On Closure Properties of Read-Once Oblivious Algebraic Branching Programs

Robert Andrews
Cheriton School of Computer Science, University of Waterloo, Canada

Jules Armand
Université Savoie Mont Blanc, CNRS, LAMA, France

Prateek Dwivedi
IT University of Copenhagen, Denmark

Magnus Rahbek Dalgaard Hansen
IT University of Copenhagen, Denmark

Nutan Limaye
IT University of Copenhagen, Denmark

Srikanth Srinivasan
Department of Computer Science, University of Copenhagen, Denmark

Sébastien Tavenas
Université Savoie Mont Blanc, CNRS, LAMA, France

Abstract

We investigate the closure properties of read-once oblivious Algebraic Branching Programs (roABPs) under various natural algebraic operations and prove the following.

- **Non-closure under factoring:** There is a sequence of explicit polynomials $(f_n(x_1, \ldots, x_n))_n$ that have poly(n)-sized roABPs such that some irreducible factor of f_n requires roABPs of superpolynomial size in *any* order.
- **Non-closure under powering:** There is a sequence of polynomials $(f_n(x_1, \ldots, x_n))_n$ with poly(n)-sized roABPs such that any super-constant power of f_n does not have roABPs of polynomial size in any order (and f_n^n requires exponential size in any order).
- **Non-closure under symmetric operations:** There are symmetric polynomials $(f_n(e_1, \ldots, e_n))_n$ that have roABPs of polynomial size such that $f_n(x_1, \ldots, x_n)$ do not have roABPs of subexponential size. (Here, $e_1, \ldots, e_n$ denote the elementary symmetric polynomials in n variables.)

These results should be viewed in light of known results on models such as algebraic circuits, (general) algebraic branching programs, formulas and constant-depth circuits, all of which are known to be closed under these operations.

To prove non-closure under factoring, we construct hard polynomials based on expander graphs using gadgets that lift their hardness from sparse polynomials to roABPs. For symmetric compositions, we show that the *circulant* polynomial requires roABPs of exponential size in every variable order.

2012 ACM Subject Classification Theory of computation → Complexity classes; Theory of computation → Problems, reductions and completeness; Theory of computation → Circuit complexity; Theory of computation → Algebraic complexity theory

Keywords and phrases Factoring, Closure Properties, Sparsity Bounds, Symmetric Polynomials, roABP, Expander Graphs

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.9

Related Version *Full Version*: https://arxiv.org/abs/2509.10725

Funding PD, MH, and NL thank Independent Research Fund Denmark (grant agreement No. 10.46540/3103-00116B) and the support of Basic Algorithms Research Copenhagen (BARC), funded by VILLUM Foundation Grant 54451.
Srikanth Srinivasan: Supported by European Research Council (ERC) under grant agreement no. 101125652 (ALBA).
Sébastien Tavenas: Supported by ANR project VONBICA (ANR-22-CE48-0007).

Acknowledgements This research in this paper was carried out during a visit of some of the authors to Université Savoie Mont Blanc. The authors thank the Laboratoire de Mathématiques (LAMA) at Université Savoie Mont Blanc, which is supported by the AAP GAFA project, for their hospitality and the conducive environment for research. NL would like to thank Université Savoie Mont Blanc for hosting her as a visiting researcher.

1 Introduction

Given any computational model, it is natural to study the closure properties of the model with respect to simple operations. In Boolean complexity, these simple operations typically take the form of Boolean operations such as union, intersection, complement etc. In the setting of *algebraic complexity*, the object of computation is a multivariate polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$. Here, it is intuitive to consider closure properties under algebraic operations.

In this paper, we study the closure properties of a very well studied model of algebraic computation, namely *read-once oblivious Algebraic Branching programs* (roABPs, see definition 6). The interest in this model stems from the fact that it is both expressive enough to capture many natural algorithmic paradigms while at the same time possible to analyze using standard "complexity measures" [44].

In particular, roABPs can efficiently compute several polynomials of interest, including elementary symmetric polynomials and iterated matrix multiplication[1], the latter being provably hard to compute for constant-depth circuits [40, 6, 43]. In addition, roABPs subsume well-studied models such as sparse polynomials, set-multilinear and diagonal depth-3 circuits [38], as well as polynomials with low partial derivative dimension [9]. On the other hand, this is also one of the few models where we have a perfect characterization of the complexity of any given polynomial (in the form of the rank of an associated matrix) and where we also have a perfect understanding of border complexity [25]. As a consequence, this model has played a central role in research on lower bounds, polynomial identity testing algorithms and "debordering" results [21, 22, 14].

We study the closure properties of this model under basic algebraic operations such as factorization, powering, and inversion under composition with an important algebraic map (the elementary symmetric polynomial map). Apart from being natural questions about any computational model, such investigations have played a vital role in understanding hardness-randomness tradeoffs [35, 23, 17, 10] and the complexity of basic algebraic problems such as the Resultant and GCD [5, 11] in other algebraic models.

1.1 Main Results

In contrast with what is known for other models, our results are mostly negative. Specifically, we show the following.

roABP factor non-closure

Our first main result shows that there are explicit polynomial sequences that have small roABPs but with an irreducible factor that has roABP complexity super-polynomial in n. Specifically, we prove roABP complexity lower bound for a *root*, which is an irreducible factor of the form $x_n - f(x_1, \ldots, x_{n-1})$, even when the roABP is allowed to scan the variables in any order. The formal statement is as follows.

[1] This does not imply any completeness result as roABP is not closed under projection.

▶ **Theorem 1** (roABP factor non-closure). *The following holds over any field. Let $n \in \mathbb{N}$ be a parameter and $d \geq n$. There exists an n-variate polynomial f of degree d computable by an* roABP *of width $w := 2^{O(n)}$, such that one of its (irreducible) factors g requires an* roABP *of width $w^{\Omega(\log d)}$ in every variable order.*

Note that, an roABP computing an n-variate polynomial by definition has only n layers. Hence, the size and the width of an roABP are polynomially related. Secondly, the size and width parameters in the theorem above are not polynomial in the number of variables, but they can be easily made polynomial by padding with some additional "dummy" variables. In particular, one should think of n above as logarithmic in the number of "actual" variables and d as a growing parameter, up to a polynomial in the number of variables.

This is in contrast to other algebraic models such as algebraic circuits [36, 37], branching programs [52], formulas and constant-depth circuits [10], all of which satisfy the property that factors of a polynomial f have complexity comparable to that of f. An exception to this rule is the family of sparse polynomials [57], and our construction is based on "lifting" this example to the setting of roABP.

roABP complexity of Symmetric Composition

We study an analogue of the result of Bläser and Jindal [16] for roABP. More specifically, a classical result in the theory of symmetric functions says that any symmetric polynomial[2] $f_{\text{sym}}(x_1, \ldots, x_n)$ can be written as a unique polynomial combination f of the elementary symmetric polynomials $\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n$, where ESym_n^d is the n-variate elementary symmetric polynomial of degree d. Looking for a computational analogue of this theorem, Lipton and Regan [41], asked: what is the complexity of f_{sym} vis-à-vis that of f?

Bläser and Jindal [16] showed that the complexity of f and f_{sym} are polynomially related in the algebraic circuit model. Recently, the work of Bhattacharjee, Kumar, Rai, Ramanathan, Saptharishi and Saraf [11] extended this result to formulas and constant-depth circuits to show that fundamental computations such as GCD, resultants and discriminants have efficient constant-depth circuits in any characteristic. This generalizes a similar result of Andrews and Wigderson [5] in characteristic 0.

We show in this paper that the roABP complexity of a polynomial f and its symmetric counterpart f_{sym} can differ significantly. Taking $f_{\text{sym}} = \sum_{d=0}^{n} \mathsf{ESym}_n^d(x_1^k, \ldots, x_n^k)$, we can show that f_{sym} is easy but f is exponentially hard.

▶ **Theorem 2.** *The following holds over fields of characteristic zero. Let $n \in \mathbb{N}$ be a parameter. There exists an n-variate polynomial f such that the symmetric polynomial $f_{\mathsf{sym}} := f(\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n)$ is computable by an* roABP *of constant width in every variable order, but any* roABP *computing f in any variable order must have width $2^{\Omega(n)}$.*

In the other direction, our next result shows that even if a polynomial f is easy to compute by roABP, its symmetric counterpart f_{sym} can still be hard for roABP – once again in sharp contrast to the known results for circuits, formulas, and constant-depth circuits. Specifically, the lower bound for a power of the elementary symmetric polynomial yields an example where f is easy but f_{sym} is exponentially hard.[3]

[2] A polynomial is symmetric if it is invariant under any permutation of its variables.
[3] This is an especially strong contrast to the other models where it is trivial to show that if f is easy, then so is f_{sym}.

