On the Hardness of Order Finding and Equivalence Testing for ROABPs

C. Ramya ✉

The Institute of Mathematical Sciences, Chennai, India

Pratik Shastri ✉

The Institute of Mathematical Sciences, Chennai, India

—— Abstract ——

The complexity of representing a polynomial by a Read-Once Oblivious Algebraic Branching Program (ROABP) is highly dependent on the chosen variable ordering. Bhargava et al. [5] prove that finding the optimal ordering is NP-hard, and provide some evidence (based on the Small Set Expansion hypothesis) that it is also hard to approximate the optimal ROABP width. In another work, Baraskar et al. [3] show that it is NP-hard to test whether a polynomial is in the GL_n orbit of a polynomial of sparsity at most s.

Building upon these works, we show the following results: first, we prove that approximating the minimum ROABP width up to any constant factor is NP-hard, when the input is presented as a circuit. This removes the reliance on stronger conjectures in the previous work [5]. Second, we show that testing if an input polynomial given in the sparse representation is in the affine GL_n orbit of a width-w ROABP is NP-hard. Furthermore, we show that over fields of characteristic 0, the problem is NP-hard even when the input polynomial is homogeneous. This provides the first NP-hardness results for membership testing for a dense subclass of polynomial sized algebraic branching programs (VBP). Finally, we locate the source of hardness for the order finding problem at the lowest possible non-trivial degree, proving that the problem is NP-hard even for quadratic forms.

1 Introduction

Algebraic circuits provide a powerful framework for understanding the complexity of computing multivariate polynomial over a field. These are directed acyclic graphs whose in-degree 0 vertices are labeled by variables or field constants and internal vertices are either addition or multiplication gates. Several computational problems concerning polynomials such as identity testing, polynomial factoring, equivalence testing and reconstruction have been studied intensively for various structured subclasses of circuits.

In this article, we are interested in *Read-Once Oblivious Algebraic Branching Programs* (ROABPs for short), the algebraic analogs of ordered binary decision diagrams (OBDDs). Informally, an ROABP is layered DAG with a designated source and sink vertex whose edges are labeled by univariate polynomials. More importantly, all edges in the same layer use the same variable and a variable occurs in exactly one layer. The polynomial computed by the ROABP is the sum over all source-to-sink paths of the product of edge weights along each path. In this work, we study the computational complexity of two problems concerning ROABPs: *order-finding* and *equivalence testing*. Before delving into the details of these two problems, we note that in algorithms concerning polynomials, a polynomial $f(x_1, \ldots, x_n)$ of degree d can be given as an input to an algorithm in one of the following standard representations:

45 ▪ Dense Representation: a list (of size $\binom{n+d}{d}$) of coefficients for all possible monomials up
46 to degree d.

47 ▪ Sparse Representation: a list of pairs, where each pair consists of a non-zero coefficient
48 and its corresponding monomial (represented by its exponent vector).

49 ▪ Circuit Representation: an algebraic circuit computing f.

50 ▪ Black-Box Access: an oracle access to evaluations of f.

51 It is important to note that the choice of representation can critically affect the complexity
52 of a computational problem. The input representations above are ordered in increasing order
53 of compactness. As a rule, problems considered in this paper become harder when the input
54 is presented more compactly. Conversely, proving hardness becomes easier.

55 First, we begin with the order finding problem for ROABPs. It is easy to see that with
56 every ROABP computing a polynomial $f(x_1, \ldots, x_n)$ we can associate a unique permutation
57 $\sigma : [n] \to [n]$ which we call the *order* of the ROABP. The size of an ROABP, particularly its
58 *width*, which is the maximum number of vertices in any of its layers serves as a key measure of
59 complexity. A crucial feature of ROABPs is that the width required to compute a polynomial
60 f is critically dependent on the order. A poor choice of ordering can lead to an exponential
61 blow-up in the required width compared to an optimal one. For instance, the minimal widths
62 of ROABPs computing $(x_1 + y_1)(x_2 + y_2) \cdots (x_n + y_n)$ in orders $(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$
63 and $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ are drastically different. This sensitivity gives rise to the natural
64 computational question of order finding introduced in Bhargava et al. [5]:

