Explicit Commutative ROABPs from Partial Derivatives

Vishwas Bhargava [*] Anamay Tengse [†]

July 14, 2024

Abstract

The dimension of partial derivatives (Nisan and Wigderson, 1997) is a popular measure for proving lower bounds in algebraic complexity. It is used to give strong lower bounds on the *Waring decomposition* of polynomials (called *Waring rank*). This naturally leads to an interesting open question: does this measure essentially characterize the Waring rank of any polynomial?

The well-studied model of Read-once Oblivious ABPs (ROABPs for short) lends itself to an interesting hierarchy of 'sub-models': Any-Order-ROABPs (ARO), Commutative ROABPs, and Diagonal ROABPs. It follows from previous works that for any polynomial, a bound on its Waring rank implies an analogous bound on its Diagonal ROABP complexity (called the *duality trick*), and a bound on its dimension of partial derivatives implies an analogous bound on its 'ARO complexity': ROABP complexity in any order (Nisan, 1991). Our work strengthens the latter connection by showing that a bound on the dimension of partial derivatives in fact implies a bound on the commutative ROABP complexity. Thus, we improve our understanding of partial derivatives and move a step closer towards answering the above question.

Our proof builds on the work of Ramya and Tengse (2022) to show that the *commutative-ROABP-width* of any homogeneous polynomial is at most the dimension of its partial derivatives. The technique itself is a generalization of the proof of the *duality trick* due to Saxena (2008).

1 Introduction

How many points do we need to evaluate an expression like the following on, to deterministically tell if it is computing the zero polynomial?

$$f(x_1, \ldots, x_n) = (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n)^d + \cdots + (a_{s,1}x_1 + \cdots + a_{s,n}x_n)^d \tag{1.1}$$

[*]David R. Cheriton School of Computer Science, Univeristy of Waterloo, Waterloo, Canada. Email: vishwas1384@gmail.com.

[†]School of Computer Sciences, NISER, Bhubaneswar. A major part of this work was done as a postdoc at the Univeristy of Haifa (ISF grant no. 716/20), and Reichman University, Herzliya (ISF grant no. 843/23). Email: anamay.tengse@gmail.com.

As of today, the answer to this question stands at $(nds)^{O(\log\log n)}$, just a (rather annoying) smidgen away from a legit efficient algorithm. The above bound follows from a combination of the works of Forbes, Saptharishi and Shpilka [FSS14] and Gurjar, Korwar and Saxena [GKS17].

An expression like (1.1) is called a *Waring decomposition for* f of size s; the name comes from 'Waring's problem' in number theory[1]. Analogously, for a homogeneous polynomial $f(\mathbf{x})$ of degree d, its *Waring rank* is the smallest number s for which f can be written as a sum of d-th powers of s-many linear forms; that is, the size of its smallest Waring decomposition. The Waring rank of different polynomials has been studied in mathematics for over a century now (see e.g. [IK99]), and some recent works have even found its applications in parameterized algorithms (e.g. [Pra19]). It is known that any polynomial has a finite Waring rank [Fis94, CCG12], except for over finite fields of small characteristic. We now also know the Waring rank of monomials exactly [RS11]. For example, it is known that the monomial $x_1x_2\cdots x_n$ has Waring rank exactly 2^{n-1}.

The corresponding algebraic model of computation: called a "depth-3-powering circuit", was first introduced in algebraic circuit complexity by Saxena [Sax08], who studied it from the perspective of polynomial identity testing (PIT for short). PIT is the algorithmic task mentioned above: determine whether the given circuit computes the identically zero polynomial. In what is sometimes called a "whitebox PIT", the algorithm has access to the circuit itself; Saxena [Sax08] gave an efficient whitebox test for a more general model. In a "blackbox PIT", the algorithm cannot access the expression and can only query it on a few points (independent of the actual circuit), which is exactly the question stated at the start.

Dimension of partial derivatives

All the currently known blackbox PITs for depth 3 powering circuits build on the fact that any n-variate, degree-d polynomial with Waring rank s has at most $s(d+1)$ *dimension of partial derivatives* (see Definition 1.5). The measure was introduced by Nisan and Wigderson [NW97] as a tool to prove lower bounds against sums of *products* of linear forms, and thus the above statement is implicit from their work. The myriad variants of this measure now form the basis of several strong lower bounds throughout algebraic circuit complexity (see e.g. [SY10, Sap15]).

Returning to Waring decompositions, almost all known lower bounds on Waring ranks of different polynomials use the dimension of partial derivatives in one way or the other. In view of this, and given the strong connections between proofs of hardness and derandomization of PIT (see e.g. [KS19]), it stands to reason that obtaining an efficient blackbox PIT for depth 3 powering circuits requires us to answer the following question.

Question 1.2. *Is it the case that any n-variate polynomial with dimension of partial derivatives r has a Waring rank that is at most* $\mathrm{poly}(n,r)$*?*

[1] See this wikipedia article for a summary.

To the best of our knowledge, there aren't even any candidate negative examples to this question, except for the symbolic determinant: Det_n. The $n \times n$ determinant has a dimension of partial derivatives that is $2^{\Theta(n)}$, but the best known upper bound on its Waring rank stands at $2^{O(n \log n)}$.

The only other "deviation" that these two measures — dimension of partial derivatives and Waring rank — exhibit, comes from their respective connections with a different well-studied model, which we will now see.

1.1 Read-once Oblivious ABPs (ROABPs)

An ROABP is an expression of the form: $\mathbf{u}^\intercal \cdot M_1(x_1) \cdot M_2(x_2) \cdots M_n(x_n) \cdot \mathbf{v}$, where $\mathbf{u}, \mathbf{v}$ are vectors over the base field and each $M_j(x_j)$ is a univariate polynomial with matrices as coefficients, as follows.

$$M_j(x_j) = A_{j,0} + A_{j,1}x_i + A_{j,2}x_i^2 + \cdots + A_{j,d}x_j^d \tag{1.3}$$

That is, there is exactly one 'matrix-polynomial' corresponding to each variable. Thus, each variable is "read" exactly once, oblivious to the other variables; hence the name. We formally define ROABPs in Definition 2.1.

Here, the dimension of $\mathbf{u}$, $\mathbf{v}$ and all the $n(d+1)$ many matrices (assumed to be the same without loss of generality) is said to be the *width* of the ROABP, and is typically denoted by w. Note that the width of an ROABP is the single parameter that dictates its complexity, since n and d arise straight from the polynomial being computed. A subtle point here is that for the same polynomial, the smallest possible ROABP-width can vary widely depending on the order in which the variables appear (see Observation 2.8), and hence the order of an ROABP is also an important parameter. Nevertheless, for any polynomial and any order, the exact size of the smallest corresponding ROABP can be obtained using a characterization given by Nisan [Nis91]. As we will soon see, even this characterization is in a way connected to the partial derivatives of the given polynomial; we provide a formal definition and statement in Definition 2.5 and Theorem 2.6.

