomials in $\mathbf{x}$ with following properties:

1. for all $\mathbf{a} \in \mathbb{N}^n \setminus \{\mathbf{0} = (0, \ldots, 0)\}, \mathbf{1} \prec \mathbf{x}^{\mathbf{a}}$.
2. for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$, if $\mathbf{x}^{\mathbf{a}} \prec \mathbf{x}^{\mathbf{b}}$ then $\mathbf{x}^{\mathbf{a}+\mathbf{c}} \prec \mathbf{x}^{\mathbf{b}+\mathbf{c}}$.

For more on monomial ordering see [CLO15, Chapter 2].

Suppose that M is a matrix whose rows and columns are indexed by A and B, respectively. Then for every $S \subseteq A$ and $T \subseteq B$, $M_{S,T}$ denotes the submatrix of M with rows and columns are indexed by S and T, respectively. The next lemma is a well known phenomenon in matroid theory which, informally, says that given distinct weights to the elements of a matroid there exists a unique minimum weight base. Here, we describe it in a language which is suitable for our context.

Lemma 2.2. *Let k be a positive integer and $M_{n,d}$ be the set of all n-variate monomials in $\mathbf{x}$ with individual degree $\leq d$. Let M be a matrix over $\mathbb{F}$ of rank r such that its rows are indexed by $[k]$ and the columns are indexed by $M_{n,d}$. Let $\prec$ be a monomial ordering on the set of monomials in $\mathbf{x}$. Then there exists a unique subset $B \subseteq M_{n,d}$ of size r such that $\mathrm{rank}(M_{[k],B}) = r$ and for every other subset $B' \subseteq M_{n,d}$ with $\mathrm{rank}(M_{[k],B'}) = r$, $\prod_{\mathbf{e} \in B} \mathbf{x}^{\mathbf{e}} \prec \prod_{\mathbf{e}' \in B'} \mathbf{x}^{\mathbf{e}'}$.*

Here we give a very brief sketch of the proof. Using the monomial ordering $\prec$, greedily choose r linealy independent columns of M as follows: at each step pick the least $\prec$-indexed column of M such that it increses the rank of the chosen vectors, and denote that set by $B = \{m_1, \ldots, m_r\}$ with $m_1 \prec \cdots \prec m_r$. Let B' be an another subset of $M_{n,d}$ with r linearly lindependent columns of M, and $B' = \{m'_1, \ldots, m'_r\}$ with $m'_1 \prec \cdots \prec m'_r$. Then one can show that $B \preceq B'$ point-wise, that is $m_i \preceq m'_i$ for all $i \in [r]$, and there exists an $i_0 \in [r]$ such that $m_{i_0} \prec m'_{i_0}$. This implies that $\prod_{i \in [r]} m_i \prec \prod_{i \in [r]} m'_i$. For more details one can see [FSS13, Lemma 5.2 and 5.3].

Next, we give an expression for the product of a "fat" matrix with a "tall" matrix. It is known as known as Cauchy-Binet formula. It will be useful to prove the rank concentration results in Section 3.

Lemma 2.3 (Cauchy-Binet formula, [Zen93])**.** *Let $n \geq m$ be two positive integers. Let M and N two $m \times n$ and $n \times m$ matrices, respectively, over $\mathbb{F}$. Then*

$$\det(AB) = \sum_{S \in \binom{[n]}{m}} \det(M_{[m],S}) \cdot \det(M_{S,[m]}).$$

2.1 Hitting sets

Definition 2.4. *Let $\mathcal{C}$ be a set of n-variate polynomial class over a field $\mathbb{F}$. A set of points $\mathcal{H} \subseteq \mathbb{F}^n$ is called a* hitting set *for $\mathcal{C}$ if for every polynomial $f \in \mathcal{C}$, f is nonzero if and only if there exists a point $\boldsymbol{\alpha} \in \mathcal{H}$ such that $f(\boldsymbol{\alpha}) \neq 0$.*

We say a hitting set $\mathcal{H}$ is *computable in time T* if there exists an algorithm which computes all the points in the set $\mathcal{H}$ in time T. When $\mathbb{F}$ is a finite field, we are allowed to pick points from $\mathbb{K}^n$ where $\mathbb{K}$ is a polynomially large extension of $\mathbb{F}$. In PIT literature, a common method of designing hitting sets is via hitting set generator.

Definition 2.5. *Let $\mathcal{C}$ be a set of n-variate polynomial class over a field $\mathbb{F}$. A polynomial map $\mathbf{g}(\mathbf{t})$ from $\mathbb{F}^m$ to $\mathbb{F}^n$ is called* hitting set generator *for $\mathcal{C}$ if for every $f \in \mathcal{C}$, f is nonzero if and only if $f(\mathbf{g}) \neq 0$.*

*Furthermore, $\mathbf{g}(\mathbf{t})$ is called $t(m,n)$-*explicit *if there exists an n-output circuit which computes $\mathbf{g}(\mathbf{t})$ and the circuit is computable in $t(m,n)$ time.*

Hitting set generators immediately give us hitting sets.

Observation 2.6. *Let $\mathcal{C}$ be an n-variate polynomial class over a field $\mathbb{F}$ such that the degree of each polynomial is at most d. Let $\mathbf{g}(\mathbf{t}) : \mathbb{F}^m \leftarrow \mathbb{F}^n$ be a hitting set generator for $\mathcal{C}$ such that the individual degree of each coordinate of $\mathbf{g}$ is at most r. Let S be a subset of $\mathbb{F}$ of size $dr+1$. Then $\mathcal{H} := \mathbf{g}(S^m)$ is a hitting set for $\mathcal{C}$. Moreover, if $\mathbf{g}(t)$ is t-explicit then the hitting set $\mathcal{H}$ is computable in* $\mathrm{poly}(t(dr)^m)$ *time.*

Proof. Since $\mathbf{g}$ is a hitting set generator for $\mathcal{C}$ and each coordinate of $\mathbf{g}$ is a m-variate polynomial, for every nonzero $f \in \mathcal{C}$, $f(\mathbf{g})$ is a nonzero m-variate polynomial. Also, the individual degree of $f(\mathbf{g})$ is at most dr. Thus, there exists a point $\boldsymbol{\alpha} \in S^m$ such that $f(\mathbf{g}(\boldsymbol{\alpha})) \neq 0$. Therefore, $\mathcal{H}$ is a hitting set for $\mathcal{C}$. Since $\mathbf{g}$ is t-explicit, each point in $\mathcal{H}$ is computable in time $\mathrm{poly}(t)$. Therefore, $\mathcal{H}$ is computable in time $\mathrm{poly}(t(dr)^m)$. □

2.2 Some useful polynomial maps

Suppose that $\mathbf{g}(\mathbf{t}) = (g_1, \ldots, g_n)$ be a polynomial map from $\mathbb{F}^m$ to $\mathbb{F}^n$. Then, we say $\mathbf{g}$ is a $t(m,n)$-*explicit* polynomial map if there exists an n-output circuit C which computes the polynomials $(g_1, \ldots, g_n)$ and the circuit C is computable in time $t(m,n)$. Let $\mathbf{g}(\mathbf{y})$ be a polynomial map from $\mathbb{F}^m$ to $\mathbb{F}^n$ and $\mathbf{h}(\mathbf{x}) = (h_1, \ldots, h_k)$ be a polynomial map from $\mathbb{F}^n$ to $\mathbb{F}^k$. Then $\mathbf{h} \circ \mathbf{g}$ denotes the composition of $\mathbf{g}$ with $\mathbf{h}$, that is $\mathbf{h}(\mathbf{g}) = (h_1(\mathbf{g}), \ldots, h_k(\mathbf{g}))$. A polynomial map $L(\mathbf{x}) = (\ell_1, \ldots, \ell_n)$ from $\mathbb{F}^n$ to $\mathbb{F}^n$ is called an *invertible linear transformation* if each ℓ_i is a linear polynomial of form $\ell_{i1}x_1 + \ldots + \ell_{in}x_n$ and all ℓ_i's are linearly independnet. An *invertible affine transformation* is a polynomial map of form $L(\mathbf{x}) + \mathbf{b}$ where $L(\mathbf{x})$ is an invertible linear transformation and $\mathbf{b} \in \mathbb{F}^n$. Next, we describe some well known polynomial maps and their properties which are frequently used in designing PIT algorithms and they also will be useful for us. First, we describe the generator for sparse polynomial due to Klivans and Spielman [KS01].

Lemma 2.7 (Klivans-Spielman generator [KS01]). *Let n, d, s, m be positive integers such that $m = \Theta(\log_{nd} s)$. Let $\mathbb{F}$ be a field of size $\geq \mathrm{poly}(nd)$. Then there exists a* $\mathrm{poly}(nd)$*-explicit polynomial map $\mathcal{G}^{KS}_{n,d,s}(\mathbf{s}, \mathbf{t})$ from $\mathbb{F}^m \times \mathbb{F}^m$ to $\mathbb{F}^n$ such that*

1. *for all $i \in [n]$, $(\mathcal{G}^{KS}_{n,d,s})_i$ is a polynomial of individual degree $\leq \mathrm{poly}(nd)$.*
2. *for every subset S of at most s monomials in n-variables with individual degree at most d, there exists an $\boldsymbol{\alpha} \in \mathbb{F}^m$ such that the polynomials $\{(\mathcal{G}^{KS}_{n,d,s}(\boldsymbol{\alpha}, \mathbf{t}))^{\mathbf{e}}\}_{\mathbf{e} \in S}$ are nonzero, distinct monomials in $\mathbf{t}$.*

The above generator is a slight variation of the construction given in [KS01], but it can be constructed from their techniques. For proof sketch see [FSS13, Theorem 2.3]. Next, we define total degree D independent monomial map from [FSS14].