▶ **Theorem 3.** *The following holds over fields of characteristic zero. Let $n \in \mathbb{N}$ be a parameter. There exists an n-variate polynomial f computable by an* roABP *of constant width such that its respective symmetric polynomial $f_{\mathsf{sym}} = f(\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n)$ requires an* roABP *of width $2^{\Omega(n)}$ in every variable order.*

roABP non-closure corollaries

We also investigate the power of roABPs in relation to powering an efficiently computable polynomial. It is well-known that constant powers of such polynomials also have small roABPs (see e.g. [4, Lemma 2.5]). However, we show that for larger powers, a superpolynomial blow-up in width is unavoidable.

▶ **Corollary 4** (roABP powering non-closure)**.** *The following holds over fields of characteristic zero. There exists an n-variate polynomial f computable by an* roABP *of width $O(n)$ such that for any d, any* roABP *computing f^d requires width at least $\binom{d+n/2}{n/2}$ in every variable order.*

▶ Remark. We give two example polynomials to prove the hardness of powering for roABP. The first is the elementary symmetric polynomial (this lower bound will also prove Theorem 3) and the second is a quadratic polynomial inspired by the proof of Theorem 1.

Another corollary of Theorem 3 is that computing the resultant and the discriminant is hard for roABP.

▶ **Corollary 5** (roABP discriminant non-closure)**.** *The following holds over fields of characteristic zero. For all n, there exists an n-variate polynomial $f(\boldsymbol{x}, y)$ computable by an* roABP *of width $O(n)$ such that any* roABP *computing the discriminant $\mathrm{Disc}_y(f)$ requires width at least $2^{\Omega(n)}$ in every variable order.*

▶ Remark. As an immediate consequence of the corollary above, we get that roABP is not closed under taking resultants.

Related Work

There have been many lines of investigation into roABPs from the point of view of lower bounds [44, 38, 4], PIT algorithms [46, 12, 2, 31, 27, 26, 4, 2, 32, 8, 49], border complexity [21, 22, 14, 13], algebraic meta-complexity [7, 9] and so on.

Our work is closely related to that of Kayal, Nair, and Saha [38], who proved separations between the power of roABPs and multilinear depth-3 circuits. Non-closure results of a similar flavour to ours have also been proved by Saha and Thankey [49, Appendix E.1]. They construct explicit families of polynomials that require roABP of exponential size, but arise from applying invertible linear transformations to sparse polynomials f that have linear roABP complexity. Some of their ideas, such as those involving the use of expander graphs, also appear in our work.

Similar separations between roABPs and other models (such as read-twice ABPs) were also addressed in the work of Anderson, Forbes, Saptharishi, Shpilka and Volk [4]. We re-prove a result from this work separating depth-2 algebraic circuits (products of linear polynomials) from roABPs in order to understand the roABP complexity of some explicit symmetric functions. Our lower bound is proved for the specific case of the determinant of a *Circulant matrix*, which is a naturally occurring mathematical object and hence may be independently interesting.

1.2 Proof Techniques

The main technique for understanding the roABP complexity of a polynomial is a characterization due to Nisan [44], who showed that the roABP complexity of a polynomial f (or more precisely the *width* of the smallest roABP computing f) in a given order is captured by the ranks of certain matrices related to f, also known as the *evaluation dimension of* f (formally defined in Definition 11). We also heavily rely on this notion in our work.

Factor non-closure

To construct our examples of polynomials that are efficiently computable by roABPs but hard to factor, we start with an analogous construction for a weaker setting, that of *sparse polynomials.* The following is a well-known construction due to [57, Example 5.1].

$$f(x_1,\ldots,x_n) \;=\; \prod_{i=1}^{n}(x_i^d-1) = \prod_{i=1}^{n}(x_i-1)\cdot \underbrace{\prod_{i=1}^{n}(1+x_i+\cdots+x_i^{d-1})}_{g(x_1,\ldots,x_n)}.$$

Note that the polynomial f has 2^n monomials while its factor g has d^n monomials. This thus yields an example of a polynomial whose factors have many more monomials than the polynomial itself.

We would like to extend this to the setting of roABP. Unfortunately, the example above does not work as is, as the polynomial g is a product of univariate polynomials and hence has a small roABP. Our idea is to "lift" this sparsity lower bound to an roABP lower bound.

The basic idea of lifting, which has proven powerful in the area of Boolean complexity [20] and also Algebraic Proof complexity [28], is to start with a function f that is hard for a simpler computational model (in this case sparse polynomials) and convert it to a function g that is difficult for a much more powerful model by replacing the variables of f by functions (typically called "gadgets") in a small number of new variables to obtain g. A version of this idea can be used to lift degree lower bounds on the multilinear representation for some functions to lower bounds for algebraic proof systems based on roABPs [28].

Inspired by [28], we replace the variables of the polynomial f by quadratic multilinear monomials in a new set of variables $y_1,\ldots,y_m$ where $m=\Omega(n)$. We can associate this replacement with an undirected graph G on m vertices and n edges. We show that, *as long as G is a sufficiently good constant-degree expander*, the corresponding "lifted" polynomials f_G and g_G are easy and hard respectively for roABPs with similar parameters to the case of sparse polynomials.

The crucial property of expander graphs that allows us to prove a lower bound on g_G is the Expander Mixing lemma. It can be used to show that given any balanced partition of the vertices of G, there is a large induced matching between the two sets in the parts. This allows us to find a large identity matrix as a submatrix of the evaluation matrix of g_G, leading to strong bounds on its evaluation dimension.

The complexity of powering

We give two examples to demonstrate that roABPs are not closed under powering.

The first is a quadratic polynomial g whose monomials again correspond to a constant-degree expander graph as in the previous result. The Expander Mixing lemma can again be used to argue that large powers of g have large evaluation dimension.

The second example is just an elementary symmetric polynomial. Symmetric polynomials are particularly natural to study in the setting of roABPs, since the polynomials have the same complexity under any variable ordering. In particular, studying the complexity of a symmetric polynomial turns into understanding the ranks of combinatorially defined matrices. In the setting of a power of the elementary symmetric polynomial, we are able to show that this matrix has large rank.

No Bläser-Jindal type results for roABPs

Already the example of the elementary symmetric polynomial above shows that for the simple polynomial $f(y_1, \ldots, y_n) = y_i^d$, the symmetric polynomial $f(\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n)$ is hard to compute for roABPs.

To prove a converse result, we use the symmetric polynomial $f_{\text{sym}} := \sum_{d=0}^{n} \mathsf{ESym}_n^d(x_1^k, \ldots, x_n^k)$. In this case, we need to understand the complexity of the polynomial f (such as $f(\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n) = f_{\text{sym}}$). It turns out that the polynomial f in this case is completely understood [1] and is closely related to the determinant of the Circulant matrix. To prove the lower bound, we prove an roABP lower bound on this determinant, which we believe is independently interesting.

Outline

We begin with preliminaries in Section 2. Section 3 contains the proof of Theorem 1. In Section 4, we prove Theorem 2 and Theorem 3. Finally, in Section 5, we prove all the corollaries.

2 Notations and Preliminaries

Throughout the paper, we will use a growing parameter $n > 0$ to denote the number of variables in the polynomial. Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ be the set of indeterminates. A monomial of the form $x_1^{e_1} \cdots x_n^{e_n}$ is denoted as $\boldsymbol{x}^{\boldsymbol{e}}$, where $\boldsymbol{e} = (e_1, \ldots, e_n) \in \mathbb{N}^n$. The degree of a monomial $\boldsymbol{x}^{\boldsymbol{e}}$ is defined as $\deg(\boldsymbol{x}^{\boldsymbol{e}}) := e_1 + \cdots + e_n$. The degree of a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is defined as the maximum degree of its constituent monomials. We use $\text{coef}_{\boldsymbol{x}^{\boldsymbol{e}}}(f)$ to denote the coefficient of the monomial $\boldsymbol{x}^{\boldsymbol{e}}$ in f.