ROABPs were formally introduced by Forbes and Shpilka [FS13] as algebraic analogues of ROBPs from the boolean world, where they showed a quasi-polynomial time blackbox PIT for ROABPs, inspired by Nisan's PRG construction against ROBPs [Nis92]. As the name suggests, ROABPs are a special case of "algebraic branching programs" which are an algebraic analogue of the (boolean) branching programs. However, we omit those definitions of ABPs and ROABPs, as seeing them as the matrix-vector product expressions like above would be more useful for the discussions in this paper. We now introduce the structured variants of ROABPs that are relevant to this work.

1.2 Variants of ROABPs

Since the ROABP-complexity of some polynomials depends heavily on the underlying order, we can further cut out a subclass of polynomials that admit $\text{poly}(n,d)$-sized ROABPs: those that admit $\text{poly}(n,d)$-sized ROABPs *in every order*. This class of polynomials is sometimes referred to as "Any-order ROABPs" (AROs for short)[2].

A *syntactic* way of ensuring that a polynomial computed by an efficient ROABP belongs to ARO, is to ensure that all the $n(d+1)$-many coefficient matrices ($A_{j,*}$s in (1.3)) commute with each other under multiplication. This then means that for any $j, j' \in [n]$, we have that $M_j(x_j)M_{j'}(x_{j'}) = M_{j'}(x_{j'})M_j(x_j)$, and then the layers of the same ROABP can be shuffled to work for any order. Such an ROABP with commuting coefficient matrices is called a *commutative ROABP* (commRO for short); a formal definition is in Definition 2.2.

Finally, an easy way to pick coefficient matrices that commute with each other is to choose all of them as diagonal matrices. Such an ROABP is called a *diagonal ROABP* (diagRO for short), defined in Definition 2.3.

The above variants of ROABPs appear implicitly in some previous works on ROABPs, but they were explicitly defined and proposed as objects of study in a recent work of Ramya and Tengse [RT22]. As mentioned earlier, our proof technique also borrows from the algebraic machinery that appears in their work.

We now proceed to look at the connections between Waring rank, dimension of partial derivatives and these structured ROABPs, before stating our main result.

1.3 Waring rank, partial derivatives and ROABPs

The aforementioned whitebox PIT for depth 3 powering circuits due to Saxena [Sax08] has the following result at its core.

Theorem 1.4 (Duality trick [Sax08, Lemma 1] (Informal)). *For any linear form $\ell(\mathbf{x}) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, and any d, the polynomial $\ell(\mathbf{x})^d$ can be expressed as:*

$$\ell(\mathbf{x})^d = \sum_{i=1}^{t} \beta_i \cdot g_{i,1}(x_1) \cdot g_{i,2}(x_2) \cdots g_{i,n}(x_n),$$

for constants $\beta_1, \ldots, \beta_t$ and degree-d univariates $g_{1,1}, \ldots, g_{t,n}$, with $t \leq nd + 1$.

Note that this gives an ROABP of width $t = O(nd)$ for the d-th power of any n-variate linear form, by using the $g_{i,j}$s appropriately to obtain each of the matrix polynomials $M_j(x_j)$ and using β_is in the vector $\mathbf{u}$ (or $\mathbf{v}$). In fact, the "coefficient matrices" (the $A_{j,*}$s from (1.3)) of this ROABP are

[2]Contrary to what the name suggests, this is not a special type of ROABPs, it is a class of polynomials.

just diagonal matrices. Consequently, an n-variate, degree-d polynomial with Waring rank r has a diagRO of width $O(ndr)$.

The duality trick actually provides diagROs for a more general model called "depth 4 diagonal circuits", and the corresponding whitebox PIT also holds for this more general model. In fact, this relation between powering circuits and diagROs is a crucial component of the current state-of-the-art blackbox PIT for depth 3 powering circuits [FSS14, GKS17] mentioned earlier.

Given that polynomials with small Waring rank have small diagROs, it is natural to ask what happens to polynomials with small dimension of partial derivatives.

ROABPs and partial derivatives. Suppose we are given an n-variate, degree-d polynomial $f(\mathbf{x})$, whose dimension of partial derivatives is at most r. It turns out, via Nisan's characterization, that such a polynomial has an ROABP of width at most r *in every order* (see Observation 2.7). That is, for any $\sigma \in s_n$, we are guaranteed *some* ROABP, say $R_\sigma(\mathbf{x})$, that computes f in that order. However, it is not clear from this non-constructive upper bound whether the ROABPs R_σ across different σs are related in any way. This brings us to our main result.

1.4 Our contribution

We first formally define the measure: dimension of partial derivatives.

Definition 1.5 (Dimension of partial derivatives)**.** *For a polynomial $f(x_1, \ldots, x_n)$, the dimension of its partial derivatives is defined as follows.*

$$\dim \partial^{<\infty}(f) := \dim\left(\operatorname{span}_{\mathbb{C}}\{\partial_{\mathbf{e}} f : \mathbf{e} \in \mathbb{N}^n\}\right)$$

Here $\partial_{\mathbf{e}} f$ denotes the partial derivative of f with respect to the monomial $\mathbf{x}^{\mathbf{e}} = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$. ◊

For a polynomial f, let $\mathrm{commRO}(f)$ denote the width of the smallest commRO that computes it; our main result is as follows.

Theorem 1.6. *For any homogeneous polynomial $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$, $\mathrm{commRO}(f) \leq \dim \partial^{<\infty}(f)$.*

Since the dimension of partial derivatives of any homogeneous component of f is at most $\deg(f)$ times that of f (see Lemma 2.4), we get the following result in the general case.

Corollary 1.7. *For any $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$ of degree d, $\mathrm{commRO}(f) \leq (d+1)^2 \cdot \dim \partial^{<\infty}(f)$.*

Set multilinear upper bounds In fact, our method for constructing commutative ROABPs using $\dim \partial^{<\infty}(f)$ also lets us obtain what we call "commutative set-multilinear ABPs" for f with a minor tweak in our proof. Informally, a degree-d polynomial $f(\mathbf{x})$ is called set-multilinear under a partition $\mathbf{x} = \mathbf{x}_1 \sqcup \mathbf{x}_2 \sqcup \cdots \sqcup \mathbf{x}_d$, if each of its monomials contains exactly one variable from each of

the $\mathbf{x}_i$s. A(n ordered) set-multilinear ABP is then a product of matrices with linear polynomials as entries, with the variables in those polynomials obeying the partition (see definitions 4.2 and 4.3).

Theorem 1.8. *For any set-multilinear polynomial $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$, the commutative-set-multilinear-ABP-width$(f) \leq \dim \partial^{<\infty}(f)$.*

Explicitness. We note that our proof provides an explicit construction of a commRO for any polynomial f, given the *dependencies* between the partial derivatives of f. In fact, as mentioned earlier, this construction itself is a generalization of the proof of the duality trick from Saxena's work [Sax08] (see Remark 3.7). We describe a width-$2^{O(n)}$ commRO, and a commutative set-multilinear ABP for the $n \times n$ determinant to illustrate this point in Section 4.

2 Preliminaries

Throughout the paper, we work with the field of complex numbers, but most of our proofs extend to fields whose characteristic is zero or large enough.