Definition 2.8. *For some positive integers n and D, a polynomial map $\mathbf{g}(\mathbf{s}, \mathbf{t})$ from $\mathbb{F}^m \times \mathbb{F}^{m'}$ to $\mathbb{F}^n$ is called* total degree D independent monomial map *if there exists an $\boldsymbol{\alpha} \in \mathbb{F}^m$ such that the polynomials $\{\mathbf{g}(\boldsymbol{\alpha}, \mathbf{t})^{\mathbf{e}}\}_{|\mathbf{e}|_1 \leq D}$ are nonzero, distinct monomials in $\mathbf{t}$.*

In the following lemma, we describe a construction of total degree D independent monomial map using Klivans-Spielman generator.

Lemma 2.9. *Let n, d, D be positive integers. Let $|\mathbb{F}| \geq \mathrm{poly}(nd)$. Then, $\mathcal{G}^{KS}_{n,d,n^D}$ is a* $\mathrm{poly}(ndD)$*-explicit total degree D independent monomial map from $\mathbb{F}^m \times \mathbb{F}^m$ to $\mathbb{F}^n$ where $m = O(D)$.*

For proof see [FSS13, Lemma 6.4]. Next, we describe a polynomial map introduced by Shpilka and Volkovich [SV09]. It is a widely used tool in PIT and other related results [SV09, FSS14, SV15, MV17, KV21, MS21, ST21], and also crucial for proving our results.

Definition 2.10 (Shpilka-Volkovich generator [SV09]). *Fix a positive integer n and a set of n distinct elements $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}$. Let $L_i(t)$ be the ith Lagarange interpolation polynomial for the set $\mathcal{A}$. That is, $L_i(t)$ is an univariate polynomial of degree $n-1$ such that $L_i(\alpha_j) = \delta_{ij}$. Let $\mathbf{s} = (s_1, \ldots, s_k)$ and $\mathbf{t} = (t_1, \ldots, t_k)$. Then $\mathcal{G}^{SV}_{n,k}(\mathbf{s}, \mathbf{t})$ is the polynomial map from $\mathbb{F}^k \times \mathbb{F}^k$ to $\mathbb{F}^n$ defined as follows: for all $i \in [n]$*

$$(\mathcal{G}^{SV}_{n,k})_i = \sum_{j=1}^{k} L_i(s_j) t_j.$$

The above definition gives the following properties of Shpilka-Volkovich generator.

Observation 2.11. *Fix a set of k distinct elements $S = \{i_1, \ldots, i_k\} \subseteq [n]$. Let $\boldsymbol{\alpha} = (\alpha_{i_1}, \ldots, \alpha_{i_k})$. Then, for all $j \in [k]$, $(\mathcal{G}^{SV}_{n,k}(\boldsymbol{\alpha}, \mathbf{t}))_{i_j} = t_j$, and the other coordinates of $\mathcal{G}^{SV}_{n,k}(\boldsymbol{\alpha}, \mathbf{t})$ are zero. Furthermore, for all $i \in [n]$, the degree of the polynomial $(\mathcal{G}^{SV}_{n,k})_i$ is at most n.*

Using Shpilka-Volkovich generator, the following lemma describes a nonzeroness preserving variable reduction for polynomials having a "low-support" monomial with nonzero coefficient.

Lemma 2.12. *Let $f(\mathbf{x})$ be an n-variate polynomial over $\mathbb{F}$ such that there exists a monomial $\mathbf{x}^{\mathbf{e}}$ with nonzero coefficient in f and the support-size of $\mathbf{e}$ is at most ℓ. Then $f \circ \mathcal{G}^{SV}_{n,\ell} \neq 0$.*

Proof. Let $\{x_{i_1}, \ldots, x_{i_\ell}\}$ be the support set of the monomial $\mathbf{x}^{\mathbf{e}}$. Then, from Observation 2.11, there exists an $\boldsymbol{\alpha} \in \mathbb{F}^{\alpha}$ such that for all $j \in [\ell]$, $(\mathcal{G}^{SV}_{n,\ell}(\boldsymbol{\alpha}, \mathbf{t}))_{i_j} = t_j$ and the other coordinates of $\mathcal{G}^{SV}_{n,\ell}(\boldsymbol{\alpha}, \mathbf{t})$ are zero. This implies that $f(\mathcal{G}^{SV}_{n,\ell}(\boldsymbol{\alpha}, \mathbf{t})) \neq 0$, and therefore $f \circ \mathcal{G}^{SV}_{n,\ell} \neq 0$. $\square$

2.3 Algebraic independence

Suppose that $\mathcal{A} = \{g_1, \ldots, g_k\}$ is a set of n-variate polynomials over a field $\mathbb{F}$. We say that the set of polynomials $\mathcal{A}$ are *algebraically dependent* over $\mathbb{F}$ if there exists a nonzero k-variate polynomial $A(z_1, \ldots, z_k)$ over $\mathbb{F}$ such that $A(g_1, \ldots, g_k) = 0$. Otherwise, they are called *algebraically independent* (over $\mathbb{F}$). In the following lemma, we describe a well known criteria regarding algebraic independence of a set of linear polynomials.

Lemma 2.13. *Let $m \geq n$ be two positive integers. Let $L(\mathbf{x}) = (\ell_1, \ldots, \ell_n)$ be a linear transformation from $\mathbb{F}^m$ to $\mathbb{F}^n$ such that all ℓ_i's are linearly independent. Then, all ℓ_i's are also algebraically independent.*

Proof. For the sake of contradiction assume that all ℓ_i's are not algebraically independent. Then there exists a nonzero polynomial $A(z_1, \ldots, z_n)$ such that $A(L(\mathbf{x})) = A(\ell_1, \ldots, \ell_n) = 0$. Let $\mathbf{x} = (x_1, \ldots, x_m)$ and $A'(\mathbf{x}) = A(L(\mathbf{x}))$. Since all ℓ_i's are linearly independent, there exists a tuple of linear polynomials $U(\mathbf{x}) = (u_1, \ldots, u_m)$ and a subset $\{i_1, \ldots, i_n\}$ of $[m]$ such that for all $j \in [n]$,

$$\ell_j(U(\mathbf{x})) = x_{i_j}.$$

This implies that $A'(U(\mathbf{x})) = A(x_{i_1}, \ldots, x_{i_m}) = 0$ which is a contradiction. Therefore, all ℓ_i's are algebraically independent. $\square$

2.4 Various notions of rank concentration

We define various notions of rank concentration and show the relation between them. Suppose that $G(\mathbf{x})$ be an n-variate polynomial over the vector space $\mathbb{F}^k$. The *coefficient space* of G is the vector space spanned by the coefficient vectors of G.

Definition 2.14 (Rank Concentration). *We say that G has*

1. ℓ-support concentration *if there exists a set of monomials B such that the support-size of each monomial in B is at most ℓ and their coefficients form a basis for the coefficient space of G.*
2. ℓ-cone concentration *if there exists a set of monomials B such that the cone-size of each monomial in B is at most ℓ and their coefficients form a basis for the coefficient space of G.*
3. *a* cone-closed basis *if there is a cone-closed set of monomials B whose coefficients in G form a basis of the coefficient space of G.*

In the next lemma, we show that cone-closed basis notion subsumes the other two notions of rank concentration.

Lemma 2.15. *Let $G(\mathbf{x})$ be a polynomial in $\mathbb{F}[\mathbf{x}]^k$. Suppose that $G(\mathbf{x})$ has a cone-closed basis. Then, $G(\mathbf{x})$ has k-cone concentration and $\log k$-support concentration.*

Proof. Let B be a cone-closed set of monomials whose coefficients in G form a basis for the coefficient space of G. Since the cardinality of B is at most k and it is closed under submonomials, the cone-size of each monomial B is at most k. Therefore, G has k-cone concentration.

Let $m \in B$ and S be the support set of m. Let m' be the monomial defined as $m' = \prod_{i \in S} x_i$. Since B is cone-closed, every sub-monomial m' is also in B. Thus the cardinality of S can be at most $\log k$. Therefore, G has $\log k$-support concentration. $\square$

3 Achieving Cone-closed basis by shift

In this section, we show our rank concentration results for polynomials over the vector space $\mathbb{F}^k$. By $M_{n,d}$, we denote the set of n-variate monomials with individual degree at most d. We also use $M_{n,d}$ to denote the exponent vectors for those monomials since there is one-to-one correspondence between monomials and their exponent vectors. For any $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$ with $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$, $\binom{\mathbf{a}}{\mathbf{b}}$ denotes $\prod_{i=1}^n \binom{a_i}{b_i}$.