2.1 Read-Once Oblivious Algebraic Branching Programs (roABP)

Our model of interest arises as a natural restriction of Algebraic Branching Programs (ABPs), which we describe next. An *Algebraic Branching Program* (ABP) is a layered and directed graph with a source vertex s and a sink vertex t. All edges connect vertices from layer i to $i+1$. Further, the edges are labeled with affine polynomials over the underlying field $\mathbb{F}$. For every path γ from s to t, $\text{wt}(\gamma)$ is the product of labels on the edges of the path γ. The polynomial computed by the ABP is defined as

$$f := \sum_{\text{path } \gamma : s \rightsquigarrow t} \text{wt}(\gamma).$$

The *depth* of an ABP is defined as the number of layers in the graph, and the *width* is the maximum number of nodes in a layer across the graph. The number of vertices used in the graph is the *size* of the ABP. The roABP model is a restriction of ABPs, which we define below.

▶ **Definition 6** (roABP). *Let $n \in \mathbb{N}$ be arbitrary and fix a permutation $\pi : [n] \to [n]$. An* roABP *in the order π computing an n-variate polynomial $f(\boldsymbol{x})$ is an* ABP *where in the i-th layer the edge labels are univariate polynomials over $x_{\pi(i)}$.*

The size of an roABP *is defined as the number of vertices it contains, and the width is defined as the maximum number of vertices in any layer.*

In a foundational work, Nisan [44] characterized the complexity of an ABP in the non-commutative setting with the rank of certain matrices. Remarkably, the characterization extends to roABP as well. We define the relevant matrix to formally state this characterization.

▶ **Definition 7** (Nisan Matrix). *Consider an n-variate polynomial $f(\boldsymbol{x})$ and a variable partition $Y \sqcup Z = \{x_1, \ldots, x_n\}$. The* Nisan matrix *of f with respect to Y, Z, denoted as $M_{Y,Z}(f)$, is the matrix whose rows are indexed by monomials m_Y over Y and whose columns are indexed by monomials m_Z over Z. Its entry at (m_Y, m_Z) is defined as*

$$M_{Y,Z}(f)\Big[m_Y, m_Z\Big] \;=\; \mathrm{coef}_{m_Y \cdot m_Z}(f).$$

Historically, the Nisan Matrix has also been referred to as the coefficient matrix or partial derivative matrix. The width of an roABP computing a polynomial f can be exactly characterized by the rank of the Nisan matrix of f [29, Lemma 4.5.8].

▶ **Theorem 8** (roABP characterization). *Let $f(\boldsymbol{x})$ be an n-variate polynomial, and fix a permutation π on variables. For each $i \in [n]$, consider the partition $Y_i \coloneqq \{\pi(x_1), \ldots, \pi(x_i)\}$ and $Z_i = \{\pi(x_{i+1}), \ldots, \pi(x_n)\}$, and let $M_{Y_i,Z_i}(f)$ denote the corresponding Nisan matrix. The width of the smallest* roABP *computing f in the order π is exactly $\max_{i\in[n]} \mathrm{rank}(M_{Y_i,Z_i}(f))$. Moreover, the size of the smallest* roABP *is exactly $\sum_{i\in[n]} \mathrm{rank}(M_{Y_i,Z_i}(f))$.*

We next prove a lemma to demonstrate the usefulness of the roABP characterization, which will be used in our later proofs.

▶ **Observation 9.** *Consider an n-variate polynomial as follows*

$$f \;\coloneqq\; \prod_{i\in[n]} \left(1 + x_i + x_i^2 + \ldots + x_i^{d-1}\right).$$

Let $Y = \{y_1, \ldots, y_n\}$ and $Z = \{z_1, \ldots, z_n\}$ be disjoint set of variables. Define a $2n$-variate polynomial $\widetilde{f} \coloneqq f(y_1 z_1, \ldots, y_n z_n)$. The rank of the Nisan matrix $M_{Y,Z}(\widetilde{f})$ is d^n.

▶ Remark 10. Note that f itself can be computed by a constant width roABP in any order.

Proof. Observe that for every monomial m_Y over Y such that each variable has degree at most $d-1$ in m_Y, there is a unique monomial m_Z of the same form over Z such that $\mathrm{coef}_{m_Y \cdot m_Z}(\widetilde{f})$ is not zero, and reciprocally, for any monomial m_Z over Z there is a unique monomial m_Y. Consequently, the Nisan matrix $M_{Y,Z}(\widetilde{f})$ is a permutation matrix, and hence has rank d^n. ◀

Evaluation Dimension

An alternative perspective on the Nisan matrix was introduced by Saptharishi [27, Section 6]. As we will see in our proofs, this viewpoint often makes it easier to reason about roABP complexity.

▶ **Definition 11** (Evaluation Dimension). *Let $f(\boldsymbol{x})$ be an n-variate polynomial on $X = \{x_1, \ldots, x_n\}$ over a field $\mathbb{F}$, and a subset of variables Y and $Z \coloneqq X \backslash Y$. The* evaluation dimension *of f with respect to the partition $Y \sqcup Z$ is defined as*

$$\text{evalDim}_{Y,Z}(f) \coloneqq \text{rank}\left(\left\{f(Y, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathbb{F}^{|Z|}\right\}\right).$$

Over large fields, the evaluation dimension is equivalent to the rank of the Nisan matrix. However, this equivalence does not hold when restricting the evaluation points, e.g. to the Boolean cube. Nevertheless, the evaluation dimension is always a lower bound of the rank of the Nisan matrix ([50, Lemma 11.9], and see also [29, Corollary 4.5.12]).

▶ **Theorem 12.** *Let $f(\boldsymbol{x})$ be an n-variate polynomial, and fix a permutation π on variables. For a variable partition $Y \sqcup Z$ with $Y = \{x_{\pi(1)}, \ldots, x_{\pi(i)}\}$ and $Z = \{x_{\pi(i+1)}, \ldots, x_{\pi(n)}\}$, any* roABP *that computed f in the order π has width at least* $\text{evalDim}_{Y,Z}(f)$.

Conversely, if the field $\mathbb{F}$ is infinite, there is a roABP *computing f of width* $\text{evalDim}_{Y,Z}(f)$.

2.2 Elementary Symmetric Polynomials

Symmetric polynomials are those that are invariant under any permutation of the variables. A fundamental and well-studied family within symmetric polynomials is the elementary symmetric polynomials, which are defined as follows.

▶ **Definition 13** (Elementary Symmetric Polynomial). *The* elementary symmetric polynomial *of degree d, on variables $x_1, \ldots, x_n$, is defined as*

$$\mathsf{ESym}_n^d(x_1, \ldots, x_n) \coloneqq \sum_{1 \le i_1 < \ldots < i_d \le n} x_{i_1} \ldots x_{i_d}.$$

Whenever clear from the context, we write $e_d \coloneqq \mathsf{ESym}_n^d$ to denote the degree-d elementary symmetric polynomial in n variables. A more convenient way to define these polynomials is via the following generating functions:

$$\prod_{i \in [n]} (1 + x_i \cdot t) = \sum_{i=0}^{n} \mathsf{ESym}_n^i(\boldsymbol{x}) \cdot t^i. \tag{1}$$

These polynomials are called *elementary* because they form the fundamental building blocks for all symmetric polynomials. For any n-variate polynomial $f(\boldsymbol{x})$, we define the n-variate symmetric polynomial $f_{\mathsf{sym}} \coloneqq f(e_1, \ldots, e_n)$.

▶ **Theorem 14** (Fundamental Theorem of Symmetric Polynomials). *Let R be any commutative ring, and let $g \in R[x_1, \ldots, x_n]$ be a symmetric polynomial. Then there exists a unique polynomial $f \in R[y_1, \ldots, y_n]$ such that*

$$g = f_{\mathsf{sym}} \coloneqq f(\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n).$$

We refer to [39, Theorem IV.6.1] for the proof of Fundamental Theorem of Symmetric Polynomials (see also [15]). We will also need the following variable partitioning lemma, which is a special case of [42, Theorem 1.1].