Notation

- For a vector $\mathbf{e} \in \mathbb{N}^n$, we write $\mathbf{t}^{\mathbf{e}}$ for the monomial $t_1^{e_1} t_2^{e_2} \cdots t_n^{e_n}$, where $\mathbf{t}$ is a set of variables. We also use $\mathbf{e}!$ to refer to the product of factorials $e_1!e_2! \cdot e_n!$.
- For a monomial m, we write $\partial_m f$ for the partial derivative $\frac{\partial^{|\mathbf{e}|} f}{\partial \mathbf{t}^{\mathbf{e}}}$. When $m = \mathbf{t}^{\mathbf{e}}$, we shorten it further to $\partial_{\mathbf{e}} f$.

2.1 Formal definitions

Definition 2.1 (Read-once Oblivious ABP (ROABP))**.** *For any $n, d, w \in \mathbb{N}$, and an n-variate polynomial $f(\mathbf{x})$ of individual degree d, we say that it has a width w ROABP, if there exists a permutation $\sigma \in s_n$ for which there exist matrices $\{A_{j,k}\}$ in $\mathbb{C}^{w \times w}$ for all $j \in [n]$ and $0 \leq k \leq d$, and vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^w$, such that the following holds.*

$$f(\mathbf{x}) = \mathbf{u}^{\intercal} \cdot M_{\sigma(1)}(x_{\sigma(1)}) \cdot M_{\sigma(2)}(x_{\sigma(2)}) \cdots M_{\sigma(n)}(x_{\sigma(n)}) \cdot \mathbf{v},$$
$$\text{where for all } j \in [n],$$
$$M_j(x_j) = A_{j,0} + A_{j,1}x_j + A_{j,2}x_j^2 + \cdots + A_{j,d}x_j^d.$$

We call the matrices $\{A_{j,k}\}$ the coefficient matrices *of the ROABP.* ◊

Definition 2.2 (Commutative ROABP (commRO))**.** *An ROABP is said to be a* commutative ROABP, *if all its coefficient matrices commute with each other pairwise.*

For a polynomial f, we use commRO(f) *to denote the smallest width w such that there is width-w commRO computing f.* ◊

Definition 2.3 (Diagonal ROABP (diagRO))**.** *An ROABP is said to be a* diagonal ROABP*, if all its coefficient matrices are diagonal matrices.*

For a polynomial f, we use diagRO(f) *to refer to the smallest width w such that there is width-w diagRO computing f.* ◊

Partial Derivatives and the Nisan matrix

Lemma 2.4. *Let $f(\mathbf{x})$ be a polynomial of degree d and let $h(\mathbf{x})$ be some homogeneous component of f. Then* $\dim \partial^{<\infty}(h) \leq (d+1) \cdot \dim \partial^{<\infty}(f)$.

Proof. Note that for any nonzero scalar α, the polynomial $f_\alpha(\mathbf{x}) := f(\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$ satisfies $\dim \partial^{<\infty}(f_\alpha) = \dim \partial^{<\infty}(f)$, since it is an invertible operation. Next, for distinct $\alpha_0, \alpha_1, \ldots, \alpha_d \in \mathbb{C}$, we can use interpolation to write h as a linear combination of $f_{\alpha_0}, f_{\alpha_1}, \ldots, f_{\alpha_d}$. Thus, $\dim \partial^{<\infty}(h) \leq \sum_{0 \leq i \leq d} \dim \partial^{<\infty}(f_{\alpha_i}) \leq (d+1) \cdot \dim \partial^{<\infty}(f)$. □

Definition 2.5 (Nisan Matrix [Nis91])**.** *For an n-variate polynomial $f(\mathbf{x})$ of individual degree d, and a partition $S \sqcup T = [n]$, the (S,T)-*Nisan matrix *for f, $M^f_{(S,T)}$, is a $(d+1)^{|S|} \times (d+1)^{|T|}$ matrix as follows.*

- *The rows are indexed by all the individual degree d monomials over $\{x_i \mid i \in S\}$,*
- *The columns are indexed by all the individual degree d monomials over $\{x_j \mid j \in T\}$,*
- *The entry $M^f_{(S,T)}[m, m']$ is the coefficient of the monomial $m \cdot m'$ in f.*

◊

Theorem 2.6 (Nisan's characterization [Nis91])**.** *For any n-variate polynomial $f(\mathbf{x})$, and any order $\sigma \in s_n$ on the variables, define $S_i = \{\sigma(1), \ldots, \sigma(i)\}$ and $T_i = \{\sigma(i+1), \ldots, \sigma(n)\}$ for each $i \in [n]$. Then the size of the smallest ROABP for f in the order σ is exactly $\sum_{i \in [n]} \operatorname{rank}(M^f_{(S_i,T_i)})$. Further, the width of the ROABP is exactly $\max_{i \in [n]} \operatorname{rank}(M^f_{(S_i,T_i)})$.*

It is not difficult to see that for any polynomial, the Nisan matrix for any partition is a scaling of a sub-matrix of a matrix whose rows are all the partial derivatives of that polynomial. This then leads to the following observation, which is a weaker and non-constructive version of Theorem 1.6.

Observation 2.7. *Let $n, d \in \mathbb{N}$ be arbitrary and $\mathbb{F}$ be any field of characteristic 0 or greater than d. Then for any n-variate $f(\mathbf{x})$ of individual degree d, and any partition $S \sqcup T = [n]$, $\operatorname{rank}(M^f_{(S,T)}) \leq \dim \partial^{<\infty}(f)$.*

Thus, any polynomial f has an ROABP in every order of width at most $\dim \partial^{<\infty}(f)$.

Observation 2.8. *The polynomial $(x_1 + y_1)(x_2 + y_2) \cdots (x_n + y_n)$ has width-2 ROABPs in the order $(x_1, y_1, \ldots, x_n, y_n)$, but requires width 2^n in the order $(x_1, \ldots, x_n, y_1, \ldots, y_n)$.*

2.2 Concepts from algebra

We will need a few concepts from elementary algebraic geometry; the reader may refer to any standard texts for more details on these concepts (e.g. [CLO07, IK99]).

Definition 2.9 (Ideal). *For a set of polynomials $\{f_1, \ldots, f_s\} \subset \mathbb{C}[\mathbf{x}]$, the ideal generated by them is the smallest set of polynomials I that satisfies the following.*

- $\forall g \in \mathbb{C}[\mathbf{x}]$ *and* $\forall f \in I$, $fg \in I$.
- $\forall f, f' \in I$, *we have* $f + f' \in I$.