Let $G(\mathbf{x})$ be an n-variate polynomial over $\mathbb{F}^k$ with individual degree at most d. After shifting $G(\mathbf{x})$ by $\mathbf{z}$, the coefficients of the shifted polynomial $G'(\mathbf{x}) = G(\mathbf{x}+\mathbf{z})$ can be written as follows: for all $\mathbf{e} \in M_{n,d}$,

$$\mathrm{coef}_{\mathbf{x}^{\mathbf{e}}}(G') = \sum_{\mathbf{f} \in M_{n,d}} \binom{\mathbf{f}}{\mathbf{e}} \mathrm{coef}_{\mathbf{x}^{\mathbf{f}}}(G) \mathbf{z}^{\mathbf{f}-\mathbf{e}}.$$

The above equation can be written in matrix form as follows:

$$F'(\mathbf{z}) = W^{-1}(\mathbf{z}) T W(\mathbf{z}) F, \tag{1}$$

where

- F and $F'(\mathbf{z})$ are the matrices with entries from $\mathbb{F}$ and $\mathbb{F}[\mathbf{z}]$, respectively. The rows of both the matrices are indexed by the elements of $M_{n,d}$, and for any monomial $\mathbf{e} \in M_{n,d}$, the rows indexed by $\mathbf{e}$ in F and F' are $\mathrm{coef}_{\mathbf{x}^{\mathbf{e}}}(G)$ and $\mathrm{coef}_{\mathbf{x}^{\mathbf{e}}}(G')$, respectively.
- $W(\mathbf{z})$ be the diagonal matrix whose rows and columns are indexed by the elements of $M_{n,d}$ and for all $\mathbf{e} \in M_{n,d}$, $W(\mathbf{z})_{\mathbf{e},\mathbf{e}} = \mathbf{z}^{\mathbf{e}}$.
- T is a square matrix such that the rows and columns are indexed by $M_{n,d}$ and for all $\mathbf{e}, \mathbf{f} \in M_{n,d}$, $T_{\mathbf{e},\mathbf{f}} = \binom{\mathbf{f}}{\mathbf{e}}$. In the literature, T is known as *transfer matrix.*

In the following lemma, we recall a property of transfer matrix from [FGS18].

Lemma 3.1 (Lemma 18 [FGS18])**.** *Let $\mathbb{F}$ be a field of characteristic 0 or greater than d. Then, for every $B \subseteq M_{n,d}$, there exists a cone-closed set $A \subseteq M_{n,d}$ such that $T_{A,B}$ is full rank over $\mathbb{F}$.*

Next, we show our first rank concentration result. Informally, we prove that if $G(\mathbf{x})$ is shifted by algebraically independent polynomials, the new polynomial has a cone-closed basis.

Lemma 3.2. *Let $\mathbb{F}$ be a field of characteristic 0 or greater than d. Let $G(\mathbf{x}) \in \mathbb{F}^k[\mathbf{x}]$ be an n-variate polynomial with individual degree at most d. Let $\mathbf{g}(\mathbf{z}) = (g_1, \ldots, g_n)$ be a polynomial map from $\mathbb{F}^n$ to $\mathbb{F}^n$ such that all g_i's are algebraically independent. Then $G(\mathbf{x}+\mathbf{g})$ has a cone-closed basis over $\mathbb{F}(\mathbf{z})$.*

Proof. First we show that $G'(\mathbf{x}) = G(\mathbf{x}+\mathbf{z})$ has a cone-closed basis over $\mathbb{F}(\mathbf{z})$. This part of our proof closely follows the proof outline of [FGS18, Theorem 2]. From Equation 1, we know that the shifted polynomial $G(\mathbf{x}+\mathbf{z})$ yields the following matrix equation:

$$F'(\mathbf{z}) = W(\mathbf{z})^{-1} T W(\mathbf{z}) F.$$

Let k' be the rank of the matrix F. Then we divide our proof in two cases:

Case 1 ($k' < k$): We reduce this case to the other one where $k' = k$. Since the rank of F is k', there exists a $S \subseteq [k]$ of size k' such that $F_{M,S}$ is full rank where $M = M_{n,d}$. Let $G_S(\mathbf{x})$ and $G'_S(\mathbf{x})$ be the projections of $G(\mathbf{x})$ and $G'(\mathbf{x})$ on the coordinates indexed by S. Then $G'_S(\mathbf{x}) = G_S(\mathbf{x}+\mathbf{z})$. One can observe that for any set of monomials A, if their coefficients in $G_S(\mathbf{x})$ forms a basis for its coefficient space, then their coefficients in $G(\mathbf{x})$ also forms a basis for the coefficients space of $G(\mathbf{x})$. Similarly, this is also true between $G'_S(\mathbf{x})$ and $G'(\mathbf{x})$. Now from the case 2, $G'_S(\mathbf{x})$ has a cone-closed basis over $\mathbb{F}(\mathbf{z})$, that is, there exists a cone-closed set of monomials A such that their coefficients in $G'_S(\mathbf{x})$ forms a basis for its coefficient space. This implies that $G'(\mathbf{x})$ also has a cone-closed basis over $\mathbb{F}(\mathbf{z})$.

Case 2 ($k' = k$): The rows of F are indexed by the monomials in $M_{n,d}$. Fix a monomial ordering $\prec$ on the monomials in $\mathbf{z}$. For example, assume $\prec$ is the lexicographic monomial ordering. Then, from Lemma 2.2, we have a unique subset B of $M_{n,d}$ with the following properties: $\mathrm{rank}(F_{B,[k]}) = k$, and for every other subset C of $M_{n,d}$ with $\mathrm{rank}(F_{C,[k]}) = k$,

$$\prod_{\mathbf{e}\in B} \mathbf{z}^{\mathbf{e}} \prec \prod_{\mathbf{e}'\in C} \mathbf{z}^{\mathbf{e}'}.$$

Using Lemma 3.1, we have a cone-closed subset A of $M_{n,d}$ such that $T_{A,B}$ has full rank. Now

$$\det(F'(\mathbf{z})_{A,[k]}) = \det(W(\mathbf{z})_{A,A})^{-1} \cdot \det((TW(\mathbf{z})F)_{A,[k]}). \tag{2}$$

Applying Lemma 2.3, we get that

$$\det((TW(\mathbf{z})F)_{A,[k]}) = \sum_{C\in\binom{M_{n,d}}{k}} \det(T_{A,C})\det(F_{C,[k]}) \prod_{\mathbf{e}\in C} \mathbf{z}^{\mathbf{e}}. \tag{3}$$

For every $C \in \binom{M_{n,d}}{k} \setminus \{B\}$ such that $F_{C,[k]}$ is a full rank matrix, the following holds: $\prod_{\mathbf{e}\in B} \mathbf{z}^{\mathbf{e}} \prec \prod_{\mathbf{e}'\in C} \mathbf{z}^{\mathbf{e}'}$. Therefore, the coefficient of $\prod_{\mathbf{e}\in B} \mathbf{z}^{\mathbf{e}}$ in the above polynomial does not get cancelled by other monomials. Also, the coefficient of $\prod_{\mathbf{e}\in B} \mathbf{z}^{\mathbf{e}}$, $\det(T_{A,B})\det(T_{B,[k]}) \neq 0$. Therefore, the polynomial $\det((TW(\mathbf{z})F)_{A,[k]})$ is a nonzero polynomial in $\mathbf{z}$. Also, $\det(W(\mathbf{z})_{A,A})^{-1}$ is a nonzero polynomial in $\mathbf{z}$. Therefore, $\det(F'(\mathbf{z})_{A,[k]})$ is nonzero in $\mathbb{F}(\mathbf{z})$. This implies that $G'(\mathbf{x}) = G(\mathbf{x}+\mathbf{z})$ has a cone-closed basis over $\mathbb{F}(\mathbf{z})$.

Now we show that $G(\mathbf{x}+\mathbf{g})$ has a cone-closed basis over $\mathbb{F}(\mathbf{z})$. In Equation 2, since both $\det(W(\mathbf{z})_{A,A})$ and $\det((TW(\mathbf{z})F)_{A,[k]})$ are nonzero polynomials in $\mathbf{z}$. Therefore, after we evaluating them on any n algebraically independent polynomials, they will remain nonzero. Thus, $\det(F'(\mathbf{g})_{A,[k]})$ remains nonzero. This implies that for the polynomial $G(\mathbf{x}+\mathbf{g})$, the coefficients of the monomials in A form a cone-closed basis (over $\mathbb{F}(\mathbf{z})$) for its coefficient space. □

The above lemma combined Lemma 2.15 implies that the polynomial $G(\mathbf{x}+\mathbf{g})$ also has k-cone concentration over $\mathbb{F}(\mathbf{t})$. Here, we would like to mention that although the above rank concentration result is described in terms of cone-closed basis, to design our hitting sets, proving k-cone concentration property of $G(\mathbf{x}+\mathbf{g})$ is sufficient. The similar thing is also true for our next rank concentration result.

Lemma 3.3. *Let $\mathbb{F}$ be a field of characteristic zero or greater than d. Let $G(\mathbf{x})$ be an n-variate individual degree $\leq d$ polynomial over $\mathbb{F}^k$ such that the coefficients of all the monomials of total degree up to D spans the coefficient space of G. For some $N \geq n$, let $L(\mathbf{y}) = (\ell_1, \ldots, \ell_n)$ be a linear transformation from $\mathbb{F}^N$ to $\mathbb{F}^n$ such that all ℓ_i's are linearly independent. Let $\mathbf{g}(\mathbf{s},\mathbf{t})$ be a total degree*

Dk independent monomial map from $\mathbb{F}^m \times F^{m'}$ to $\mathbb{F}^N$. Then $G(\mathbf{x}+\mathbf{g}')$, where $\mathbf{g}' = uL \circ \mathbf{g}$, has a cone-closed basis over $F(u, \mathbf{s}, \mathbf{t})$.