65 ▶ **Problem 1** (CktROWidth-d). *[Decision version of order-finding]: Given a polynomial*
66 $f \in \mathbb{F}[x_1, \ldots, x_n]$ *of degree at most d as an algebraic circuit and an integer w in binary,*
67 *decide whether there exists an ROABP for f of width at most w, in some order.*

68 ▶ **Problem 2** (SearchCktROWidth-d). *[Search version of order-finding]: Given an algebraic*
69 *circuit C computing an n-variate polynomial f of degree $\leq d$, find an order $\sigma \in S_n$ that*
70 *minimizes the ROABP width for f.*

71 Depending on the input representation, other variations of these problems are defined
72 analogously. For instance, DenseROWidth-d is the decision version of the problem when the
73 input is provided in the dense representation.

74 Bhargava, Dutta, Ghosh, and Tengse [5] study the complexity of the order-finding problem.
75 In particular, they show that DenseROWidth-6 is NP-hard. Their proof is an interesting
76 reduction from the *cutwidth* problem for graphs. This is a *linear arrangement problem* in
77 which given a graph the goal is to find an ordering (a.k.a linear arrangement) of the vertices
78 that minimizes the maximum number of edges between any prefix and the corresponding
79 suffix in that ordering. It is known that the cutwidth problem is NP hard even for graphs
80 with maximum degree 3. Their reduction is parameter preserving: The graph is transformed
81 into a polynomial in such a way that ROABP width of the polynomial is 2 more than the
82 cutwidth of the graph. The degree of the polynomial constructed is exactly 2Δ, where Δ
83 denotes the maximum degree of the graph.

84 Furthermore, Bhargava et al. [5] also study the problem of approximating ROABP width.
85 They provide two pieces of evidence that indicate hardness of approximation, both stemming
86 from their reduction. First, as noted earlier, the reduction in [5] is parameter preserving.
87 Hence, hardness of approximation for the cutwidth problem directly translates to hardness
88 of approximation for ROABP width. Austrin et al. [2] showed that cutwidth is hard to
89 approximate assuming the *small set expansion* (SSE) hypothesis thus implying hardness of
90 approximating ROABP width assuming the SSE hypothesis, even when the input is given
91 in the dense representation. Second, they develop a *tensoring technique* through which

they show that a constant factor approximation for Search-CktROWidth would imply a PTAS for Search-CktROWidth, and therefore, by their reduction, for cutwidth. This is (potentially stronger) evidence against the existence of a constant factor approximation for Search-CktROWidth, since Ambühl et al. [1] show that for a problem related to cutwidth, a PTAS does not exist under assumptions weaker than SSE (but stronger than $P \neq NP$).

In this work, we prove NP-Hardness of approximating Search-CktROWidth up to any arbitrary constant factor.

▶ **Theorem 3** (Inapproximability of Search-CktROWidth-d). *Let $\alpha \in \mathbb{R}$ be an arbitrary constant. Let $n, d \in \mathbb{N}$ be given as input, in unary. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ of degree d be given as input, as an arithmetic circuit. Let $w \in \mathbb{N}$ also be give as input, in binary. It is NP-hard to distinguish between the following two cases:*

1. *f has an ROABP of width $\leq w$ in some order.*
2. *Every ROABP for f has width $> \alpha \cdot w$.*

Our reduction is natural, direct, and again, from cutwidth. It works over any field. We use the power of the circuit representation to construct, from a graph G, a depth three circuit for a polynomial f_G such that for every subset S of vertices, rank of the Nisan matrix of f_G with respect to the set S is exactly $2^{|\text{cut}(S)|}$. For a subset of vertices S, $\text{cut}(S)$ denotes the number of edges going out of S. See Section 2 for definition of Nisan matrices. This already gives NP-hardness of 2-approximation. Then, we use the tensoring technique from [5] to get hardness of α-approximation for any constant α.