The ideal is denoted by $\langle \{f_1, \ldots, f_s\} \rangle$. ◊

Definition 2.10 (Variety of an ideal). *For an ideal $I \subset \mathbb{C}[\mathbf{x}]$, the* variety of I, *written as* $\mathbf{V}(I)$, *is the largest set of points $V \subset \mathbb{C}^{|\mathbf{x}|}$ such that $\forall f \in I$ and $\forall \mathbf{a} \in V$, $f(\mathbf{a}) = 0$.* ◊

Derivative operators

Definition 2.11 (Derivative Operator). *A derivative operator is a linear combination of finitely many partial derivatives of the form $D = \sum_{i=1}^{r} \alpha_i \partial_{m_i}$. It acts on polynomials naturally: $Df = \sum_{i=1}^{r} \alpha_i \partial_{m_i} f$.*

Clearly, for any polynomial $g = \sum_m g_m m$, we can define a derivative operator $D_g = \sum_m g_m \partial_m$, and vice versa. Therefore, we always refer to a derivative operator as D_g with an implicit polynomial g. ◊

Definition 2.12 (Closed space of derivative operators). *A vector space of operators Δ is said to be closed if for every $D_g \in \Delta$, and any monomial m such that $g' := \partial_m g \not\equiv 0$, the corresponding operator $D_{g'}$ is also in Δ.* ◊

Observation 2.13. *For any $f(\mathbf{t}), g(\mathbf{t}) \in \mathbb{C}[\mathbf{t}]$, we have the following.*

$$\left(D_f g\right)(\mathbf{0}) = \sum_{\mathbf{e}} \mathrm{coeff}_f(\mathbf{t}^{\mathbf{e}}) \cdot \mathbf{e}! \cdot \mathrm{coeff}_g(\mathbf{t}^{\mathbf{e}}) = \left(D_g f\right)(\mathbf{0})$$

Primary ideals and derivative operators The following result follows from the joint works of Möller, Marinari and Mora [MMM93], and Möller and Stetter [MS95]. A proof, with a statement as follows, can be found in [RT22].

Theorem 2.14 ([MMM93, MS95]). *Let $J \subseteq \mathbb{C}[\mathbf{t}]$ be an ideal with the variety $\mathbf{V}(J) = \{\mathbf{0}\}$, and suppose that the quotient ring $R_J := \mathbb{C}[\mathbf{t}]/J$ is a w-dimensional vector space over $\mathbb{C}$. Then, there exists a w-dimensional $\mathbb{C}$-vector space of derivative of operators $\Delta(J)$ that characterizes the quotient ring R_J.*

That is, for any basis $\{D_1, \ldots, D_w\}$ of $\Delta(J)$, there is an invertible *matrix $M \in \mathbb{C}^{w \times w}$ such that for any polynomial $g(\mathbf{t}) \in \mathbb{C}[\mathbf{t}]$,*

$$[D_1(g)(\mathbf{0}) \;\; D_2(g)(\mathbf{0}) \;\; \cdots \;\; D_w(g)(\mathbf{0})]^{\mathsf{T}} = M \cdot \overline{\mathrm{coeff}}([g]),$$

where $\overline{\mathrm{coeff}}([g])$ is the coefficient vector of $[g] := (g \bmod J)$.

The above correspondence works for any point $\mathbf{a} \in \mathbb{C}^n$ in the variety; we will work with $\mathbf{0}$ to keep the exposition simple, since that is the only case relevant for our application.

Definition 2.15 (Operator space of an ideal)**.** *For an ideal $J \subseteq \mathbb{C}[\mathbf{t}]$ with $\mathbf{V}(J) = \{\mathbf{0}\}$, we define the corresponding space of derivative operators $\Delta(J)$ as follows.*

$$\Delta(J) := \left\{ D_g \in \mathbb{C}[\partial\mathbf{t}] : \forall h \in J, (D_g h)(\mathbf{0}) = 0 \right\} \qquad \Diamond$$

Definition 2.16 (Ideal of an operator space)**.** *Let Δ be a closed space of derivative operators. We define the corresponding annihilating ideal (at the point $\mathbf{0}$), denoted by $\mathbf{I_0}(\Delta)$ as follows.*

$$\mathbf{I_0}(\Delta) := \{ h \in \mathbb{C}[\mathbf{t}] : \forall D \in \Delta, (Dh)(\mathbf{0}) = 0 \} \qquad \Diamond$$

2.3 Multiplication tables: from ideals to matrices

Univariate ideals

Let $J = \langle p(t) \rangle \subseteq \mathbb{C}[t]$ be an ideal, and consider the quotient ring $R := {}^{\mathbb{C}[t]}/_{J}$. If $p(t)$ has degree d, then the *multiplication table* for t in the ring R, is a $d \times d$ matrix whose *minimal polynomial* is $p(t)$. Such a matrix, say A, can easily be defined by setting $A_{i,j} = \text{coeff}_{t^j}(\left[t \cdot t^i\right])$, for all $0 \leq i, j \leq (d-1)$. Here, $[t \cdot t^i]$ is $(t^{i+1} \bmod J)$.

For instance, when $p(t) = t^5 - 10t^4 - 7t^3 + 2t^2 - 3$, the multiplication table would be the following 5×5 matrix; it can be checked that $p(t)$ is indeed the minimal polynomial of A.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & -2 & 7 & 10 \end{bmatrix}$$

Further, A satisfies that $g(A)_{i,j}$ is exactly $\text{coeff}_{t^j}(\left[g(t) \cdot t^i\right])$, for any $g(t) \in \mathbb{C}[t]$. In particular, this means that the first row of $g(A)$ is precisely the coefficient vector of $[g(t)]$.

Multivariate ideals

One key change when we move to the multivariate setting, is that there is no inherent ordering on the monomials; so we have to choose one. A *monomial ordering* is any 'total order' on monomials, which respects divisions and has 1 as the least monomial. We will work with the degree-wise lexicographical ordering ("deg-lex") with respect to $t_1 \prec t_2 \prec \cdots \prec t_r$. We use this monomial ordering to uniquely identify the leading ("greatest") and trailing ("least") monomials in any polynomial in $\mathbb{C}[t_1, \ldots, t_r]$.

This then allows us to identify a set of leading monomials of the ideal, and then define what is called a normal set and the quotient ring corresponding to the ideal, as follows.

Definition 2.17 (Leading monomials and normal set)**.** *Given an ideal $I \subset \mathbb{C}[\mathbf{x}]$, and a monomial ordering, the set of its leading monomials is defined as* $\mathrm{LM}(I) := \{\mathrm{LM}(f) \mid f \in I\}$.

The complement of $\mathrm{LM}(I)$ *is called the* normal set of I*, denoted by* $\mathrm{N}(I)$. ◊

Definition 2.18 (Quotient ring)**.** *For any ideal $I \subset \mathbb{C}[\mathbf{x}]$, and any polynomial $g \in \mathbb{C}[\mathbf{x}]$, we can define g* mod *I to be the polynomial g_0 all of whose monomials are from* $\mathrm{N}(I)$ *and which satisfies $g - g_0 \in I$. We denote the polynomial g* mod *I by $[g]$ when the ideal is clear from the context.*

We can thus define the quotient ring *corresponding to I denoted by $\mathbb{C}[\mathbf{x}]/I$, by reducing each polynomial in $\mathbb{C}[\mathbf{x}]$ modulo I.* ◊

Intuitively, the quotient ring $\mathbb{C}[\mathbf{t}]/J$ is obtained by "setting all polynomials in J to zero". Then any monomial from $\mathrm{LM}(J)$ can be written in terms of those in the normal set, and the polynomials in the quotient ring are supported entirely on the monomials from $\mathrm{N}(J)$.

