

Pseudorandomness for Multilinear Read-Once Algebraic Branching Programs, in any Order

Michael A. Forbes*

Ramprasad Saptharishi[†]Amir Shpilka[‡]

September 22, 2013

Abstract

We give deterministic black-box polynomial identity testing algorithms for multilinear read-once oblivious algebraic branching programs (ROABPs), in $n^{\mathcal{O}(\lg^2 n)}$ time.¹ Further, our algorithm is oblivious to the order of the variables. This is the first sub-exponential time algorithm for this model. Furthermore, our result has no known analogue in the model of read-once oblivious *boolean* branching programs with unknown order, as despite recent work (eg. [BPW11, IMZ12, RSV13]) there is no known pseudorandom generator for this model with sub-polynomial seed-length (for unbounded-width branching programs).

This result extends and generalizes the result of Forbes and Shpilka [FS12b] that obtained a $n^{\mathcal{O}(\lg n)}$ -time algorithm when given the order. We also extend and strengthen the work of Agrawal, Saha and Saxena [ASS12] that gave a black-box algorithm running in time $\exp((\lg n)^{\Omega(d)})$ for set-multilinear formulas of depth d . We note that the model of multilinear ROABPs contains the model of set-multilinear algebraic branching programs, which itself contains the model of set-multilinear formulas of arbitrary depth. We obtain our results by recasting, and improving upon, the ideas of Agrawal, Saha and Saxena [ASS12]. We phrase the ideas in terms of *rank condensers* and *Wronskians*, and show that our results improve upon the classical multivariate Wronskian, which may be of independent interest.

In addition, we give the first $n^{\mathcal{O}(\lg \lg n)}$ black-box polynomial identity testing algorithm for the so called model of diagonal circuits. This model, introduced by Saxena [Sax08] has recently found applications in the work of Mulmuley [Mul12], as well as in the work of Gupta, Kamath, Kayal, Saptharishi [GKKS13]. Previously, Agrawal, Saha and Saxena [ASS12], Forbes and Shpilka [FS12b], and Forbes and Shpilka [FS13] had given $n^{\Theta(\lg n)}$ -time algorithms for this class. More generally, our result holds for any model computing polynomials whose partial derivatives (of all orders) span a low dimensional linear space.

*Email: miforbes@mit.edu, Department of Electrical Engineering and Computer Science, MIT CSAIL, 32 Vassar St., Cambridge, MA 02139. This work supported by the Center for Science of Information (CSoI), an NSF Science and Technology Center, under grant agreement CCF-0939370.

[†]Email: ramprasad@cmi.ac.in, Microsoft Research India, Bangalore, India.

[‡]Faculty of Computer Science, Technion — Israel Institute of Technology, Haifa, Israel, shpilka@cs.technion.ac.il. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 257575.

¹All logarithms are base 2 in this paper, except where otherwise noted.

1 Introduction

Polynomial Identity Testing (PIT for short) is the problem of *deterministically* deciding whether a given algebraic circuit computes the identically zero polynomial. Recall that algebraic circuits are the algebraic analogs of boolean circuits that use the algebraic operations $\{+, \times\}$ to compute polynomials over an underlying field \mathbb{F} . The complexity of the problem comes from the requirement that the algorithm be deterministic. Indeed, efficient randomized algorithms follow easily from the Demillo-Lipton-Schwartz-Zippel Lemma [DL78, Sch80, Zip79]. The importance of the PIT problem stems from its many applications — it is tightly connected to the problem of obtaining lower bounds for algebraic circuits (see for example, [HS80, KI04, Agr05, DSY09]) and it has applications in algorithms (see for example, [KUW86, MVV87, AKS04]). For more on PIT see the survey of Shpilka and Yehudayoff [SY10].

PIT comes in two flavors. In the *white-box* setting, the algorithm is given the circuit, namely, it is given the graph of computation. In the *black-box* setting, the algorithm can access the circuit only through queries. A black-box PIT algorithm can be observed to be equivalent to a *hitting set*, which is a small set of points so that any nonzero polynomial will evaluate to nonzero on one of these points. Thus, the black-box model allows weaker access, and thus algorithms in this model are correspondingly stronger results. We seek algorithms in this restricted model, as they more closely match the performance of the randomized algorithm, which is black-box.

In recent years, there has been much work on PIT focused on restricted models of algebraic circuits. From the works of Agrawal and Vinay [AV08] and Gupta, Kamath, Kayal and Saptharishi [GKKS13] it follows that solving PIT for depth-3 circuits would yield a solution to the case of general algebraic circuits. This has increased the focus on restricted models, and yielded a long line of works focused on PIT for depth-3 and depth-4 circuits [DS06, KS07, KS11, KS09, SS11, KMSV10, SV11, SSS11].

Another active line of research has considered models of computation with other types of restrictions. One line considers models that are *set-multilinear*, in particular focusing on *set-multilinear algebraic branching programs (ABPs)* [RS05, AMS08, FS12a, FS12b, ASS12, FS13]. One reason for the focus on this model is that it captures the *partial derivative* technique that is the main technique today for proving lower bounds for algebraic circuits. Another reason for the interest shown in this model is that it is the algebraic analog for the branching program model in boolean complexity. In fact, the PIT problem for *read-once oblivious ABPs (ROABPs)* can be viewed as the algebraic analog of the famous L vs. RL question. Indeed, the PIT algorithm of Forbes and Shpilka [FS12b] for ROABPs is very close in nature to Nisan’s [Nis92] pseudo-random generator (PRG) for read-once oblivious (boolean) branching programs, which are a non-uniform version of randomized log-space Turing machines. For more on ROABPs we refer the reader to the introduction of the paper Forbes-Shpilka [FS12b].

The work of Forbes and Shpilka [FS12b] highlighted a difference between known results for the boolean case and the algebraic case. While over the boolean domain we do not have an improvement to Nisan’s PRG when the branching program is of bounded width, in the algebraic setting Forbes and Shpilka [FS12b] give an $n^{\lg n / \lg \lg n}$ PIT algorithm for the case of bounded width ROABPs, which, intuitively, would correspond to a PRG with seed-length $\mathcal{O}(\lg^2 n / \lg \lg n)$. Obtaining such a seed length in the boolean setting is a long-standing open problem (see [Vad12, Open Problem 8.6]).

In this work, we obtain new PIT algorithms for ROABPs that, again, do not yet have boolean

analogues. Previous work on read-once branching programs, for both the boolean and algebraic models, only worked for a fixed variable order. That is, the branching program is read-once and reads each variable in a fixed *known* order. If this order is known, then black-box PIT algorithms, or PRG constructions, exist in previous work. However, once the order becomes unknown, much less is known. However, recently Agrawal, Saha, and Saxena [ASS12] introduced the idea of *shifting* and *rank concentration*, and using these ideas gave black-box PIT algorithms for sub-models of unknown-order ROABPs. In this work, we extend and reinterpret their ideas, and consequently construct a quasipolynomial time black-box PIT algorithm for (multilinear) ROABPs when the order of the variables is unknown. In contrast, in the boolean setting the best algorithm when the order of the variables is unknown runs in time $\exp(\sqrt{n})$, due to Impagliazzo, Meka and Zuckerman [IMZ12].

1.1 The models

In this work, we consider various restricted models of computation, which we now define. They are all variants, or sub-models, of algebraic branching programs (ABPs). Algebraic branching programs were first defined in the work of Nisan [Nis91] who proved exponential lower bounds on the size of non-commutative ABPs computing the determinant or permanent polynomials. We shall consider several variants of the basic model.

Definition 1.1 (Nisan [Nis91]). An *algebraic branching program with unrestricted weights* of depth D and width $\leq r$, on the variables x_1, \dots, x_n , is a directed acyclic graph such that

- The vertices are partitioned in $D + 1$ layers V_0, \dots, V_D , so that $V_0 = \{s\}$ (s is the source node), and $V_D = \{t\}$ (t is the sink node). Further, each edge goes from V_{i-1} to V_i for some $0 < i \leq D$.
- $\max |V_i| \leq r$.
- Each edge e is weighted with a polynomial $f_e \in \mathbb{F}[\mathbf{x}]$.

Each s - t path is said to compute the polynomial which is the product of the labels of its edges, and the algebraic branching program itself computes the sum over all s - t paths of such polynomials.

- In an *algebraic branching program (ABP)*, for each edge e the weight $f_e(\mathbf{x})$ is an affine function. The *size* is nDr .
- In a *read-once oblivious ABP (ROABP)* of (individual) degree $< d$, we have $n = D$, and there is some permutation $\pi : [n] \rightarrow [n]$ such that for each edge e from V_{i-1} to V_i , the weight is a univariate polynomial $f_e(x_{\pi(i)}) \in \mathbb{F}[x_{\pi(i)}]$ of degree $< d$. The *size* is ndr . We say the *variable order is known* if this permutation is the identity permutation, and it is *unknown* otherwise.
- A polynomial is computed by a *width- r commutative ROABP*, if it is computable by a width- r ROABP in *every* variable order.
- In a *set-multilinear algebraic branching program (SMABP)* the dn variables $\{x_1, \dots, x_{dn}\}$ are partitioned into d sets of size n , $\mathbf{x} = \mathbf{x}_1 \sqcup \dots \sqcup \mathbf{x}_d$. For each edge e from V_{i-1} to V_i , f_e is a (homogeneous) linear function in the variable set X_i . We say the *partition is known* if $\mathbf{x}_i = \{x_{(i-1)n+1}, \dots, x_{(i-1)n+n}\}$ and it is *unknown* otherwise. \diamond

Note that a polynomial computed by a commutative ROABP is trivially computed by a ROABP. This class of polynomials coincide with the notion of polynomials with low *evaluation dimension*, a notion of Saptharishi, as reported in Forbes-Shpilka [FS12b].

The definition of a SMABP is in line with the term coined by Nisan and Wigderson [NW96] that defined a set-multilinear monomial to be a multilinear monomial that contains exactly one variable from each x_i and a set-multilinear polynomial as a polynomial consisting of set-multilinear monomials. Thus, it is clear from the definition that a set-multilinear ABP computes a set-multilinear polynomial. It is also not hard to see that any set-multilinear polynomial can be computed by a set-multilinear ABP, but perhaps requiring large size.

Another model that we consider in this paper is the so called *diagonal circuit* model, first defined by Saxena [Sax08]. While this model is somewhat less motivated than small depth circuits or ABPs, it has found recent applications in the work of Mulmuley [Mul12] concerning derandomization of Noether's Normalization Lemma, see also Forbes-Shpilka [FS13] for a discussion. Furthermore, this model and the tools used to understand it were used in the recent work of Gupta-Kamath-Kayal-Saptharishi [GKKS13]. Lastly, this model is the weakest model known for which polynomial-time black-box PIT algorithms are not currently known.

Definition 1.2 (Diagonal circuits). A *diagonal circuit* in the n variables \mathbf{x} , of degree d , and size s , computes polynomials $f(\mathbf{x})$ of degree at most d that can be expressed as a sum of s powers of linear functions. Namely, $f(\mathbf{x}) = \sum_{i=1}^s L_i(\mathbf{x})^{d_i}$, where each L_i is a linear function and $d_i \leq d$. \diamond

Diagonal circuits are examples of polynomials where the space of partial derivatives is low-dimensional. We present the formal definition of this notion in Section 7.

1.2 Our results

We now give a summary of our results, and start by defining the notion of a hitting set, which is the object we seek to construct.

Definition 1.3 (Hitting Set). Let \mathcal{C} be a class of n -variate polynomials, with coefficients in \mathbb{F} . A set $\mathcal{H} \subseteq \mathbb{F}^n$ is a *hitting set* for \mathcal{C} if for all $f \in \mathcal{C}$, $f \equiv 0$ iff $f|_{\mathcal{H}} \equiv 0$.

The hitting set \mathcal{H} is $t(n)$ -*explicit* if given an index into \mathcal{H} , the corresponding element of \mathcal{H} can be computed in $t(n)$ -time. \diamond

Our main result is an explicit quasipolynomial-size hitting set for multilinear ROABPs, for unknown variable order. As a special case (see Lemma 2.2), we obtain the same parameter hitting sets for set-multilinear ABPs, when the partition to the sets is unknown.

Theorem 1 (Hitting set for multilinear unknown order ROABPs, informal version of Theorem 6.5). *Let \mathcal{C} be the set of n -variate multilinear polynomials computable by a width- r ROABP in any variable order. If $|\mathbb{F}| \geq \text{poly}(n, r)$, then \mathcal{C} has a $\text{poly}(n, r)$ -explicit hitting set, of size $\leq \text{poly}(n, r)^{\mathcal{O}(\lg r \cdot \lg n)}$.* \triangle

For polynomials with individual degree d (so each variable has degree d), the exponent in the hitting set increases by a factor of d . To achieve this result, we used the ideas of Agrawal, Saha and Saxena [ASS12], who gave results for sub-models of unknown-order ROABPs. As we reinterpret their ideas, we rederive some of their results. One such result we give below.

Theorem 2 (Hitting set for commutative ROABPs, informal version of Corollary 4.3). *Let \mathcal{C} be the set of n -variate polynomials with individual degree $< d$ that are computable by a width- r commutative ROABPs (and thus computable by a ROABP in every variable order). If $|\mathbb{F}| \geq \text{poly}(n, d)$, then \mathcal{C} has a $\text{poly}(n, d, r)$ -explicit hitting set, of size $\leq \text{poly}(n, d)^{\mathcal{O}(\lg r)}$.* \triangle

The proofs of the above results, while yielding sub-exponential-size hitting sets, do not readily suggest a path to obtaining polynomial-size hitting sets. In particular, at first glance it seems difficult to see how the above proof strategies could yield hitting sets of size $n^{o(\lg n)}$. However, our next result shows that for certain sub-models of commutative ROABPs, such as diagonal circuits, we can in fact achieve $n^{\mathcal{O}(\lg \lg n)}$ -size hitting sets.

Theorem 3 (Informal version of [Theorem 7.7](#)). *Let \mathcal{C} be the set of n -variate polynomials of degree d computable by size s diagonal circuits. If $|\mathbb{F}| \geq \text{poly}(n, d, s)$, then \mathcal{C} has a $\text{poly}(n, d, s)$ -explicit hitting set, which has size $\leq \text{poly}(n, d, s)^{\mathcal{O}(\lg \lg(ds))}$.*

Let \mathcal{C} be the set of multilinear n -variate polynomials computable by width- r commutative ROABPs. If $|\mathbb{F}| \geq \text{poly}(n, r)$, then \mathcal{C} has a $\text{poly}(n, r)$ -explicit hitting set, which has size $\leq \text{poly}(n, r)^{\mathcal{O}(\lg \lg r)}$. \triangle

We also show that the above holds more generally for polynomials with a small space of partial derivatives, see [Section 7](#). We can also extend the above result, by relaxing the multilinearity of the commutative ROABP to individual degree d , in which case the exponent grows by a factor of $\lg d$. In the previous theorem, the resulting exponent was independent of d , but that exponent has a worse dependence on r .

The proof of our results combines various works. We start by extending and reinterpreting the ideas of shifting and rank concentration, of Agrawal, Saha and Saxena [[ASS12](#)]. We then build on these techniques by incorporating new recursion schemes, as well as existing tools in the literature such as the Klivans and Spielman [[KS01](#)] generator for sparse polynomials, the generator of Shpilka and Volkovich [[SV09](#)] for read-once formulas, the generator of Forbes and Shpilka [[FS12b](#)] for ROABPs, as well as perfect hash functions.

1.3 Related work

Boolean Pseudorandomness: The PIT problem can be seen as the algebraic analog of the task of constructing pseudorandom generators for boolean computation. That is, for a class \mathcal{C} of boolean circuits, we can seek to construct a *pseudorandom generator* (PRG) $\mathcal{G} : \{0, 1\}^s \rightarrow \{0, 1\}^n$ for \mathcal{C} , such that for any circuit $C \in \mathcal{C}$ on n inputs, we have the ε -closeness of distributions $C(\mathcal{G}(U_s)) \approx_\varepsilon C(U_n)$, where U_k denotes the uniform distribution on $\{0, 1\}^k$. Nisan [[Nis92](#)] studied pseudorandom generators for space-bounded computation, and for space s computation gave a generator with seed length $s = \mathcal{O}(\lg^2 s)$. Randomized space-bounded computation can be modeled with read-once oblivious (boolean) branching programs, and these generators apply to this model of computation as well. Note that in the context of space-bounded derandomization, the order that the randomness is read is known, as this information is dictated when simulating the space-bounded machine.

Despite Nisan's result, the seed length has not been improved for general read-once branching programs, despite much work on the problem (see for example [[Nis92](#), [INW94](#), [RR99](#), [NZ96](#), [BDVY13](#), [SZ11](#), [GMR⁺12](#), [BRRY10](#), [BV10](#), [KNP11](#), [De11](#), [Ste12](#), [Tzu09](#), [BPW11](#), [RSV13](#), [IMZ12](#)] among others). While past PRG work for read-once branching programs has examined restricted branching programs (such as *regular* or *permutation*), more recently it has been observed that existing PRGs depend heavily on the order the variables are read, and Tzur [[Tzu09](#)] even showed that certain instantiations provably fail for adversarially chosen read orders. Starting with the work of Bogdanov, Papakonstantinou and Wan [[BPW11](#)], there have been attempts to obtain PRGs for read-once branching programs in any variable order. In recent works, Impagliazzo, Meka and Zuckerman [[IMZ12](#)] gave a generator with seed length $n^{1/2+o(1)}$ for general branching programs in any variable order, and Reingold, Steinke and Vadhan [[RSV13](#)] gave a seed-length of $\mathcal{O}(\lg^2 n)$ for

constant-width permutation read-once branching programs in any variable order.

In comparison, the work of Forbes and Shpilka [FS12b] studied read-once oblivious (algebraic) branching programs, and achieved a quasi-polynomial-sized hitting set, which would correspond to a “seed length” of $\mathcal{O}(\lg^2 s)$ for ABPs of size s . This result is analogous (in some sense) to the generator of Nisan for space bounded computations. Correspondingly, it only applies when the variable order of the ROABP is known. Independently, Agrawal, Saha and Saxena [ASS12] gave results for sub-models of ROABPs, and in their models it is somewhat less natural to assume that the variable order is known.

Thus, motivated by the analogous questions in boolean pseudorandomness, as well as by the positive results for the unknown order case by Agrawal, Saha and Saxena [ASS12], this work studies general ROABPs when the order of variables is unknown. We give a quasi-polynomial-sized hitting set, corresponding to a seed of length $\mathcal{O}(\lg^3 s)$ for ABPs of size s . It is an interesting question as to whether any insights of this paper (and other recent works) can be used to obtain a similar seed length in the boolean regime, or in general whether there are any formal connections between algebraic and boolean pseudorandomness for read-once oblivious branching programs.

The Partial Derivative Method: The PIT algorithm of Raz and Shpilka [RS05] works for any model of computation that outputs polynomials whose space of partial derivatives is (relatively) low-dimensional.² Set-multilinear ABPs, non-commutative ABPs, low-rank tensors, and so called pure algebraic circuits (defined in Nisan and Wigderson [NW96]) are all examples of algebraic models that compute polynomials with that property, and so the algorithm of Raz and Shpilka [RS05] works for them. In some sense using information on the dimension of partial derivatives of a given polynomial is the most applicable technique when trying to prove lower bounds for algebraic circuits (see e.g., [Nis91, NW96, Raz06, Raz09, RSY08, RY09, GKKS12]) and so it was an interesting problem to understand whether this powerful technique could be carried over to the black-box setting. The work Forbes and Shpilka [FS12b] achieved a quasi-polynomial hitting set for this model when the order of variables is known in advance. Here we remove this restriction thus providing a black-box analog of Raz and Shpilka [RS05] (for multilinear polynomials), albeit with a quasi-polynomial running time.

Furthermore, when the polynomial has the property that the set of all of its partial derivatives spans a low-dimensional space (i.e., of polynomial dimension), then we get a nearly polynomial time algorithm, namely, an $n^{\mathcal{O}(\lg \lg n)}$ algorithm, as stated in Section 7.