Next, we move on to the problem of testing equivalence to ROABPs. Polynomial equivalence testing is a well-studied problem in algebraic complexity theory: given two polynomials the goal is to decide if one is equivalent to the other via an invertible affine transformation of the variables. Several special cases of the polynomial equivalence problem have been studied time and again. In order to understand recent progress on this problem, we consider the notion of *orbits* of polynomial families. Let $\mathbf{x}$ denote $(x_1, \ldots, x_n)$. The *orbit* of an n-variate polynomial f is the set of polynomials obtained from f by applying an invertible affine transformation to the variables, i.e., $\text{orbit}(f) = \{f(A\mathbf{x} + \mathbf{b}) \mid A \in \text{GL}_n(\mathbb{F}) \text{ and } \mathbf{b} \in \mathbb{F}^n\}$. For any class C of polynomials, the orbit of C is the union of orbits of polynomials in C. The orbits of the determinant and permanent polynomials are central to geometric complexity theory.

In the equivalence problem for a certain class C of circuits we are given a polynomial f (in some representation) and the goal is to determine if f is in the (GL_n) orbit of a certain circuit class C. In other words, decide if f affine equivalent (under invertible transformations) to some polynomial in C. Medini and Shpilka [9] study the orbit of the continuant polynomial which is the trace of a certain product of matrices of dimension two and design polynomial time reconstruction algorithms for the same.

In the context of testing whether a given polynomial promised to be in the orbit of a certain circuit class is identically zero or not, Medini and Shpilka [9] construct hitting sets for orbits of read-once formulas[1] and certain *dense* subclasses of depth three circuits. Saha and Thankey [12] designed hitting sets for orbits of ROABPs. Recently, Bhargava and Ghosh [6] obtained smaller hitting sets for the same class of polynomials. It is known [12] that orbits of polynomial size ROABPs are a dense subclass of the the class of polynomial size *general* algebraic branching programs.

---

[1] Read-once formulas are arithmetic formulas where every variable appears as a leaf at most once.

Gupta et al. [8] consider the equivalence problem for read-once arithmetic formulas and give a randomized polynomial-time algorithm (with oracle access to quadratic form equivalence) for the same over fields of characteristic zero. Baraskar et al. [4] give a randomized algorithm to test equivalence to *design polynomials*[2] over fields of sufficiently large size and characteristic. In a recent, beautiful work, Baraskar et al. [3] show NP hardness of testing equivalence to *sparse polynomials* over any field when the input polynomial is given in the sparse representation. The problem is as follows: given f in the sparse representation and in integer w, does there exist an $A \in \mathrm{GL}_n$, $\mathbf{b} \in \mathbb{F}^n$ and a polynomial $g(\mathbf{x})$ with at most w non-zero monomials such that $f = g(A\mathbf{x} + \mathbf{b})$? They also show that a related problem, that of deciding equivalence to constant support polynomials, is NP hard.

In this work, we consider the problem of testing equivalence to ROABPs.

▶ **Problem 4** (ROABP-Equivalence). *Given an n-variate polynomial $f \in \mathbb{F}[x_1 \dots, x_n]$ in its sparse representation and an integer w in binary, decide if there exists an $A \in GL_n(\mathbb{F})$ and a $\mathbf{b} \in \mathbb{F}^n$ such that $f(A\mathbf{x} + \mathbf{b})$ has an ROABP of width at most w.*

We show that this problem is NP-hard over all fields. Over fields of characteristic 0, it remains hard even when the input polynomial is homogeneous. To the best of our knowledge, this provides the first NP-hardness result for membership testing for a dense subclass of polynomial size ABPs:

▶ **Theorem 5.** *Over fields of characteristic* 0*, the* ROABP-Equivalence *problem is* NP*-hard even when the input polynomial f is homogeneous. Over fields of prime characteristic, the* ROABP-Equivalence *problem is* NP*-hard.*

Our proof combines ideas from the papers of Baraskar et al. [3] and Bhargava et al. [5]. Specifically, we reduce from cutwidth and construct a polynomial f such that the linear transformation which minimizes the ROABP width of $f(A\mathbf{x} + \mathbf{b})$ is always the product of a diagonal matrix and a permutation matrix.

In our final result, we pinpoint the hardness of the original order-finding problem to the simplest non-trivial class of polynomials. We show that ROABP order finding is NP-hard even when the input is restricted to be a quadratic form (Theorem 25).