Proof. First we study the shifted polynomial $G'(\mathbf{x}) = G(\mathbf{x} + u\mathbf{z})$. To do so, we revisit the proof of our Lemma 3.2. There we considered the lexicographic monomial ordering over the monomials in $\mathbf{z}$. Here we consider the *deg-lex* monomial ordering, that is, first order the monomials from lower degree to higher degree and then within each degree arrange them in lexicographic order. Like Equation 1, the matrix equation for the shifted polynomial $G'(\mathbf{x})$ will be

$$F'(u\mathbf{z}) = W^{-1}(u\mathbf{z})TW(u\mathbf{z})F, \tag{4}$$

that is scaling of each variable in Equation 1 by u. Applying Lemma 2.2, let B be the unique subset of $M_{n,d}$ such that the rows of F indexed by B form the least basis for the row-space of F with respect to the deg-lex monomial ordering. From the hypothesis of the lemma, there exists a subset $C \subseteq M_{n,d}$ such that the rows in F indexed by C forms a basis for the row-space of F (same as the coefficient space of G) and $\deg(C) = \sum_{\mathbf{e}\in C} |\mathbf{e}|_1 \leq Dk$. Therefore, $\deg(B)$ is also $\leq Dk$ since the rows indexed by B forms the least basis (with respect to deg-lex monomial ordering) for the row-space of F. As promised by Lemma 3.1, let A be a cone-closed subset of $M_{n,d}$ such that $T_{A,B}$ is full rank. Now we see how Equation 2 and 3 in the proof of Lemma 3.2 change here. Like Equation 2, we get

$$\det(F'(u\mathbf{z})_{A,[k]}) = \det(W(u\mathbf{z})_{A,A})^{-1} \cdot \det((TW(u\mathbf{z})F)_{A,[k]}) \tag{5}$$

and Equation 3 changes as follows:

$$\det((TW(u\mathbf{z})F)_{A,[k]}) = \sum_i \left(\sum_{C \in \binom{M_{n,d}}{k} : \deg(C)=i} \det(T_{A,C}) \det(F_{C,[k]}) \prod_{\mathbf{e}\in C \mathbf{z}^{\mathbf{e}}} \right) u^i. \tag{6}$$

Since B is the least basis (with respect to deg-lex monomial ordering), the coefficient of $u^{\deg(B)}$ is a nonzero degree $\deg(B)$ homogeneous polynomial in $\mathbf{z}$. Thus, $\det(F'(u\mathbf{z})_{A,[k]})$ is a nonzero-polynomial in $(u, \mathbf{z})$. This implies the coefficients of the monomials in A is a cone-close basis for $G(\mathbf{x} + u\mathbf{z})$. For $G(\mathbf{x} + uL)$, the polynomial $\det((TW(uL)F)_{A,[k]})$ looks like the following:

$$\det((TW(uL)F)_{A,[k]}) = \sum_i \left(\sum_{C \in \binom{M_{n,d}}{k} : \deg(C)=i} \det(T_{A,C}) \det(F_{A,C}) \prod_{\mathbf{e}\in C} L^{\mathbf{e}} \right) u^i.$$

Since all ℓ_i's are linearly independent, from Lemma 2.13, they are also algebraically independent. Therefore, the coefficient of $u^{\deg(B)}$ in $\det((TW(uL)F)_{A,[k]})$ is also a nonzero degree $\deg(B)$ homogeneous polynomial in $\mathbf{y}$. Also, $\deg(B) \leq Dk$. Therefore, after substituting $\mathbf{z}$ by $L \circ \mathbf{g}$ in Equation 6, we get $\det((TW(\mathbf{g}')F)_{A,[k]})$ which is a nonzero polynomial in $(u, \mathbf{s}, \mathbf{t})$. Since $\det(W(\mathbf{g}'))$ is also a nonzero polynoimal in $(u, \mathbf{s}, \mathbf{t})$, $\det(F'(\mathbf{g}')_{A,[k]})$ is nonzero in $\mathbb{F}(u, \mathbf{s}, \mathbf{t})$. This implies that $G(\mathbf{x} + \mathbf{g}')$ has a cone-closed basis over $\mathbb{F}(u, \mathbf{s}, \mathbf{t})$. ∎

4 Hitting set for orbit of *any-order* ROABPs

In this section, we describe our hitting set for the orbit of *any-order* ROABPs. As mentioned earlier, the notion of low-cone concentration plays an important role is designing our hitting sets.

We begin by showing that for w-width n-variate *any-order* ROABPs, w^2-cone concentration can be established by showing w^2-cone concentration for every $\Omega(\log w)$-size subset of variables.

Lemma 4.1. *Let $\mathbb{F}$ be a field of characteristic 0 or greater than d. Let $G(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{w\times w}$ be an n-variate polynomial over $\mathbb{F}$ with individual degree at most d and computed by a w-width any-order ROABP. Let $\ell = \lfloor 2\log w\rfloor + 1$. Let $\mathbf{g}(\mathbf{t}) = (g_1, \ldots, g_n)$ be a polynomial map such that for all $S \subseteq [n]$ of size ℓ, the polynomials $\{g_i \mid i \in S\}$ are algebraically independent. Then $G(\mathbf{x} + \mathbf{g})$ has w^2-cone concentration over $\mathbb{F}(\mathbf{t})$.*

Proof. Let $G' = G(\mathbf{x} + \mathbf{g})$. For every $\mathbf{a} \in M_{n,d}$, the coefficient of $\mathbf{x}^{\mathbf{a}}$ in G' is same as the evaluation of $\partial_{\mathbf{x}^{\mathbf{a}}}(G)$ at $\mathbf{g}$. Consider some derivative $\partial_{\mathbf{x}^{\mathbf{a}}}(G)$ for $\mathbf{a} \in M_{n,d}$. We show that its evaluation at $\mathbf{g}$ is in $\mathbb{F}(\mathbf{t})$-linear span of the derivatives of cone-size $\leq w^2$, evaluated at $\mathbf{g}$. If the cone-size of $\mathbf{x}^{\mathbf{a}}$ is already $\leq w^2$, it is trivial. Therefore, assume that the cone-size of $\mathbf{x}^{\mathbf{a}}$ is greater than w^2. We can write $\mathbf{x}^{\mathbf{a}}$ as $\mathbf{y}^{\mathbf{b}}\mathbf{z}^{\mathbf{c}}$ over two disjoint sets of variables such that the cone-size of $\mathbf{b}$ is greater than w^2 but the support-size of $\mathbf{b}$ is $\leq \ell$. If the support-size of $\mathbf{a} \leq \ell$, take S as the support of $\mathbf{a}$. Otherwise, take S as some subset of the support of $\mathbf{a}$ such that $|S| = \ell$. Then, take $\mathbf{y}^{\mathbf{b}} = \prod_{i\in S} x_i^{a_i}$ and $\mathbf{z}^{\mathbf{c}} = \prod_{i\in \bar{S}} x_i^{a_i}$. One can observe that in both the cases the cone-size of $\mathbf{b}$ is greater than w^2, but the support-size of $\mathbf{b}$ is $\leq \ell$.

Since G is computed by a w-width *any-order* ROABP, $G(\mathbf{x})$ can be written as

$$G(\mathbf{x}) = M(\mathbf{y})N(\mathbf{z})$$

such that both M and N are computed by w-width *any-order* ROABPs. After shifting G by $\mathbf{g}$, the new polynomial $G'(\mathbf{x})$ becomes

$$M(\mathbf{y} + \mathbf{g}|_{\mathbf{y}})N(\mathbf{z} + \mathbf{g}|_{\mathbf{z}}),$$

where $\mathbf{g}|_{\mathbf{y}}$ and $\mathbf{g}|_{\mathbf{z}}$ denotes the restriction of $\mathbf{g}$ to $\mathbf{y}$ and $\mathbf{z}$, respectively. From our choice of $\mathbf{y}$, $M(\mathbf{y})$ is a polynomial (over $\mathbb{F}^{w\times w}$) of at most ℓ variables. Also, the hypothesis of our lemma ensures that the polynomials in $\mathbf{g}|_{\mathbf{y}}$ are algebraically independent. Therefore, from Lemma 3.2, $M(\mathbf{y} + \mathbf{g}|_{\mathbf{y}})$ has a cone-closed basis over $\mathbb{F}(\mathbf{t})$. Applying Lemma 2.15, we get that $M(\mathbf{y} + \mathbf{g}|_{\mathbf{y}})$ has also w^2-cone concentration over $\mathbb{F}(\mathbf{t})$. This implies that

$$\partial_{\mathbf{y}^{\mathbf{b}}}(M)(\mathbf{g}|_{\mathbf{y}}) \in \mathrm{span}_{\mathbb{F}(\mathbf{t})}\left\{\partial_{\mathbf{y}^{\mathbf{e}}}(M)(\mathbf{g}|_{\mathbf{y}}) \mid \text{cone-size}(\mathbf{e}) \leq w^2\right\}.$$