Previous Work: As mentioned before, the work Forbes and Shpilka [FS12b] gave a hitting set of quasi-polynomial size for the class of ROABPs when the order of variables is known in advance. The basic idea in that work, which follows the idea of the prior work of Forbes and Shpilka [FS12a], is that of preserving dimension of linear spaces while reducing the number of variables. To achieve this reduction, Forbes and Shpilka [FS12b] used a variant of a construction of Gabizon and Raz [GR08a] which in this work we refer to as a *rank condenser*. This is then used in a recursive merge-and-reduce scheme. In each step, the variables in the ROABP are partitioned into adjacent pairs according to the variable order, and these variables are merged (in parallel) in a brute-force manner. This halves the number of variables, but in a certain sense squares the degree of the polynomial. The

²More accurately, it works for the set-multilinear model with a given ordering of the sets and we only consider derivatives according to variables from consecutive sets. That is, in the ABP model we consider only derivatives according to variables in adjacent layers.

rank condenser then allows these new variables to be sampled pseudorandomly (and in parallel), such that the degree is then reduced appropriately. Thus, the number of variables is halved, and no other parameters are changed. However, the pseudorandom sampling requires a “seed” of length $\mathcal{O}(\lg s)$, and there are $\lg n$ such seeds, giving a total of $\mathcal{O}(\lg n \lg s)$ seed length. Note that this process crucially uses the variable order, as it needs to know which variables are neighbors and thus can be merged together.

Recently, Agrawal, Saha and Saxena [ASS12] obtained results on black-box derandomization of PIT for small-depth set-multilinear formulas (as well as generalizations to when the multilinearity condition is relaxed), when the partition of the variables into sets is unknown. They obtained a hitting set of size $\exp((2h^2 \lg(s))^{h+1})$, for size s formulas of multiplicative-depth h .³ In the language of pure formulas, they consider pure formulas of multiplicative-depth h . We note that this model is a strict subset of the more general model of pure formulas which itself is a strict sub-model of set-multilinear ABP.⁴ Thus, our result significantly improves upon the multilinear results of Agrawal-Saha-Saxena [ASS12], and in particular the size of our hitting set does not depend on the depth of the formula.

In this work we also present black-box PIT results for the model of diagonal circuits, or more generally, polynomials with a low dimensional space of partial derivatives. Saxena [Sax08] defined this model as a way capture some of the complexity of depth-4 circuits. He gave a polynomial-time white-box PIT algorithm, by using algorithm of Raz and Shpilka [RS05]. Later, Saha, Saptharishi and Saxena [SSS11], generalized Saxena’s results to the so-called semi-diagonal model. Simultaneously and independently (using very different techniques), Agrawal, Saha and Saxena [ASS12], and Forbes and Shpilka [FS12b] gave $s^{\mathcal{O}(\lg s)}$ black-box PIT algorithms for size s semi-diagonal depth-4 circuits. Later, Forbes and Shpilka [FS13] gave another such algorithm, that was somewhat simpler. In this work, we give a $s^{\mathcal{O}(\lg \lg s)}$ -size hitting set for diagonal circuits, and the techniques can be seen as merging the ideas of Agrawal-Saha-Saxena [ASS12], Forbes-Shpilka [FS12b] and Forbes-Shpilka [FS13].

1.4 Proof technique

The work of Agrawal, Saha and Saxena [ASS12] introduced a new technique which they called *rank-concentration*. By shifting the variables x , to $x + t$ for a careful choice of t , they showed that for depth-3 set-multilinear formulas, they can reduce to the case where the partial derivative space is spanned by derivatives of small order, which allowed them to conclude that the shifted polynomial contains a low degree monomial. They then used induction on the depth to obtain rank-concentration for higher depth formulas as well. Once this is achieved it is relatively easy to find a nonzero substitution to the polynomial. The main difficulty comes from finding a good shift that guarantees the rank-concentration property.

In this work we present the idea of Agrawal-Saha-Saxena [ASS12] in the language of rank-condensers, and of which the notion of a *Wronskian* is a special case. Specifically, we show that shifts act on the space of partial derivatives as a rank condenser (see Section 3). This can be phrased as a Wronskian-result, as it says that the rank of certain matrices of partial derivatives capture linear independence in multivariate polynomials. Using this terminology we are able to easily

³The multiplicative-depth is the maximal number of product gates in an input-output path. In the bounded depth model this is essentially half the total depth.

⁴The usual transformation from formulas to ABPs can be done preserving set-multilinearity.

compute good shifts. We believe that the language of rank condensers offers a convenient language for these results, and thus do not use various notions from Agrawal-Saha-Saxena [ASS12] such as Hadamard algebras.

We now discuss the notion of a rank condenser (and defer the discussion of Wronskians to Subsection 3.1), and how shifting can be viewed this way. Let $f_1(\mathbf{x}), \dots, f_r(\mathbf{x})$ be n -variate polynomials. We can express these polynomials as a matrix M whose rows are indexed by monomials \mathbf{x}^α and whose columns are indexed by $i \in [r]$, such that $M_{\alpha,i}$ is the coefficient of \mathbf{x}^α in f_i . Note that this captures all of the information about the f_i . In particular, these polynomials are zero iff the matrix M is zero. More generally, any linear combination of these polynomials is zero iff the corresponding linear combination of columns of M is zero. We can test if such a linear combination of the columns M is zero, by reading a subset of the rows, in particular, it suffices to examine a basis for the row-span of M . However, from an algebraic perspective, we do not have unfettered query access to M . Rather, some rows (corresponding to monomials) are easier to access than others. In particular, those monomials of low degree, or even those of small support, are easier to examine via brute force. Thus, the condition we would like on M is that it has a row-basis among small-support monomials. In particular, we say the f_i have *support- ℓ rank concentration* if M has such a basis among support- ℓ monomials. If such rank concentration occurs, it follows that a linear combination of the f_i is nonzero iff it has a nonzero monomial of support- ℓ . Such a monomial can then be found via brute-force.

However, as the monomial $x_1 x_2 \cdots x_n$ shows, small-support rank concentration does not happen always. However, if we perturb this monomial to $\prod_i (x_i + 1)$, then it suddenly does have small-support rank concentration. Thus, we seek to find a small set \mathcal{H} such that some shift $\mathbf{x} \rightarrow \mathbf{x} + \alpha$ for some $\alpha \in \mathcal{H}$ induces small-support rank-concentration. Taking a different perspective, we can ask for a shift $\mathbf{x} \rightarrow \mathbf{x} + \mathbf{t}$, where \mathbf{t} is an algebraically simple polynomial map.

To show how to construct such shifts \mathbf{t} , we need to study how the shifting process affects the matrix M . First, we see that this action is linear, and thus there is some *transfer matrix* $T(\mathbf{t})$ describing its action. As shifting by \mathbf{t} then shifting by $-\mathbf{t}$ gives the identity map, it follows that $T(\mathbf{t})$ is invertible. But we want something more, that shifting by \mathbf{t} induces rank concentration. In particular, it follows that shifting to small-support rank concentration means that we want

$$\text{rank}(M) = \text{rank}((T(\mathbf{t})^{\text{small}})M),$$

where $T(\mathbf{t})^{\text{small}}$ is the set of rows in T corresponding to small-support monomials. Thus, while T is square, $T(\mathbf{t})^{\text{small}}$ is a short, fat matrix. Yet, we still want it to preserve the rank of M after multiplication. Such matrices we call rank condensers. One primary tool in understanding whether T is a rank condenser is the following.

Lemma (Informal version of Lemma 3.10). *There is a generic recipe to turn any good error-correcting code into a good rank condenser. \triangle*

Thus, to show $T(\mathbf{t})^{\text{small}}$ is a rank condenser, we simply show it has some error-correcting code properties. This establishes that shifting will condense rank, for generic \mathbf{t} . However, by itself this is not helpful as \mathbf{t} has too many variables. In the case of a commutative ROABP, as argued in Agrawal-Saha-Saxena [ASS12], it can be shown that \mathbf{t} need only be a good shift for all small sets of variables, in which case \mathbf{t} can be found in quasipolynomial time.

To extend the rank concentration idea to general ROABPs and set-multilinear ABPs, we follow the merge-and-reduce idea of Forbes and Shpilka [FS12b]. However, the rank condenser used in that work seemingly can only be implemented if the variable order is known. However, we

observe that the shifting idea of Agrawal-Saha-Saxena [ASS12] is actually a rank condenser, and is insensitive to variable order. However, to implement this, we must create a variant of the shifting rank condenser, that only seeks to condense rank from a “known basis”. That is, if we seek to condense *all* rank, then this will be too expensive. Instead, we shift several times. In each shift, we progressively make the rank more concentrated, and we save on seed length by only condensing rank from where we already concentrated it.

To establish the hitting sets of size $s^{\mathcal{O}(\lg \lg s)}$ for sub-models of commutative ROABPS, we need to combine a variety of tools in this area. The rank concentration idea shows that we can shift commutative ROABPs such that they only have $\lg s$ essential variables, where this is possible for multilinear commutative ROABPs because of the Klivans-Spielman [KS01] generator. We then use hashing to reduce the problem to one on these essential variables. However, we will need to do this in a manner compatible with the read-once nature of the computation, and thus use the Shpilka-Volkovich [SV09] generator. After these steps, we have a commutative ROABP in $\lg s$ variables, and the Forbes-Shpilka [FS12b] generator, while quasipolynomial, has a very good dependence on the number of variables of the ROABP. Thus, by composing with this generator, we then reduce to $\lg \lg s$ variables, at which point we can interpolate to get a $s^{\mathcal{O}(\lg \lg s)}$ -size hitting set.

1.5 Organization

The paper is organized as follows. In Section 2 we give some basic tools and definitions that we shall use throughout the paper. In Section 3 we discuss shifts and rank condensers. Section 4 contains the proof of Theorem 2. In Section 5 and Section 6 we prove Theorem 1. Finally, in Section 7 we prove Theorem 3.

1.6 Notation and definitions

For a polynomial $f \in \mathbb{F}[\mathbf{x}]$, we shall use $\text{Coeff}_{\mathbf{x}^a}(f)$ to denote the coefficient of the monomial \mathbf{x}^a in f . We will sometimes identify the monomial \mathbf{x}^a with its exponent vector a . We shall often encounter *Hasse derivatives*, where we define $\partial_{\mathbf{x}^b}(f)(\mathbf{t}) := \text{Coeff}_{\mathbf{x}^b}(f(\mathbf{x} + \mathbf{t}))$. We will use $\partial_{\mathbf{x}^b}(f)$ for the derivative evaluated at the original variables \mathbf{x} . As the derivative is linear, we will also view the derivative $\partial_{\mathbf{x}^b}$ as a linear operator acting on $\mathbb{F}[\mathbf{x}]$, and will also consider linear combinations of these operators, which we refer to as differential operators. We use Hasse derivatives as they work well in fields of arbitrary characteristic, but have most of the usual properties of normal derivatives in zero characteristic. For more, see Dvir-Kopparty-Saraf-Sudan [DKSS09] or Forbes-Shpilka [FS13].

We will use the notation $[n]$ to denote $\{1, \dots, n\}$, and $\llbracket n \rrbracket$ to denote $\{0, \dots, n-1\}$. We will occasionally index vectors and matrices from zero, and will use $\llbracket n \rrbracket$ to denote this, as $\mathbb{F}^{\llbracket n \rrbracket \times \llbracket m \rrbracket}$ will denote an $n \times m$ matrix, indexed from zero. For a set S and an integer k we denote by $\binom{S}{k}$ the set of all subsets of S of size k .

We will often work with vectors and matrices, and they will often contain entries that are polynomials. Operations on polynomials, such as extracting coefficients, or taking derivatives, will be extended to vectors and matrices coordinate-wise. Vectors, such as $\mathbf{f}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^r$, will be written in bold, where as matrices, such as $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{n \times m}$ will be written with capital letters. We will also sometimes identify matrices of polynomials in $\mathbb{F}[\mathbf{x}]^{n \times m}$ with vectors of polynomials in $\mathbb{F}[\mathbf{x}]^{nm}$. Given an $n \times m$ matrix M and sets $S \subseteq [n]$ and $T \subseteq [m]$, we use the notation $M|_{S \times T}$ to denote the submatrix of M with rows from S and columns from T . When we do not restrict the rows (respectively, the columns) of A , we will use the symbol ‘ \bullet ’ in place of S (respectively, T).

When the sets S and T are singletons, we will use the more standard notation of $M_{i,j}$ to refer to the (i, j) -th entry of M . Given matrices M_i , their non-commutative product $\prod_{i \in [n]} M_i$ will have the natural order associated, that is, the product $M_1 \cdots M_n$. Similarly, for a vector $v \in \mathbb{F}^n$ and $S \subseteq [n]$ we denote by $v|_S$ the restriction of v to the coordinates of S . In a similar fashion, when we have two sets of variables (\mathbf{x}, \mathbf{y}) and a vector v of length $|\mathbf{x}| + |\mathbf{y}|$ we denote with $v|_{\mathbf{x}}$ the restriction of v to the coordinates associated with the variables in \mathbf{x} , and similarly define $v|_{\mathbf{y}}$.

Similar to the above abuse of notation, we will extend the notion of a ROABP to compute matrices. That is, we will say a matrix $M(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{r \times r}$ is computable by a width- r ROABP if $M(\mathbf{x}) = \prod_{i \in [n]} M_i(x_i)$ for $M_i(x_i) \in \mathbb{F}[x_i]^{r \times r}$.

For a vector $\mathbf{a} \in \mathbb{N}^n$, we denote $|\mathbf{a}|_0 = |\{i \mid a_i \neq 0\}|$, $|\mathbf{a}|_1 := a_1 + \cdots + a_n$, $|\mathbf{a}|_\infty = \max_i a_i$, and $\mathbf{a}! = a_1! \cdots a_n!$. Given a monomial $\mathbf{x}^{\mathbf{a}}$, we will say it has (total) degree $|\mathbf{a}|_1$, individual degree $|\mathbf{a}|_\infty$, and support $|\mathbf{a}|_0$. We will define the support of a monomial, denoted $\text{supp}(\mathbf{x}^{\mathbf{a}})$, to be either the coordinates $\{i : a_i \neq 0\}$, or the corresponding variables $\{x_i : a_i \neq 0\}$, and this will depend on context. For any $a < b$, we shall set $\binom{a}{b}$ to be zero. Also, for vectors $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$, we shall define $\binom{\mathbf{a}}{\mathbf{b}} = \prod_i \binom{a_i}{b_i}$.

For a set of vectors T we denote with $\dim_{\mathbb{F}}(T)$ the dimension of the vector space spanned by the vectors in T , over \mathbb{F} . For a polynomial $f(\mathbf{x})$ and a variable x_i we denote the degree of f in x_i by $\deg_{x_i}(f)$.

2 Tools

In this section we state some known results about ABPs and state some results from the literature that will be used throughout the paper.

ABPs and Iterated Matrix Multiplication: We start by giving the well known equivalence of ABPs and iterated matrix multiplication (see, e.g., Lemma 3.1 of Forbes-Shpilka [FS12b]).

Lemma 2.1. *Let $f \in \mathbb{F}[\mathbf{x}]$ be computed by a depth D , width $\leq r$ ABP with unrestricted weights, such that the variable layers are V_0, \dots, V_D . For $0 < i \leq D$, define $M_i \in \mathbb{F}[\mathbf{x}]^{V_{i-1} \times V_i}$ such that the (u, v) -th entry in M_i is the label on the edge from $u \in V_{i-1}$ to $v \in V_i$, or 0 if no such edge exists. Then, $f(\mathbf{x})$ is a linear combination of the entries in $\prod_{i \in [D]} M_i(\mathbf{x}) := M_1(\mathbf{x})M_2(\mathbf{x}) \cdots M_D(\mathbf{x})$.*

Further, for an ABP, the matrix M_i has entries that are affine forms, and for a ROABP of individual degree $< d$, the matrix M_i has entries which are univariate polynomials in $x_{\pi(i)}$ of degree $< d$ (where π is the permutation determining the order of variables). For a set-multilinear ABP on the variable sets $\mathbf{x} = \mathbf{x}_1 \sqcup \mathbf{x}_2 \sqcup \cdots \sqcup \mathbf{x}_d$ the matrix M_i has entries that are linear forms in the variables \mathbf{x}_i . \triangle

Given the above, we will focus on iterated matrix multiplication, in particular for matrices that are all $r \times r$. Further, as it is more amenable to recursion, we will more focus on the matrix product $\prod_i M_i(\mathbf{x})$ than the polynomial $f(\mathbf{x})$.

Set-Multilinear and ROABPs: We note here that set-multilinear ABPs can be expressed as multilinear ROABPs of slightly larger width, and thus will focus on ROABPs.

Lemma 2.2. *Let $f(x_1, \dots, x_d)$ be computed by a set-multilinear ABP of width- r . Then f can be computed by a multilinear ROABP of width- $2r$ in the dn variables, in some variable order.*

Proof: Consider first a single homogeneous linear form L in some partition \mathbf{x}_i , so that $L(\mathbf{x}_i) = \sum_{j \in [n]} a_{i,j} x_{i,j}$. Note that

$$\begin{bmatrix} 1 & L(\mathbf{x}_i) \\ 0 & 1 \end{bmatrix} = \prod_{j \in [n]} \begin{bmatrix} 1 & a_{i,j} x_{i,j} \\ 0 & 1 \end{bmatrix}.$$

Now consider any $r \times r$ matrix $M_i(\mathbf{x}_i)$ in a set-multilinear ABP. By using the above transformation, and appealing to block-matrix multiplication, we can construct width- $2r$ matrices $M_{i,j}$ so that $\prod_{j \in [n]} M'_{i,j}(x_{i,j})$ embeds $M_i(\mathbf{x}_i)$. Further, as this embedding is regular, it follows there are $2r \times 2r$ matrices P and Q such that $P \cdot \prod_{j \in [n]} M'_{i,j}(x_{i,j}) \cdot Q = M_i(\mathbf{x}_i)$. Incorporating P and Q into the product, shows that $M_i(\mathbf{x}_i)$ can be computed by the requisite ROABP. Applying this argument to each partition \mathbf{x}_i and multiplying the resulting matrices gives the result. \square

PIT results: The first PIT result that we need is a generator of Klivans and Spielman [KS01] for sparse polynomials. We will not need to hit sparse polynomials themselves, but rather will need the hashing properties of this generator that allow us to reduce to fewer variables.

Theorem 2.3 (Klivans-Spielman generator [KS01]). *Let $|\mathbb{F}| \geq \text{poly}(n, d)$, where $m = \Theta(\log_{nd} s)$. Then there is a $\text{poly}(n, d, m)$ -explicit polynomial $\mathcal{G}_{n,d,s}^{\text{KS}} : \mathbb{F}^m \times \mathbb{F}^m \rightarrow \mathbb{F}^n$ such that*

- For all $i \in [n]$, the polynomial $(\mathcal{G}_{n,d,s}^{\text{KS}})_i$ has individual degree $\leq \text{poly}(n, d)$.
- For every set $S \subseteq \mathbb{F}[\mathbf{x}]$ of n -variate monomials of individual degree $< d$, such that $|S| \leq s$, there is some $\boldsymbol{\alpha} \in \mathbb{F}^m$ such the polynomials $\{(\mathcal{G}_{n,d,s}^{\text{KS}}(\mathbf{t}, \boldsymbol{\alpha}))^\alpha\}_{\mathbf{x}^\alpha \in S}$ are nonzero, distinct monomials in \mathbf{t} . \triangle

The above is a slight variation of the work of Klivans and Spielman [KS01], and it can be constructed using their techniques. That is, take p a prime of size $\text{poly}(n, d)$, and consider the substitution $x_i \leftarrow t^{k^i \pmod{p}}$, so that $\mathbf{x}^\alpha \leftarrow \mathbf{t}^{\mathbf{a}(\mathbf{k}) \pmod{p}}$ (at least, when examining the substitution modulo t^p), where $\mathbf{a}(\mathbf{k}) = \sum a_i k^i$ can be regarded as a polynomial of degree $\leq n$. Thus, it follows that two monomials \mathbf{x}^α and \mathbf{x}^β agree under this substitution with probability $\leq n/p = 1/\text{poly}(n, d)$ for a random $k \in \mathbb{Z}_p$. By using the $\boldsymbol{\alpha}$ to interpolate through these choices of k , this yields the $m = 1$ construction. For $m > 1$, one takes $x_i \leftarrow t_1^{k_1^i \pmod{p}} \dots t_m^{k_m^i \pmod{p}}$, and observes that two monomials then agree with probability $\leq 1/\text{poly}(n, d)^m$. Taking a union bound over s^2 possible collisions amongst the monomials in S shows that some value of the $\{k_j\}_j$, and thus of $\boldsymbol{\alpha} \in \mathbb{F}^m$, will yield distinct monomials in \mathbf{t} .