Let the normal set of $J \in \mathbb{C}[t_1, \ldots, t_r]$ be $\{m_1, \ldots, m_w\}$, where $1 = m_1 \prec m_2 \prec \cdots \prec m_w$. The multiplication tables $A_1, A_2, \ldots, A_r$ for J are then the $w \times w$ matrices that satisfy the following, for every $\ell \in [r]$, and all $i, j \in [w]$.

$$A_\ell(i, j) = \mathrm{coeff}_{m_j}([t_\ell \cdot m_i])$$

Just as before, for any polynomial $g(\mathbf{t})$, we have that $g(A_1, \ldots, A_r)(i, j) = \mathrm{coeff}_{m_j}([g \cdot m_i])$. Thus, the first row of any matrix of the form $g(A_1, \ldots, A_r)$ is just the coefficient vector of $g(\mathbf{t})$ mod J, for any polynomial g.

3 Constructing commutative ROABPs from apolarities

3.1 Apolar ideal of a polynomial

Definition 3.1 (Apolar Ideal)**.** *Let $f(t_1, \ldots, t_n)$ be a homogeneous polynomial of degree d. The* apolar ideal of f *is defined as follows.*

$$f^\perp := \langle \{h(\mathbf{t}) \in \mathbb{C}[\mathbf{t}] : D_h f \equiv 0\} \rangle$$ ◊

Observation 3.2. *For any polynomial $f(\mathbf{t})$, the variety of its apolar ideal, $\mathbf{V}(f^\perp)$, is a single point $\mathbf{0}$.*

Proof. For each $i \in [n]$, $t_i^{d+1} \in f^\perp$ where $d = \deg(f)$; so the variety is contained in $\{\mathbf{0}\}$. Also, when $f \not\equiv 0$, any polynomial in $f^\perp$ has a zero constant term because a nonzero polynomial cannot be linearly dependent on its derivatives. Hence, $\mathbf{V}(f^\perp) = \{\mathbf{0}\}$. □

Note that the apolar ideal is a polynomial ideal, but is defined using derivative operators. The

apolar ideal of f is related to its partial derivatives in the following way.

Lemma 3.3 (Apolar ideal and partial derivatives)**.** *Let $f(\mathbf{t})$ be a homogeneous polynomial with the set $\{g_1, g_2, \ldots, g_w\}$ being a basis for its space of partial derivatives of all degrees. For the corresponding closed space of derivative operators $\Delta_f := \text{span}_{\mathbb{C}}\left\{D_{g_1}, D_{g_2}, \ldots, D_{g_w}\right\}$, and its annihilating ideal $J := \mathbf{I_0}(\Delta_f)$, we have that $J = f^{\perp}$ and equivalently, $\Delta_f = \Delta(f^{\perp})$.*

Proof. We can assume that $f = g_1$ without loss of any generality.

$f^{\perp} \subseteq J$**.** Let $h \in f^{\perp}$, and say $g = \partial_m f$ is some arbitrary partial derivative of f, so $D_g \in \Delta_f$. Now $\left(D_g h\right)(\mathbf{0}) = \sum_{\mathbf{e}} \text{coeff}_h(\mathbf{t}^{\mathbf{e}}) \cdot \mathbf{e}! \cdot \text{coeff}_g(\mathbf{t}^{\mathbf{e}}) = \left(D_h g\right)(\mathbf{0})$, from Observation 2.13. Further, $D_h g = D_h \partial_m f = D_{(h \cdot m)} f$, and since $m \cdot h \in f^{\perp}$, $D_g h = D_{(h \cdot m)} f = 0$. Since our choice of g and h was arbitrary, this is true for each $g \in \Delta_f$, and each $h \in J$, showing that $f^{\perp} \subseteq J$.

$J \subseteq f^{\perp}$**.** Let $h \in J$ be arbitrary, and consider $D_h f = \sum_{\mathbf{e}} \sum_{\mathbf{e}'} \text{coeff}_h(\mathbf{t}^{\mathbf{e}}) \cdot \text{coeff}_f(\mathbf{t}^{\mathbf{e}'}) \cdot \partial_{\mathbf{e}}(\mathbf{t}^{\mathbf{e}'})$.

$$\begin{aligned}
D_h f &= \sum_{\mathbf{e}} \sum_{\mathbf{e}' \geq \mathbf{e}} \text{coeff}_h(\mathbf{t}^{\mathbf{e}}) \cdot \text{coeff}_f(\mathbf{t}^{\mathbf{e}'}) \cdot \partial_{\mathbf{e}}(\mathbf{t}^{\mathbf{e}'}) \\
&= \sum_{\mathbf{e}} \sum_{\mathbf{e}' \geq \mathbf{e}} \text{coeff}_h(\mathbf{t}^{\mathbf{e}}) \cdot \text{coeff}_f(\mathbf{t}^{\mathbf{e}'}) \cdot \frac{\mathbf{e}'!}{(\mathbf{e}' - \mathbf{e})!} \cdot (\mathbf{t}^{\mathbf{e}' - \mathbf{e}}) \\
&= \sum_{\mathbf{e}_0 := \mathbf{e}' - \mathbf{e}} \left[\sum_{\mathbf{e}} \text{coeff}_h(\mathbf{t}^{\mathbf{e}}) \cdot (\mathbf{e} + \mathbf{e}_0)! \cdot \text{coeff}_f(\mathbf{t}^{\mathbf{e} + \mathbf{e}_0}) \cdot \left(\frac{\mathbf{t}^{\mathbf{e}_0}}{\mathbf{e}_0!} \right) \right]
\end{aligned}$$

Now let $g_0 := \partial_{\mathbf{e}_0}(f)$, and note that $\text{coeff}_{g_0}(\mathbf{t}^{\mathbf{e}}) = \frac{(\mathbf{e}_0 + \mathbf{e})!}{\mathbf{e}!} \cdot \text{coeff}_f(\mathbf{t}^{\mathbf{e}_0 + \mathbf{e}})$. Therefore, we can further simplify our expression for $D_h f$ as follows.

$$\begin{aligned}
D_h f &= \sum_{\mathbf{e}_0} \frac{\mathbf{t}^{\mathbf{e}_0}}{\mathbf{e}_0!} \cdot \left(\sum_{\mathbf{e}} \text{coeff}_h(\mathbf{t}^{\mathbf{e}}) \cdot \mathbf{e}! \cdot \text{coeff}_{g_0}(\mathbf{t}^{\mathbf{e}}) \right) \\
&= \sum_{\mathbf{e}_0} \frac{\mathbf{t}^{\mathbf{e}_0}}{\mathbf{e}_0!} \cdot \left(D_{g_0} h\right)(\mathbf{0}) && \text{(Using Observation 2.13)} \\
&= \sum_{\mathbf{e}_0} 0 \cdot \frac{\mathbf{t}^{\mathbf{e}_0}}{\mathbf{e}_0!} \equiv 0 && (D_{g_0} \in \Delta_f \text{ and } h \in J)
\end{aligned}$$

Thus, $h \in f^{\perp}$. □

3.2 Proof of Theorem 1.6

We are now ready state the general recipe for constructing a commutative ROABP for any homogeneous $f(x_1, \ldots, x_n)$. We start by defining the following polynomial over $\mathbf{x}$, and an auxiliary set of variables $\mathbf{t} = \{t_1, \ldots, t_n\}$, which is the product of the degree-d-truncations of the Taylor series

of $e^{t_i x_i}$s.