Since $\partial_{\mathbf{x}^{\mathbf{a}}}(G) = \partial_{\mathbf{y}^{\mathbf{b}}}(M)\partial_{\mathbf{z}^{\mathbf{c}}}(N)$,

$$\begin{aligned}
\partial_{\mathbf{x}^{\mathbf{a}}}(G)(\mathbf{g}) &= \partial_{\mathbf{y}^{\mathbf{b}}}(M)(\mathbf{g}|_{\mathbf{y}})\partial_{\mathbf{z}^{\mathbf{c}}}(N)(\mathbf{g}|_{\mathbf{z}}) \\
&\in \mathrm{span}_{\mathbb{F}(\mathbf{t})}\left\{\partial_{\mathbf{y}^{\mathbf{e}}}(M)(\mathbf{g}|_{\mathbf{y}})\partial_{\mathbf{z}^{\mathbf{c}}}(N)(\mathbf{g}|_{\mathbf{z}}) \mid \text{cone-sie}(\mathbf{e}) \leq w^2\right\} \\
&\in \mathrm{span}_{\mathbb{F}(\mathbf{t})}\left\{\partial_{\mathbf{x}^{\mathbf{e}+\mathbf{c}}}(G)(\mathbf{g}) \mid \text{cone-sie}(\mathbf{e}+\mathbf{c}) \leq w^2 \cdot \text{cone-size}(\mathbf{c})\right\} \\
&\in \mathrm{span}_{\mathbb{F}(\mathbf{t})}\left\{\partial_{\mathbf{x}^{\mathbf{f}}}(M)(\mathbf{g}) \mid \text{cone-sie}(\mathbf{f}) < \text{cone-size}(\mathbf{a})\right\}
\end{aligned}$$

Now repeatedly applying the above procedure for all the monomials of cone-size greater than w^2 (by properly picking a partition $\mathbf{x} = \mathbf{y} \sqcup \mathbf{z}$), we can show that for every monomial $\mathbf{x}^{\mathbf{a}}$, $\partial_{\mathbf{x}^{\mathbf{a}}}(G)(\mathbf{g})$ is in $\mathbb{F}(\mathbf{t})$-linear span of the derivatives (of G) of cone-size $\leq w^2$, evaluated at $\mathbf{g}$. Therefore, $G(\mathbf{x} + \mathbf{g})$ has w^2-cone concentration over $\mathbb{F}(\mathbf{t})$.

$\square$

Our next lemma, using Shpilka-Volkovick generator (Definition 2.10), gives the construction of a polynomial map which satisfies the condition of the above lemma.

Lemma 4.2. *Let $L(\mathbf{x}) = (\ell_1, \ldots, \ell_n)$ be an invertible linear transformation from $\mathbb{F}^n$ to $\mathbb{F}^n$. Let $\mathbf{b}$ be a point in $\mathbb{F}^n$. For some $k \leq n$, let $\mathbf{g}(\mathbf{s}, \mathbf{t}) = (g_1, \ldots, g_n)$ be the polynomial map from $\mathbb{F}^k \times \mathbb{F}^k$ to $\mathbb{F}^n$, defined as $\mathbf{g} = L \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b}$. Then for all $S \subseteq [n]$ of size k, the polynomials $\{g_i \mid i \in S\}$ are algebraically independent.*

Proof. Let S be a subset of $[n]$ of size k. Let $\mathbf{g}|_S$, $L|_S$, $\mathbf{b}|_S$ be the restrictions of $\mathbf{g}$, L and $\mathbf{b}$, respectively, to S. Then $\mathbf{g}|_S = L|_S \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b}|_S$. For the sake of contradiction, assume that the polynomials $\{g_i \mid i \in S\}$ are not algebraically independent. Then, there exists a nonzero polynomial $A(t_1, \ldots, t_k)$ such that $A(\mathbf{g}|_S) = 0$. This implies that the nonzero polynomial $A'(\mathbf{t}) = A(\mathbf{t} + \mathbf{b}|_S)$ evaluated at $\mathbf{g}'(\mathbf{y}, \mathbf{z}) = L|_S \circ \mathcal{G}^{SV}_{n,k}$ is also zero. For every $A \subseteq [n]$ and $i \in [n]$, let $\mathbf{x}_A$ denotes the projection of $\mathbf{x}$ on the coordinates indexed by A and ℓ_{iA} denotes the linear polynomial we get from ℓ_i after assigning all the variables in $\mathbf{x}_{\bar{A}}$ to zero. Since all the coordinates in $L|_S$ are linearly independent, there exists a $A \subseteq [n]$ of size k such that $L|_S(\mathbf{x}_A) = (\ell_{iA})_{i \in S}$ is an invertible linear transformation (in $\mathbf{x}_A$) from $\mathbb{F}^k$ to $\mathbb{F}^k$. From Observation 2.11, there exists an $\boldsymbol{\alpha} \in \mathbb{F}^k$ such that the set of polynomials $\{(\mathcal{G}^{SV}_{n,k}(\boldsymbol{\alpha}, \mathbf{t}))_i \mid i \in A\}$ is same as $\{t_1, \ldots, t_k\}$, that is the set of $\mathbf{t}$ variables, and the other coordinates are zero. Hence,

$$\begin{aligned} \mathbf{g}'(\boldsymbol{\alpha}, \mathbf{t}) &= L|_S \circ \mathcal{G}^{SV}_{n,k}(\boldsymbol{\alpha}, \mathbf{t}) \\ &= (\ell_{iA}(\mathbf{t}))_{i \in S}. \end{aligned}$$

From Lemma 2.13, the polynomials $\{(\mathbf{g}'(\boldsymbol{\alpha}, \mathbf{t}))_i \mid i \in [k]\}$ are algebraically independent. Therefore, $A'(\mathbf{g}'(\boldsymbol{\alpha}, \mathbf{t}))$ is nonzero. Hence $A'(\mathbf{g}')$ is also nonzero which is a contradiction. This completes our proof. □

Combining the above two lemmas, we get the following.

Corollary 4.3. *Let $\mathbb{F}$ be a field of characteristic 0 or greater than d. Let $G(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{w \times w}$ be an n-variate polynomial with individual degree at most d and computed by a width w any-order ROABP. Let $L(\mathbf{x})$ be an invertible linear transformation from $\mathbb{F}^n$ to $\mathbb{F}^n$ and $\mathbf{b}$ be a point in $\mathbb{F}^n$. Let $k = \lfloor 2 \log w \rfloor + 1$ and $\mathbf{g} = L \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b}$. Then $G(\mathbf{x} + \mathbf{g})$ has w^2-cone concentration over $F(\mathbf{s}, \mathbf{t})$.*

Proof. Let $\mathbf{g}(\mathbf{s}, \mathbf{t}) = (g_1, \ldots, g_n)$. From Lemma 4.2, for every subset $S \subseteq [n]$ of size k, the polynomials $\{g_i \mid i \in S\}$ are algebraically independent. Therefore, using Lemma 4.1, we get that $G(\mathbf{x} + \mathbf{g})$ has w^2-cone concentration over $\mathbb{F}(\mathbf{s}, \mathbf{t})$. □

Now we describe the construction of our hitting set for the orbit of *any-order* ROABPs.

Proof of Theorem 1.1. Let $f(\mathbf{x})$ be an n-variate individual degree $\leq d$ polynomial which is in the orbit of width w *any-order* ROABPs. Then, there exists an n-variate individual degree $\leq d$ polynomial $G(\mathbf{y}) \in \mathbb{F}^{w \times w}[\mathbf{y}]$ computed by a width w *any-order* ROABP, an invertible linear transformation $L(\mathbf{x})$ from $\mathbb{F}^n$ to $\mathbb{F}^n$ and a point $\mathbf{b} \in \mathbb{F}^n$ such that

$$f(\mathbf{x}) = \mathbf{a}^T \cdot G(L + \mathbf{b}) \cdot \mathbf{c},$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{F}^n$. Let $\mathbf{g}(\mathbf{s}, \mathbf{t}) = L \circ \mathcal{G}^{SV}_{n,k} + \mathbf{b}$ where $k = \lfloor 2 \log w \rfloor + 1$, and let

$$h(\mathbf{y}) = \mathbf{a}^T \cdot G(\mathbf{y} + \mathbf{g}) \cdot \mathbf{c}.$$

This implies that

$$f'(\mathbf{x}) = f(\mathbf{x} + \mathcal{G}^{SV}_{n,k}) = h(L(\mathbf{x})). \tag{7}$$