Another important tool is the generator of Shpilka-Volkovich [SV09].

Theorem 2.4 (Shpilka-Volkovich generator [SV09]). *Let \mathbb{F} be a field of size $> n$. Let $\xi_0, \xi_1, \dots, \xi_n$ be distinct elements in \mathbb{F} , and $\ell \in [n]$. Then there is a $\text{poly}(n, \ell)$ -explicit polynomial map $\mathcal{G}_{n,\ell}^{\text{SV}}(y_1, \dots, y_\ell, z_1, \dots, z_\ell) \in \mathbb{F}[\mathbf{y}, \mathbf{z}]^n$, such that*

$$(\mathcal{G}_{n,\ell}^{\text{SV}}(\mathbf{y}, \xi_{i_1}, \dots, \xi_{i_\ell}))_k = \sum_{j: i_j=k} y_j,$$

for $0 \leq i_j \leq n$, and $k \in [n]$. Specifically, $(\mathcal{G}_{n,\ell}^{\text{SV}})_k = \sum_{j \in [\ell]} \mathbb{1}_{z_j=\xi_k} \cdot y_j$, where $\mathbb{1}_{z=\xi_k}$ is a univariate polynomial in z with degree $\leq n$. \triangle

That is, the $\mathbb{1}_{z=\xi_k}$ are the Lagrange interpolation polynomials, so that $\mathbb{1}_{z_j=\xi_k} = \delta_{j,k}$. Note that this generator is in a sense ℓ -wise independent. That is, by setting the z_j appropriately, we can

insert the \mathbf{y} variables into any ℓ of the \mathbf{x} variables. Note that the setting $z_j \leftarrow \xi_0$ zeroes out the appropriate y_j in the polynomial map (a convenience for handling $< \ell$ -wise positions), where as $z_j \leftarrow \xi_i$ for $i \geq 1$ sends y_j to the x_i slot. It follows if a polynomial f depends on only ℓ of the variables in \mathbf{x} then $f \neq 0$ iff $f \circ \mathcal{G}_{n,\ell}^{SV} \neq 0$. However, $\mathcal{G}_{n,\ell}^{SV}$ also has the property that it hits polynomials with small-support, see [Lemma 3.4](#), which is more relevant for this paper.

We shall need some more tools for later theorems, and for the sake of clarity we shall state them as and when we need.

3 Shifts, Rank Condensers, and Rank Concentration

In this section we will explore the properties of the shifting map $f(\mathbf{x}) \mapsto f(\mathbf{x} + \mathbf{t})$. Following Agrawal-Saha-Saxena [[ASS12](#)] and Forbes-Shpilka [[FS12b](#)], we will look not just at one polynomial at a time, but rather at a set of polynomials, as these polynomials will represent intermediate computations in the computation. Given a vector of polynomials $\mathbf{f} = (f_1, \dots, f_r) \in \mathbb{F}[\mathbf{x}]^r$, we associate to it a matrix M such that $M_{a,i}$ is the coefficient of \mathbf{x}^a in the polynomial f_i . Thus, M will have r columns. The rows of M are drawn from all monomials in \mathbf{x} of low degree, where the degree bounds will depend on the context.

The above discussion uses the language of coefficients of monomials. This is equivalent to a notion of a Hasse derivative, the derivative language is sometimes more natural and thus will be used below. Thus, we will think of the matrix M with $M_{a,i} = \partial_{\mathbf{x}^a}(f_i)(\mathbf{0})$. Thus, the row of M associated with \mathbf{a} is the r -dimensional vector $\partial_{\mathbf{x}^a}(\mathbf{f})(\mathbf{0})$.

Given this matrix, we can then study its rank, as well as its row span. Clearly, the rank is $\leq r$ by construction. Further, the polynomials are all zero iff the rank is 0. If the polynomials are nonzero, then there is some basis of the row span of M , which yield derivatives $\partial_{\mathbf{x}^a}(\mathbf{f})(\mathbf{0})$ that are nonzero vectors. If we can access these derivatives efficiently, this will allow us to decide if \mathbf{f} is zero or not. To capture this, we follow Agrawal-Saha-Saxena [[ASS12](#)] and define the notion of rank concentration.

Definition 3.1 (Rank concentration). For a vector of polynomials $\mathbf{f} \in \mathbb{F}[\mathbf{x}]^r$, and a set of monomials $S \subseteq \mathbb{F}[\mathbf{x}]$, we shall say that \mathbf{f} is *rank concentrated on S at $\alpha \in \mathbb{F}^n$* if the derivatives of \mathbf{f} with respect to the monomials in S span all of the derivatives of \mathbf{f} . That is,

$$\text{span} \{ \partial_{\mathbf{x}^a}(\mathbf{f})(\alpha) \}_{a \in S} = \text{span} \{ \partial_{\mathbf{x}^a}(\mathbf{f})(\alpha) \}_a.$$

In particular, if \mathbf{f} is rank concentrated on the set of monomials of support size at most ℓ , then we shall say that \mathbf{f} is *support- ℓ rank concentrated*. \diamond

In this paper, we will frequently abuse this notation and apply it to matrices of polynomials $F \in \mathbb{F}[\mathbf{x}]^{n \times m}$, where we identify $\mathbb{F}[\mathbf{x}]^{n \times m} \equiv \mathbb{F}[\mathbf{x}]^{nm}$. In the above definition we have two vector spaces to consider, the span of derivatives in S , and the span of all derivatives. Note that the second vector space does not depend on the underlying point α , as stated in the following lemma, which follows from polynomial interpolation and the fact that Hasse derivatives are exactly the coefficients of the polynomial.

Lemma 3.2. *Let $\mathbf{f} \in \mathbb{F}[\mathbf{x}]^r$ be a vector of polynomials, each of degree $\leq d$, and suppose $|\mathbb{F}| > d$. Then for any $\alpha \in \mathbb{F}^n$, $\text{span} \{ \partial_{\mathbf{x}^a}(\mathbf{f})(\alpha) \}_a = \text{span} \{ \mathbf{f}(\beta) \}_{\beta \in \mathbb{F}^n}$.* \triangle

The goal of Agrawal-Saha-Saxena [[ASS12](#)], as well as this work, is to construct small sets of α 's such that \mathbf{f} must have small-support rank concentration at one such α . The next two lemmas show

why this suffices for polynomial identity testing. The first lemma shows that small-support rank concentration implies the existence of a small-support monomial with nonzero coefficient.

Lemma 3.3. *Let $\mathbf{f} \in \mathbb{F}[\mathbf{x}]^r$ be a vector of polynomials that is support- ℓ rank concentrated at $\boldsymbol{\alpha} \in \mathbb{F}^n$. Let $g(\mathbf{x}) := \langle \boldsymbol{\beta}, \mathbf{f} \rangle := \sum_{i \in [r]} \beta_i f_i$, for $\boldsymbol{\beta} \in \mathbb{F}^r$. Then $g(\mathbf{x})$ is nonzero iff there is a small-support monomial $\mathbf{x}^{\mathbf{a}}$ with $|\mathbf{a}|_0 \leq \ell$ such that $\text{Coeff}_{\mathbf{x}^{\mathbf{a}}}(h) \neq 0$, where $h(\mathbf{x}) := g(\mathbf{x} + \boldsymbol{\alpha})$.*

Proof: First, observe that $h \neq 0$ iff $g \neq 0$.

\Leftarrow : Clearly if $\text{Coeff}_{\mathbf{x}^{\mathbf{a}}}(h) \neq 0$, then $h \neq 0$, so $g \neq 0$.

\Rightarrow : That $g \neq 0$, and thus $h \neq 0$ implies there is some \mathbf{b} such that

$$\begin{aligned} 0 &\neq \text{Coeff}_{\mathbf{x}^{\mathbf{b}}}(h) \\ &= \text{Coeff}_{\mathbf{x}^{\mathbf{b}}}(\langle \boldsymbol{\beta}, \mathbf{f}(\mathbf{x} + \boldsymbol{\alpha}) \rangle) \\ &= \langle \boldsymbol{\beta}, \text{Coeff}_{\mathbf{x}^{\mathbf{b}}}(\mathbf{f}(\mathbf{x} + \boldsymbol{\alpha})) \rangle \\ &= \langle \boldsymbol{\beta}, \partial_{\mathbf{x}^{\mathbf{b}}}(\mathbf{f})(\boldsymbol{\alpha}) \rangle. \end{aligned}$$

By the rank concentration we have that $\partial_{\mathbf{x}^{\mathbf{b}}}(\mathbf{f})(\boldsymbol{\alpha}) \in \text{span}\{\partial_{\mathbf{x}^{\mathbf{a}}}(\mathbf{f})(\boldsymbol{\alpha})\}_{|\mathbf{a}|_0 \leq \ell}$, from which it follows that there is some \mathbf{a} with $|\mathbf{a}|_0 \leq \ell$ such that $\langle \boldsymbol{\beta}, \partial_{\mathbf{x}^{\mathbf{a}}}(\mathbf{f})(\boldsymbol{\alpha}) \rangle$ is nonzero. By identical logic as the above, this inner-product equals $\text{Coeff}_{\mathbf{x}^{\mathbf{a}}}(h)$, yielding the claim. \square

Thus, polynomial identity testing for polynomials with rank concentration reduces to the case when the polynomials have nonzero small support monomial. We now show how to use the generator of Shpilka-Volkovich [SV09] to hit such polynomials. Note that the ability to hit such polynomials does not follow from the usual naïve probabilistic method proof, as while such polynomials can be consider “simple” they are too numerous to use a naïve union bound. Note that Agrawal-Saha-Saxena [ASS12] did not use the Shpilka-Volkovich [SV09] generator to hit polynomials with a small-support monomial, and instead used sufficiently many inputs of low-hamming-weight. Indeed, that the SV-generator works in the below lemma can be proven by observing that this generator contains such low-hamming-weight strings in its image. However, the generator perspective will be crucial for our improvement from $n^{\mathcal{O}(\lg n)}$ to $n^{\mathcal{O}(\lg \lg n)}$ for hitting sets for diagonal circuits, as given in Section 7.

Lemma 3.4. *Let \mathbb{F} be a field with $|\mathbb{F}| > n$. Let $f \in \mathbb{F}[\mathbf{x}]$ be such that f is nonzero iff there is some \mathbf{a} with $|\mathbf{a}|_0 \leq \ell$ such that $\text{Coeff}_{\mathbf{x}^{\mathbf{a}}}(f) \neq 0$. Then $f \neq 0$ iff $f \circ \mathcal{G}_{n,\ell}^{\text{SV}} \neq 0$.*

Proof: \Leftarrow : This is clear.

\Rightarrow : Consider the monomial $\mathbf{x}^{\mathbf{a}}$ of support size $\leq \ell$ in f with nonzero coefficient. Let $\text{supp}(\mathbf{a}) = \{x_{i_1}, \dots, x_{i_k}\}$ be its support for $k \leq \ell$. In $\mathcal{G}_{n,\ell}^{\text{SV}}$ of Theorem 2.4, take $z_j = \xi_{i_j}$ for $j \in [k]$. For $j \in [\ell] \setminus [k]$, take $z_j = \xi_0$. It follows then that the variables outside $\text{supp}(\mathbf{a})$ will receive zero from $\mathcal{G}_{n,\ell}^{\text{SV}}$ and inside $\text{supp}(\mathbf{a})$ they will receive a distinct variable from \mathbf{y} . It follows then the monomials containing support outside $\text{supp}(\mathbf{a})$ are zeroed out, and those inside are preserved. As the monomial $\mathbf{x}^{\mathbf{a}}$ has a nonzero coefficient, it follows that $f \circ \mathcal{G}_{n,\ell}^{\text{SV}} \neq 0$ with this partial setting of the \mathbf{y}, \mathbf{z} , and thus is also true without any setting of \mathbf{y}, \mathbf{z} . \square

Putting these two lemmas together, we get the following corollary.

Corollary 3.5 (Rank concentration to Hitting sets). *Let $\mathbf{f} \in \mathbb{F}[\mathbf{x}]^r$ be a vector of polynomials that is support- ℓ rank concentrated at $\boldsymbol{\alpha} \in \mathbb{F}^n$. Let $g(\mathbf{x}) := \langle \boldsymbol{\beta}, \mathbf{f} \rangle := \sum_{i \in [r]} \beta_i f_i$, for $\boldsymbol{\beta} \in \mathbb{F}^r$. Then $g(\mathbf{x}) \neq 0$ iff $g \circ (\mathcal{G}_{n,\ell}^{\text{SV}} + \boldsymbol{\alpha}) \neq 0$.*

Furthermore, $g \circ (\mathcal{G}_{n,\ell}^{SV} + \alpha)$ depends on 2ℓ variables and has degree $\leq n \deg(h)$. Hence such polynomials g have a hitting set of size $\text{poly}(n, \deg(h))^{2\ell}$. \triangle

We now explore conditions on the points α that guarantee small-support rank concentration. We begin with an example.

3.1 Rank Concentration as a Wronskian

To illustrate how to achieve rank concentration, consider the case when the polynomials in \mathbf{f} are univariate of degree $\leq d$. In this case, we will seek that the rank is concentrated on low-degree derivatives (as all derivatives in this setting are trivially support-1). Specifically, we will want rank to be concentrated on the first r derivatives. Let us write the vectors of all degree derivatives $\partial_{x^i}(\mathbf{f})$ at the point $t \in \mathbb{F}$ in matrix form, yielding

$$\begin{bmatrix} f_1(t) & \cdots & f_r(t) \\ (\partial_x f_1)(t) & \cdots & (\partial_x f_r)(t) \\ \vdots & \ddots & \vdots \\ (\partial_{x^d} f_1)(t) & \cdots & (\partial_{x^d} f_r)(t) \end{bmatrix}.$$

That the rank is concentrated on low-degree means that the row-span of the first r rows, denoted V , equals the span of all of the rows, denoted W . As $V \subseteq W$, this will happen iff $\text{rank } V = \text{rank } W$. However, the columns of the above matrix are the coefficients of the polynomials f_i when expanded around t , and thus the column-rank of this matrix equals the rank of the polynomials $\{f_1, \dots, f_r\}$ as vectors in the vector space $\mathbb{F}[x]$. Invoking row-rank equalling column-rank, it follows that the rank is concentrated at t in the first r rows iff the row-rank of these rows equals the rank of the f_i in $\mathbb{F}[x]$.

The first r rows of the above matrix are known as the *Wronskian* of $\{f_1, \dots, f_r\}$, and it is classically known (for fields of polynomially large characteristic) that the rank (over $\mathbb{F}(t)$) of this matrix equals the rank of the polynomials $\{f_1, \dots, f_r\}$ as vectors in the vector space $\mathbb{F}[x]$ (see, for example, Bostan-Dumas [BD10] for a proof). Thus, by expressing this rank condition via determinants, it follows that there is a degree $\leq rd$ polynomial $p(t)$ such that if $p(a) \neq 0$, then \mathbf{f} has degree $< r$ rank concentration at a . Thus, at least in this example, we see that rank concentration happens almost everywhere, and where it fails is a simple algebraic condition we can avoid by brute-force.

In this work, we will need to generalize the above Wronskian in various ways. First, we will have multivariate polynomials. A multivariate Wronskian is known (again, see Bostan-Dumas [BD10]), but in our application it only guarantees low-degree rank concentration, while this paper needs small-support rank concentration. Further, much of the existing literature on Wronskians focus on fields of (polynomially) large characteristic, while we seek results over any characteristic. We note that several recent results in algebraic complexity (for example [CGK⁺13, KS12]) have been limited to characteristic zero because of their dependence on the classical Wronskian.

Recently Guruswami and Kopparty [GK13] explored the notion of a *subspace design*, and observed that they are in a sense dual to Wronskians. To obtain results over any characteristic, they introduced what they call a *folded* Wronskian, in reference to the folded Reed-Solomon codes of Guruswami-Rudra [GR08b]. They noted that this folded Wronskian was used in Forbes-Shpilka [FS12a] and Guruswami-Wang [GW13] in different guises.

In this work, we extend existing knowledge of Wronskians. First, we observe that the underlying algebraic object in the above is the notion of a *rank condenser*, which we define in [Subsection 3.2](#), where we give a general recipe for constructing rank condensers from error-correcting codes. That the (multivariate or univariate) Wronskian matrix characterizes the rank of polynomials can be expressed as saying that at certain derivative-related matrix is a good rank condenser. To prove this fact, we will show that this derivative-related matrix has code-like properties. Further, we observe that the folded Wronskian of Guruswami-Kopparty [[GK13](#)] can be interpreted as being a Wronskian using a different notion of derivative. Specifically, the Wronskian uses the q -derivative, a q -analogue of the usual derivative, see Kac and Cheung [[KC02](#)]. We note that Bostan, Salvy, Chowdhury, Schost and Lebreton [[BSC⁺12](#)] observed the relation between folded Reed-Solomon codes and q -derivatives.

In this version of the paper, we will develop the tools needed to achieve small-support rank concentration for multivariate polynomials over any characteristic, and this will only use Hasse derivatives. This can be easily interpreted as establishing a “small-support multivariate Wronskian” result, that works over any characteristic. In a future version of this work, we will give a multivariate rank condenser (that is a Wronskian) that simultaneously guarantees small-support and low-degree rank concentration, over any characteristic, appealing to q -derivatives in nonzero characteristic. This will strictly improve the classically known multivariate Wronskian, which may be of independent interest (for example, to the above works using Wronskians).

In the next sections, we will define the notion of a rank condenser, and give a construction based on the parity check matrix of a good error-correcting code. We shall then show that small-support derivatives have such a code structure, which will give the needed results for small-support rank concentration.

3.2 Rank Condensers from Good Codes

In this section we define rank condensers, and show how they can be generically constructed from error correcting codes, following the Cauchy-Binet proof strategy of Dvir, Gabizon and Wigderson [[DGW09](#)] (Dvir, Gabizon and Wigderson [[DGW09](#)] also had a notion of a rank extractor, but with a different notion of rank) and Forbes and Shpilka [[FS12a](#)]. We begin with the definition of rank condensers (which, given the parameters, could be considered as *lossless*).

Definition 3.6 (Rank Condenser Generator). A matrix $E(\mathbf{t}) \in \mathbb{F}[\mathbf{t}]^{n \times m}$ is said to be a (*seeded*) *rank condenser (generator)* for rank r if for every matrix $M \in \mathbb{F}^{m \times k}$ of rank $\leq r$, we have that $\text{rank}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t}) \cdot M) = \text{rank}_{\mathbb{F}}(M)$. \diamond

Note that in the above definition, the notion of rank changes, as one rank is over the field of rational functions $\mathbb{F}(\mathbf{t})$, and the other rank is over \mathbb{F} . This will be the setting we work in, but it is sometimes more convenient to think in terms of the base field \mathbb{F} , leading to the following definition.