▶ **Lemma 15** (ESym Variable Partition). *Let $Y \sqcup Z$ be a partition of the variables. Then,*

$$\mathsf{ESym}_{|Y \sqcup Z|}^d(Y, Z) = \sum_{i=0}^{d} \left(\mathsf{ESym}_{|Y|}^i(Y) \cdot \mathsf{ESym}_{|Z|}^{d-i}(Z)\right).$$

Proof. Let $Y = \{y_1, \ldots, y_m\}$ and $Z = \{z_1, \ldots, z_n\}$. Then using Equation 1 we can write,

$$\sum_{i=0}^{m} \mathsf{ESym}_m^i(Y) \cdot t^i = \prod_{i=1}^{m} (1 + y_i \cdot t)$$
$$\sum_{i=0}^{n} \mathsf{ESym}_n^i(Z) \cdot t^i = \prod_{i=1}^{n} (1 + z_i \cdot t)$$

Taking the product of the two polynomials above, and comparing the coefficients of t^d on both sides proves the lemma. ◀

As a direct consequence of extracting the coefficient of t^d from Equation 1, Shpilka and Wigderson [51] (crediting Ben-Or) presented the following identity for elementary symmetric polynomials, which yields a near-optimal roABP of width $O(n)$ computing ESym_n^d in any variable order:

▶ **Proposition 16** ([51, Theorem 5.1]). *For any $n \in \mathbb{N}$ and $d \leq n$, let ω be a primitive n-th root of unity. There exist $\beta_0, \ldots, \beta_{n-1} \in \mathbb{C}$ such that*

$$\mathsf{ESym}_n^d(x_1, \ldots, x_n) = \sum_{0 \leq j < n} \beta_j \left(1 + \omega^j x_1\right) \cdot \left(1 + \omega^j x_2\right) \cdots \left(1 + \omega^j x_n\right).$$

▶ Remark 17. ESym_n^d can also be computed by a provably tight roABP of width $\min(d + 1, n - d + 1)$ in any variable order using only coefficients 0 and 1 (see [45, Construction 1.2]).

2.3 Resultant and Discriminant

We recall the definitions and properties of resultant and discriminant from factorization literature. We encourage readers to refer to [56, Chapter 6] for a more detailed textbook treatment of these concepts.

▶ **Definition 18** (Resultant). *Consider two n-variate polynomials $f, g \in \mathbb{F}[\boldsymbol{x}][y]$ as follows:*

$$f := \sum_{i=0}^{d_1} f_i(\boldsymbol{x}) \cdot y^i \quad \text{and} \quad g := \sum_{i=0}^{d_2} g_i(\boldsymbol{x}) \cdot y^i.$$

Define the Sylvester matrix *of f and g as the following $(d_1 + d_2) \times (d_1 + d_2)$ matrix:*

$$\mathbf{S}_y(f, g) = \begin{pmatrix} f_{d_1} & & & & g_{d_2} & & & \\ f_{d_1-1} & f_{d_1} & & & g_{d_2-1} & g_{d_2} & & \\ \vdots & f_{d_1-1} & \ddots & & \vdots & g_{d_2-1} & \ddots & \\ \vdots & \vdots & \ddots & f_{d_1} & \vdots & \vdots & \ddots & g_{d_2} \\ f_0 & \vdots & & f_{d_1-1} & g_0 & \vdots & & g_{d_2-1} \\ & f_0 & \ddots & \vdots & & g_0 & \ddots & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & f_0 & & & & g_0 \end{pmatrix}$$

Then the resultant of the two polynomials with respect to y is defined as the determinant of the Sylvester matrix as:

$$\mathrm{Res}_y(f, g) := \mathsf{Det}(\mathbf{S}_y(f, g)).$$

The resultant of two polynomials is non-zero if and only if their gcd is 1. A well-known case of resultant relevant for factoring algorithms is the discriminant.

▶ **Definition 19** (Discriminant). *Consider a n-variate polynomial f. The* discriminant *with respect to y of f is defined as the resultant, with respect to y, of f and its y-derivative, i.e.,*

$$\mathrm{Disc}_y(f) \coloneqq \mathrm{Res}_y(f, \partial_y f).$$

The following well-known observation will be useful in the analyses of complexity of the resultant and the discriminant.

▶ **Observation 20** (see [19, Chapter 3]). *Let $f = \prod_{i\in[n]}(y-\alpha_i)$ and $g = \prod_{i\in[m]}(y-\beta_i)$ be two univariate polynomials. Then the resultant of f and g with respect to y is given by*

$$\mathrm{Res}_y(f,g) \;=\; \prod_{i\in[n]} g(\alpha_i).$$

3 roABP Factor Non-Closure

To prove Theorem 1, we need a polynomial of low roABP complexity, that has a factor of high roABP complexity. We will use explicit expander graphs for this purpose. The only property we require from the expander graph is that, for any sufficiently large partition of its vertex set into two parts, it contains a large induced matching between the two parts.

▶ **Lemma 21** (Induced Matching Lemma). *For every $n \in \mathbb{N}$ there exists a constant degree graph $G_n = (V, E)$ on n vertices such that the following holds: for any partition (S, T) of V with $|S| = \varepsilon n$ and $|T| = (1-\varepsilon)n$ where $\varepsilon \in \left[\frac{1}{3}, \frac{2}{3}\right]$, the graph contains $\Omega(n)$ edges between S and T that form an induced matching.*

Proof Sketch. There exists an absolute constant $\delta \in (0,1)$ such that, for any $k \in \mathbb{N}$ with $k \geq 1$, we can construct explicit k-regular expander graphs $G_n = (V, E)$ whose second-largest eigenvalue is at most k^δ; see [47].

When k is chosen to be sufficiently large such that the second-largest eigenvalue of G_n is strictly smaller than $k/3$, then the lemma follows as an easy consequence of the Expander Mixing Lemma [3] (see also [33, Lemma 2.5]). See, for example, [34, Claim 4]. ◀

Define an n-variate polynomial P_G associated with constant degree graph $G_n = (V, E)$ guaranteed by Lemma 21 as follows:

$$P_G \coloneqq \prod_{(i,j)\in E} \left((x_i x_j)^d - 1\right). \tag{2}$$

Since the degree of the graph is constant, the sparsity of P_G is $2^{|E|} = 2^{O(n)} =: w$. Therefore, P_G can be computed by an roABP of width w in every variable order. To prove the hardness of its factor, consider the following polynomial Q_G:

$$Q_G \coloneqq \prod_{(i,j)\in E} \left(1 + (x_i x_j) + (x_i x_j)^2 + \ldots + (x_i x_j)^{d-1}\right). \tag{3}$$

It is well known that $(1 + x + x^2 + \ldots + x^{d-1})(x-1) = x^d - 1$. Using the identity, we immediately obtain

$$P_G \;=\; Q_G \cdot \prod_{(i,j)\in E} (x_i x_j - 1).$$

▶ **Lemma 22.** *The polynomial Q_G defined in Equation 3 requires an* roABP *of width $d^{\Omega(n)}$ in every variable order.*

Proof. Let π be any variable order on the variables $X = \{x_1, \ldots, x_n\}$, and consider the partition $Y = \{x_{\pi(1)}, \ldots, x_{\pi(n/2)}\}$ and $Z = X \setminus Y$.

Let Y and Z also denote the partition of vertices of G_n. Then from Lemma 21, we know there exists an induced matching $\mathcal{M}$ between Y and Z of size $\Omega(n)$. Define

$$\begin{aligned}\widetilde{f} &:= \prod_{(i,j)\in\mathcal{M}} \left(1 + (x_i x_j) + (x_i x_j)^2 + \ldots + (x_i x_j)^{d-1}\right) \\ &= \prod_{i\in[t]} \left(1 + (y_i z_i) + (y_i z_i)^2 + \ldots + (y_i z_i)^{d-1}\right),\end{aligned}$$

where for every $i \in [t]$, y_i is a variable in Y and z_i is a variable in Z, and $t = \Omega(n)$. Here we have used the fact that $\mathcal{M}$ is an induced matching. In particular, $\widetilde{f}$ is obtained from Q_G by setting to zero the variables which are not in the matching $\mathcal{M}$. Hence, the rank of the Nisan matrix can only decrease. Finally, by Observation 9,

$$\operatorname{rank}\left(M_{Y,Z}(Q_G)\right) \geq \operatorname{rank}\left(M_{Y,Z}\left(\widetilde{f}\right)\right) \geq d^{\Omega(n)}.$$

We obtain the claimed lower bound for width of roABP computing Q_G by Theorem 8. ◀

We will now use the discussion so far to give the complete proof of the factor non-closure result.

▶ **Theorem 1** (roABP factor non-closure)**.** *The following holds over any field. Let $n \in \mathbb{N}$ be a parameter and $d \geq n$. There exists an n-variate polynomial f of degree d computable by an* roABP *of width $w := 2^{O(n)}$, such that one of its (irreducible) factors g requires an* roABP *of width $w^{\Omega(\log d)}$ in every variable order.*

Proof. Consider an n-variate polynomial $g := Q_{G_{n-1}} + z$, where z is an auxiliary variable and $Q_{G_{n-1}}$ is defined as in Equation 3 using a constant-degree graph G_{n-1}. We then define

$$f := g \cdot \prod_{(i,j)\in E} (x_i \cdot x_j - 1) = P_G + z \cdot \prod_{(i,j)\in E} (x_i \cdot x_j - 1).$$

As argued after Equation 2, both P_G and $\prod_{(i,j)\in E}(x_i \cdot x_j - 1)$ have sparsity $2^{O(n)}$ and hence we can compute them by an roABP of width $w = 2^{O(n)}$ in every variable order. Therefore, f itself admits an roABP of width w in every variable order.