▶ **Theorem 6.** *The problem DenseROWidth-2 is NP-hard over all fields.*

Previously, NP-hardness was known for polynomials of degree ≥ 6 [5]. To show this, we reduce from a different, more algebraic linear arrangement problem called linear rank-width (Problem 14).

2   Preliminaries

We now formally define the concepts central to our results, including ROABPs, Nisan's characterization, and the graph theoretic computational problems we reduce from.

2.1   ROABPs and Width Characterization

▶ **Definition 7** (Read-Once Oblivious ABP (ROABP)). *Let $\mathbb{F}$ be a field. An ROABP R computing an n-variate polynomial $f(x_1, \dots, x_n)$ over $\mathbb{F}$ in a variable order $\sigma \in S_n$ is a layered, directed graph with $n + 1$ layers, indexed 0 to n.*

---

[2] Design polynomials are a special class of polynomials in which the degree of the GCD of every pair of monomials is bounded.

175 ▪ *The 0th layer contains a single source vertex s, and the nth layer contains a single sink*
176 *vertex t.*
177 ▪ *Edges only exist between adjacent layers, from layer $i-1$ to layer i for $i \in [n]$.*
178 ▪ *Edges between layer $i-1$ and i are labeled with univariate polynomials in the variable*
179 $x_{\sigma(i)}$.
180 *The polynomial computed by the ROABP is the sum of products of edge weights over all paths*
181 *from s to t.*

182 ▶ **Definition 8** (Width of an ROABP). *The* width *of an ROABP is the maximum num-*
183 *ber of vertices in any of its layers. For a polynomial f and an order σ, the ROABP-*
184 *width, RO-width$_\sigma(f)$, is the width of the minimal-width ROABP for f in order σ. Then*
185 RO-width(f) *is defined as* $\min_{\sigma \in S_n}$ RO-width$_\sigma(f)$.

186 Nisan's work [10] provides an exact algebraic characterization of ROABP width, as the
187 rank of a certain matrix of coefficients.

188 ▶ **Definition 9** (Nisan Matrix). *For a polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ and a set of*
189 *variables $X_T = \{x_i\}_{i \in T}$, the* Nisan Matrix $M_T(f)$ *is a matrix whose rows are indexed by*
190 *monomials in variables from X_T and columns by monomials in variables from $\{x_1, \ldots, x_n\} \setminus$*
191 *X_T. The (m_1, m_2)-th entry is the coefficient of $m_1 \cdot m_2$ in f.*

192 ▶ **Theorem 10** (Nisan's Characterization [10]). *For any polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ and*
193 *order σ, the number of vertices in the ith layer of an optimal ROABP for f in order σ is*
194 *exactly* rank$(M_{T_i}(f))$, *where $T_i = \{\sigma(1), \ldots, \sigma(i)\}$.*

195 Next, we define two graph layout problems. They will be central to our reductions.

2.2 Graph Layout Problems

197 The authors of [5] prove that DenseROwidth-d is NP hard (for $d \geq 6$) via a reduction from a
198 particular NP-hard graph layout problem called Cutwidth. We define this problem next.

199 ▶ **Definition 11** (Cutwidth [7]). *Given a graph $G = ([n], E)$, a* linear arrangement *is a permuta-*
200 *tion $\pi : [n] \to [n]$. The* cutwidth *of G with respect to π is* $\max_{i \in [n-1]} |\text{cut}(\{\pi(1), \ldots, \pi(i)\})|$[3].
201 *The* Cutwidth *of G is the minimum cutwidth over all arrangements.*

202 It is known [7] that the following problem is NP hard, even for graphs with maximum
203 degree ≤ 3:

204 ▶ **Problem 12** (CutWidth [7]). *Given a graph $G = ([n], E)$ with maximum degree ≤ 3 and*
205 *an integer $w \in \mathbb{N}$ in binary, decide whether the cutwidfth of G is at most w.*

206 Next we define a similar looking graph layout problem, called Linear Rank-Width. Here,
207 the cut size is replaced by the rank of a certain matrix.