Definition 3.7 (Rank Condenser Hitting Set). A collection $\mathcal{E} \subseteq \mathbb{F}^{n \times m}$ is said to be a (*seeded*) *rank condenser (hitting set)* for rank r if for every matrix $M \in \mathbb{F}^{m \times k}$ of rank $\leq r$, there is some $E \in \mathcal{E}$ such that $\text{rank}_{\mathbb{F}}(E \cdot M) = \text{rank}_{\mathbb{F}}(M)$. \diamond

Remark 3.8. A more natural definition of a (linear) condenser would be a family of linear maps $\varphi_i : \mathbb{F}^m \rightarrow \mathbb{F}^n$, such that for any subspace $V \subseteq \mathbb{F}^m$ of rank $\geq r$, there is some i such that $\text{rank} \varphi_i(V) = r$. It can be readily seen that this is equivalent to the hitting set definition above. If $n = r$, then one can consider this an extractor. \diamond

By interpolation over \mathbf{t} , the generator notion yields the hitting set. Conversely, one can construct a generator by interpolating a curve through the collection \mathcal{E} . See Shpilka and Volkovich [SV09] for more on generators versus hitting sets within polynomial identity testing.

In what follows, we will omit the terms “seeded”, “generator” and “hitting set” when it is clear from context. Before turning to the construction, we need one more definition, that of a *monomial order* (see Cox, Little and O’Shea [CLO06] for more on monomial orderings).

Definition 3.9. A *monomial ordering* is a total order \prec on the nonzero monomials in $\mathbb{F}[\mathbf{x}]$ such that

- For all $\mathbf{a} \in \mathbb{N}^n$, $1 \prec \mathbf{x}^{\mathbf{a}}$.
- For all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$, $\mathbf{x}^{\mathbf{a}} \prec \mathbf{x}^{\mathbf{b}}$ implies $\mathbf{x}^{\mathbf{a}+\mathbf{c}} \prec \mathbf{x}^{\mathbf{b}+\mathbf{c}}$ ◇

For concreteness, one can consider the lexicographic ordering on monomials, which is easily seen to be a monomial ordering. We now give our first rank condenser construction.

Lemma 3.10. Let $E(\mathbf{t}) \in \mathbb{F}[\mathbf{t}]^{n \times m}$, with $E = \Lambda(\mathbf{t})^{-1} \cdot H \cdot W(\mathbf{t})$ such that

- $\Lambda(\mathbf{t}) \in \mathbb{F}[\mathbf{t}]^{n \times n}$ is a diagonal matrix, whose diagonal entries are nonzero monomials.
- $H \in \mathbb{F}^{n \times m}$ is the parity check matrix of an error correcting code of distance $> r$. That is, every r columns of H are linearly independent.
- $W(\mathbf{t}) \in \mathbb{F}[\mathbf{t}]^{m \times m}$ is a diagonal matrix, whose diagonal entries are nonzero distinct monomials.

Then $E(\mathbf{t})$ is a rank condenser for rank r .

Furthermore, let $d_i^{\max} = \max_{S \in \binom{[m]}{r}} \sum_{j \in S} \deg_{t_i} W(\mathbf{t})_{j,j}$ and $d_i^{\min} = \min_{S \in \binom{[m]}{r}} \sum_{j \in S} \deg_{t_i} W(\mathbf{t})_{j,j}$. Let $C_i \subseteq \mathbb{F} \setminus \{0\}$ have size $|C_i| > d_i^{\max} - d_i^{\min}$. Then $\mathcal{E} = \{E(\mathbf{t})\}_{\forall i, t_i \in C_i}$ is a rank condenser for rank r .

Proof: Consider any matrix $M \in \mathbb{F}^{m \times k}$ of rank $s \leq r$.

$k > s$: We show the claim by reducing to the case to when $k = s$, which we prove next. Let $M' \in \mathbb{F}^{m \times s}$ be a submatrix of M formed by taking s linearly independent columns of M . It follows then that $\text{rank}_{\mathbb{F}}(M') = \text{rank}_{\mathbb{F}}(M) \geq \text{rank}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t})M) \geq \text{rank}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t})M') = \text{rank}_{\mathbb{F}}(M')$, where we use that row-rank equals column-rank. More specifically, the first inequality uses that $\text{row-span}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t})M) \subseteq \text{row-span}_{\mathbb{F}(\mathbf{t})}(M)$ and that $\text{rank}_{\mathbb{F}}(M) = \text{rank}_{\mathbb{F}(\mathbf{t})}(M)$, and the second inequality uses that $\text{col-span}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t})M') \subseteq \text{col-span}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t})M)$. From this, we see that all inequalities must be met with equality, so $\text{rank}_{\mathbb{F}}(M) = \text{rank}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t})M)$.

$k = s$: As W is diagonal with monomial entries, it induces $w : [m] \rightarrow \mathbb{F}[\mathbf{t}]$ weighting the columns of H , indexed by $[m]$, with monomials in $\mathbb{F}[\mathbf{t}]$ (thus, $w(i) = W_{i,i}$). Let \prec be some monomial order on $\mathbb{F}[\mathbf{t}]$. As the monomials in W are distinct, the order \prec also defines a total order on $[m]$, which we will also call ‘ \prec ’, abusing notation.

As $M \in \mathbb{F}^{m \times s}$ is rank s , there are sets $T \subseteq [m]$ of size s such that $\det(M|_{T \times \bullet}) \neq 0$. As the weights in w are distinct by hypothesis on W , standard greedy/matroid arguments (for example, as seen in Lemma 5.3 with $J = \emptyset$) imply that there is a unique $T_0 \subseteq [m]$ of size s such that $\det(M|_{T_0 \times \bullet}) \neq 0$, and that minimizes $w(T_0)$ in the \prec -order, where $w(T) := \prod_{i \in T} w(i)$. Further, as every s columns of H are linearly independent, it follows that there an $S \subseteq [n]$ of size s such that $\det(H|_{S \times T_0}) \neq 0$. We now use this set to show that the rank is extracted, via the following claim.

Claim. $\det((E(\mathbf{t})M)|_{S \times \bullet}) = \det((\Lambda(\mathbf{t})^{-1}HW(\mathbf{t})M)|_{S \times \bullet}) \neq 0$.

Proof: As $\Lambda(\mathbf{t})$ is diagonal with nonzero diagonal entries, and the determinant is multiplicative, we see that

$$\det((\Lambda(\mathbf{t})^{-1}HW(\mathbf{t})M)|_{S \times \bullet}) = \det(\Lambda(\mathbf{t})|_{S \times S})^{-1} \det((HW(\mathbf{t})M)|_{S \times \bullet}).$$

As $E(\mathbf{t})$ is a matrix with polynomial entries, it follows that $\det((E(\mathbf{t})M)|_{S \times \bullet})$ is a polynomial, so $\det(\Lambda(\mathbf{t})|_{S \times S})$ is nonzero and divides $\det((HW(\mathbf{t})M)|_{S \times \bullet})$. Thus, it suffices to show that $\det((HW(\mathbf{t})M)|_{S \times \bullet}) = \det((HW(\mathbf{t}))|_{S \times \bullet} \cdot M)$ is not zero. To analyze this determinant, we invoke the Cauchy-Binet formula (for example, see Forbes and Shpilka [FS12a] for a proof), which we quote below.

Lemma (Cauchy-Binet Formula). *Let $m \geq n \geq 1$. Let $A \in \mathbb{F}^{n \times m}$, $B \in \mathbb{F}^{m \times n}$. Then $\det(AB) = \sum_{T \in \binom{[m]}{n}} \det(A|_{\bullet \times T}) \det(B|_{T \times \bullet})$ \triangle*

Applying this formula, we see that

$$\det((HW(\mathbf{t}))|_{S \times \bullet} \cdot M) = \sum_{T \in \binom{[m]}{s}} \det((HW(\mathbf{t}))|_{S \times T}) \det(M|_{T \times \bullet})$$

as W is diagonal and the determinant is multiplicative,

$$\begin{aligned} &= \sum_{T \in \binom{[m]}{s}} \det(H|_{S \times T}) \det(M|_{T \times \bullet}) \prod_{i \in T} W(\mathbf{t})_{i,i} \\ &= \det(H|_{S \times T_0}) \det(M|_{T_0 \times \bullet}) w(T_0) + \sum_{T \in \binom{[m]}{s}} \det(H|_{S \times T}) \det(M|_{T \times \bullet}) w(T) \end{aligned}$$

using the choice of T_0 and the uniqueness of its weight, there is a $c \in \mathbb{F} \setminus \{0\}$,

$$= c \cdot w(T_0) + (\text{terms of weight } \succ w(T_0))$$

from which it follows that $\det((HW(\mathbf{t}))|_{S \times \bullet} \cdot M)$, and thus $\det((E(\mathbf{t})M)|_{S \times \bullet})$, are nonzero polynomials in \mathbf{t} , as there is no cancellation of the nonzero term $c \cdot w(T_0)$. \diamond

The above claim shows that the $n \times s$ matrix $E(\mathbf{t})M$ has an $s \times s$ minor of rank s , so $\text{rank}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t}) \cdot M) = s = \text{rank}_{\mathbb{F}}(M)$ as desired.

hitting set: We derive the hitting set rank condenser from the generator via interpolation. In particular, we need to form a large enough cube of evaluation points to ensure that the nonzero polynomial $\det((E(\mathbf{t})M)|_{S \times \bullet})$ assumes a nonzero value. As the cube avoids zero in each entry, we can divide out the terms contributed by $\Lambda(\mathbf{t})$. Thus, it remains to hit $\det((HW(\mathbf{t}))|_{S \times \bullet} \cdot M)$. Examining the above expression given by the Cauchy-Binet formula, it follows that d_i^{\max} is the maximum degree in which t_i appears, and d_i^{\min} is the minimum. As $t_i \neq 0$, we can divide out by the minimum degree, leaving a polynomial with degree in t_i of $d_i^{\max} - d_i^{\min}$, for each i . Standard polynomial interpolation then shows that the determinant assumes a nonzero value at some point in the cube $C_1 \times C_2 \times \dots$, so that $\text{rank}_{\mathbb{F}}(E(\mathbf{t})M) = \text{rank}_{\mathbb{F}}(M)$ at that point, as desired. \square

Remark 3.11. By taking H so that $H_{i,j} = \omega^{ij}$, where ω has large multiplicative order, H is then the parity check matrix of the dual Reed-Solomon code. The resulting rank condenser is the one of Forbes and Shpilka [FS12a], who used it (with some modification) to construct rank-metric codes meeting a bound of Roth [Rot91] over algebraically closed fields (Roth [Rot91] also gave such constructions). \diamond

3.3 Small-Support Rank Concentration via Rank Condensers

The above recipe shows how to construct a rank condenser in a certain way. Here, we show how to instantiate this recipe, by showing that the shifting map $f(x) \mapsto f(x+t)$ has code-like properties. Consider how this shifting changes the coefficients of f ,

$$f(x+t) = \sum_b \text{Coeff}_{x^b}(f) (x+t)^b = \sum_b \text{Coeff}_{x^b}(f) \sum_a \binom{b}{a} x^a t^{b-a}. \quad (3.12)$$

Thus, the coefficient of x^a in $f(x+t)$ equals $\sum_b \text{Coeff}_{x^b}(f) \binom{b}{a} t^{b-a}$. This linear transformation is summarized in the following construction.

Construction 3.13. Let $n \geq 1, d \geq 0$. Let $T(t) \in \mathbb{F}[t]^{\llbracket d \rrbracket^n \times \llbracket d \rrbracket^n}$ be the *transfer* matrix of the shift map $f(x) \mapsto f(x+t)$ when acting on n -variate polynomials of individual degree $< d$, when these polynomials are expanded in the monomial basis. That is, $T_{a,b} = \binom{b}{a} t^{b-a} = \partial_{x^a}(x^b)(t)$.

Alternatively, this matrix changes basis, from expressing f in terms of its Hasse derivatives at $\mathbf{0}$ to expressing f in terms of its Hasse derivatives at t .

Define S_r to be the set of all monomials x^a of individual degree $< d$, such that $|a|_0 \leq \lfloor \lg r \rfloor$. Define $T_r(t)$ to be the submatrix $T|_{S_r \times \bullet}$. \diamond

Remark. For the reader acquainted with the work of Agrawal-Saha-Saxena [ASS12], we note that our matrix T is similar to the transfer matrix considered in that work. Specifically Equation (4) and Lemma 10 of [ASS12] are captured by our definition of T and Equation (3.12). The main difference is that [ASS12] state and prove their results in the language of Hadamard algebras while we simply work with polynomials. \diamond

We will now work to show that T_r is a rank condenser. To do so, we start with the following combinatorial lemma. This lemma is similar to the sorting argument of Claim 18 in Agrawal-Saha-Saxena [ASS12], and is vaguely related to the notion of “partial IDs” as explored in Wigderson-Yehudayoff [WY12].

Lemma 3.14. Let $\mathbf{b}_1, \dots, \mathbf{b}_r \in \Sigma^n$ be distinct strings. Then there is an $i_0 \in [r]$ and $|S| \subseteq [n]$ with $|S| \leq \lg r$ such that $(\mathbf{b}_{i_0})|_S \neq (\mathbf{b}_i)|_S$ for $i \neq i_0$.

Proof: By induction on r .

$r = 1$: This is vacuous, as $i \neq i_0$ never occurs, so $i_0 = 1$ and $S = \emptyset$ satisfy the requirements.

$r > 1$: As the \mathbf{b}_i are distinct, there is some coordinate $j \in [n]$ such that the $(\mathbf{b}_i)|_j$ are not all the same. Let $\sigma \in \Sigma$ be the minimum frequency symbol appearing as $(\mathbf{b}_i)|_j$ for some i . Let $T := \{i : (\mathbf{b}_i)|_j = \sigma\} \subseteq [r]$, so that $|T| \leq r/2$ by choice of σ . Apply the induction hypothesis to the $\{\mathbf{b}_i : i \in T\}$ as strings in $\Sigma^{[n] \setminus \{j\}}$, which is possible as the strings in T agree in the j -th position, so are still distinct with this position removed. Thus yields an $i'_0 \in T$ and a set $S' \subseteq [n] \setminus \{j\}$ such that $|S'| \leq \lg r - 1$ and $(\mathbf{b}_{i'_0})|_{S'} \neq (\mathbf{b}_i)|_{S'}$ for $i \in T \setminus \{i'_0\}$. Take $i_0 := i'_0$, and $S := S' \cup \{j\}$. Then for $(\mathbf{b}_{i_0})|_S \neq (\mathbf{b}_i)|_S$ for any $i \neq i_0$, where this disagreement occurs in S' for $i \in T$, and occurs at position j for $i \notin T$. \square

This combinatorial lemma shows that in any set of strings there is a small “fingerprint” that distinguishes some string from all the others. In our situation, strings will be (exponent vectors of) monomials, and we will try to distinguish monomials via derivatives. The above fingerprint will allow our derivatives to be of small-support. We now build these derivatives, starting with the univariate case.

Lemma 3.15. Fix $d \geq 0$. For $j \in \llbracket d \rrbracket$, there is a differential operator $\Delta_j = \sum_{k \in \llbracket d \rrbracket} c_k \partial_{x^k}$ such that $\Delta_j(x^i)(1) = \mathbb{1}_{i=j}$.

Proof: Consider the matrix $D \in \mathbb{F}^{\llbracket d \rrbracket \times \llbracket d \rrbracket}$ such that $D_{i,j} := \partial_{x^i}(x^j)(1) = \binom{j}{i}$. Note that this is an upper triangular matrix, with 1's along the diagonal. Thus, this matrix is invertible, and let C be its inverse. Define $c_k := C_{j,k}$. Thus $\Delta_j(x^i)(1) = \sum C_{j,k} \partial_{x^k}(x^i)(1) = \sum C_{j,k} D_{k,i} = (C|_{j \times \bullet}) \cdot (D|_{\bullet \times i}) = \mathbb{1}_{i=j}$, as desired. \square

Note that in the above, if we used normal (non-Hasse) derivatives then the diagonal of D would not have 1's, and D would not be invertible in sufficiently small characteristic. We can now combine the fingerprint of strings, with the univariate derivatives, to yield multivariate derivatives isolating some monomial.

Lemma 3.16. Let x^{b_1}, \dots, x^{b_r} be distinct monomials on the n variables x , and of individual degree $< d$. Then there is a set $T \subseteq [n]$ with $|T| \leq \lfloor \lg r \rfloor$, a differential operator

$$\Delta = \sum_{\substack{\text{supp}(\mathbf{a}) \subseteq T \\ |\mathbf{a}|_\infty < d}} c_{\mathbf{a}} \partial_{x^{\mathbf{a}}} \quad (3.17)$$

and an $i_0 \in [r]$ such that $\Delta(x^{b_i})(1) = \mathbb{1}_{i=i_0}$.

Proof: Lemma 3.14 yields the set $T \subseteq [n]$ with $|T| \leq \lfloor \lg r \rfloor$, and the index $i_0 \in [r]$. We now construct Δ . For $j \in T$, let $\Delta_j = \sum_{k \in \llbracket d \rrbracket} c_{j,k} \partial_{x_j^k}$ be the differential operator provided by Lemma 3.16 so that $\Delta_j(x_j^{b_j}) = \mathbb{1}_{b_j = (b_{i_0})|_j}$. Now let $\Delta = \prod_{j \in T} \Delta_j$, where this product is the composition of the operators. Recalling that $\partial_{x^{\mathbf{a}}} \partial_{y^{\mathbf{b}}} = \partial_{x^{\mathbf{a}} y^{\mathbf{b}}}$ for disjoint variables x, y , we see that Δ has the form of Equation 3.17. Now consider $\Delta(x^{b_i})$. As Δ_j only affects variable x_j , it follows that

$$\begin{aligned} \Delta(x^{b_i})(\mathbf{1}) &= \prod_{j \in T} \Delta_j \left(x_j^{(b_i)|_j} \right) (\mathbf{1}) \cdot \prod_{j \notin T} (x_j^{(b_i)|_j})(\mathbf{1}) \\ &= \prod_{j \in T} \mathbb{1}_{(b_i)|_j = (b_{i_0})|_j} \cdot \prod_{j \notin T} 1 \\ &= \mathbb{1}_{i=i_0}, \end{aligned}$$

where the last equality used the isolating properties of T . \square

The above shows that we can distinguish some monomial from an entire set, using small-support derivatives. Straightforward induction shows we can extend this to every monomial in the set.

Corollary 3.18. Let x^{b_1}, \dots, x^{b_r} be distinct monomials on the n variables x , and of individual degree $< d$. Then there is a permutation $\pi : [r] \rightarrow [r]$, and differential operators $\Delta_1, \dots, \Delta_r$ such that

$$\Delta_i(x^{b_{\pi(j)}})(\mathbf{1}) = \begin{cases} 1 & i = j \\ 0 & j < i \end{cases}.$$

Further, each Δ_i is a linear combination of derivatives (of individual degree $< d$) with support contained in a set of size $\leq \lfloor \lg i \rfloor$. \triangle

The above corollary shows that for any set of monomials we can construct a set of differential operators whose application on these monomials induces a triangular matrix, which clearly has full rank. We can thus use this to derive the needed properties of the T_r matrix.

Lemma 3.19. *Assume the setup of [Construction 3.13](#). Then $T_r(\mathbf{1})$ is the parity check matrix of a distance $> r$ code. That is, every r columns are linearly independent.*

Proof: Let $\mathbf{b}_1, \dots, \mathbf{b}_r$ be r distinct monomials indexing columns in T . Consider the differential operators from [Corollary 3.18](#). The operators Δ_i (evaluated at $\mathbf{1}$) acts on the monomials \mathbf{b}_j and produces a vector $\mathbf{v}_i \in \mathbb{F}^r$. By construction, each Δ_i is a linear combination of support $\leq \lfloor \lg r \rfloor$ derivatives, and thus \mathbf{v}_i a linear combination of the rows of T_r (when restricted to the columns induced by $\mathbf{b}_1, \dots, \mathbf{b}_r$). As the \mathbf{v}_i form a triangular system (in some column ordering), it follows that the rows of T_r , when restricted to the columns induced by $\mathbf{b}_1, \dots, \mathbf{b}_r$, have rank r . As row-rank equals column-rank, it follows the columns indexed by the \mathbf{b}_j are linearly independent, as desired. \square

Thus, the $T_r(\mathbf{1})$ matrix is a parity check matrix of a code of distance $> r$. The above sections showed how to use such matrices to get a rank condenser. Before we do so, we introduce the following definition. It will allow us to encapsulate the essential properties of the shifts \mathbf{t} needed to ensure rank condensation.