Observe that g is an irreducible polynomial because it is linear in the auxiliary variable z.[4] Further, by Lemma 22, any roABP computing $Q_G + z$ must have width at least $d^{\Omega(n)}$ in every variable order. Since $d \geq n$, the claimed width lower bound for roABP computing g follows. ◀

4 roABP Complexity of Symmetric Polynomials

In the following two sections we prove Theorem 2 and Theorem 3 along with their corollaries.

[4] See [57, Example 5.1] where the hardness is lifted to irreducible factor by considering $g = Q_G + n$.

4.1 f_{sym} is easy, but f is hard

In this section, we work over fields of characteristic zero. For the proof of Theorem 2, we consider $f_{\mathsf{sym}} = \sum_{d=0}^{n} \mathsf{ESym}_n^d(x_1^k, \ldots, x_n^k)$ for a suitable choice of $k \in [n]$ to be fixed later.

Let us consider the polynomial

$$g(y_1, \ldots, y_n, t, z_0, \ldots, z_{k-1}) \coloneqq \prod_{j=0}^{k-1} \left(1 + \sum_{i \in [n]} y_i \cdot (t \cdot z_j)^i\right).$$

The polynomial g is symmetric in the variables $z_0, \ldots, z_{k-1}$. So by Theorem 14, there exists a polynomial $\widetilde{g} \in \mathbb{Z}[y_1, \ldots, y_n, t, z_0, \ldots, z_{k-1}]$ such that $g(\boldsymbol{y}, t, \boldsymbol{z}) = \widetilde{g}(\boldsymbol{y}, t, e_1(\boldsymbol{z}), \ldots, e_k(\boldsymbol{z}))$. Notice that if ω is a k-th primitive root of the unity, Equation 1 implies

$$\begin{cases} e_i(\omega^0, \ldots, \omega^{k-1}) = 0 & \text{for } 1 \leq i < k, \\ e_k(\omega^0, \ldots, \omega^{k-1}) = 1. \end{cases}$$

Let us define

$$f(y_1, \ldots, y_n) \coloneqq \widetilde{g}(\boldsymbol{y}, 1, 0, \ldots, 0, 1) \in \mathbb{Z}[\boldsymbol{y}]. \tag{4}$$

The previous paragraph ensures that for any k-th primitive root of the unity ω, we have

$$f(y_1, \ldots, y_n) = \prod_{j=0}^{k-1} \left(1 + \sum_{i \in [n]} y_i \cdot \omega^{j \cdot i}\right). \tag{5}$$

The following lemma shows that f is indeed the unique polynomial inducing the symmetric polynomial $\sum_{d=0}^{n} \mathsf{ESym}_n^d(x_1^k, \ldots, x_n^k)$. The following is an argument in [1], which we reproduce here for completeness.

▶ **Lemma 23** (Circulant Polynomial). *For any $n \in \mathbb{N}$ and odd positive integer $k \leq n$,*

$$f_{\mathsf{sym}}(\boldsymbol{x}) \coloneqq f(e_1(\boldsymbol{x}), \ldots, e_n(\boldsymbol{x})) = \sum_{d=0}^{n} \mathsf{ESym}_n^d\left(x_1^k, \ldots, x_n^k\right).$$

Proof. Let ω be a k-th primitive root of the unity. Using the factorization identity $(1 - t^k) = \prod_j (1 - \omega^j \cdot t)$ together with Equation 1 we obtain the following:

$$\begin{aligned} \prod_{i \in [n]} \left(1 - x_i^k \cdot (-t)^k\right) &= \prod_{i=1}^{n} \prod_{j=0}^{k-1} \left(1 + \omega^j \cdot x_i \cdot t\right) \\ &= \prod_{j=0}^{k-1} \left(1 + \sum_{i=1}^{n} e_i(\boldsymbol{x}) \cdot (\omega^j \cdot t)^i\right). \end{aligned}$$

By Equation 5 and instantiating t by 1, we obtain

$$\prod_{i \in [n]} \left(1 + x_i^k\right) = f\left(e_1(\boldsymbol{x}), \ldots, e_n(\boldsymbol{x})\right). \qquad \blacktriangleleft$$

We call the polynomial f a circulant polynomial because it is closely related to the determinant of a Circulant matrix.[5]

In the following lemma, we show that the polynomial f is hard for roABP in every variable order over any field $\mathbb{F}$ of characteristic 0.

[5] Specifically, in the case $k = n$, the homogeneous component of degree k of the polynomial f is exactly the determinant of the circulant matrix of first row $(x_1, \ldots, x_n)$.

▶ **Lemma 24.** *For any prime k with $2 \le k \le n$, the n-variate polynomial f defined in Equation 4 requires* roABP *width at least $2^{(k-1)/2}$ in any variable order.*

Proof. By instantiating a variable, the roABP width can only decrease. So it is sufficient to consider $f'(y_1, \ldots, y_k) := f(y_1, \ldots, y_k, 0, \ldots, 0)$.

By the standard evaluation-dimension lower bound for roABP, it suffices to show the following. For any variable order π and the variable partition (U, V) where $U = \{y_{\pi(1)}, \ldots, y_{\pi((k-1)/2)}\}$ and $V = \{y_{\pi((k-1)/2+1)}, \ldots, y_{\pi(k)}\}$ we have

$$\text{evalDim}_{U,V}(f') \;=\; \text{rank}\left(\left\{f'(\boldsymbol{u}, \boldsymbol{a}) \;\mid\; \boldsymbol{a} \in \mathbb{F}^{|V|}\right\}\right) \;\ge\; 2^{\Omega(k)}.$$

Re-writing Equation 5 in terms of variable partition (U, V), we have

$$f'(\boldsymbol{u}, \boldsymbol{a}) \;=\; \prod_{j=0}^{k-1} \Big(\ell_j(\boldsymbol{u}) + \ell'_j(\boldsymbol{a}) + 1\Big), \tag{6}$$

where $\ell_j(\boldsymbol{u})$ and $\ell'_j(\boldsymbol{v})$ are linear polynomials in U and V, respectively.

Arranging the coefficients in the linear forms $\{\ell_j(\boldsymbol{u}) + \ell'_j(\boldsymbol{v})\}_j$ as the rows of a $k \times k$ matrix yields a matrix M whose (j, i)-th entry is $\omega^{j \cdot \pi(i)}$ for $j \in \{0, \ldots, k-1\}$ and $i \in [k]$. Note that M can be obtained from the standard $k \times k$ DFT matrix $(\omega^{j \cdot i})_{i,j \in [k]}$ by permuting columns.

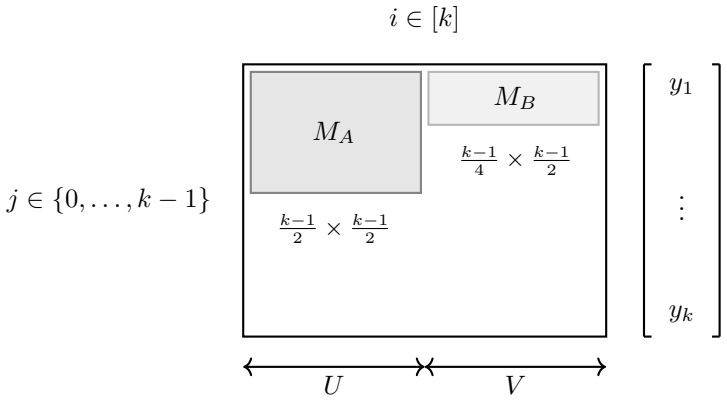

Figure 1 The matrix M with (j, i)-th entry $\omega^{j\pi(i)}$, corresponding to the natural variable order. The highlighted submatrices M_A and M_B are used in the analysis of evaluation dimension.

When k is prime, Chebotarev's theorem on roots of unity [53] states that every square submatrix of the DFT matrix (and hence also M) is nonsingular; see also [54, Lemma 1.3] and [30]. Since $|U| = (k-1)/2$, we can fix a subset $A \subseteq \{0, \ldots, k-1\}$ of size $(k-1)/2$ such that the set $\{\ell_j(\boldsymbol{u})\}_{j \in A}$ corresponds to a square submatrix M_A of M. Such a submatrix M_A is non-singular due to Chebotarev's theorem. Consequently, the set $\{\ell_j(\boldsymbol{u})\}_{j \in A}$ is linearly independent. We can assume that $\ell_i(\boldsymbol{u}) = u_i$ for $i \in A$, since an invertible linear transformation on the variables in U does not change the evaluation dimension $\text{evalDim}_{U,V}(f')$.