$$G(\mathbf{x}, \mathbf{t}) := \prod_{i=1}^{n} \left(1 + t_i x_i + \frac{1}{2!} t_i^2 x_i^2 + \cdots + \frac{1}{(d-1)!} t_i^{d-1} x_i^{d-1} + \frac{1}{d!} t_i^d x_i^d\right) \tag{3.4}$$

Observation 3.5. *Let $D := f(\partial t_1, \partial t_2, \ldots, \partial t_n)$. Then $(D \circ G) = f(\mathbf{x})$.*

Lemma 3.6. *Suppose $f(\mathbf{x})$ is a homogeneous polynomial with dimension of partial derivatives exactly w. Then, there exists a vector $\mathbf{v} \in \mathbb{C}^w$, such that for the multiplication tables $A_1, \ldots, A_n$ of the apolar ideal $f^\perp$, we have that*

$$\sum_{j \in [w]} v_j \cdot G(A_1, \ldots, A_n, x_1, \ldots, x_n)[1, j] = f(\mathbf{x}).$$

Proof. Since $A_1, \ldots, A_n$ are multiplication tables of $f^\perp$, we get that the first row of $G(\mathbf{A}, \mathbf{x})$ is exactly the coefficient vector of $(G(\mathbf{t}, \mathbf{x}) \bmod f^\perp(\mathbf{t}))$ which is an object in $\mathbb{C}[\mathbf{t}][\mathbf{x}]/_{f^\perp(\mathbf{t})} = (\mathbb{C}[\mathbf{t}]/_{f^\perp})[\mathbf{x}]$.

Next, suppose that $\{g_1(\mathbf{t}), \ldots, g_w(\mathbf{t})\}$ is a basis for the partial derivatives of $f(\mathbf{t})$. Then by Lemma 3.3, we know that $\Delta(f^\perp)$ has a basis given by the operators $\{D_{g_1}, \ldots, D_{g_w}\}$. Also, the variety of $f^\perp$ is exactly the singleton set $\{\mathbf{0}\}$. Thus, by Theorem 2.14, the coefficients of $[G(\mathbf{t}, \mathbf{x})] := G(\mathbf{t}, \mathbf{x}) \bmod f^\perp(\mathbf{t})$ are spanned by $D_{g_1}(G)(\mathbf{0}), D_{g_2}(G)(\mathbf{0}), \ldots, D_{g_w}(G)(\mathbf{0})$. More importantly, the set of $D_{g_i}(G)$'s is spanned by the coefficients of $[G(\mathbf{t}, \mathbf{x})]$, and further, $D_{g_1}(G) = D_f(G) = f(\mathbf{x})$.

Thus, the vector $\mathbf{v}$ can be obtained from the matrix M guaranteed by Theorem 2.14, as claimed. □

This proves the main theorem, restated below.

Theorem 1.6. *For any homogeneous polynomial $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$, $\mathrm{commRO}(f) \leq \dim \partial^{<\infty}(f)$.*

Remark 3.7. *Note that Saxena's proof of the duality trick [Sax08, Lemma 1] can be seen as starting with the same "template polynomial" as (3.4), homogenizing it through interpolation, and then just evaluating it on the "points" given by the Waring decomposition for f. Since it is known by the* Apolarity lemma *(see e.g. [IK99]) that the points given by a Waring decomposition of f define a radical ideal J that sits inside $f^\perp$, the action of evaluating on those points can be viewed as going modulo J.*

In that sense, our proof generalizes this method by directly going modulo $f^\perp$. As this uses a less strict property of f, the resulting expression is less simple, and is therefore a commRO instead of a diagRO. ◊

4 The Determinant

In this section, we will use the proof of Theorem 1.6 to construct explicit commutative ROABPs. In particular, we will construct a commutative ROABP for the determinant (Det_n) of width $2^{\Theta(n)}$.

The choice of this example is deliberate, as the determinant is the only candidate where there is an asymptotic gap between Waring rank upper bounds and partial derivative dimension.

The determinant of n-dimensional symbolic matrix has partial derivative dimension exactly $\binom{2n}{n} = 2^{\Theta(n)}$. But, the best upper bound for the Waring rank of the determinant is $2^{O(n \log n)}$. In fact, there are reasons to believe that the Waring rank of the determinant is $2^{\omega(n)}$. This is due to the fact that the set-multilinear depth-3 complexity or *Tensor rank* of Det_n, and (to the best of our knowledge) even the best constant-depth multilinear formula that we know of for the determinant, is $2^{O(n \log n)}$. See [KM18, Raz10] for details on tensor rank and syntactic multilinear formulas of the determinant.

For Det_n, Theorem 1.6 directly gives a commutative ROABP of width $2^{\Theta(n)}$. We show the explicit calculations behind this commutative ROABP below. Let's recall what our overall step-by-step process will be for any polynomial $f \in \mathbb{C}[\mathbf{x}]$:

1. Compute the closed derivative space $\Delta = \partial^{<\infty} f$, the apolar ideal corresponding to it $I_{\mathbf{0}}(\Delta) = f^{\perp}$ and the normal set of $\mathrm{N}(f^{\perp})$. Let, $m := \left|\mathrm{N}(f^{\perp})\right| = |\Delta|$.
2. Compute the multiplication tables (M_i) corresponding to each of the variables.
3. The final commutative ROABP of $f \equiv \mathbf{a}^{\intercal} \cdot \prod_{i \in [n]} (1 + x_i M_i) \cdot \mathbf{b}$ for $\mathbf{a}, \mathbf{b} \in \mathbb{C}^m$.

4.1 Derivative Space, Apolar Ideal, and its Normal Set

In this subsection, we will state and discuss some facts about the derivative space, apolar ideal, and the normal set of the apolar ideal of the determinant. We will use X to denote the $n \times n$ symbolic matrix, that is, $X = (x_{i,j})_{i,j \in [n]}$. Similarly, let $U = (t_{i,j})_{i,j \in [n]}$ be a symbolic matrix in t-variables. Let S, T be arbitrary subsets of $[n]$. We will denote the minor (of X) picked by selecting rows from S and columns from T by $X_{S,T}$.

We will start with the well-known fact that the derivative space of determinant is just the determinant of its minors. Formally, the following set is a basis of $\partial^{<\infty} \mathsf{Det}_n(X)$,

$$\left\{ \mathsf{Det}(X_{S,T}) : \text{ for } S, T \subseteq [n] \text{ such that } |S| = |T| \right\}.$$

The apolar ideal of the determinant is generated by permanents of 2×2 minors and certain unacceptable degree two monomials, as stated formally below.

Theorem 4.1 (e.g. [Sha15, Theorem 2.12]). $\mathsf{Det}_n^{\perp}(X) = \langle \mathcal{P}_X, \mathcal{U}_X \rangle$, *where $\mathcal{P}_X$ is the collection of permanents of all 2×2 minors of X, and $\mathcal{U}_X$ denotes all quadratic unacceptable monomials, that is, monomials that don't divide any monomial in the support of* $\mathsf{Det}_n(X)$.