Definition 3.20. Let $\mathbf{g} : \mathbb{F}^m \times \mathbb{F}^{m'} \rightarrow \mathbb{F}^n$ be a polynomial map. It is an *individual degree $< d$, ℓ -wise independent monomial map* if for every $S \subseteq [n]$ of size $\leq \ell$, there is an $\alpha \in \mathbb{F}^{m'}$ such that polynomials $\{\mathbf{g}(\mathbf{t}, \alpha)^a\}_{\text{supp}(a) \subseteq S, |a|_\infty < d}$ are nonzero, distinct monomials in \mathbf{t} . \diamond

As a trivial example, if we have n independent variables, these form an n -wise independent monomial map. Note the order of quantification, that the choice of α can depend on the set S . When this is applied, the values for α will be interpolated over some cube, which will implicitly union bound over all S . We now put the ingredients together to get our rank condenser.

Corollary 3.21. *Assume the setup of [Construction 3.13](#). Let $\mathbf{g} : \mathbb{F}^m \times \mathbb{F}^{m'} \rightarrow \mathbb{F}^n$ be an individual degree $< d$, n -wise independent monomial map. Then $T_r(\mathbf{g}(\mathbf{t}, \mathbf{s}))$ is a rank condenser for rank r .*

Proof: Fix the $\alpha \in \mathbb{F}^{m'}$ guaranteed by the monomial map \mathbf{g} , when asking for independence on all n variables, so that we can now regard $\mathbf{g}(\mathbf{t}, \alpha)$ as a polynomial map in $\mathbb{F}[\mathbf{t}]$. Now note that $(T_r(\mathbf{t}))_{\mathbf{a}, \mathbf{b}} = \binom{\mathbf{b}}{\mathbf{a}} \mathbf{t}^{\mathbf{b}-\mathbf{a}} = (\mathbf{t}^{\mathbf{a}})^{-1} \cdot T_r(\mathbf{1}) \cdot \mathbf{t}^{\mathbf{b}}$. Thus, we can decompose $T_r(\mathbf{g}(\mathbf{t}, \alpha)) = \Lambda(\mathbf{t}, \alpha)^{-1} \cdot T_r(\mathbf{1}) \cdot W(\mathbf{t}, \alpha)$, where Λ , $T_r(\mathbf{1})$ and W fit the hypothesis of [Lemma 3.10](#), as \mathbf{g} is n -wise independent monomial map for degree $< d$, and by [Lemma 3.19](#). Thus, $T_r(\mathbf{g}(\mathbf{t}, \alpha))$ is a rank condenser for rank r . Removing the substitution of \mathbf{s} , it follows that $T_r(\mathbf{g}(\mathbf{t}, \mathbf{s}))$ is a rank condenser as well. \square

Reinterpreting the above, we get the main result of this section, showing how to achieve rank concentration (recall [Definition 3.1](#)).

Corollary 3.22. *Let $\mathbf{f} \in \mathbb{F}[\mathbf{x}]^r$ be polynomials of individual degree $< d$ on the n -variables \mathbf{x} . Let $\mathbf{g} : \mathbb{F}^m \times \mathbb{F}^{m'} \rightarrow \mathbb{F}^n$ be an individual degree $< d$, n -wise independent monomial map. Then \mathbf{f} has support- $\lfloor \lg r \rfloor$ rank concentration at $\mathbf{g}(\mathbf{t}, \mathbf{s})$ over the field $\mathbb{F}(\mathbf{t}, \mathbf{s})$.*

Proof: Expand the polynomials \mathbf{f} in terms of their Hasse derivatives at zero, giving the matrix M , so that $M_{\mathbf{b}, i} = \partial_{\mathbf{x}^{\mathbf{b}}}(f_i)(\mathbf{0})$. Consider the multiplication $T_r(\mathbf{g}(\mathbf{t}, \mathbf{s})) \cdot M$. By [Corollary 3.21](#) it follows

that $\text{rank}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} T_r(\mathbf{g}(\mathbf{t}, \mathbf{s}))M = \text{rank}_{\mathbb{F}} M$. Thus, $T_r(\mathbf{g}(\mathbf{t}, \mathbf{s}))M$ and M have the same $\mathbb{F}(\mathbf{t}, \mathbf{s})$ -row-span. From the definition of T_r and [Equation 3.12](#), we then get that

$$\begin{aligned} \text{span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} \{ \partial_{\mathbf{x}^{\mathbf{a}}}(\mathbf{f})(\mathbf{g}(\mathbf{t}, \mathbf{s})) \}_{\substack{|\mathbf{a}|_0 \leq \lfloor \lg r \rfloor \\ |\mathbf{a}|_\infty < d}} &= \text{row-span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})}(T_r(\mathbf{g}(\mathbf{t}, \mathbf{s}))M) \\ &= \text{row-span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})}(M) \\ &= \text{span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} \{ \partial_{\mathbf{x}^{\mathbf{a}}}(\mathbf{f})(\mathbf{0}) \}_{\mathbf{a}} \\ &= \text{span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} \{ \partial_{\mathbf{x}^{\mathbf{a}}}(\mathbf{f})(\mathbf{g}(\mathbf{t}, \mathbf{s})) \}_{\mathbf{a}} \end{aligned}$$

where we used [Lemma 3.2](#) in the last equality to change the point of derivation. \square

4 Hitting Sets for Commutative ROABPs

In this section, we give $n^{\mathcal{O}(\lg n)}$ -size hitting sets for polynomials that are computed by ROABPs in *all* variable orders, and thus are in some sense *commutative*. This class is also characterized by having low *evaluation dimension* a concept of Saptharishi, as reported in Forbes-Shpilka [[FS12b](#)], who gave $n^{\mathcal{O}(\lg n)}$ -size hitting sets for this class. The analysis of the hitting sets will follow quickly from the rank concentration results of [Subsection 3.3](#), and can be seen as an alternative proof of some of the results of the work of Agrawal-Saha-Saxena [[ASS12](#)].⁵ While this does not improve upon the parameters of the results of Agrawal-Saha-Saxena [[ASS12](#)] or Forbes-Shpilka [[FS12b](#)], we will see in [Section 7](#) how to combine the rank concentration ideas with the generator of Forbes-Shpilka [[FS12b](#)] (using techniques from hashing, and the generator of Shpilka-Volkovich [[SV09](#)]) to obtain $n^{\mathcal{O}(\lg \lg n)}$ size hitting sets for certain subclasses of these polynomials, such as diagonal circuits.

We begin by showing that for commutative ROABPs, establishing small-support rank concentration for all n variables follows from small-support rank concentration for all size- $\Omega(\lg r)$ subsets of variables. Establishing rank concentration for these small subsets of variables can then be done by brute-force using the rank condensers of [Subsection 3.3](#).

Theorem 4.1. *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{r \times r}$ be of individual degree $< d$, and be computed by a width- r commutative ROABP. Let $\mathbf{g}(\mathbf{t}, \mathbf{s})$ be an individual degree $< d$, $(\lfloor \lg r^2 \rfloor + 1)$ -wise independent monomial map. Then, $F(\mathbf{x})$ has support- $\lfloor \lg r^2 \rfloor$ rank concentration at $\mathbf{g}(\mathbf{t}, \mathbf{s})$ over the field $\mathbb{F}(\mathbf{t}, \mathbf{s})$.*

Proof: Consider some derivative $\partial_{\mathbf{x}^{\mathbf{a}_0}}(F)$, with $\mathbf{a}_0 \in \llbracket d \rrbracket^n$. We wish to show that this derivative, evaluated at $\mathbf{g}(\mathbf{t}, \mathbf{s})$, is contained in the $\mathbb{F}(\mathbf{t}, \mathbf{s})$ -span of the derivatives of small-support, evaluated at $\mathbf{g}(\mathbf{t}, \mathbf{s})$. Thus, if the derivative is already support $\leq \lfloor \lg r^2 \rfloor$, then this is trivial. Now consider when this is not true. Thus, we can partition the monomial $\mathbf{x}^{\mathbf{a}_0}$ into $\mathbf{y}^{\mathbf{b}_0} \mathbf{z}^{\mathbf{c}_0}$ such that \mathbf{y} has $\lfloor \lg r^2 \rfloor + 1$ variables and \mathbf{b}_0 has full-support.

As F is computable by a width- r commutative ROABP, we can express it then as $F(\mathbf{x}) = F(\mathbf{y}, \mathbf{z}) = G(\mathbf{y}) \cdot H(\mathbf{z})$, for $G \in \mathbb{F}[\mathbf{y}]^{r \times r}$ and $H \in \mathbb{F}[\mathbf{z}]^{r \times r}$.⁶ By bilinearity of matrix multiplication,

⁵This section does not give $n^{\mathcal{O}(\lg n)}$ -size hitting sets for depth-3 set-multilinear polynomials, one of the core results of Agrawal-Saha-Saxena [[ASS12](#)]. The results of [Section 6](#) do cover this class of polynomials, by giving a $n^{\mathcal{O}(\lg^2 n)}$ -size hitting set for a more general model. However, the techniques of this section do recover the Agrawal-Saha-Saxena [[ASS12](#)] result, essentially by changing $x_i^j \mapsto x_{i,j}$ in all of our arguments. This changes the transfer matrix, and the set of monomials that the monomial map must preserve. However, the techniques (to show the transfer matrix is a rank condenser, that we can shift using low-wise independent maps, etc.) can be adapted to these changes in a straightforward manner.

⁶This is where we use the commutativity of the ROABP.

we can factor the derivative as $\partial_{\mathbf{x}^{a_0}}(F) = \partial_{\mathbf{y}^{b_0}}(G) \cdot \partial_{\mathbf{z}^{c_0}}(H)$. Now observe that the output of $\mathbf{g}(\mathbf{t}, \mathbf{s})$, when restricted to \mathbf{y} , is still an individual degree $< d$, $(\lfloor \lg r^2 \rfloor + 1)$ -wise independent monomial map. Thus, as \mathbf{y} has $\leq \lfloor \lg r^2 \rfloor + 1$ variables, it follows from [Corollary 3.22](#) that $G(\mathbf{y})$ has support- $\lfloor \lg r^2 \rfloor$ rank concentration at $\mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{y}}$, over $\mathbb{F}(\mathbf{t}, \mathbf{s})$. Rephrasing, this means that

$$\partial_{\mathbf{y}^{b_0}}(G)(\mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{y}}) \in \text{span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} \{ \partial_{\mathbf{y}^b}(G)(\mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{y}}) \}_{|b|_0 \leq \lfloor \lg r^2 \rfloor}.$$

Invoking again the bilinearity of matrix multiplication, it follows that we can multiply the above equation by $\partial_{\mathbf{z}^{c_0}}(H)$, yielding

$$\begin{aligned} \partial_{\mathbf{x}^{a_0}}(F)(\mathbf{g}(\mathbf{t}, \mathbf{s})) &= \partial_{\mathbf{y}^{b_0}}(G)(\mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{y}}) \cdot \partial_{\mathbf{z}^{c_0}}(H)(\mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{z}}) \\ &\in \text{span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} \{ \partial_{\mathbf{y}^b}(G)(\mathbf{g}(\mathbf{t}, \mathbf{s})) \partial_{\mathbf{z}^{c_0}}(H)(\mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{z}}) \}_{|b|_0 \leq \lfloor \lg r^2 \rfloor} \\ &\subseteq \text{span}_{\mathbb{F}(\mathbf{t}, \mathbf{s})} \{ \partial_{\mathbf{x}^a}(F)(\mathbf{g}(\mathbf{t}, \mathbf{s})) \}_{|a|_0 < |\text{supp}(\mathbf{a}_0)|}. \end{aligned}$$

Thus, this shows that for any derivative $\partial_{\mathbf{x}^{a_0}}(F)$ with support $> \lfloor \lg r^2 \rfloor$, its evaluation at $\mathbf{g}(\mathbf{t}, \mathbf{s})$ is contained in the $\mathbb{F}(\mathbf{t}, \mathbf{s})$ -span of derivatives with smaller support. Applying this argument repeatedly (each time with a new partition $\mathbf{x}^{a_0} = \mathbf{y}^{b_0} \mathbf{z}^{c_0}$) thus yields the claim. \square

Thus, the above shows that given the appropriate monomial map, we can achieve small-support rank concentration for commutative ROABPs. We now observe that the generator of Shpilka and Volkovich [[SV09](#)] gives such a monomial map.

Lemma 4.2. *Let \mathbb{F} be a field with $|\mathbb{F}| > n$. Then the SV-generator $\mathcal{G}_{n, \ell}^{\text{SV}} : \mathbb{F}^\ell \times \mathbb{F}^\ell \rightarrow \mathbb{F}^n$ of [Theorem 2.4](#) is an individual degree $< d$, ℓ -wise independent monomial map.*

Proof: As argued in [Lemma 3.4](#), for any subset $S \subseteq [n]$ of size $\leq \ell$, we can set the \mathbf{z} variables appropriately such that $|S|$ of the \mathbf{y} variables are exactly planted into the positions $\mathbf{x}|_S$. It is then clear that this is a monomial map, and all individual degree $< d$ monomials of this map are distinct. \square

Thus, we have seen that shifting by a monomial map yields rank concentration, how to construct such a monomial map, and how rank concentration yields hitting sets. Putting this all together, we obtain hitting sets as presented in the following corollary.

Corollary 4.3. *Let $|\mathbb{F}| > nd$. Let $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be of individual degree $< d$, and be computed by a width- r commutative ROABP. Then $f \not\equiv 0$ iff $f \circ \mathcal{G}_{n, 1+2\lfloor 2\lg r \rfloor}^{\text{SV}} \not\equiv 0$.*

In particular, there is a $\text{poly}(n, d)^{\mathcal{O}(\lg r)}$ size $\text{poly}(n, d, r)$ -explicit hitting set for width- r commutative ROABPs on n variables, of individual degree $< d$.

Proof: generator: We have by definition that f is a linear combination of the entries of $F(\mathbf{x})$, where $F(\mathbf{x})$ is computed by a matrix-valued commutative ROABP (recall [Lemma 2.1](#)). By [Theorem 4.1](#) it follows that $F \circ \mathcal{G}_{n, \lfloor 2\lg r \rfloor + 1}^{\text{SV}}$ is support- $\lfloor \lg r^2 \rfloor$ rank concentrated. Thus, [Corollary 3.5](#) shows that $f \not\equiv 0$ iff $f \circ \left(\mathcal{G}_{n, \lfloor 2\lg r \rfloor}^{\text{SV}} + \mathcal{G}_{n, \lfloor 2\lg r \rfloor + 1}^{\text{SV}} \right) \not\equiv 0$, where $\mathcal{G}_{n, \lfloor 2\lg r \rfloor}^{\text{SV}}(\mathbf{y}, \mathbf{z})$ and $\mathcal{G}_{n, \lfloor 2\lg r \rfloor + 1}^{\text{SV}}(\mathbf{y}', \mathbf{z}')$ are on disjoint variables. However, the SV-generator construction of [Theorem 4.1](#) is additive, in that as polynomial maps we have the equality $\mathcal{G}_{n, \lfloor 2\lg r \rfloor}^{\text{SV}}(\mathbf{y}, \mathbf{z}) + \mathcal{G}_{n, \lfloor 2\lg r \rfloor + 1}^{\text{SV}}(\mathbf{y}', \mathbf{z}') = \mathcal{G}_{n, 1+2\lfloor 2\lg r \rfloor}^{\text{SV}}(\mathbf{y}'', \mathbf{z}'')$, where $\mathbf{y}'' = (\mathbf{y}, \mathbf{y}')$ and $\mathbf{z}'' = (\mathbf{z}, \mathbf{z}')$.

hitting set: The hitting set is the evaluation of $\mathcal{G}_{n, 1+2\lfloor 2\lg r \rfloor}^{\text{SV}}$ on a sufficiently large product space of inputs, and the correctness follows from interpolation. That is, $f \circ \mathcal{G}^{\text{SV}}$ only has $1 + 2\lfloor 2\lg r \rfloor$ variables, and individual degree $< nd$. \square

Note that the SV-generator is in some sense an algebraic analogue of ℓ -wise independence. However, it is not the case that *any* ℓ -wise independent map will fool commutative ROABPs. For example, the polynomial $x_1 + \dots + x_n$ is computable in this model, but is not fooled by the $n - 1$ independent polynomial map given by $(x_1, x_2, \dots, x_{n-1}, -(x_1 + \dots + x_{n-1}))$.

To improve the above hitting sets of size $n^{\Theta(\lg n)}$, note that there are two sources of $n^{\Theta(\lg n)}$ factors in the above construction: the monomial map used to shift into rank concentration, and the conversion from rank concentration to hitting sets. In [Section 7](#), we will see an improved way to convert from rank concentration to hitting sets, that will only result in an $n^{\mathcal{O}(\lg \lg n)}$ overhead, but will be specific for commutative ROABPs. Unfortunately, no such improvement to the monomial map is yet known, but one can give a better monomial map when the individual degree of the polynomials is small. This alternative monomial map is based on the hashing ideas of Klivans-Spielman [[KS01](#)].

Lemma 4.4. *Let $|\mathbb{F}| \geq \text{poly}(n, d)$. Then the KS-generator $\mathcal{G}_{n,d,\ell}^{\text{KS}} : (\mathbb{F}^{\mathcal{O}(\ell \log_{nd} d)})^2 \rightarrow \mathbb{F}^n$ of [Theorem 2.3](#) is a $\text{poly}(n, d, \ell)$ -explicit, individual degree $< d$, ℓ -wise independent monomial map.*

Proof: Note that for any subset $S \subseteq [n]$ of size $\leq \ell$, there are at most d^ℓ monomials of individual degree $< d$. Thus, it follows from [Theorem 2.3](#) that the KS-generator with sparsity $s = d^\ell$ will map these monomials distinctly, as desired. \square

Note that the above KS-generator monomial map is better than the SV-generator monomial map when d is small, as we will be taking $\ell = \lg r$. As the individual degree of the KS-generator is $\text{poly}(n, d)$, and we have $\mathcal{O}(\log_{nd} d^\ell)$ variables, interpolating through this generator yields $\text{poly}(n, d)^{\mathcal{O}(\ell \log_{nd} d)} = \text{poly}(d^\ell)$ many points. In particular, when $d = \mathcal{O}(\text{polylog}(r, n))$, this will yield $\text{poly}(n, r)^{\mathcal{O}(\lg \lg(nr))}$ shifts such that one shift will yield rank concentration. In contrast, the SV-generator adds ℓ new variables, and multiplies their degree from d to dn , as the generator has degree n . Thus, even when d is small the number of shifts needed will be $\Omega(n^{\lg r})$. We will exploit this further in [Section 7](#), where we show techniques for reducing the complexity of hitting polynomials with rank concentration.

Lastly, we note that while the SV-generator is sufficient for the commutative ROABP results, it will not be sufficient for the results on general ROABPs with unknown orders in [Section 6](#). Instead, the KS-generator will be used.

5 Condensing Rank from Matrices with a Known Basis

This section will develop a new recipe for constructing (a variant of) rank condensers from error-correcting codes, and will then instantiate it with the transfer matrix of [Subsection 3.3](#). That is, while the rank condenser recipe of [Lemma 3.10](#) is sufficient for the results in [Section 4](#) on commutative ROABPs, the results of [Section 6](#) about unknown-order ROABPs need rank condensers that have smaller “seed length” than the above result. In the context of [Lemma 3.10](#), this means that the condition on the matrix W , that all monomials are distinct, is too stringent. We will want to apply a rank condenser in the setting with many variables, and keeping all such monomials distinct would prevent the construction of generators inputting few variables. To achieve better parameters, we will weaken the requirements on the rank condenser.

In particular, observe that the above rank condenser is in some sense “information theoretic”, as the matrices involved are all completely written down, without any notion of “simplicity”. To

achieve better parameters, we can impose that the matrices we wish to extract from are simple in some sense. Here, we will restrict to condensing rank from matrices that have a row-basis in some known “medium-sized” subset of the rows — small enough so the seed length can decrease, but large enough so that the problem is non-trivial. In particular, we will try to construct the following type of rank condenser.