Consider any $B \subseteq A$. By Chebotarev's theorem, the submatrix M_B with rows indexed by B and columns $v_2, \ldots, v_{|B|+1}$ is invertible (the choice $|A| = (k-1)/2$ ensures that V contains enough variables). So, for any $b \in \mathbb{F}$, there is a unique point $\beta_{B,b} \in \mathbb{F}^{|B|}$ such that for any j in B, $\ell'_j(b, \beta_{B,b}, 0, \ldots, 0) + 1 = 0$. Similarly, for any other row index

$\widetilde{j} \in \{0,\ldots,k-1\} \setminus B$, there exists a unique point $\gamma_{B,\widetilde{j}} \in \mathbb{F}^{|B|+1}$ such that for any j in $B \cup \{\widetilde{j}\}$, we have $\ell'_j(\gamma_{B,\widetilde{j}}, 0, \ldots, 0) + 1 = 0$. It follows that $\gamma_{B,\widetilde{j}}$ is of the form $(b_{\widetilde{j}}, \beta_{B,b_{\widetilde{j}}})$ for a particular $b_{\widetilde{j}} \in \mathbb{F}$.

Since $\mathbb{F}$ is infinite, we can choose b in $\mathbb{F}$ outside of $\left\{b_{\widetilde{j}} \mid \widetilde{j} \in \{0,\ldots,k-1\} \setminus B\right\}$, and define $\alpha_B \coloneqq (b, \beta_{B,b}, 0, \ldots, 0)$. For any j in $\{0,\ldots,k-1\}$:

$$\ell'_j(\alpha_B) + 1 = 0 \iff j \in B.$$

Consequently $f'(\boldsymbol{u}, \alpha_B) = \left(\prod_{j\in B} u_j\right) \cdot \left(\prod_{j\in[k]\setminus B} (\ell_j(U) + c_{B,j})\right)$ where the $(c_{B,j})_{j\notin B}$ are non-zero constants. Since for each B, $f'(\boldsymbol{u}, \alpha_B)$ has a distinct lowest degree monomial $\left(\prod_{j\in B} u_j\right)$, the set $\{f'(\boldsymbol{u}, \alpha_B) \mid B \subseteq A\}$ is linearly independent. Therefore,

$$\mathrm{evalDim}_{U,V}\big(f'\big) \geq \dim\{f'(\boldsymbol{u}, \alpha_B) \mid B \subseteq A\} = 2^{(k-1)/2}.$$

By the evaluation-dimension lower bound of Theorem 12, any roABP computing f (in any order) must have width at least $2^{(k-1)/2}$. ◀

▶ Remark 25. A close look at the above proof reveals that the lower bound also applies to the circulant polynomial $\prod_{j=0}^{k-1}(\sum_{i=1}^{n} y_i \omega^{ij})$ which is exactly the determinant of the circulant matrix.

The lower bound established in Lemma 24 serves as the key technical ingredient needed to prove Theorem 2.

▶ **Theorem 2.** *The following holds over fields of characteristic zero. Let $n \in \mathbb{N}$ be a parameter. There exists an n-variate polynomial f such that the symmetric polynomial $f_{\mathsf{sym}} \coloneqq f(\mathsf{ESym}^1_n, \ldots, \mathsf{ESym}^n_n)$ is computable by an* roABP *of constant width in every variable order, but any* roABP *computing f in any variable order must have width $2^{\Omega(n)}$.*

Proof. Fix k to be a prime number between $n/2$ and n. We consider the symmetric polynomial $f_{\mathsf{sym}} \coloneqq \sum_{d=0}^{n} \mathsf{ESym}^d_n(x_1^k, \ldots, x_n^k)$. By applying Equation 1 with each x_i replaced by x_i^k, we obtain that f_{sym} admits an roABP of constant width in every variable order. Moreover, by Lemma 24, the width of any roABP computing f is at least $2^{(k-1)/2} = 2^{\Omega(n)}$. ◀

4.2 f is easy, but f_{sym} is hard

To prove Theorem 3, it suffices to show the following technical lemma, which shows that taking powers of elementary symmetric polynomials is hard for roABPs. This lemma also implies Corollary 4 from the introduction. In Subsection 5.1, we will present an alternative proof of Theorem 3 using a quadratic polynomial based on graph-based polynomial from Section 3.

▶ **Lemma 26** (Powers of ESym)**.** *Let $k \leq n/2$. Any* roABP *computing $\left(\mathsf{ESym}^k_n\right)^d$ in any variable order requires width at least $\binom{k+d}{k}$.*

▶ **Theorem 3.** *The following holds over fields of characteristic zero. Let $n \in \mathbb{N}$ be a parameter. There exists an n-variate polynomial f computable by an* roABP *of constant width such that its respective symmetric polynomial $f_{\mathsf{sym}} = f(\mathsf{ESym}^1_n, \ldots, \mathsf{ESym}^n_n)$ requires an* roABP *of width $2^{\Omega(n)}$ in every variable order.*

Proof. Let $k = \lfloor n/2 \rfloor$. Consider the polynomial $f(x_1, \ldots, x_n) = x_k^k$. It is easy to see that f can be computed by an roABP of constant width. However, by Lemma 26, any roABP computing the symmetrisation

$$f_{\mathsf{sym}} = f\left(\mathsf{ESym}_n^1, \ldots, \mathsf{ESym}_n^n\right) = \left(\mathsf{ESym}_n^k\right)^k$$

must have width at least

$$\binom{2\lfloor n/2 \rfloor}{\lfloor n/2 \rfloor} = \Omega\left(2^n/\sqrt{n}\right). \qquad \blacktriangleleft$$

▶ Remark 27. We recall that $\mathsf{ESym}_n^{\lfloor n/2 \rfloor}$ can be expressed as a sum of n many products of univariate polynomials (see Proposition 16). Consequently, using the multinomial theorem, it follows that $(\mathsf{ESym}_n^{\lfloor n/2 \rfloor})^{\lfloor n/2 \rfloor}$ can be expressed as a sum of at most $O(2^{1.5n})$ many products of univariate polynomials. Hence, the bound we obtain in Theorem 3 is almost optimal.

Proof of Lemma 26. Assume that $(e_k)^d$ is computed by an roABP of width w and variable order π. Let $Y = \{x_{\pi(1)}, \ldots, x_{\pi(k)}\}$ and $Z = X \setminus Y$ be a partition of the variables X. By Theorem 12, we know that

$$w \geq \mathrm{evalDim}_{Y,Z}\left((e_k)^d\right).$$

Using Lemma 15, and the multinomial theorem, we can write the powers of the elementary symmetric polynomial e_k as follows:

$$\begin{aligned}(e_k(X))^d &= \left(\sum_{t=0}^{k} e_t(Y) \cdot e_{k-t}(Z)\right)^d \\ &= \sum_{\substack{t_0+\cdots+t_k=d \\ t_i \geq 0}} \binom{d}{t_0, \ldots, t_k} \left(e_0^{t_0}(Y) \cdots e_k^{t_k}(Y)\right) \cdot \left(e_{k-0}^{t_0}(Z) \cdots e_{k-k}^{t_k}(Z)\right). \qquad (7)\end{aligned}$$

To argue about the evaluation dimension of $(e_k(X))^d$, we will need the following elementary fact from linear algebra.

▶ **Proposition 28.** *If a matrix $M = \sum_{i=1}^{r} u_i v_i^T$ where $\{u_1, \ldots, u_r\}$ and $\{v_1, \ldots, v_r\}$ are linearly independent sets of vectors, then M has rank exactly r.*

To use the above fact, we note that the algebraic independence of the elementary symmetric polynomials (a consequence of Theorem 14) implies that the sets

$$E = \{e_0^{t_0}(Y) \cdots e_k^{t_k}(Y) : t_0 + \cdots + t_k = d\} \text{ and } \widetilde{E} = \{e_{k-0}^{t_0}(Z) \cdots e_{k-k}^{t_k}(Z) : t_0 + \cdots + t_k = d\}$$

are both linearly independent sets of polynomials ($\widetilde{E}$ can be obtained from E by just changing the underlying variable). Further, each term on the right-hand side of Equation 7 (corresponding to a tuple $(t_0, \ldots, t_k)$ summing to d) has an evaluation matrix that is the outer product of the coefficient vectors of the corresponding polynomials in E and $\widetilde{E}$, scaled by a suitable multinomial coefficient (which is non-zero because we have assumed that the characteristic of the underlying field is 0). This implies that the evaluation matrix of $(e_k(X))^d$ has rank exactly the number of terms which is $\binom{k+d}{k}$. $\blacktriangleleft$

5 Non-closure corollaries for roABP

We will now give the proofs of corollaries stated in Subsection 1.1. We use observations from the earlier sections to show that operations such as powering, computing resultant, and discriminant can be hard for roABP.