From Corollary 4.3, $G(\mathbf{y}+\mathbf{g})$ has w^2-cone concentration over $\mathbb{F}(\mathbf{s},\mathbf{t})$. This implies that there exists a monomial $\mathbf{y}^{\mathbf{e}}$ in h with cone-size $\leq w^2$ such that $\mathrm{coef}_{\mathbf{y}^{\mathbf{e}}}(h)$ is nonzero. For a monomial of cone-size $\leq w^2$, its total degree is less than w^2 and the support-size is $\leq \log w^2$. Since the individual degree of each variable in $G(\mathbf{y})$ is at most d, Therefore, the degree of $\mathbf{y}^{\mathbf{e}}$ is $\leq \ell$ where $\ell = \min\{w^2, 2d\log w\}$. Hence, $\mathrm{hom}_{\leq \ell}(h(\mathbf{y}))$ is a nonzero polynomial in $\mathbf{y}$. Since

$$\mathrm{hom}_{\leq \ell}(h(L(\mathbf{x}))) = (\mathrm{hom}_{\leq \ell}(h))(L(\mathbf{x})),$$

from Lemma 2.13, $\mathrm{hom}_{\leq \ell}(h(L(\mathbf{x})))$ is a nonzero polynomial. Therefore, from Equation 7, $\mathrm{hom}_{\leq \ell}(f'(\mathbf{x}))$ is a nonzero polynomial over $\mathbb{F}(\mathbf{s},\mathbf{t})$. This implies that there exists a monomial $\mathbf{x}^{\mathbf{e}}$ of support-size $\leq \ell$ such that its coefficient in f' is nonzero. Thus, from Lemma 2.12, $f'(\mathcal{G}^{SV}_{n,\ell}) = f(\mathcal{G}^{SV}_{n,k+\ell})$ is a $k+\ell$-variate nonzero polynomial over $\mathbb{F}$. The total degree of f is at most nd, and from Observation 2.11, the individual degree of each coordinate of $\mathcal{G}^{SV}_{n,k+\ell}$ is at most n. Also, $\mathcal{G}^{SV}_{n,k+\ell}$ is $\mathrm{poly}(ndw)$-explicit. Thus, from Observation 2.6, f has a hitting set computable in time $(ndw)^{O(\ell)}$. $\square$

5 Hitting Set for orbit of ROABPs

Here, we discuss the construction of our hitting set for the orbit of ROABPs. Towards that, first we need to construct some polynomial map which helps us in achieving low-cone concentration for ROABPs. At this step, we also have to be more careful as we are dealing with the orbit of ROABPs. Lemma 5.2 describes inductive construction of a polynomial map, by taking sum of logarithmically many variable disjoint copies of total degree D independent monomial maps (Definition 2.8) for some small D, such that the following holds: by shifting its composition with any invertible affine transformation we can achieve low-cone concentration for ROABPs. We begin by showing how to achieve cone-closed basis for the product of two polynomials in disjoint set of variables with the property that each polynomial also has a cone-closed basis.

Lemma 5.1. *Let $\mathbf{y}$ and $\mathbf{z}$ be two disjoint set of variables. Let $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{w\times w}$ and $H(\mathbf{z}) \in \mathbb{F}[\mathbf{z}]^{w\times w}$ be two n-variate individual degree $\leq d$ polynomials such that both have cone-closed bases. Let $L(\mathbf{x}) = (\ell_1, \ldots, \ell_{|\mathbf{y}\sqcup\mathbf{z}|})$ be a linear transformation from $\mathbb{F}^{|\mathbf{x}|}$ to $\mathbb{F}^{|\mathbf{y}|}\times\mathbb{F}^{|\mathbf{z}|}$ such that all ℓ_is are linearly independent. Let $D = 2w^2\cdot\min\{w^2, 2d\log w\}$, $\mathbf{g}(\mathbf{s},\mathbf{t})$ be a total degree D independent monomial map form $\mathbb{F}^{|\mathbf{s}|}\times F^{|\mathbf{t}|}$ to $\mathbb{F}^{|\mathbf{x}|}$, and $\mathbf{g}' = uL\circ\mathbf{g}$. Then $G(\mathbf{y}+\mathbf{g}'|_{\mathbf{y}})H(\mathbf{z}+\mathbf{g}'|_{\mathbf{z}})$ has a cone-closed basis over $F(u,\mathbf{s},\mathbf{t})$, where $\mathbf{g}'|_{\mathbf{y}}$ and $\mathbf{g}'|_{\mathbf{z}}$ are the restrictions of $\mathbf{g}'$ over $\mathbf{y}$ and $\mathbf{z}$, respectively.*

Proof. Let B_1 and B_2 be the set of monimials (in $\mathbf{y}$ and $\mathbf{z}$, respectively) such that their coefficients form cone-closed bases for the coefficient space of G and H, respectively. Let

$$B_1B_2 = \{m_1m_2 \mid m_1 \in B_1 \text{ and } m_2 \in B_2\}.$$

We show that the coefficients of the monomials in B_1B_2 span the coefficient space of GH. Let m be a monomial in $\mathbf{y}\sqcup\mathbf{z}$. Since $\mathbf{y}$ and $\mathbf{z}$ are disjoint set of variables, the monomial m can be uniquely written as a product $m_{\mathbf{y}}m_{\mathbf{z}}$ where $m_{\mathbf{y}}$ and $m_{\mathbf{z}}$ are monomials in $\mathbf{y}$ and $\mathbf{z}$, respectively. Also, $\mathrm{coef}_m(GH)$ is same as $\mathrm{coef}_{m_{\mathbf{y}}}(G)\cdot\mathrm{coef}_{m_{\mathbf{z}}}(H)$. Now

$$\begin{aligned}
\mathrm{coef}_m(GH) &= \mathrm{coef}_{m_{\mathbf{y}}}(G)\cdot\mathrm{coef}_{m_{\mathbf{z}}}(H)\\
&\in \mathrm{span}_{\mathbb{F}}\left\{\mathrm{coef}_{m_1}(G) \mid m_1\in B_1\right\}\cdot\mathrm{span}_{\mathbb{F}}\left\{\mathrm{coef}_{m_2}(H) \mid m_2\in B_2\right\}\\
&\in \mathrm{span}_{\mathbb{F}}\left\{\mathrm{coef}_{m_1}(G)\cdot\mathrm{coef}_{m_2}(H) \mid m_1\in B_1,\ m_2\in B_2\right\}\\
&\in \mathrm{span}_{\mathbb{F}}\left\{\mathrm{coef}_{m}(GH) \mid m\in B_1B_2\right\}.
\end{aligned}$$

Since B_1 and B_2 are cone-closed sets, the cone-size of every monomial in $B_1 \cup B_2$ is at most w^2. This implies that the degree of every monomial in $B_1 \cup B_2$ is at most w^2 and the support-size is at most $2 \log w$. Since both G and H are polynomials of individual degree at most d, the degree of every monomial in $B_1 B_2$ is at most $k = 2 \cdot \min\{w^2, 2d \log w\}$. Also, the coefficients of the monomials in $B_1 B_2$ spans the coefficient space of GH. This implies that the coefficients of monomials in GH of degree at most k spans its coefficient space. From the hypothesis, $\mathbf{g}(\mathbf{s}, \mathbf{t})$ is a total degree $D = kw^2$ independent monomial map. Therefore, from Lemma 3.3, $G(\mathbf{y} + \mathbf{g}'|_{\mathbf{y}})H(\mathbf{z} + \mathbf{g}'|_{\mathbf{z}})$ has a cone-closed basis over $F(u, \mathbf{s}, \mathbf{t})$. □

Applying the above lemma repeatedly, the next one gives the construction of a polynomial map which helps us to achieve low-cone concentration for ROABPs.

Lemma 5.2. *Let $n \geq 0$, $N = 2^n$ and $d, w \geq 1$. Let $D = 2w^2 \cdot \min\{w^2, 2d \log w\}$. Let $\mathbf{g}(\mathbf{s}, \mathbf{t})$ be a total degree D independent monomial map from $\mathbb{F}^m \times \mathbb{F}^{m'}$ to $\mathbb{F}^N$. Let $\mathbf{t}_0 = (t, t^2, \ldots, t^N)$. Let*

$$\mathcal{G}_{n,d,w} = \mathbf{t}_0 + \sum_{i=1}^{n} u_i \mathbf{g}(\mathbf{s}_i, \mathbf{t}_i),$$

where all $\mathbf{s}_i$'s and $\mathbf{t}_i$'s are disjoint set of variables.

Let π be permutation on $[N]$. Let $F(\mathbf{x}) = \prod_{i=1}^{N} M_i(x_{\pi(i)})$ such that each $M_i(x_{\pi(i)})$ is a polynomial in $\mathbb{F}[x_{\pi(i)}]^{w \times w}$ with individual degree at most d. Then for every invertible linear transformation $L(\mathbf{x})$ from $\mathbb{F}^N$ to $\mathbb{F}^N$ and $\mathbf{b} \in \mathbb{F}^N$, $F(\mathbf{x} + \mathbf{b} + L \circ \mathcal{G}_{n,d,w})$ has a cone-closed basis over the field $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i \in [n]})$.

Proof. Let $L(\mathbf{x}) = (\ell_1, \ldots, \ell_N)$. Let $\mathbf{h}_0 = \mathbf{b} + L(\mathbf{t}_0)$, and for all $k \in [n]$,

$$\mathbf{h}_k = \mathbf{h}_{k-1} + u_k L \circ \mathbf{g}(\mathbf{t}_k, \mathbf{s}_k).$$

Then $\mathbf{h}_n = \mathbf{b} + L \circ \mathcal{G}_{n,d,w}$. For all $1 \leq i \leq j \leq N$, let

$$F_{ij}[\mathbf{x}] = \prod_{r=i}^{j} M_r(x_{\pi(r)}).$$

Using induction, we show that for all $k \in \{0, 1, \ldots, n\}$ and $i, j \in [n]$ with $j - i + 1 = 2^k$, $F_{ij}[\mathbf{x} + \mathbf{h}_k]$ has a cone-closed basis over $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i \in [k]})$.