Definition 5.1 (Rank Condenser Generator for Known Bases). A matrix $E(\mathbf{t}) \in \mathbb{F}[\mathbf{t}]^{n \times m}$ is said to be a (seeded) rank condenser (generator) for rank r and rows $P \subseteq [m]$ if for every matrix $M \in \mathbb{F}^{m \times k}$ of rank $\leq r$ such that $\text{rank}_{\mathbb{F}}(M) = \text{rank}_{\mathbb{F}}(M|_{P \times \bullet})$, we have that $\text{rank}_{\mathbb{F}(\mathbf{t})}(E(\mathbf{t}) \cdot M) = \text{rank}_{\mathbb{F}}(M)$. \diamond

An obvious approach to construct the above would be to ignore the rows outside P , by zeroing out parts of the rank condenser, and plugging in a rank condenser for the P . However, this is not compatible with the black-box access of polynomials. Thus, we must consider rank condensers that naturally arise in the shifting/partial-derivative process.

In particular, we will relax the restriction, on the matrix W of Lemma 3.10, that all monomials are distinct. Recall though, that in the above rank condenser, this distinctness property drove the uniqueness of the minimum weight term, which was crucial in showing that some determinant does not vanish in the Cauchy-Binet sum. If non-distinctness of these weights is allowed, then the weight minimization may not be unique and hence the corresponding monomial could be canceled out. To ensure uniqueness, it will be enough that the *small weights* are distinct. In the rank condenser context, this will correspond to the rows in the P getting distinct weights, and that these distinct weights are smaller than any non-distinct weights. As this regime in greedy/matroid optimization seems somewhat less standard, we prove the required uniqueness property. For concreteness, we only discuss this optimization within our context, but the results apply to any matroid. We begin with a property of the greedy algorithm.

Lemma 5.2. *Let $M \in \mathbb{F}^{n \times m}$ be a matrix of rank r . Using some total order \prec on $[m]$, greedily choose r linearly independent columns (at each step, pick the least- \prec -indexed column that increases the rank of the chosen vectors), and denote this set $T = \{i_1, \dots, i_r\}$ with $i_1 \prec \dots \prec i_r$. Let $T' \subseteq [m]$ be any set of r linearly independent columns, and denote $T' = \{i'_1, \dots, i'_r\}$ with $i'_1 \prec \dots \prec i'_r$. Then $T \preceq T'$ point-wise, that is, $i_j \preceq i'_j$ for $j \in [r]$. Further, if $T \neq T'$, then $i_{j_0} \prec i'_{j_0}$ for some $j_0 \in [r]$.*

Proof: Suppose not, so that $T \not\preceq T'$, for contradiction. Let j_0 be the first $j \in [r]$ such that $i_j \succ i'_j$. Denote $T_k = \{i_1, \dots, i_k\}$ and $T'_k = \{i'_1, \dots, i'_k\}$ for $k \in [r]$. Thus T_{j_0-1} indexes $r-1$ linearly independent columns and T'_{j_0} indexes r linearly independent columns. By the Steinitz Exchange Lemma of linear algebra, it follows there is some $i'_{j_1} \in T'_{j_0} \setminus T_{j_0-1}$ such that $T_{j_0-1} \cup \{i'_{j_1}\}$ indexes r linearly independent columns. Using that $i'_{j_1} \preceq i'_{j_0} \prec i_{j_0}$, it follows that there is some $j_2 \in [j_0-1]$ such that $i_{j_2} \prec i'_{j_1} \prec i_{j_2+1}$.

When T_{j_2} is being greedily extended to T_{j_2+1} , the least rank-increasing column after all elements in T_{j_2} will be chosen. By hypothesis, i_{j_2+1} was chosen. However, as adding i'_{j_1} increases the rank of T_{j_0-1} , and $T_{j_2} \subseteq T_{j_0-1}$, it follows that adding i'_{j_1} increases the rank of T_{j_2} . As $i_{j_2} \prec i'_{j_1} \prec i_{j_2+1}$, it follows that i_{j_2+1} could not have been chosen, as i'_{j_1} is a better choice, yielding the desired contradiction. Thus $T \preceq T'$ point-wise, as desired.

If $T \neq T'$, then not all indices can be equal, so by the above $i_{j_0} \prec i'_{j_0}$ for some j_0 . \square

We next state the uniqueness lemma when minimizing the monomial weight of bases of the columns of a matrix, when only the small weights are distinct. As above, this statement can be interpreted for general greedy/matroid optimization, but for concreteness we only discuss our

context. Note that the usual setting for greedy/matroid optimization is maximization with distinct weights. In the below setting, we have minimization and thus we minimize only over full-rank sets of columns, as else the empty set is trivially the minimum weight set. Further, in our applications it is crucial that we allow some weights to be repeated. While the resulting uniqueness result follows from standard arguments, it is somewhat non-standard so we include it for completeness.

Lemma 5.3. *Let $M \in \mathbb{F}^{n \times m}$ be a matrix of rank r . Let \prec be a monomial ordering on $\mathbb{F}[\mathbf{x}]$, and let $w : [m] \rightarrow \mathbb{F}[\mathbf{x}]$ weight the columns in M with monomials in $\mathbb{F}[\mathbf{x}]$. Suppose the partition $[m] = I \sqcup J$ is so that w is injective on I , and that $w(i) \prec w(j)$ for all $i \in I$ and $j \in J$. Suppose further that the $\text{rank}(M|_{\bullet \times I}) = r$. Then there is a unique set $T \subseteq [m]$ of size r , with $\text{rank}(M|_{\bullet \times T}) = r$, that minimizes $w(T) := \prod_{i \in T} w(i)$ with respect to the monomial order. Further, $T \subseteq I$.*

Proof: The monomial order, as a total order on $\mathbb{F}[\mathbf{x}]$, induces a partial order on $[m]$ via the weight function w . Extend this partial order arbitrarily to a total order on $[m]$, and denote it by ' \prec ' also, abusing notation. From this it follows that for $i, i' \in [m]$, $i \prec i'$ implies $w(i) \preceq w(i')$. Thus, it follows that I comes before J in the \prec -order on $[m]$.

Choose the set T of r linearly independent columns greedily, using the \prec -order on $[m]$. As there is some set of r linearly independent columns $T' \subseteq I$, it follows from [Lemma 5.2](#) that $T \preceq T'$ point-wise, so then $T \subseteq I$, as I comes before J in the \prec -order on $[m]$. Now consider any set $T' \subseteq [m]$ of r linearly independent columns, with $T \neq T'$. Again, $T \preceq T'$, so in particular $w(T) \preceq w(T')$. However, using [Lemma 5.2](#) further, we see there is some index $j_0 \in [r]$ so that $i_{j_0} \prec i'_{j_0}$ when we write $T = \{i_1, \dots, i_r\}$ and $T' = \{i'_1, \dots, i'_r\}$. As $i_{j_0} \in T \subseteq I$, and the weights in I are distinct and all strictly below the weights in J , it follows that $w(i_{j_0}) \prec w(i'_{j_0})$. From this it follows that $w(T) \prec w(T')$. Thus $T \subseteq I$ is the unique minimizer of the weight w over sets of r linearly independent columns. \square

To use this uniqueness lemma in our rank condenser, we need a notion of what a ‘‘small’’ weight will be. Here, we will use a new variable u , such that the smallness of a monomial will correspond to its degree in u .

Lemma 5.4. *Fix $d \geq 0$. Let $E_d(\mathbf{t}, u) \in \mathbb{F}[\mathbf{t}, u]^{n \times m}$, with $E_d = \Lambda(\mathbf{t}, u)^{-1} \cdot H \cdot W(\mathbf{t}, u)$ such that*

- $\Lambda(\mathbf{t}, u) \in \mathbb{F}[\mathbf{t}, u]^{n \times n}$ is a diagonal matrix, whose diagonal entries are nonzero monomials.
- $H \in \mathbb{F}^{n \times m}$ is the parity check matrix of an error correcting code of distance $> r$. That is, every r columns of H are linearly independent.
- $W(\mathbf{t}, u) \in \mathbb{F}[\mathbf{t}, u]^{m \times m}$ is a diagonal matrix, whose diagonal entries are nonzero monomials. The monomials in $W(\mathbf{t}, u)|_{P_d \times P_d}$ are distinct, where $P_d = \{j : j \in [m], \deg_u W(\mathbf{t}, u)_{j,j} < d\}$.

Then $E(\mathbf{t}, u)$ is a rank condenser for rank r and rows P_d .

Proof: Consider any matrix $M \in \mathbb{F}^{m \times k}$ of rank $s \leq r$ with $\text{rank}_{\mathbb{F}}(M) = \text{rank}_{\mathbb{F}}(M|_{P_d \times \bullet})$.

$k > s$: Choose the submatrix $M' \in \mathbb{F}^{m \times s}$ of M , such that M' has rank s . As $\text{rank}_{\mathbb{F}}(M|_{P_d \times \bullet}) = s$ we can choose M' so that $\text{rank}_{\mathbb{F}}(M'|_{P_d \times \bullet}) = s$ also. Now apply the $k = s$ case, just as in the proof of [Lemma 3.10](#).

$k = s$: As in the proof of [Lemma 3.10](#), W induces a weight function $w : [m] \rightarrow \mathbb{F}[\mathbf{t}, u]$. Let \prec be a lexicographic monomial order on $\mathbb{F}[\mathbf{t}, u]$, such that u comes before all variables in \mathbf{t} . It then follows from that [Lemma 5.3](#) applies, using the partition $[m] = P_d \sqcup ([m] \setminus P_d)$, so that there is a unique set

$T_0 \subset [m]$ such that $\det(M|_{T_0 \times \bullet}) \neq 0$ minimizing $w(T_0)$ with respect to the \prec -order. The rest of the proof then follows exactly as in the proof of [Lemma 3.10](#). \square

With this new recipe, we now instantiate it with the transfer matrix of [Subsection 3.3](#). To do so, we need now the notion of a monomial map with independence with respect to *total degree*.

Definition 5.5. Let $g : \mathbb{F}^m \times \mathbb{F}^{m'} \rightarrow \mathbb{F}^n$ be a polynomial map. It is a *total-degree- $(< D)$ independent monomial map* if there is an $\alpha \in \mathbb{F}^{m'}$ such that the polynomials $\{g(t, \alpha)^a\}_{|a|_1 < D} \subseteq \mathbb{F}[t]$ are nonzero, distinct monomials in t . \diamond

Note that the main difference from [Definition 3.20](#) is that now we consider monomials in many variables whereas previously we only considered monomials in ℓ variables. We also now restrict the total degree, so in the above D should be considered small. The variable u of [Lemma 5.4](#) is used to grade with respect to degree, and thus take advantage the the total degree is not too large.

We now use such maps to get a rank condenser.

Corollary 5.6. Assume the setup of [Construction 3.13](#). Let $g : \mathbb{F}^m \times \mathbb{F}^k \rightarrow \mathbb{F}^n$ be an total-degree- $(< D)$ independent monomial map. Then $T_r(u \cdot g(t, s))$ is a rank condenser for rank r and rows corresponding to monomials of total degree $< D$.

Proof: Fix the $\alpha \in \mathbb{F}^{m'}$ guaranteed by the monomial map g , so that we can now regard $g(t, \alpha)$ as a polynomial map in $\mathbb{F}[t]$. As in [Corollary 3.21](#), we can express $T_r(ug(t, \alpha)) = \Lambda(u, t, \alpha)^{-1} \cdot T_r(\mathbf{1}) \cdot W(u, t, \alpha)$. As before, Λ and $T_r(\mathbf{1})$ fit the hypothesis of [Lemma 5.4](#), where for the latter we use [Lemma 3.19](#). Further, $W(u, t, \alpha)$ has the desired monomial distinctness properties as g is a monomial map with independence up to total degree $< D$. Thus, $T_r(ug(t, \alpha))$ is a rank condenser for rank r . Removing the substitution of s , it follows that $T_r(ug(t, s))$ is a rank condenser as well. \square

Reinterpreting the above in terms of rank concentration, we get the main result of this section.

Corollary 5.7. Let $f \in \mathbb{F}[x]^r$ be polynomials of individual degree $< d$ on the n -variables x . Let $g : \mathbb{F}^m \times \mathbb{F}^{m'} \rightarrow \mathbb{F}^n$ be an total degree- $(< d\ell)$ independent monomial map. Then if f has support- ℓ rank concentration at $\alpha \in \mathbb{F}^n$, then f has support- $\lfloor \lg r \rfloor$ rank concentration at $\alpha + u \cdot g(t, s)$ over the field $\mathbb{F}(u, t, s)$.

Proof: Expand the polynomials f in terms of their Hasse derivatives at α , giving the matrix M , so that $M_{b,i} = \partial_{x^b}(f_i)(\alpha)$. Let $P_{d\ell} \subseteq \llbracket d \rrbracket^n$ index the rows of M given by monomials of total degree $< d\ell$. Thus $P_{d\ell}$ contains all monomials with support $\leq \ell$. Thus, by hypothesis $\text{rank}_{\mathbb{F}}(M) = \text{rank}_{\mathbb{F}}(M|_{P_{d\ell} \times \bullet})$.

Now consider the multiplication $T_r(ug(t, s)) \cdot M$. By [Corollary 5.6](#) it follows that $\text{rank}_{\mathbb{F}(u,t,s)} T_r(ug(t, s))M = \text{rank}_{\mathbb{F}} M$. Thus, $T_r(ug(t, s))M$ and M have the same $\mathbb{F}(u, t, s)$ -row-span. Thus, as in [Corollary 3.22](#), we have that the definition of T_r and [Equation 3.12](#) imply that,

$$\begin{aligned} \text{span}_{\mathbb{F}(u,t,s)} \{ \partial_{x^a}(f)(\alpha + ug(t, s)) \}_{|a|_0 \leq \lfloor \lg r \rfloor} &= \text{row-span}_{\mathbb{F}(u,t,s)} (T_r(ug(t, s))M) \\ &= \text{row-span}_{\mathbb{F}(u,t,s)} (M) \\ &= \text{span}_{\mathbb{F}(u,t,s)} \{ \partial_{x^a}(f)(\alpha) \}_a \\ &= \text{span}_{\mathbb{F}(u,t,s)} \{ \partial_{x^a}(f)(\alpha + ug(t, s)) \}_a \end{aligned}$$

where, again, we used [Lemma 3.2](#) in the last equality to change the point of derivation. \square

Note that α could be a polynomial map in auxiliary variables t' (and this will happen in later sections), in which case the above lemma would use the field $\mathbb{F}(t')$.

6 Hitting Sets for Unknown Order ROABPs

In this section, we present hitting sets of size $\text{poly}(d, n, r)^{d \lg r \cdot \lg n}$ for ROABPs on n variables, width- r and individual degree $< d$, when the order of the variables is unknown. While this gives worse parameters than the size- $\text{poly}(d, n, r)^{\lg n}$ hitting set of Forbes-Shpilka [FS12b] results for ROABPs, that hitting set only worked for a fixed variable order. Further, while the results of this section have a poor dependence on the individual degree d , note that $d = 2$ is sufficiently interesting, as it covers all of the set-multilinear models considered by Agrawal-Saha-Saxena [ASS12].

The results of Section 4 showed that, in commutative ROABPs, rank concentration can be achieved in n variables by reducing it to achieving rank concentration in all size- $\Theta(\lg r)$ subsets of variables. Then, rank concentration can be brute-force achieved in quasipolynomial time. However, this connection crucially used commutativity to reorder the variables, and seems to break down otherwise.

In considering general ROABPs, we will still use shifts to concentrate rank on smaller-support derivatives. However, instead of relying on a single shift, we will shift $\lg n$ times, each time halving the support of the derivatives needed. While the rank concentration results of Subsection 3.3 can achieve this, such results are too expensive when applied to all n variables at once. Instead, we will use the rank concentration results of Section 5, which allow each shift to build on previous shifts.

More specifically, suppose we have two ROABPs $F(\mathbf{x})$ and $G(\mathbf{y})$, each with support- ℓ rank concentration. First, we observe a simple merge, that is, $F(\mathbf{x})G(\mathbf{y})$ has support- 2ℓ rank concentration. By itself, this merge step contains no work. Now we seek to reduce the support. This can be done with a rank condenser, and in particular, since FG has support- 2ℓ rank concentration, FG has a “known basis” that we can condense. In this case, the result of Corollary 5.7 will condense to support- $\lg r^2$, using a single shift of (\mathbf{x}, \mathbf{y}) . Thus, if we take $\ell = \lg r^2$, then this merge-and-reduce process has doubled the number of variables, while maintaining support- ℓ rank concentration. By applying this $\lg n$ times, we can shift n -variate ROABP into small-support rank concentration.

Given the proof outline, we begin the formalities by observing that rank concentration of two ROABPs on disjoint variables implies rank concentration of their product. The proof shares the bilinearity-based ideas of Theorem 4.1, but we must now preserve the order of the variables.

Lemma 6.1. *Let \mathbf{x} and \mathbf{y} be disjoint sets of n variables. Consider $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{r \times r}$ and $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{r \times r}$. Then if $F(\mathbf{x})$ is support- ℓ rank concentrated at $\alpha \in \mathbb{F}^n$ and $G(\mathbf{y})$ is support- k rank concentrated at $\beta \in \mathbb{F}^n$, then $F(\mathbf{x})G(\mathbf{y})$ is support- $(\ell + k)$ rank concentrated at (α, β) .*

Proof: Consider a derivative $\partial_{\mathbf{x}^{a_0} \mathbf{y}^{b_0}}(FG)$. The rank concentration implies that

$$\partial_{\mathbf{x}^{a_0}}(F)(\alpha) \in \text{span}_{\mathbb{F}}\{\partial_{\mathbf{x}^a}(F)(\alpha)\}_{|a|_0 \leq \ell}$$

and

$$\partial_{\mathbf{y}^{b_0}}(G)(\beta) \in \text{span}_{\mathbb{F}}\{\partial_{\mathbf{y}^b}(G)(\beta)\}_{|b|_0 \leq k}$$

Thus, as matrix multiplication is bilinear, and the variables \mathbf{x} and \mathbf{y} are disjoint, it follows that

$$\begin{aligned}\partial_{\mathbf{x}^{a_0}\mathbf{y}^{b_0}}(FG) &= \partial_{\mathbf{x}^{a_0}}(F)(\boldsymbol{\alpha})\partial_{\mathbf{y}^{b_0}}(G)(\boldsymbol{\beta}) \\ &\in \text{span}_{\mathbb{F}}\{\partial_{\mathbf{x}^a}(F)(\boldsymbol{\alpha})\partial_{\mathbf{y}^b}(G)(\boldsymbol{\beta})\}_{|a|_0 \leq \ell, |b|_0 \leq k} \\ &= \text{span}_{\mathbb{F}}\{\partial_{\mathbf{x}^a\mathbf{y}^b}(FG)(\boldsymbol{\alpha}, \boldsymbol{\beta})\}_{|a|_0 \leq \ell, |b|_0 \leq k} \\ &\subseteq \text{span}_{\mathbb{F}}\{\partial_{\mathbf{z}^c}(FG)(\boldsymbol{\alpha}, \boldsymbol{\beta})\}_{|c|_0 \leq \ell+k}\end{aligned}$$

where $\mathbf{z} = (\mathbf{x}, \mathbf{y})$. □

Note that if we take $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ as polynomial maps in auxiliary variables \mathbf{t} (as will happen later), then the above lemma still holds simply by changing the field \mathbb{F} under consideration to the field $\mathbb{F}(\mathbf{t})$.

This lemma shows that we can combine support- ℓ rank concentration on disjoint sets of n variables into support- 2ℓ rank concentration on $2n$ variables. However, this process does not change the ratio of the support to the number of variables. Nevertheless, by applying the rank condenser of [Corollary 5.7](#), we can compress back down to support- $\lfloor \lg r^2 \rfloor$, as we summarize in the following corollary.