5.1 Hardness of Powering: a second example

In this section, we give a second proof of (a slightly weaker form of) Corollary 4. Note that we already proved this in the form of Lemma 26. By Proposition 16 and the following remark, we know that ESym^n_{2n} admits an roABP of width $O(n)$ in any variable order. On the other hand, any roABP that computes $(\mathsf{ESym}^n_{2n})^d$ must have width at least $\binom{n+d}{n}$.

Inspired by the graph-based polynomial which was used to prove factor non-closure in Section 3, we can even define a quadratic polynomial Q and prove that powering Q is hard for this polynomial roABP. The lower bound we obtain is slightly weaker, but the example is even simpler since Q is just a quadratic polynomial, as opposed to the high-degree and high-sparsity elementary symmetric polynomial.

▶ **Corollary 29** (Variant of Corollary 4)**.** *The following holds over fields of characteristic zero. There exists an n-variate quadratic polynomial Q computable by an* roABP *of width $O(n)$ such that for any d, any* roABP *computing Q^d requires width at least $\binom{d+m}{m}$ in every variable order where $m = \Omega(n)$.*

Proof. Let $G = (V, E)$ be a constant degree graph on n vertices such that Lemma 21 holds. Define the quadratic polynomial:

$$Q_G \;=\; \sum_{(i,j)\in E} x_i x_j \tag{8}$$

where variables x_i correspond to the vertices of G. It is easy to observe that Q_G can be computed by an roABP of width $|E| = O(n)$ in any variable order. We will prove that any roABP computing Q_G^d must have large width.

Let π be any variable order on the variables $X = \{x_1, \ldots, x_n\}$, and consider the partition $Y = \{x_{\pi(1)}, \ldots, x_{\pi(n/2)}\}$ and $Z = X \setminus Y$. Let Y and Z also denote the partition of vertices on G. By Lemma 21, there exists an induced matching $\mathcal{M}$ between Y and Z of size $\Omega(n)$. By renaming the variables if necessary we assume that the matching is between the vertices corresponding to y_i and z_i where $i \in [t]$ and $t = \Omega(n)$.

Define the polynomial:

$$\widetilde{Q}^{\,d} \;=\; \left(\sum_{(i,j)\in\mathcal{M}} x_i \cdot x_j\right)^d \;=\; \left(\sum_{i\in[t]} y_i \cdot z_i\right)^d .$$

In particular, $\widetilde{Q}^{\,d}$ is obtained from Q_G^d by setting to zero the variables which are not in the matching $\mathcal{M}$. Hence, the rank of the Nisan matrix corresponding to $\widetilde{Q}$ is a lower bound on the evaluation dimension of Q w.r.t. the partition (Y, Z).

By construction, for every monomial m_Y of degree exactly d over Y, there exists a unique monomial m_Z over Z such that the coefficient of $m_Y \cdot m_Z$ in $\widetilde{Q}^{\,d}$ is nonzero (cf. Observation 9). Therefore,

$$\operatorname{rank}\left(M_{Y,Z}(Q_G^d)\right) \;\geq\; \operatorname{rank}\left(M_{Y,Z}\left(\widetilde{Q}^{\,d}\right)\right) \;\geq\; \binom{d+t-1}{t-1}.$$

Applying Theorem 8, we obtain the desired lower bound on the width of any roABP computing Q_G^d. ◀

5.2 Hardness of computing resultant and discriminant

We design a polynomial that is simple for roABP, but which turns out to be difficult for roABP when one computes its discriminant. This, in turn, immediately implies that computing resultant is also hard for roABP.

▶ **Corollary 5** (roABP discriminant non-closure). *The following holds over fields of characteristic zero. For all n, there exists an n-variate polynomial $f(\boldsymbol{x}, y)$ computable by an* roABP *of width $O(n)$ such that any* roABP *computing the discriminant $\mathrm{Disc}_y(f)$ requires width at least $2^{\Omega(n)}$ in every variable order.*

Proof. Let g be an $(n-1)$-variate polynomial to which the lower bound in Corollary 4 is applicable. Fix any $d = \Omega(n)$. Define

$$f \coloneqq y^d - g(\boldsymbol{x}) \cdot y.$$

Then we have $\partial_y f = d \cdot y^{d-1} - g$. It is easy to see that the roots of f are $\alpha_0 = 0$ and $\alpha_i = \omega^i \cdot g^{1/(d-1)}$ for $1 \le i \le d-1$, where ω is a primitive $(d-1)$-th root of unity. Here we work over a suitable field extension of the base field $\mathbb{F}$ to ensure that we have an $(d-1)$-th root of unity.

The discriminant of f is defined as the resultant of f and $\partial_y f$ with respect to y, i.e., $\mathrm{Disc}_y(f) = \mathrm{Res}_y(f, \partial_y f)$. Then using Observation 20 we can compute:

$$\begin{aligned}\mathrm{Disc}_y(f) &= \prod_{i=0}^{d-1} \partial_y f(\alpha_i) = -g \cdot \prod_{i=1}^{d-1} (d-1) \cdot g \\ &= -(d-1)^{d-1} g^d.\end{aligned}$$

Thus, computing the discriminant of f amounts to powering the polynomial g, for which we have the required lower bound by Corollary 4. The upper bound on the roABP complexity of f follows from the one for g. ◀

6 Conclusions and Open Problems

In this work, we proved that a width-w roABP computes a polynomial whose irreducible factor requires roABPs of width at least $w^{\log d}$, yielding a quasipolynomial separation. This showed that roABPs are not closed under factoring (see Section 3). A natural next step is to search for polynomials that exhibit an exponential separation between the roABP complexity of a polynomial and that of its factor.

Our non-factor closure proof relied on the idea that polynomials that are hard for the simpler sparse model but easy for roABPs can be transformed, using simple gadgets, into polynomials that are hard even for roABPs. This raises an intriguing question about the scope of such hardness lifting. Specifically, given a polynomial $f(\boldsymbol{x})$ of sparsity s, can we always lift using a gadget ϕ such that the composed polynomial $f(\phi \circ \boldsymbol{x})$ requires an roABP of size $\Omega(s)$?

One consequence of our study of graph-based polynomials and symmetric compositions is the proof that powering is hard for roABPs (see Subsection 5.1). This naturally raises the question in the other direction: does there exist a polynomial $f \coloneqq g^d$ that is easy to compute by an roABP, while g is hard for roABP? An affirmative answer would, once again, stand in sharp contrast to other models such as circuits, algebraic branching programs, and formulas, where low complexity of f leads to low complexity of g. Interestingly, the analogous question for sparse polynomials was answered affirmatively for $d = 2$ in classical works by Rényi [48] and Erdős [24], and was subsequently extended to arbitrary d in later works [55, 18].

References

1 achille hui. Evaluating elementary symmetric polynomial at n^{th} powers. Mathematics Stack Exchange, 2021. URL: https://math.stackexchange.com/a/4259092.

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

3 Noga Alon and Fan R. K. Chung. Explicit construction of linear sized tolerant networks. *Discret. Math.*, 306(10-11):1068–1071, 2006. doi:10.1016/J.DISC.2006.03.025.

4 Matthew Anderson, Michael A. Forbes, Ramprasad Saptharishi, Amir Shpilka, and Ben Lee Volk. Identity testing and lower bounds for read-k oblivious algebraic branching programs. *ACM Trans. Comput. Theory*, 10(1):3:1–3:30, 2018. doi:10.1145/3170709.

5 Robert Andrews and Avi Wigderson. Constant-depth arithmetic circuits for linear algebra problems. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science—FOCS 2024*, pages 2367–2386. IEEE Computer Society, 2024. doi:10.1109/FOCS61266.2024.00138.

6 C. S. Bhargav, Sagnik Dutta, and Nitin Saxena. Improved lower bound, and proof barrier, for constant depth algebraic circuits. In *47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria*, volume 241 of *LIPIcs*, pages 18:1–18:16. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.MFCS.2022.18.

7 Vishwas Bhargava, Pranjal Dutta, Sumanta Ghosh, and Anamay Tengse. The complexity of order-finding for roabps. *CoRR*, abs/2411.18981, 2024. doi:10.48550/arXiv.2411.18981.