Now, for the normal set computation, we will focus on the degree-wise lexicographical ordering of monomials ("deg-lex"); the ordering on variables is in the "row-major" form:

$$x_{1,1} \succ x_{1,2} \succ \ldots \succ x_{1,n} \succ x_{2,1} \succ \ldots \succ x_{n,n}.$$

The trailing monomial of $\mathsf{Det}(X_{S,T})$ in this ordering is just the product of the anti-diagonal entries of $X_{S,T}$. To see this, note that the only variable you can pick from the first row is the last element. Now that we have picked something from the last column and the first row, we can strip them off as none of the variables can contribute anymore. Now focus on the resulting minor (after stripping) and proceed by induction. Let's denote this trailing monomial by $\tau_{S,T} := \text{anti-diag}(X_{S,T})$.

We now claim that the normal set of J is just a collection of these anti-diagonal monomials corresponding to all minors, as follows.

$$\mathrm{N}(J) = \{\text{anti-diag}(X_{S,T}) : \text{ for } S, T \subseteq [n] \text{ such that } |S| = |T|\}$$

To see this, observe that any non-anti-diagonal monomial (for any minor) will be a multiple of the leading term of a 2×2 minor's permanent and thus will be in $\mathrm{LM}(\mathsf{Det}^{\perp})$. At the same time, the anti-diagonal monomial will never be a multiple of such terms, so it is never in $\mathrm{LM}(\mathsf{Det}^{\perp})$. Note that here, $|\Delta| = |\mathrm{N}(J)| = \binom{2n}{n}$.

4.2 Multiplication tables for the apolar ideal

Let $A_{i,j}$ be the matrix corresponding to $t_{i,j}$ with dimension $|\mathrm{N}(J)| \times |\mathrm{N}(J)|$. For any row of $A_{i,j}$, indexed by (S, T) such that $|S| = |T|$, we have that

$$row(S,T)(A_{i,j}) = \begin{cases} 0 & \text{if } i \in S \text{ or } j \in T \\ \mathrm{sgn}(\tau_{S',T'}) \cdot \mathrm{sgn}(\tau_{S,T} \cdot x_{i,j}) \cdot \tau_{(S\cup\{i\},T\cup\{j\})} & \text{if } i \notin S, j \notin T \end{cases}.$$

Here, sgn of any monomial denotes the sgn of its corresponding permutation (obtained by viewing $S, T \equiv \{1, \ldots, |S|\}$). To see this, note that by definition $row(S,T)(A_{i,j})$ is just the coefficient vector of $(t_{i,j} \cdot \tau_{S,T} \bmod J)$.

Thus, as discussed (in proof of Theorem 1.6) we get

$$\mathsf{Det}_n(X) = \mathbf{a}^{\mathsf{T}} \cdot \prod_{i,j\in[n]} (I + A_{i,j}x_{i,j}) \cdot \mathbf{b} \qquad \text{for } \mathbf{a}, \mathbf{b} \in \mathbb{C}^{\binom{2n}{n}}.$$

Below, we give an explicit description of the commutative ROABP for Det_2. Here, the normal set is $\mathrm{N}(\mathsf{Det}_2^{\perp}) = \{1, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, x_{1,2}x_{2,1}\}$. Running our analysis to compute the multiplication tables followed by then replacing it in the template polynomial yields that the $\mathsf{Det}_2(X)$ is the

$(1,n)$-th entry of the product of the following four matrices (in any order).

$$M_{1,1} = \begin{pmatrix} 1 & x_{1,1} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -x_{1,1} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \; M_{1,2} = \begin{pmatrix} 1 & 0 & x_{1,2} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & x_{1,2} \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$M_{2,1} = \begin{pmatrix} 1 & 0 & 0 & x_{2,1} & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & x_{2,1} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \; M_{2,2} = \begin{pmatrix} 1 & 0 & 0 & 0 & x_{2,2} & 0 \\ 0 & 1 & 0 & 0 & 0 & -x_{2,2} \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

4.3 Commutative Set-multilinear ABP

The commutative matrices $A_{i,j}$ generated in the previous subsections using multiplication tables from $\mathsf{Det}_n^{\perp}$ can in fact be used to design a *commutative* set-multilinear ABP for Det as well.

The benefit of studying this model stems from the fact that if we could somehow "diagonalize" these commutative matrices, then that would indeed give a set-multilinear depth-3 representation of the determinant of size $2^{O(n)}$. That, in turn, would yield that the Waring rank of the determinant is also $2^{O(n)}$. By "diagonalizable," we simply mean if the above matrices can be replaced by diagonal matrices with at most a polynomial blow-up in the dimension.

In fact, the commutative matrices constructed for Det_n are provably not diagonalizable by invertible transformations. But for Perm_n, the matrices that we will get by running our entire analysis are indeed "diagonalizable"! In the sense that we can replace them by diagonal matrices of similar dimension to compute Perm_n.

Let $\sqcup_{j\in[d]}\mathbf{x}_j$ be a partition of the set $\mathbf{x}$ of input variables. Then a polynomial is set-multilinear under partition $\sqcup_{j\in[d]}\mathbf{x}_j$ if each monomial of the polynomial picks up *exactly* one variable from each part in the partition. Note that, Det is set-multilinear w.r.t. the variable partition being the row variables (or column variables).

Definition 4.2 (Set-multilinear ABP (smABP))**.** *Let $n,d,w \in \mathbb{N}$, and let $f(\mathbf{x})$ be an n-variate set-multilinear polynomial under the partition $\mathbf{x}_1 \sqcup \mathbf{x}_2 \sqcup \cdots \sqcup \mathbf{x}_d$. We say that f has a width w set-multilinear ABP[3], if there exists a permutation $\sigma \in s_d$ for which there exist matrices $\{A_{j,k}\}$ in $\mathbb{C}^{w\times w}$ for all $j \in [d]$*

[3]Strictly speaking this defines *ordered* set-multilinear algebraic branching programs, but we drop this detail for brevity.

and $1 \leq k \leq |\mathbf{x}_j|$*, and vectors* $\mathbf{u}, \mathbf{v} \in \mathbb{C}^w$*, such that the following holds.*

$$f(\mathbf{x}) = \mathbf{u}^\intercal \cdot M_{\sigma(1)}(\mathbf{x}_{\sigma(1)}) \cdot M_{\sigma(2)}(\mathbf{x}_{\sigma(2)}) \cdots M_{\sigma(d)}(\mathbf{x}_{\sigma(d)}) \cdot \mathbf{v},$$
$$\text{where for all } j \in [d],$$
$$M_j(\mathbf{x}_j) = A_{j,1}x_{j,1} + A_{j,2}x_{j,2} + \cdots + A_{j,|\mathbf{x}_j|}x_{j,|\mathbf{x}_j|}.$$

We call the matrices $\{A_{j,k}\}$ *the* coefficient matrices *of the smABP.* ◊

Definition 4.3 (Commutative smABP)**.** *An smABP is said to be a* commutative smABP *if all its coefficient matrices pairwise commute with each other.* ◊

Now, we will show that by simply changing the template polynomial (from (3.4)) appropriately, we can get a commutative set-multilinear ABP representation for Det_n.

$$\text{Define, } G(\mathbf{x}, \mathbf{t}) := \prod_{i=1}^{n} \left(\sum_{j \in [n]} t_{i,j} x_{i,j} \right). \tag{4.4}$$

Again, just like Observation 3.5, we have that $\mathsf{Det}_n(\partial_{t_{1,1}}, \partial_{t_{1,2}}, \ldots, \partial_{t_{n,n}}) \circ G = \mathsf{Det}_n(X)$. And this gives that,

$$\mathsf{Det}_n(X) = \mathbf{a}^\intercal \cdot \prod_{i=1}^{n} \left(\sum_{j \in [n]} A_{i,j} x_{i,j} \right) \cdot \mathbf{b} \qquad \text{for some } \mathbf{a}, \mathbf{b} \in \mathbb{C}^{\binom{2n}{n}}.$$

We remark that the above analysis works for any set-multilinear polynomial, along the same lines as the proof of Theorem 1.6. This directly gives us the following theorem.