Corollary 6.2. *Let \mathbf{x} and \mathbf{y} be disjoint sets of n distinct variables. Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{r \times r}$ and $G(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]^{r \times r}$ be of individual degree $< d$, and have support- ℓ rank concentration at $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}^n$ respectively.*

Let $\mathbf{g}(\mathbf{t}, \mathbf{s})$ be an independent monomial map for total degree $< 2d\ell$ mapping into the $2n$ variables (\mathbf{x}, \mathbf{y}) , where u, \mathbf{t} and \mathbf{s} are new variables. Then $F(\mathbf{x})G(\mathbf{y})$ has support- $\lfloor \lg r^2 \rfloor$ rank concentration at $(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (u \cdot \mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{x}}, u \cdot \mathbf{g}(\mathbf{t}, \mathbf{s})|_{\mathbf{y}})$ over the field $\mathbb{F}(u, \mathbf{t}, \mathbf{s})$. △

We now apply the above corollary recursively. We maintain blocks of variables that have support- $\lg r^2$ rank concentration, and then merge pairs of blocks. This raises the support to $2 \lg r^2$, which is then brought back down to $\lg r^2$ with a shift. In this entire process, the variables (and their blocks) will respect the order of the ROABP. However, this order is only needed to be known for the analysis, as the construction is oblivious to it. In particular, we can construct the needed monomial maps in a way oblivious to the order, as seen in [Lemma 6.4](#) below. We now prove that this scheme works.

Lemma 6.3. *Let $n \geq 0$, $N = 2^n$ and $d, r \geq 1$. Let $\mathbf{g} : \mathbb{F}^m \times \mathbb{F}^{m'} \rightarrow \mathbb{F}^N$ be an independent monomial map for total degree $< 2d(\lfloor \lg r^2 \rfloor + 1)$. Define $\mathcal{G}_{n,d,r} : (\mathbb{F} \times \mathbb{F}^m \times \mathbb{F}^{m'})^n \rightarrow \mathbb{F}^N$ to be the polynomial map defined by*

$$\mathcal{G}_{n,d,r}(u_1, \mathbf{t}_1, \mathbf{s}_1, \dots, u_n, \mathbf{t}_n, \mathbf{s}_n) = \sum_{i \in [n]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i).$$

Let π be a permutation $\pi : [N] \rightarrow [N]$. Let $F(\mathbf{x}) = \prod_{i \in [N]} M_i(x_{\pi(i)})$, where for $i \in [N]$, $M_i(x_{\pi(i)}) \in \mathbb{F}[x_{\pi(i)}]^{r \times r}$ is of individual degree $< d$. Then $F(\mathbf{x})$ has support- $(\lfloor \lg r^2 \rfloor + 1)$ rank concentration at $\mathcal{G}((u_i, \mathbf{t}_i, \mathbf{s}_i)_{i \in [n]})$ over the field $\mathbb{F}((u_i, \mathbf{t}_i, \mathbf{s}_i)_i)$.

Proof: We proceed by induction on n .

$n = 0$: In this case, we have a single variable x and the matrix $F(x)$. The generator \mathcal{G} is then the zero polynomial map, as the summation defining it is empty. Thus, $F(x)$ clearly has support-1 rank concentration at $\mathbf{0}$, as there is only 1 variable to consider. As $1 \leq \lfloor \lg r^2 \rfloor + 1$, the claim follows.

$n > 0$: Divide the 2^n variables in half, into \mathbf{y} and \mathbf{z} , respecting the order $x_{\pi(1)}, \dots, x_{\pi(N)}$. Thus, we can write $F(\mathbf{x}) = G(\mathbf{y})H(\mathbf{z})$. Now note that $\mathbf{g}(\cdot, \cdot)|_{\mathbf{y}}$ is a good monomial map for \mathbf{y} , and similarly

$\mathbf{g}(\cdot, \cdot)|_z$ is a good monomial map for z . Thus, if we apply the induction hypothesis on these cases, using their respective pieces of the monomial map \mathbf{g} , it follows that G is support- $(\lfloor \lg r^2 \rfloor + 1)$ rank-concentrated at $\sum_{i \in [n-1]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i)|_y$, and similarly H is support- $(\lfloor \lg r^2 \rfloor + 1)$ rank-concentrated at $\sum_{i \in [n-1]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i)|_z$. It follows then from [Corollary 6.2](#) that $F(\mathbf{x}) = G(\mathbf{y})H(\mathbf{z})$ is support- $(\lfloor \lg r^2 \rfloor + 1)$ rank concentrated at

$$\begin{aligned} & \left(\sum_{i \in [n-1]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i)|_y, \sum_{i \in [n-1]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i)|_z \right) + (u_n \cdot \mathbf{g}(\mathbf{t}_n, \mathbf{s}_n)|_y, u_n \cdot \mathbf{g}(\mathbf{t}_n, \mathbf{s}_n)|_z) \\ &= \left(\sum_{i \in [n]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i)|_y, \sum_{i \in [n]} u_i \cdot \mathbf{g}(\mathbf{t}_i, \mathbf{s}_i)|_z \right) = \mathcal{G}_{n,d,r}((u_i, \mathbf{t}_i, \mathbf{s}_i)_{i \in [n]}), \end{aligned}$$

as desired. \square

We now instantiate the above corollary with specific monomial maps for individual degree. We begin by noting that the SV-generator does not yield such a monomial map. That is, for any monomial \mathbf{x}^a of low-total-degree (for example degree $d \lg r$, as in the above lemma), the generator $\mathcal{G}_{n,d \lg r}^{\text{SV}}(\mathbf{y}, \mathbf{z})$ will have some setting $\mathbf{z} \leftarrow \alpha_a$ so that \mathbf{x}^a is preserved as a monomial in \mathbf{y} . However, the choice of α_a will depend on a , and thus a different monomial \mathbf{x}^b of low degree may be zeroed out in the substitution $\mathbf{z} \leftarrow \alpha_a$. That is, we need that there exists a (*single*) setting of \mathbf{z} that preserves *all* relevant monomials, whereas the SV-generator reverses the order of these quantifiers. Thus, we will instead use the KS-generator as alluded to above, as recorded in the next lemma.

Lemma 6.4. *Let $|\mathbb{F}| \geq \text{poly}(n, d)$. Then the KS-generator $\mathcal{G}_{n,d,n^D}^{\text{KS}} : (\mathbb{F}^{\mathcal{O}(D \log_{nd} n)})^2 \rightarrow \mathbb{F}^n$ of [Theorem 2.3](#) is a $\text{poly}(n, d, D)$ -explicit, independent monomial map for total degree $< D$.*

Proof: By writing n -variate monomials of total degree k as strings in $[n]^k$, it follows that there are $\leq \sum_{k \in [D]} n^k = \frac{n^D - 1}{n - 1} \leq n^D$ monomials in n variables of total degree $< D$. Thus, it follows from [Theorem 2.3](#) that the KS-generator with sparsity $s = n^D$ will map these monomials distinctly, as desired. \square

Combining the above, we get the desired hitting sets for ROABPs with unknown variable order, yielding the main result of this paper.

Theorem 6.5 (Main). *Let $n \geq 0$, $N = 2^n$, $d, r \geq 1$ and $|\mathbb{F}| \geq \text{poly}(N, d)$. Define $\mathcal{G}'_{N,d,r} : (\mathbb{F} \times (\mathbb{F}^{\mathcal{O}(d \lg r \cdot \log_{Nd} N)})^2)^n \rightarrow \mathbb{F}^N$ be the polynomial map defined by*

$$\mathcal{G}'_{N,d,r}(u_1, \mathbf{t}_1, \mathbf{s}_1, \dots, u_n, \mathbf{t}_n, \mathbf{s}_n) = \sum_{i \in [n]} u_i \cdot \mathcal{G}_{N,d,N^{2d(\lfloor \lg r^2 \rfloor + 1)}}^{\text{KS}}(\mathbf{t}_i, \mathbf{s}_i).$$

Then, for $i \in [N]$, the polynomial $(\mathcal{G}'_{N,d,r})_i$ has individual degree $\leq \text{poly}(N, d)$. Further, $\mathcal{G}'_{N,d,r}$ is $\text{poly}(N, d, r)$ explicit.

Further, for any N -variate $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ of individual degree $< d$, computed by a ROABP of width $\leq r$ in some variable order, $f \neq 0$ iff $f \circ (\mathcal{G}'_{N,d,r} + \mathcal{G}_{\lfloor \lg r^2 \rfloor + 1}^{\text{SV}}) \neq 0$.

Thus, for any N , there is a $\text{poly}(N, d)^{\mathcal{O}(d \lg r \cdot \lg N)}$ size $\text{poly}(N, d, r)$ -explicit hitting set for width- r ROABPs on N variables, of individual degree $< d$, in any variable order.

Proof: generator: That the $\mathcal{G}' + \mathcal{G}^{\text{SV}}$ generator above is correct follows from instantiating [Lemma 6.3](#) with the monomial map of [Lemma 6.4](#).

degree, explicitness: These follow from [Theorem 2.3](#).

hitting set: The hitting set follows by interpolating the polynomial $f \circ (\mathcal{G}' + \mathcal{G}^{\text{SV}})$. This polynomial has individual degree $\text{poly}(N, d)$, and has $\lg N \cdot \mathcal{O}(d \lg r \cdot \log_{dN} N) + \mathcal{O}(\lg r)$ variables. Thus, the number of points in the interpolation is $\text{poly}(N, d)^{\mathcal{O}(d \lg r \cdot \lg N \cdot \log_{dN} N) + \mathcal{O}(\lg r)} = N^{\mathcal{O}(d \lg r \cdot \lg N)}$. \square

We now briefly comment on why our methods have a poor dependence on the individual degree of the polynomial f . Based on our paradigm of merge-and-reduce, as embodied by [Corollary 6.2](#), we seek to move from support- $\lg r^2$ rank concentration, merge to support- $2 \lg r^2$ concentration, and then reduce back to support- $\lg r^2$ concentration. To do this reduction step, we use a rank condenser, that condenses rank from a known-basis. This known-basis is among the monomials of support- $2 \lg r^2$. Ideally, we could construct a rank condenser that condenses just from this basis. However, as discussed in [Section 5](#), our rank condenser must be compatible with black-box access to polynomials. The notion of “support” of a monomial is not easily compatible with black-box access, and so it unclear how to make small-support monomials both distinct, as well as “smaller” than all large-support monomials, such that the uniqueness arguments of [Section 5](#) (when we have that all small weights are distinct) can be applied.

Thus, as we cannot condense from small-support monomials, the above results observe that when the individual degree d is small, small-support and low-degree become nearly equivalent notions. The notion of being low-degree is then compatible with black-box access to polynomials, via homogenization, and thus the results proceed as detailed above.

7 Better Hitting Sets for Commutative ROABPs

In [Section 4](#) we gave quasipolynomial-size hitting sets for the class of commutative ROABPs. In this section, we improve these $n^{\mathcal{O}(\lg n)}$ results to $n^{\mathcal{O}(\lg \lg n)}$, for two subclasses of commutative ROABPs: diagonal circuits, and commutative ROABPs with small individual degree.

To understand this improvement, recall the strategy of [Section 4](#), which involved two different parts. First, we found a small set of shifts, such that we could shift the polynomial into small-support rank concentration, and this yielded a nonzero monomial of small support. As mentioned at the end of [Section 4](#), we do not have good ways to reduce the number of shifts needed, and thus focus on improving the second step, which is where we try to hit a commutative ROABP that is promised to have a small support monomial. To do this, we used [Lemma 3.4](#), which composed the polynomial f with the SV-generator $\mathcal{G}_{n,\ell}^{\text{SV}}$, where ℓ is the size of the small-support monomial, and observed that $f \neq 0$ iff $f \circ \mathcal{G}_{n,\ell}^{\text{SV}} \neq 0$. We then interpolated this generator into a hitting set.

If we wish to improve the hitting sets under the promise of a support- ℓ monomial, it seems that properties of f must be used, as otherwise it seems unlikely hitting sets smaller than $\text{poly}(n)^\ell$ can be devised as there are too many such polynomials to hit. To take advantage of f , we thus ask: what is the complexity of $f \circ \mathcal{G}_{n,\ell}^{\text{SV}}$? Note that it has $2\ell \approx \lg r$ variables, which is quite small. If $f \circ \mathcal{G}_{n,\ell}^{\text{SV}}$ itself can be expressed as a small circuit, then we could use PIT for this class. In particular, if we have hitting sets for size- s , n -variate circuits in this class of size $\text{poly}(s, n)^{\lg n}$, then this would

yield the desired result, as $n \approx \lg r$ in this new circuit class. While this strategy can work⁷ for diagonal circuits, this section will give a different composition that work more generally for any commutative ROABP with the promise of a small-support monomial.

To hit such commutative ROABPs with a support- ℓ monomial, we will first hash the n original variables to $\approx \ell$ buckets, and then give each bucket its own variable. Some hash function in the family will hash each variable of the support- ℓ monomial distinctly, which will allow us to ensure that this monomial is not canceled out, thus preserving non-zeros. However, we now would like to also preserve the property of being a ROABP. Without modification, using the SV-generator will result in a polynomial that is not read-once in the variables z . We resolve this issue by giving each bucket its own SV-generator for support-1. By commutativity, we can reorder the n variables such that they are grouped by the buckets they hash into. Thus, each *bucket* is then read-once, which implies that we now have an ROABP in $\approx \ell$ variables. We can then apply the hitting set result of Forbes-Shpilka [FS12b] as it has the desired $\text{poly}(s, n)^{\lg \ell} = \text{poly}(s, n)^{\lg \lg s}$ dependence.

We now turn to the details. We begin by quoting the tools we will need. We begin by quoting results showing that diagonal circuits, and the more general notion of “low rank” polynomials, have a small-support monomial, without any shifting.

Lemma 7.1. *For $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, define*

$$\dim(\partial(f)) := \dim_{\mathbb{F}}\{\partial_{\mathbf{x}^{\mathbf{a}}}(f)\}_{\mathbf{a}}$$

to be the dimension of its partial derivatives, over the field \mathbb{F} . Then f is computed by a width- $\dim(\partial(f))$, individual degree $< (\deg f + 1)$ commutative ROABP. Further, $f \neq 0$ iff it contains a nonzero monomial of support $\leq \lg r$. In particular, if f is computed by a diagonal circuit of size s , then $\dim(\partial(f)) \leq \text{poly}(s, \deg(f))$.

Proof: The structural results relating diagonal circuits, dimension of partial derivatives, and commutative ROABPs, are due to Saptharishi, as reported in Section 6 of Forbes-Shpilka [FS12b]. The small-support monomial result is due to Theorem 6.9 in Forbes-Shpilka [FS13]. \square

We note that Agrawal-Saha-Saxena [ASS12] gave a set of shifts, of polynomial size, that will shift any diagonal circuit to have small-support, while the above shows that no shift is needed.

We now quote the hitting set of Forbes-Shpilka [FS12b] for ROABPs with variable order $x_1 < \dots < x_n$. Note that commutative ROABPs are ROABPs in *any* variable order, so fixing the variable order is not a restriction in this setting. While this hitting set is of quasipolynomial size, and the hitting sets of Section 4 for commutative ROABPs are also of quasipolynomial size, the exponents of these quasipolynomials are qualitatively different in their dependencies on the parameters. The former is of the form $\text{poly}^{\lg n}$, and the latter is always at least $d^{\lg r}$. Thus, as we are seeking to reduce the number of variables n , only the former is in a position to use this improvement.

Theorem 7.2 (Forbes-Shpilka hitting set [FS12b]). *Let $|\mathbb{F}| \geq \text{poly}(n, d, r)$. There is a $\text{poly}(n, d, r)$ -explicit, polynomial map $\mathcal{G}_{n,d,r}^{\text{FS}} : \mathbb{F}^{\mathcal{O}(\lg n)} \rightarrow \mathbb{F}^n$ of degree $\text{poly}(n, d, r)$, such that for any $f(\mathbf{x})$ computed by n -variable, individual degree $< d$, width- r ROABP, we have that $f \neq 0$ iff $f \circ \mathcal{G}_{n,d,r}^{\text{FS}} \neq 0$. \triangle*

Finally, we will need the usage of good hash functions, and we now define the particular property we need.

⁷It can be shown that when f is a (depth-3) diagonal circuit, then $f \circ \mathcal{G}_{n,\ell}^{\text{SV}}$ is computable by a depth-4 diagonal circuit in $\approx \lg r$ variables. The hitting sets for depth-4 diagonal circuits of Forbes-Shpilka [FS12b] are of desired $\text{poly}(s, n)^{\lg n}$ form, thus giving the $n^{\mathcal{O}(\lg \lg n)}$ result for depth-3 diagonal circuits.

Definition 7.3. A family $\mathcal{H} = \{h : [n] \rightarrow [m]\}$ is a (n, m, ℓ) -perfect hash function family if for every $S \subseteq [n]$ of size $|S| \leq \ell$, there is an $h \in \mathcal{H}$ such that h is injective on S . \diamond

There is an extensive literature on such hash functions. Mehlhorn [Meh82] gave matching lower and (non-constructive) upper bounds on the size of \mathcal{H} in such a family. Schmidt and Siegel [SS89] gave optimal constructive upper bounds in a certain regime of parameters. However, for our range of parameters we can more simply use pairwise independent hash functions, as seen in the following standard lemma, which we instantiate with explicit pairwise independent hash functions (for example, see Carter and Wegman [CW79] or the survey of Vadhan [Vad12]).

Lemma 7.4. Let \mathcal{H} be a family of pairwise independent hash functions from $[n] \rightarrow [m]$, where $m \geq \ell^2$. Then \mathcal{H} is a (n, m, ℓ) -perfect hash function family. In particular, there is an $\text{poly}(n, m, \ell)$ -explicit (n, m, ℓ) -perfect hash family with $m = 2^{\lceil \lg \ell^2 \rceil}$ and $|\mathcal{H}| \leq \text{poly}(n, m, \ell)$. \triangle

We now turn to the actual construction. One part of the construction will simply interpolate through the different hash functions in the hash family. More interestingly, we will hash the n variables into buckets, giving each bucket its own SV-generator.

Construction 7.5. Let \mathcal{H} be a (n, m, ℓ) -perfect hash family. Let $|\mathbb{F}| > |\mathcal{H}|, n$. Associate a distinct element $\eta_h \in \mathbb{F}$ for each $h \in \mathcal{H}$. Define $\mathcal{G}^H : (\mathbb{F}^2)^m \times \mathbb{F} \rightarrow \mathbb{F}^n$ by

$$\left(\mathcal{G}_{n,m,\ell}^H(y_1, \dots, y_m, z_1, \dots, z_m, u) \right)_i := \sum_{h \in \mathcal{H}} \left(\mathcal{G}_{n,1}^{\text{SV}}(y_{h(i)}, z_{h(i)}) \right)_i \cdot \mathbb{1}_{u=\eta_h}$$

for $i \in [n]$, where $\mathbb{1}_{w=\eta_h}$ denotes the Lagrange interpolation polynomial for the points $\{\eta_h\}_{h \in \mathcal{H}}$, of degree $\leq |\mathcal{H}|$. \diamond

In words, for every function $h \in \mathcal{H}$ we assign the SV generator on variables (y_k, z_k) to the x -variables that were mapped by h to the k -th bucket. We now give the desired properties of this construction.

Lemma 7.6. Assume the setup of [Construction 7.5](#), and the setup of the SV-generator of [Theorem 2.4](#). Let $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be computed by a width- r , individual degree $< d$, commutative ROABP. Suppose that f has a nonzero support- $(\leq \ell)$ monomial. Then there is a value of $\alpha \in \mathbb{F}$ such that $f \circ \mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \mathbf{y}^{dn^2}, \alpha)$ is a nonzero width- r , individual degree $< d^2 n^4$, commutative ROABP in m variables.