For $k = 0$: Let $\mathbf{b} = (b_1, \ldots, b_N)$. We need to show that for all $i \in [N]$, $M_i(x_{\pi(i)} + \ell_{\pi(i)}(\mathbf{t}_0) + b_{\pi(i)})$ has a cone-closed basis over $\mathbb{F}(t)$. Since $L(\mathbf{x})$ is an invertible linear transformation, each ℓ_i is a nonzero linear polynomial over $\mathbf{x}$. Therefore, $\ell_i(\mathbf{t}_0)$ is a nonzero polynomial in t. This implies that each $\ell_i(\mathbf{t}_0) + b_i$ is an algebraically independent polynomial over $\mathbb{F}$. Hence, using Lemma 3.1, for all $i \in [N]$, $M_i(x_{\pi(i)} + \ell_{\pi(i)}(\mathbf{t}_0) + b_{\pi(i)})$ has a cone-closed basis over $\mathbb{F}(t)$.

For $k > 0$: Let $i, j \in [N]$ such that $j - i + 1 = 2^k$. Let $\mathbf{y}$ and $\mathbf{z}$ be partition of the variables $(x_{\pi(i)}, \ldots, x_{\pi(j)})$ into two equal halves such that they respect the permutation π. Then $F_{ij}[\mathbf{x}]$ can be written as $G(\mathbf{y})H(\mathbf{z})$ where $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{w \times w}$ and $H(\mathbf{z}) \in \mathbb{F}[\mathbf{z}]^{w \times w}$. From the induction hypothesis, we know that both

$$G'(\mathbf{y}) = G(\mathbf{y} + \mathbf{h}_{k-1}|_{\mathbf{y}}) \text{ and } H'(\mathbf{z}) = H(\mathbf{z} + \mathbf{h}_{k-1}|_{\mathbf{z}})$$

have cone-closed bases over $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i\in[k-1]})$. Let $F'_{ij}(\mathbf{x}) = G'(\mathbf{y})H'(\mathbf{z})$. Then, using Lemma 5.1,

$$F_{ij}(\mathbf{x} + \mathbf{h}_k) = F'_{ij}(\mathbf{x} + u_k L \circ \mathbf{g}(\mathbf{s}_k, \mathbf{t}_k))$$

has a cone-closed basis over $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i\in[k]})$. This completes our proof. $\square$

From Lemma 2.9, using Klivans-Spielman generator (Lemma 2.7), we can construct a total degree D independent monomial map. Therefore, Klivans-Spielman generator combined with the above lemma we get the following corollary.

Corollary 5.3. *Let $n \geq 0$, $N = 2^n$ and $d, w \geq 1$. Let $D = 2w^2 \cdot \min\{w^2, 2d \log w\}$. Let*

$$\mathcal{G}'_{n,d,w} = \mathbf{t}_0 + \sum_{i=1}^{n} u_i \mathcal{G}^{KS}_{N,d,N^D}(\mathbf{s}_i, \mathbf{t}_i). \tag{8}$$

Let π be permutation on $[N]$. Let $F(\mathbf{x}) = \prod_{i=1}^{N} M_i(x_{\pi(i)})$ such that each $M_i(x_{\pi(i)})$ is a polynomial in $\mathbb{F}[x_{\pi(i)}]^{w\times w}$ with individual degree at most d. Then,

1. *for every invertible linear tansformation $L(\mathbf{x})$ from $\mathbb{F}^N$ to $\mathbb{F}^N$ and $\mathbf{b} \in \mathbb{F}^N$, the polynomial $F(\mathbf{x} + \mathbf{b} + L \circ \mathcal{G}'_{n,d,w})$ has a cone-closed basis over the field $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i\in[n]})$.*
2. *$\mathbf{b} + \mathcal{G}'_{n,d,w}$ is a polynomial map from $\mathbb{F} \times (\mathbb{F} \times \mathbb{F}^m \times \mathbb{F}^m)^n$ to $\mathbb{F}^N$ where $m = O(D)$.*
3. *$\mathcal{G}'_{n,d,w}$ is* poly(dND)*-explicit polynomial map and its each coordinate is a polynomial of individual degree at most* poly(dN).

Proof. From Lemma 2.9, $\mathcal{G}^{KS}_{N,d,N^D}(\mathbf{s}, \mathbf{t})$ is a poly(NDd)-explicit total degree D independent monomial map from $\mathbb{F}^m \times \mathbb{F}^m$ to $\mathbb{F}^N$, where $m = O(D)$. Also, each coordinate of $\mathcal{G}^{KS}_{N,d,N^D}$ is a polynomial of individual degree at most poly(dN). Now this combined with Lemma 5.2 prove the above corollary. $\square$

Now we describe the construction of hitting set for orbit of ROABPs.

Proof of Theorem 1.2. Let $f(\mathbf{x})$ be an n-variate individual degree $\leq d$ polynomial which is in the orbit of width w ROABPs. Then, there exists an n-variate individual degree $\leq d$ polynomial $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{w\times w}$ computed by a w-width ROABP, an invertible linear transformation $L(\mathbf{x})$ from $\mathbb{F}^n$ to $\mathbb{F}^n$ and $\mathbf{b} \in \mathbb{F}^n$ such that

$$f(\mathbf{x}) = \mathbf{a}^T \cdot G(L(\mathbf{x}) + \mathbf{b}) \cdot \mathbf{c},$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{F}^n$. Let $D = 2w^2 \cdot \min\{w^2, d \log w^2\}$. Let $\mathcal{G}'_{\lceil \log n\rceil,d,w}$ be defined as Equation 8 in Corollary 5.3, that is

$$\mathcal{G}'_{\lceil \log n\rceil,d,w} = \mathbf{t}_0 + \sum_{i=1}^{\lceil \log n\rceil} u_i \mathcal{G}^{KS}_{n,d,n^D}(\mathbf{s}_i, \mathbf{t}_i),$$

where $\mathbf{t}_0 = (t, t^2, \ldots, t^n)$. Then, $\mathcal{G}'_{\lceil \log n\rceil,d,w}$ is a polynomial map from $\mathbb{F} \times (\mathbb{F} \times \mathbb{F}^m \times F^m)^{\lceil \log n\rceil}$ to $\mathbb{F}^n$ where $m = O(D)$. This implies that the number of variables used in $\mathcal{G}'_{\lceil \log n\rceil,d,w}$ is $O(D \log n)$. Let

$$g(\mathbf{y}) = \mathbf{a}^T \cdot G(\mathbf{y} + \mathbf{b} + L \circ \mathcal{G}'_{\lceil \log n\rceil,d,w}) \cdot \mathbf{c}.$$

Then

$$f'(\mathbf{x}) = f(\mathbf{x} + \mathcal{G}'_{\lceil \log n\rceil,d,w}) = g(L(\mathbf{x})). \tag{9}$$

From Corollary 5.3,

$$G'(\mathbf{y}) = G(\mathbf{y} + \mathbf{b} + L \circ \mathcal{G}'_{\lceil \log n \rceil, d, w})$$

has a cone-closed basis over $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i \in [\lceil \log n \rceil]})$. Therefore, from Lemma 2.15, $G'(\mathbf{y})$ has also w^2-cone concentration. This implies that $g(\mathbf{y})$ has a monomial of nonzero coefficient and its cone-size is at most w^2. For every monomial of cone-size at most w^2, its degree is also at most w^2 and its support-size is at most $2 \log w$. Therefore, for every monomial of cone-size $\leq w^2$ and individual degree $\leq d$, its degree is at most $k = \min\{w^2, 2d \log w\}$. Therefore, $\mathrm{hom}_{\leq k}(g(\mathbf{y}))$ is a nonzero polynomial in $\mathbf{y}$ over $\mathbb{F}(t, (u_i, \mathbf{s}_i, \mathbf{t}_i)_{i \in [\lceil \log n \rceil]})$. Since

$$\mathrm{hom}_{\leq k}(g(L(\mathbf{x}))) = (\mathrm{hom}_{\leq k}(g))(L(\mathbf{x})),$$

from Lemma 2.13, $\mathrm{hom}_{\leq k}(g(L(\mathbf{x})))$ is also nonzero polynomial. Therefore, from Equation 9, $\mathrm{hom}_{\leq k}(f'(\mathbf{x}))$ is also a nonzero polynomial. This implies that there exists a monomial $\mathbf{x}^{\mathbf{e}}$ of support-size at most k such that $\mathrm{coef}_{\mathbf{x}^{\mathbf{e}}}(f')$ is nonzero. Thus, from Lemma 2.12,

$$f'(\mathcal{G}^{SV}_{n,k}) = f(\mathcal{G}^{SV}_{n,k} + \mathcal{G}'_{\lceil \log n \rceil, d, w})$$

is a nonzero polynomial. Let $\mathcal{G} = \mathcal{G}^{SV}_{n,k} + \mathcal{G}'_{\lceil \log n \rceil, d, w}$. Then, $\mathcal{G}$ is a polynomial map in $O(kw^2 \log n)$ many variables and the individual degree of each coordinate is at most $\mathrm{poly}(ndw)$. Since both $\mathcal{G}^{SV}_{n,k}$ and $\mathcal{G}'_{\lceil \log n \rceil, d, w}$ both are $\mathrm{poly}(ndw)$-explicit, $\mathcal{G}$ is also $\mathrm{poly}(ndw)$-explicit. Thus, applying Observation 2.6, we have a hitting set for f computable in time $(ndw)^{O(\ell)}$ where $\ell = (w^2 \log n) \cdot \min\{w^2, d \log w^2\}$. $\square$

6 Conclusion

In this paper, we studied the hitting set problem for the orbits of ROABPs and *any-order* ROABPs. We have designed improved hitting sets for these two polynomial classes. In low-width but high-individual-degree setting, our hitting sets are more efficient than the previous ones given by Saha and Thankey. On the technical front, we have shown some stronger rank concentration results by establishing low-cone concentration for polynomials over vector spaces. These new rank concentration results have played significant role in designing our hitting sets. However, our hitting sets for the orbits of ROABPs and *any-order* ROABPs are yet to match the time complexity of hitting sets known for ROABPs and its variants. Therefore, it would be an interesting open question to close this gap.