Theorem 1.8. *For any set-multilinear polynomial* $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$*, the commutative-set-multilinear-ABP-width*$(f) \leq \dim \partial^{<\infty}(f)$.

5 Discussion

In summary, we utilize the knowledge of commuting matrices outlined in [RT22] to provide a generic recipe for explicit constructions of commutative branching programs. For the specific setting of ROABPs, this improves upon the earlier known connection (Observation 2.7) and takes us a step closer towards answering Question 1.2. An immediate direction for further study is the following.

Can we show any bounds on the commRO width of a polynomial in terms of its diagRO width? In addition to shedding further light on Question 1.2, such a result should also provide us with a new hardness measure for structured ROABPs and possibly even depth 3 powering circuits, particularly if the bound is a super-linear lower bound on diagRO width. As alluded to

in the introduction, perhaps a new hardness measure against diagRO or depth 3 powering circuits is what is required to fully derandomize blackbox PIT for the model. A concrete way in which this is true is that a polynomial time blackbox PIT for width-w, degree-d, $O(\log dw)$-variate diagRO would give a polynomial time blackbox PIT for depth 3 powering circuits [BS21, Lemma 2.12]. This gives the lower bound question a much larger and more interesting context.

Acknowledgements

VB thanks Rafael Oliveira and Abhiroop Sanyal for numerous insightful discussions. AT thanks Prerona Chatterjee, C Ramya, and Ramprasad Saptharishi for several fruitful discussions about ROABPs over the recent years. AT is also deeply grateful to Ramprasad Saptharishi, Susmita Biswas and Lulu, for hosting him during a part of this work.

References

[BS21] Pranav Bisht and Nitin Saxena. Blackbox identity testing for sum of special ROABPs and its border class. *Computational Complexity*, 30(1):8, 2021. [Cited on page 17.]

[CCG12] Enrico Carlini, Maria Virginia Catalisano, and Anthony V. Geramita. The solution to the Waring problem for monomials and the sum of coprime monomials. *Journal of Algebra*, 370:5–14, 2012. [Cited on page 2.]

[CLO07] David A. Cox, John B. Little, and Donal O'Shea. *Ideals, Varieties and Algorithms*. Undergraduate texts in mathematics. Springer, 2007. [Cited on page 8.]

[Fis94] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994. [Cited on page 2.]

[FS13] Michael A. Forbes and Amir Shpilka. Quasipolynomial-Time Identity Testing of Non-commutative and Read-Once Oblivious Algebraic Branching Programs. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013)*, pages 243–252, 2013. Full version at arXiv:1209.2408. [Cited on page 3.]

[FSS14] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC 2014)*, pages 867–875, 2014. [Cited on pages 2 and 5.]

[GKS17] Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Identity Testing for Constant-Width, and Commutative, Read-Once Oblivious ABPs. *Theory of Computing*, 13(1):1–21, 2017.

Preliminary version in the *31st Annual Computational Complexity Conference (CCC 2016)*. arXiv:1601.08031. [Cited on pages 2 and 5.]

[IK99] Anthony Iarrobino and Vassil Kanev. *Power Sums, Gorenstein Algebras, and Determinantal Loci*. Springer-Verlag Berlin Heidelberg, 1999. [Cited on pages 2, 8, and 12.]

[KM18] Siddharth Krishna and Visu Makam. On the tensor rank of 3s×3 permanent and determinant. *CoRR*, abs/1801.00496, 2018. Pre-print available at arXiv:1801.00496. [Cited on page 13.]

[KS19] Mrinal Kumar and Ramprasad Saptharishi. Hardness-Randomness Tradeoffs for Algebraic Computation. *Bulletin of EATCS*, 1(129), 2019. [Cited on page 2.]

[MMM93] M.G. Marinari, H.M. Möller, and T. Mora. Gröbner Bases Of Ideals Defined By Functionals With An Application To Ideals Of Projective Points. *Applicable Algebra in Engineering, Communication and Computing*, 4(2):103–145, 1993. [Cited on page 8.]

[MS95] H. Michael Möller and Hans J. Stetter. Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numerische Mathematik*, 70, 1995. [Cited on page 8.]

[Nis91] Noam Nisan. Lower bounds for non-commutative computation. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC 1991)*, pages 410–418, 1991. Available on citeseer:10.1.1.17.5067. [Cited on pages 3 and 7.]

[Nis92] Noam Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992. [Cited on page 3.]

[NW97] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1997. Available on citeseer:10.1.1.90.2644. [Cited on page 2.]

[Pra19] Kevin Pratt. Waring Rank, Parameterized and Exact Algorithms. In *Proceedings of the 60th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2019)*, pages 806–823. IEEE Computer Society, 2019. [Cited on page 2.]

[Raz10] Ran Raz. Tensor-rank and lower bounds for arithmetic formulas. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (STOC 2010)*, pages 659–666, 2010. Pre-print available at eccc:TR10-002. [Cited on page 13.]

[RS11] Kristian Ranestad and Frank-Olaf Schreyer. On the rank of a symmetric form. *Journal of Algebra*, 346(1):340–342, 2011. [Cited on page 2.]

[RT22] C. Ramya and Anamay Tengse. On Finer Separations Between Subclasses of Read-Once Oblivious ABPs. In *39th International Symposium on Theoretical Aspects of Computer Science, STACS 2022, March 15-18, 2022, Marseille, France (Virtual Conference)*, volume 219 of *LIPIcs*, pages 53:1–53:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. [Cited on pages 4, 8, and 16.]

[Sap15] Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. Github survey, 2015. [Cited on page 2.]

[Sax08] Nitin Saxena. Diagonal Circuit Identity Testing and Lower Bounds. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP 2008)*, pages 60–71, 2008. Pre-print available at eccc:TR07-124. [Cited on pages 2, 4, 6, and 12.]

[Sha15] Sepideh Masoumeh Shafiei. APOLARITY FOR DETERMINANTS AND PERMANENTS OF GENERIC MATRICES. *Journal of Commutative Algebra*, 7(1):89–123, 2015. [Cited on page 13.]

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic Circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5:207–388, March 2010. [Cited on page 2.]