Proof: $f \circ \mathcal{G}^H \not\equiv 0$: Let the nonzero support- $(\leq \ell)$ monomial be $\mathbf{x}^{\mathbf{a}}$. Let $S = \text{supp}(\mathbf{a}) \subseteq [n]$, thus $|S| \leq \ell$. It follows that there is some hash $h \in \mathcal{H}$ such that h is injective on S . Let $\alpha \leftarrow \eta_h$. Thus, we have that $(\mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \mathbf{z}, \alpha))_i = (\mathcal{G}_{n,1}^{\text{SV}}(y_{h(i)}, z_{h(i)}))_i$. For $j \in [m]$, set $z_j \leftarrow \xi_{h^{-1}(j) \cap S}$, where $h^{-1}(j) \cap S$ is the unique element in S that hashes to j , or otherwise we take it to be 0. Call this assignment $\mathbf{z} \leftarrow \xi_0$.

Recalling that taking $z_j \leftarrow \xi_0$ zeroes out the corresponding y_j , and that taking $z_j \leftarrow \xi_k$ makes y_j only appear in the k -th output slot, we see that $\mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \xi_0, \alpha)$ places distinct variables of \mathbf{y} into the set $\text{supp}(\mathbf{x}^{\mathbf{a}})$, and otherwise outputs 0. It follows that $f \circ \mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \xi_0, \alpha)$ contains exactly those monomials in f whose support is contained in $\text{supp}(\mathbf{x}^{\mathbf{a}})$, and there is no cancellation. Therefore, the nonzero monomial $\mathbf{x}^{\mathbf{a}}$ survives this assignment, thus $f \circ \mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \xi_0, \alpha) \not\equiv 0$ and hence $f \circ \mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \mathbf{z}, \alpha) \not\equiv 0$.

Now note that f has individual degree $< d$, and thus total degree $< dn$. The generator $\mathcal{G}_{n,m,\ell}^H$ has individual degree $\leq n$ in \mathbf{y} and \mathbf{z} . It follows that $f \circ \mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \mathbf{z}, \alpha)$ has individual degree $< dn^2$

in each variable in \mathbf{y} and \mathbf{z} . Thus, applying the Kronecker substitution it follows that we can substitute $\mathbf{z} \leftarrow \mathbf{y}^{dn^2}$ and preserve nonzero-ness.

individual deg $< d^2n^4$: As argued above, before the substitution “ $\mathbf{z} \leftarrow \mathbf{y}^{dn^2}$ ” we had individual degree $< dn^2$, and the substitution multiplies this by another dn^2 factor.

$f \circ \mathcal{G}^H$ has a small commutative ROABP: Let $\pi : [m] \rightarrow [n]$ be any permutation, so that we wish to show that $f \circ \mathcal{G}^H$ has a small ROABP in the variable order $y_{\pi(1)}, \dots, y_{\pi(m)}$. Note that π induces an partial order \prec on $[n]$ via the hash function h chosen above. That is, say that for $i, j \in [n]$ that $i \prec j$ if $\pi^{-1}(h(i)) < \pi^{-1}(h(j))$. Now extend \prec to a total order on $[n]$ arbitrarily, and also call the induced permutation $\sigma : [n] \rightarrow [n]$. Thus, σ is the permutation that orders the variables according to \prec .

As f has a commutative ROABP, it follows that $f(\mathbf{x})$ is a linear function of the entries of a matrix-valued ROABP $F(\mathbf{x}) = \prod_{i \in [n]} M_i(x_{\sigma(i)})$ for $M_i(x_{\sigma(i)}) \in \mathbb{F}[x_{\sigma(i)}]^{r \times r}$ of individual degree $< d$. Now we plug in the above generator, and this yields that $f \circ \mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \mathbf{y}^{dn^2}, \alpha)$ is a linear combination of the entries of

$$\begin{aligned} \prod_{i \in [n]} M_i \left(\left(\mathcal{G}_{n,m,\ell}^H(\mathbf{y}, \mathbf{y}^{dn^2}, \alpha) \right)_{\sigma(i)} \right) &= \prod_{i \in [n]} M_i \left(\mathcal{G}_{n,1}^{\text{SV}} \left(y_{h(\sigma(i))}, y_{h(\sigma(i))}^{dn^2} \right) \right) \\ &= \prod_{j \in [m]} \prod_{h(\sigma(i))=\pi(j)} M_i \left(\mathcal{G}_{n,1}^{\text{SV}} \left(y_{\pi(j)}, y_{\pi(j)}^{dn^2} \right) \right) \\ &= \prod_{j \in [m]} M'_j(y_{\pi(j)}) \end{aligned}$$

where the above products are always increasing in $i \in [n]$ and $j \in [m]$ (so that this respects the non-commutativity of this matrix product, via the choice of π and σ), and

$$M'_j(y_{\pi(j)}) := \prod_{h(\sigma(i))=\pi(j)} M_i \left(\mathcal{G}_{n,1}^{\text{SV}} \left(y_{\pi(j)}, y_{\pi(j)}^{dn^2} \right) \right)$$

so that $M'_j(y_{\pi(j)}) \in \mathbb{F}[y_{\pi(j)}]^{r \times r}$. It follows that we have expressed $f \circ \mathcal{G}^H$ as a width- r ROABP in the order defined by π , and as π was arbitrary, it follows that $f \circ \mathcal{G}^H$ has a width- r commutative ROABP. \square

Thus, we have shown that commutative ROABPs with small-support monomials can have their number of variables essentially reduced to the size of that small-support monomial. We now combine this with the results of Forbes-Shpilka [FS12b] to derive our improved hitting sets.

Theorem 7.7. *Let $|\mathbb{F}| \geq \text{poly}(n, d, r, \ell)$. There is a $\text{poly}(n, d, r, \ell)$ -explicit, polynomial map $\mathcal{G}_{n,d,r,\ell}^{\text{H+FS}} : \mathbb{F}^{\mathcal{O}(\lg \ell)} \rightarrow \mathbb{F}^n$ of degree $\text{poly}(n, d, r, \ell)$, such that for any $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ computed by a width- r , individual degree $< d$ commutative ROABP, where $f \neq 0$ iff f has a nonzero support- $(\leq \ell)$ monomial, we have that $f \neq 0$ iff $f \circ \mathcal{G}_{n,d,r,\ell}^{\text{H+FS}} \neq 0$.*

In particular, when $|\mathbb{F}| \geq \text{poly}(n, d, s)$, the class of size- s , n -variable, total degree d diagonal circuits has $\text{poly}(n, d, s)$ -explicit hitting sets of size $\text{poly}(n, d, s)^{\mathcal{O}(\lg \lg(ds))}$. More generally, when $|\mathbb{F}| \geq \text{poly}(n, r)$, the class of n -variate polynomials f with $\dim(\partial f) \leq r$ has $\text{poly}(n, r)$ -explicit hitting sets of size $\text{poly}(n, r)^{\mathcal{O}(\lg \lg r)}$.

Similarly, if $|\mathbb{F}| \geq \text{poly}(n, d, r)$, the class of width- r , n -variable, individual degree $< d$ commutative ROABPs has a $\text{poly}(n, d, r)$ -explicit hitting set of size $\text{poly}(n, d^{\lg r}) \cdot \text{poly}(n, d, r)^{\mathcal{O}(\lg \lg r)}$.

Proof: \Leftarrow : Clear.

\Rightarrow : By assumption, $f \neq 0$ and has a support- $(\leq \ell)$ monomial. We can instantiate the hashing generator \mathcal{G}^H of Lemma 7.6 with the perfect hashing family of Lemma 7.4, so that $f \circ \mathcal{G}_{n, \mathcal{O}(\ell^2), \ell}^H$ is nonzero and computable by a width- r , individual degree $\text{poly}(d, n)$, commutative ROABP on $\mathcal{O}(\ell^2)$ variables, for some value of the variable u . It thus follows from Theorem 7.2 that $f \circ \mathcal{G}_{n, \mathcal{O}(\ell^2), \ell}^H \circ \mathcal{G}_{\mathcal{O}(\ell^2), \text{poly}(n, d), r}^{\text{FS}} \neq 0$, as this was true for some value of u , so is also true when u is symbolic. Taking $\mathcal{G}^{\text{H+FS}} := \mathcal{G}^H \circ \mathcal{G}^{\text{FS}}$ with the relevant parameters, we see that this generator has the desired explicitness, degree bound, and number of variables.

diagonal/low-rank circuits: Lemma 7.1 recalled that nonzero low-rank polynomials have, without shifting, a nonzero monomial of support $\mathcal{O}(\lg(sd))$ (or $\mathcal{O}(\lg r)$ for low-rank circuits), and are computed by commutative ROABPs of width- $\text{poly}(s, d)$ (or width- $\text{poly}(r)$ for low-rank circuits), so applying the above generator and interpolating gives the result.

low individual degree commutative ROABPs: Given such an f , we can shift it to have support- $\mathcal{O}(\lg r)$ rank concentration, by instantiating Theorem 4.1 with the $\mathcal{O}(\lg r)$ -wise independent monomial map from the KS-generator given in Lemma 4.4. This $\text{poly}(n, d, r)$ -explicit monomial map has individual degree $\text{poly}(n, d)$, and $\mathcal{O}(\lg r \cdot \log_{nd} d)$ variables. As this gives a small-support monomial, we can then hit f by adding in the $\mathcal{G}^{\text{H+FS}}$ generator above, and then interpolate the entire polynomial. The KS-generator will use $\text{poly}(n, d^{\lg r})$ possible values, and this will multiply on the number of values from the $\mathcal{G}^{\text{H+FS}}$ generator. \square

Note that the last result on commutative ROABPs becomes $(nr)^{\mathcal{O}(\lg \lg r)}$ when $d = \mathcal{O}(1)$.

Acknowledgements

This work was done while the first two authors were visiting the third. The first two authors would like to thank Chandan Saha for explaining the work of Agrawal-Saha-Saxena [ASS12] to them.

References

- [Agr05] M. Agrawal. Proving lower bounds via pseudo-random generators. In *Proceedings of the 25th FSTTCS*, volume 3821 of LNCS, pages 92–105, 2005.
- [AKS04] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Annals of Mathematics*, 160(2):781–793, 2004.
- [AMS08] V. Arvind, P. Mukhopadhyay, and S. Srinivasan. **New results on noncommutative and commutative polynomial identity testing**. In *Proceedings of the 23rd Annual CCC*, pages 268–279, 2008.
- [ASS12] M. Agrawal, C. Saha, and N. Saxena. **Quasi-polynomial hitting-set for set-depth- Δ formulas**. *Electronic Colloquium on Computational Complexity (ECCC)*, 19(113), 2012.
- [AV08] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings of the 49th Annual FOCS*, pages 67–75, 2008.
- [BD10] A. Bostan and P. Dumas. Wronskians and linear independence. *American Mathematical Monthly*, 117(8):722–727, 2010.

- [BDVY13] A. Bogdanov, Z. Dvir, E. Verbin, and A. Yehudayoff. **Pseudorandomness for width-2 branching programs**. *Theory of Computing*, 9:283–293, 2013.
- [BPW11] A. Bogdanov, P. A. Papanikolaou, and A. Wan. **Pseudorandomness for read-once formulas**. In *FOCS*, pages 240–246, 2011.
- [BRRY10] M. Braverman, A. Rao, R. Raz, and A. Yehudayoff. **Pseudorandom generators for regular branching programs**. In *Proceedings of the 51st annual FOCS*, pages 40–47, 2010.
- [BSC⁺12] A. Bostan, B. Salvy, M. F. I. Chowdhury, É. Schost, and R. Lebreton. **Power series solutions of singular (q)-differential equations**. In *ISSAC*, pages 107–114, 2012.
- [BV10] J. Brody and E. Verbin. **The coin problem and pseudorandomness for branching programs**. In *Proceedings of the 51st annual FOCS*, pages 30–39, 2010.
- [CGK⁺13] A. Chattopadhyay, B. Grenet, P. Koiran, N. Portier, and Y. Strozecki. **Factoring bivariate lacunary polynomials without heights**. In *ISSAC*, pages 141–148, 2013.
- [CLO06] D. A. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2006.
- [CW79] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18:143–154, 1979.
- [De11] A. De. **Pseudorandomness for permutation and regular branching programs**. In *IEEE Conference on Computational Complexity*, pages 221–231, 2011.
- [DGW09] Z. Dvir, A. Gabizon, and A. Wigderson. **Extractors and rank extractors for polynomial sources**. *Computational Complexity*, 18(1):1–58, 2009.
- [DKSS09] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan. **Extensions to the method of multiplicities, with applications to kakeya sets and mergers**. In *FOCS*, pages 181–190, 2009.
- [DL78] R. A. DeMillo and R. J. Lipton. A probabilistic remark on algebraic program testing. *Inf. Process. Lett.*, 7(4):193–195, 1978.
- [DS06] Z. Dvir and A. Shpilka. Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM J. on Computing*, 36(5):1404–1434, 2006.
- [DSY09] Z. Dvir, A. Shpilka, and A. Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. on Computing*, 39(4):1279–1293, 2009.
- [FS12a] M. A. Forbes and A. Shpilka. **On identity testing of tensors, low-rank recovery and compressed sensing**. In *Proceedings of the 44th annual STOC*, pages 163–172, 2012.
- [FS12b] M. A. Forbes and A. Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. *Electronic Colloquium on Computational Complexity (ECCC)*, 19(115), 2012.
- [FS13] M. A. Forbes and A. Shpilka. **Explicit Noether normalization for simultaneous conjugation via polynomial identity testing**. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:33, 2013.

- [GK13] V. Guruswami and S. Kopparty. **Explicit subspace designs**. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:60, 2013.
- [GKKS12] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi. **An exponential lower bound for homogeneous depth four arithmetic circuits with bounded bottom fanin**. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:98, 2012.
- [GKKS13] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi. **Arithmetic circuits: A chasm at depth three**. *Electronic Colloquium on Computational Complexity (ECCC)*, 20(26), 2013.
- [GMR⁺12] P. Gopalan, R. Meka, O. Reingold, L. Trevisan, and S. P. Vadhan. **Better pseudorandom generators from milder pseudorandom restrictions**. In *Proceedings of the 53rd Annual FOCS*, pages 120–129, 2012.
- [GR08a] A. Gabizon and R. Raz. **Deterministic extractors for affine sources over large fields**. *Combinatorica*, 28(4):415–440, 2008.
- [GR08b] V. Guruswami and A. Rudra. **Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy**. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.
- [GW13] V. Guruswami and C. Wang. **Linear-algebraic list decoding for variants of reed-solomon codes**. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013.
- [HS80] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute (extended abstract). In *Proceedings of the 12th annual STOC*, pages 262–272, 1980.
- [IMZ12] R. Impagliazzo, R. Meka, and D. Zuckerman. Pseudorandomness from shrinkage. In *Proceedings of the 53rd annual FOCS*, pages 111–119, 2012.
- [INW94] R. Impagliazzo, N. Nisan, and A. Wigderson. **Pseudorandomness for network algorithms**. In *Proceedings of the 26th annual STOC*, pages 356–364, 1994.
- [KC02] V. Kac and P. Cheung. *Quantum calculus*. Universitext. Springer-Verlag, New York, 2002.
- [KI04] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.
- [KMSV10] Z. S. Karnin, P. Mukhopadhyay, A. Shpilka, and I. Volkovich. Deterministic identity testing of depth 4 multilinear circuits with bounded top fan-in. In *Proceedings of the 42nd Annual STOC*, pages 649–658, 2010.
- [KNP11] M. Koucký, P. Nimbhorkar, and P. Pudlák. **Pseudorandom generators for group products: extended abstract**. In *STOC*, pages 263–272, 2011.
- [KS01] A. Klivans and D. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the 33rd Annual STOC*, pages 216–223, 2001.
- [KS07] N. Kayal and N. Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity*, 16(2):115–138, 2007.

- [KS09] N. Kayal and S. Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *Proceedings of the 50th Annual FOCS*, pages 198–207, 2009.
- [KS11] Z. S. Karnin and A. Shpilka. **Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in**. *Combinatorica*, 31(3):333–364, 2011.
- [KS12] N. Kayal and C. Saha. **On the sum of square roots of polynomials and related problems**. *TOCT*, 4(4):9, 2012.
- [KUW86] R. M. Karp, E. Upfal, and A. Wigderson. **Constructing a perfect matching is in random NC**. *Combinatorica*, 6(1):35–48, 1986.
- [Meh82] K. Mehlhorn. **On the program size of perfect and universal hash functions**. In *FOCS*, pages 170–175, 1982.
- [Mul12] K. 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.
- [MVV87] K. Mulmuley, U. Vazirani, and V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987.
- [Nis91] N. Nisan. Lower bounds for non-commutative computation. In *Proceedings of the 23rd Annual STOC*, pages 410–418, 1991.
- [Nis92] N. Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992.
- [NW96] N. Nisan and A. Wigderson. Lower bound on arithmetic circuits via partial derivatives. *Computational Complexity*, 6:217–234, 1996.
- [NZ96] N. Nisan and D. Zuckerman. Randomness is linear in space. *J. of Computer and System Sciences*, 52(1):43–52, 1996.
- [Raz06] R. Raz. **Separation of multilinear circuit and formula size**. *Theory of Computing*, 2(1):121–135, 2006.
- [Raz09] R. Raz. **Multi-linear formulas for permanent and determinant are of super-polynomial size**. *J. ACM*, 56(2), 2009.
- [Rot91] R. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, 1991.
- [RR99] R. Raz and O. Reingold. **On recycling the randomness of states in space bounded computation**. In *Proceedings of the 31st annual STOC*, pages 159–168, 1999.
- [RS05] R. Raz and A. Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005.
- [RSV13] O. Reingold, T. Steinke, and S. P. Vadhan. **Pseudorandomness for regular branching programs via fourier analysis**. In *APPROX-RANDOM*, pages 655–670, 2013.

- [RSY08] R. Raz, A. Shpilka, and A. Yehudayoff. A lower bound for the size of syntactically multilinear arithmetic circuits. *SIAM J. on Computing*, 38(4):1624–1647, 2008.
- [RY09] R. Raz and A. Yehudayoff. **Lower bounds and separations for constant depth multilinear circuits**. *Computational Complexity*, 18(2):171–207, 2009.
- [Sax08] N. Saxena. **Diagonal circuit identity testing and lower bounds**. In *ICALP (1)*, pages 60–71, 2008.
- [Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.
- [SS89] J. P. Schmidt and A. Siegel. **On aspects of universality and performance for closed hashing (extended abstract)**. In *Proceedings of the 21st annual STOC*, pages 355–366, 1989.
- [SS11] N. Saxena and C. Seshadhri. Blackbox identity testing for bounded top fanin depth-3 circuits: the field doesn’t matter. In *Proceedings of the 43rd Annual STOC*, pages 431–440, 2011.
- [SSS11] C. Saha, R. Saptharishi, and N. Saxena. **A case of depth-3 identity testing, sparse factorization and duality**. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:21, 2011.
- [Ste12] T. Steinke. **Pseudorandomness for permutation branching programs without the group theory**. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:83, 2012.
- [SV09] A. Shpilka and I. Volkovich. Improved polynomial identity testing for read-once formulas. In *APPROX-RANDOM*, pages 700–713, 2009.
- [SV11] S. Saraf and I. Volkovich. **Black-box identity testing of depth-4 multilinear circuits**. In *Proceedings of the 43rd annual STOC*, pages 421–430, 2011.
- [SY10] A. Shpilka and A. Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010.
- [SZ11] J. Síma and S. Zák. **Almost k -wise independent sets establish hitting sets for width-3 1-branching programs**. In *CSR*, pages 120–133, 2011.
- [Tzu09] Y. Tzur. **Notions of weak pseudorandomness and $GF(2^n)$ -polynomials**. Master’s thesis, Weizmann Institute of Science, 2009.
- [Vad12] S. P. Vadhan. **Pseudorandomness**. *Foundations and Trends in Theoretical Computer Science*, 7(1-3):1–336, 2012.
- [WY12] A. Wigderson and A. Yehudayoff. **Population recovery and partial identification**. In *FOCS*, pages 390–399, 2012.
- [Zip79] R. Zippel. **Probabilistic algorithms for sparse polynomials**. In *EUROSAM*, pages 216–226, 1979.