References

[AGKS15] 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. 2

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of mathematics*, pages 781–793, 2004. 1

[ASS13] Manindra Agrawal, Chandan Saha, and Nitin Saxena. Quasi-polynomial hitting-set for set-depth-Δ formulas. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 321–330, 2013. 6

[ASSS12] Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. Jacobian hits circuits: hitting-sets, lower bounds for depth-d occur-k formulas & depth-3 transcendence degree-k circuits. In *STOC*, pages 599–614, 2012. 2

[BMS13] M. Beecken, J. Mittmann, and N. Saxena. Algebraic Independence and Blackbox Identity Testing. *Inf. Comput.*, 222:2–19, 2013. (Conference version in ICALP 2011). 2

[BT88] Michael Ben-Or and Prasoon Tiwari. A deterministic algorithm for sparse multivariate polynominal interpolation (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 301–309, 1988. 2

[CKS18] Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Hardness vs randomness for bounded depth arithmetic circuits. In *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, pages 13:1–13:17, 2018. 2

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Publishing Company, Incorporated, 4th edition, 2015. 9

[DdOS14] Zeev Dvir, Rafael Mendes de Oliveira, and Amir Shpilka. Testing Equivalence of Polynomials under Shifts. In *41st International Colloquium on Automata, Languages, and Programming, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 417–428, 2014. 1

[DL78] Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193 – 195, 1978. 1

[dOSV15] Rafael Mendes de Oliveira, Amir Shpilka, and Ben Lee Volk. Subexponential size hitting sets for bounded depth multilinear formulas. In *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, pages 304–322, 2015. 2

[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. 2

[DSY09] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009. 2

[FGS18] Michael A. Forbes, Sumanta Ghosh, and Nitin Saxena. Towards blackbox identity testing of log-variate circuits. In *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*, pages 54:1–54:16, 2018. 2, 6, 7, 13

[FGT16] Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite perfect matching is in quasi-NC. In *48th Annual ACM Symposium on Theory of Computing*, pages 754–763, 2016. 1, 2

[For15] Michael A Forbes. Deterministic divisibility testing via shifted partial derivatives. In *56th Annual Symposium on Foundations of Computer Science*, pages 451–465, 2015. 2, 6

[FS13a] Michael A Forbes and Amir Shpilka. Explicit noether normalization for simultaneous conjugation via polynomial identity testing. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 527–542. Springer, 2013. 2

[FS13b] Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 243–252. IEEE Computer Society, 2013. 2

[FSS13] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Pseudorandomness for multilinear read-once algebraic branching programs, in any order. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:132, 2013. Conference version of this article is accepted in STOC 2014. 7, 9, 11

[FSS14] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Symposium on Theory of Computing (STOC), New York, NY, USA, May 31 - June 03, 2014*, pages 867–875, 2014. 1, 2, 6, 7, 8, 11

[GG20] Zeyu Guo and Rohit Gurjar. Improved explicit hitting-sets for roabps. In Jaroslaw Byrka and Raghu Meka, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2020, August 17-19, 2020, Virtual Conference*, volume 176 of *LIPIcs*, pages 4:1–4:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. 3

[GKS17] 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. 1, 2, 6

[GKSS19] Zeyu Guo, Mrinal Kumar, Ramprasad Saptharishi, and Noam Solomon. Derandomization from algebraic hardness. *Electronic Colloquium on Computational Complexity (ECCC)*, 26:65, 2019. Preliminary version in FOCS 2019. 2

[GKST15] Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf. Deterministic identity testing for sum of read-once oblivious arithmetic branching programs. In *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, pages 323–346, 2015. 6

[GT17] Rohit Gurjar and Thomas Thierauf. Linear matroid intersection is in quasi-nc. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 821–830, 2017. 2

[HS80] Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute (extended abstract). In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA*, pages 262–272, 1980. 2

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004. Preliminary version in the 35th Annual ACM Symposium on Theory of Computing (STOC), 2003. 2

[KS01] Adam R. Klivans and Daniel A. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 216–223, 2001. 2, 10, 11

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

[KS09] Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 198–207, 2009. 2

[KS11] Zohar Shay Karnin and Amir Shpilka. Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. *Combinatorica*, 31(3):333–364, 2011. 2

[KS17] Mrinal Kumar and Shubhangi Saraf. Arithmetic circuits with locally low algebraic rank. *Theory of Computing*, 13(1):1–33, 2017. Preliminary version in the 31st Conference on Computational Complexity (CCC), 2016. 2

[KSS14] Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of polynomial identity testing and deterministic multivariate polynomial factorization. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 169–180, 2014. 1

[KV21] Mrinal Kumar and Ben Lee Volk. A polynomial degree bound on equations for non-rigid matrices and small linear circuits. In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPIcs*, pages 9:1–9:9. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 11

[Lov79] László Lovász. On determinants, matchings, and random algorithms. In *FCT*, volume 79, pages 565–574, 1979. 1

[LV03] Richard J. Lipton and Nisheeth K. Vishnoi. Deterministic identity testing for multivariate polynomials. In *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms, January 12-14, 2003, Baltimore, Maryland, USA.*, pages 756–760, 2003. 2

[MS21] Dori Medini and Amir Shpilka. Hitting sets and reconstruction for dense orbits in vp_{e} and $\Sigma\Pi\Sigma$ circuits. *CoRR*, abs/2102.05632, 2021. 3, 11

[Mul12] Ketan D. Mulmuley. Geometric complexity theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether's normalization lemma. In *FOCS*, pages 629–638, 2012. 2

[MV17] Daniel Minahan and Ilya Volkovich. Complete derandomization of identity testing and reconstruction of read-once formulas. In Ryan O'Donnell, editor, *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, volume 79 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. 11

[NW97] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1997. Preliminary version in the 36th Annual Symposium on Foundations of Computer Science (FOCS), 1995. 4

[PSS18] Anurag Pandey, Nitin Saxena, and Amit Sinhababu. Algebraic independence over positive characteristic: New criterion and applications to locally low-algebraic-rank circuits. *Computational Complexity*, 27(4):617–670, 2018. Preliminary version in the 41st International Symposium on Mathematical Foundations of Computer Science (MFCS), 2016. 2

[RS05] Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005. 2

[Sax08] Nitin Saxena. Diagonal circuit identity testing and lower bounds. In *ICALP*, volume 5125 of *Lecture Notes in Computer Science*, pages 60–71. Springer, 2008. 2

[Sax09] Nitin Saxena. Progress on polynomial identity testing. *Bulletin of the EATCS*, 99:49–79, 2009. 2

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, October 1980. 1

[Sha90] Adi Shamir. Ip=pspace. In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I*, pages 11–15, 1990. 1

[SS11] Nitin Saxena and C. Seshadhri. An almost optimal rank bound for depth-3 identities. *SIAM J. Comput.*, 40(1):200–224, 2011. 2

[SS12] Nitin Saxena and C. Seshadhri. Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM Journal on Computing*, 41(5):1285–1298, 2012. 2

[SS13] Nitin Saxena and C. Seshadhri. From sylvester-gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *J. ACM*, 60(5):33:1–33:33, 2013. 2

[SSS13] Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. A case of depth-3 identity testing, sparse factorization and duality. *Computational Complexity*, 22(1):39–69, 2013. 2

[ST17] Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-nc. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 696–707, 2017. 1, 2

[ST21] Chandan Saha and Bhargav Thankey. Hitting sets for orbits of circuit classes and polynomial families. *Electron. Colloquium Comput. Complex.*, 28:15, 2021. 1, 3, 4, 5, 6, 11

[SV09] Amir Shpilka and Ilya Volkovich. Improved polynomial identity testing for read-once formulas. In Irit Dinur, Klaus Jansen, Joseph Naor, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 12th International Workshop, APPROX 2009, and 13th International Workshop, RANDOM 2009, Berkeley, CA, USA, August 21-23, 2009. Proceedings*, volume 5687 of *Lecture Notes in Computer Science*, pages 700–713. Springer, 2009. 8, 11

[SV15] Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. *Comput. Complex.*, 24(3):477–532, 2015. 11

[SY10] 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. 2

[Tut47] W. T. Tutte. The factorization of linear graphs. *Journal of the London Mathematical Society*, s1-22(2):107–111, 1947. 1

[Zen93] Jiang Zeng. A bijective proof of Muir's identity and the Cauchy-Binet formula. *Linear Algebra and its Applications*, 184:79–82, 1993. 10

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, 1979. 1

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il