8 Vishwas Bhargava and Sumanta Ghosh. Improved hitting set for orbit of roabps. *Comput. Complex.*, 31(2):15, 2022. doi:10.1007/S00037-022-00230-9.

9 Vishwas Bhargava and Anamay Tengse. Explicit commutative roabps from partial derivatives. In *44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2024, December 16-18, 2024, Gandhinagar, Gujarat, India*, volume 323 of *LIPIcs*, pages 10:1–10:15. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.FSTTCS.2024.10.

10 Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. Closure under factorization from a result of Furstenberg. *CoRR*, abs/2506.23214, 2025. doi:10.48550/arXiv.2506.23214.

11 Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. Constant-depth circuits for polynomial GCD over any characteristic. *CoRR*, abs/2506.23220, 2025. doi:10.48550/arXiv.2506.23220.

12 Pranav Bisht and Nitin Saxena. Blackbox identity testing for sum of special roabps and its border class. *Comput. Complex.*, 30(1):8, 2021. doi:10.1007/S00037-021-00209-Y.

13 Markus Bläser, Julian Dörfler, and Christian Ikenmeyer. On the complexity of evaluating highest weight vectors. In *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 29:1–29:36. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.29.

14 Markus Bläser, Christian Ikenmeyer, Meena Mahajan, Anurag Pandey, and Nitin Saurabh. Algebraic branching programs, border complexity, and tangent spaces. In *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 169 of *LIPIcs*, pages 21:1–21:24. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.CCC.2020.21.

15 Ben Blum-Smith and Samuel Coskey. The Fundamental Theorem on Symmetric Polynomials: History's First Whiff of Galois Theory. *College Mathematics Journal*, 48(1):18–29, 2017. doi:10.4169/college.math.j.48.1.18.

16 Markus Bläser and Gorav Jindal. On the Complexity of Symmetric Polynomials. In *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.ITCS.2019.47.

17 Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Closure results for polynomial factorization. *Theory Comput.*, 15:Paper No. 13, 34, 2019. doi:10.4086/toc.2019.v015a013.

18 Don Coppersmith and James Davenport. Polynomials whose powers are sparse. *Acta Arith.*, 58:79–87, 1991. URL: https://eudml.org/doc/206337.

19 David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, NY, 2 edition, 2005. doi:10.1007/b138611.

20 Susanna F. de Rezende, Mika Göös, and Robert Robere. Guest column: Proofs, circuits, and communication. *SIGACT News*, 53(1):59–82, 2022. doi:10.1145/3532737.3532746.

21 Pranjal Dutta, Prateek Dwivedi, and Nitin Saxena. Demystifying the border of depth-3 algebraic circuits. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 92–103, 2022. doi:10.1109/FOCS52979.2021.00018.

22 Pranjal Dutta and Nitin Saxena. Separated borders: Exponential-gap fanin-hierarchy theorem for approximative depth-3 circuits. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 200–211. IEEE, 2022. doi:10.1109/FOCS54457.2022.00026.

23 Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009. doi:10.1137/080735850.

24 Paul Erdős. On the number of terms of the square of a polynomial. *Nieuw Arch. Wiskunde (2)*, 23:63–65, 1949. URL: https://users.renyi.hu/~p_erdos/1949-08.pdf.

25 Michael Forbes. Some concrete questions on the border complexity of polynomials. Video lecture, Workshop on Algebraic Complexity Theory (WACT), Tel Aviv, 2016. URL: https://www.youtube.com/watch?v=1HMogQIHT6Q.

26 Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 867–875. ACM, 2014. doi:10.1145/2591796.2591816.

27 Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science—FOCS 2013*, pages 243–252. IEEE Computer Soc., Los Alamitos, CA, 2013. doi:10.1109/FOCS.2013.34.

28 Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. *Theory Comput.*, 17:Paper No. 10, 88, 2021. doi:10.4086/toc.2021.v017a010.

29 Michael Andrew Forbes. *Polynomial Identity Testing of Read-Once Oblivious Algebraic Branching Programs*. PhD thesis, Massachusetts Institute of Technology, 2014. URL: https://dspace.mit.edu/handle/1721.1/89843.

30 P. E. Frenkel. Simple proof of chebotarev's theorem on roots of unity, 2004. doi:10.48550/arXiv.math/0312398.

31 Zeyu Guo and Rohit Gurjar. Improved explicit hitting-sets for roabps. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2020, August 17-19, 2020, Virtual Conference*, volume 176 of *LIPIcs*, pages 4:1–4:16. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.APPROX/RANDOM.2020.4.

32 Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf. Deterministic identity testing for sum of read-once oblivious arithmetic branching programs. *Comput. Complex.*, 26(4):835–880, 2017. doi:10.1007/S00037-016-0141-Z.

33 Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006. doi:10.1090/S0273-0979-06-01126-8.

34 Stasys Jukna. Expanders and time-restricted branching programs. *Theoretical computer science*, 409(3):471–476, 2008. doi:10.1016/j.tcs.2008.09.012.

35 Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Comput. Complexity*, 13(1-2):1–46, 2004. doi:10.1007/s00037-004-0182-6.

36 Erich Kaltofen. Factorization of polynomials given by straight-line programs. *Adv. Comput. Res.*, 5:375–412, 1989. URL: https://api.semanticscholar.org/CorpusID:14414372.

37 Erich Kaltofen and Barry M. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symbolic Comput.*, 9(3):301–320, 1990. doi:10.1016/S0747-7171(08)80015-6.

38 Neeraj Kayal, Vineet Nair, and Chandan Saha. Separation between read-once oblivious algebraic branching programs (roabps) and multilinear depth-three circuits. *ACM Trans. Comput. Theory*, 12(1):2:1–2:27, 2020. doi:10.1145/3369928.

39 Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, New York, NY, revised 3rd edition, 2002. doi:10.1007/978-1-4613-0041-0.

40 Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Journal of the ACM*, 72(4):1–35, 2025. doi:10.1145/3734215.

41 Richard J. Lipton and Ken W. Regan. Arithmetic complexity and symmetry. Blog post, Gödel's Lost Letter and P=NP, 2009. URL: https://rjlipton.com/2009/07/10/arithmetic-complexity-and-symmetry/.

42 Mircea Merca. A convolution for complete and elementary symmetric functions. *Aequationes Mathematicae*, 86(3):217–229, 2013. doi:10.1007/s00010-012-0170-x.

43 N. Nisan and A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 16–25, 1995. doi:10.1109/SFCS.1995.492458.

44 Noam Nisan. Lower bounds for non-commutative computation (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 410–418. ACM, 1991. doi:10.1145/103418.103462.

45 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)*, volume 219 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 53:1–53:23, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.STACS.2022.53.

46 Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Comput. Complex.*, 14(1):1–19, 2005. doi:10.1007/S00037-005-0188-8.

47 Omer Reingold, Salil P. Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, pages 3–13. IEEE Computer Society, 2000. doi:10.1109/SFCS.2000.892006.

48 Alfréd Rényi. On the minimal number of terms of the square of a polynomial. *Hungarica Acta Math*, 1:30–34, 1947. URL: https://static.renyi.hu/renyi_cikkek/1947_On_the_minimal_number_of_terms_of_the_square_of_a_polynomial.pdf.

49 Chandan Saha and Bhargav Thankey. Hitting sets for orbits of circuit classes and polynomial families. *ACM Trans. Comput. Theory*, 16(3):14:1–14:50, 2024. doi:10.1145/3665800.

50 Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. GitHub repository, version 9.0.3, 2021. A community curated survey. URL: https://github.com/dasarpmar/lowerbounds-survey.

51 Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Comput. Complex.*, 10(1):1–27, 2001. doi:10.1007/PL00001609.

52 Amit Sinhababu and Thomas Thierauf. Factorization of polynomials given by arithmetic branching programs. *Comput. Complexity*, 30(2):Paper No. 15, 47, 2021. doi:10.1007/s00037-021-00215-0.

53 P. Stevenhagen and H. W. Lenstra. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996. doi:10.1007/BF03027290.

54 Terence Tao. An uncertainty principle for cyclic groups of prime order. 2004. doi:10.48550/arXiv.math/0308286.

55 W. Verdenius. On the number of terms of the square and the cube of polynomials. *Indag. Math.*, 11:459–465, 1949.

56 Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, third edition, 2013. doi:10.1017/CBO9781139856065.

57 Joachim von zur Gathen and Erich L. Kaltofen. Factoring sparse multivariate polynomials. *J. Comput. Syst. Sci.*, 31(2):265–287, 1985. doi:10.1016/0022-0000(85)90044-3.