208 ▶ **Definition 13** (Linear Rank-Width$_\mathbb{F}$ [11]). *Let $G = ([n], E)$ be a graph and let $\pi : [n] \to [n]$ be*
209 *a linear arrangement. For $i \in [n-1]$, let A_i be a matrix over $\mathbb{F}$ with rows indexed by vertices*
210 *$\{v \mid \pi(v) \leq i\}$ and columns by vertices $\{v \mid \pi(v) > i\}$. The entry (u, v) is 1 if $\{u, v\} \in E$*
211 *and 0 otherwise. The* linear rank-width *of G with respect to π is* $\max_{i \in [n-1]}$ rank(A_i). *The*
212 *linear rank-width of G is the minimum linear rank-width over all arrangements.*

---

[3] For a graph $G = ([n], E)$ and a subset $S \subseteq [n]$ of vertices, cut(S) denotes the number of edges with one
endpoint in S and the other in $[n] \setminus S$

It is known [11] that the the analogous decision problem of minimizing linear rank-width is also NP-hard, over any field.

▶ **Problem 14** (Linear Rank-Width$_{\mathbb{F}}$ [7]). *Given a graph $G = ([n], E)$ and an integer $w \in \mathbb{N}$ in binary, decide whether the linear rank-width of G over $\mathbb{F}$ is at most w.*

3   Inapproximability of ROABP Order-Finding

In this section, we show the NP-hardness of approximating ROABP width up to an arbitrary constant factor, when the input is a circuit. We will require the following Lemma of Bhargava et al.

▶ **Lemma 15** ([5]). *Given a polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ with individual degree d and an $l \in \mathbb{N}$, define*

$$f^{\otimes l}(x_1, \ldots, x_n) = \prod_{k=0}^{l-1} f\left(x_1^{(d+1)^k}, \ldots, x_n^{(d+1)^k}\right)$$

For every subset $S \subseteq [n]$, we have $\mathrm{Rank}(M_S(f^{\otimes l})) = \mathrm{Rank}(M_S(f))^l$.   □

▶ **Theorem 16** (Inapproximability of Search-CktROwidth). *Let $\alpha \in \mathbb{R}$ be an arbitrary constant. Let $n, d \in \mathbb{N}$ be given as input, in unary. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ of degree d be given as input, as an arithmetic circuit. Let $w \in \mathbb{N}$ also be give as input, in binary. It is NP-hard to distinguish between the following two cases:*
1. *f has an ROABP of width $\leq w$ in some order.*
2. *Every ROABP for f has width $> \alpha \cdot w$.*

Proof. We reduce from CutWidth for graphs with maximum degree ≤ 3. Given a graph $G = ([n], E)$, we first construct a small $\Pi\Sigma\Pi$ circuit computing a polynomial $f_G(x_1, \ldots, x_n)$ such that for any $S \subseteq [n]$, $\mathrm{Rank}(M_S(f_G)) = 2^{|\mathrm{cut}(S)|}$. For a vertex $i \in [n]$ and a neighbour j of i, let $n_i(j)$ denote the number of neighbours of i less than or equal to j.

Define

$$f_G(x_1, \ldots, x_n) = \prod_{\{i,j\} \in E} \left(1 + x_i^{n_i(j)} x_j^{n_j(i)}\right) = \sum_{T \subseteq E} \left(\prod_{\{i,j\} \in T} x_i^{n_i(j)} x_j^{n_j(i)}\right)$$

Let $S \subseteq [n]$ be arbitrary. Define the following sets of edges: $E_1 = \{\{i,j\} \mid \{i,j\} \in E \text{ and } i,j \in S\}$, $E_2 = \{\{i,j\} \mid \{i,j\} \in E \text{ and } i,j \in [n] \setminus S\}$ and $E_3 = \mathrm{cut}(S) = E \setminus (E_1 \cup E_2)$. Then, the non-zero rows of $M_S(f_G)$ are indexed by monomials m of the following type: m is characterized by a subset $E_1' \subseteq E_1$ and a subset $E_3' \subseteq E_3$ such that $m =$

$$\left(\prod_{\{i,j\} \in E_1'} x_i^{n_i(j)} x_j^{n_j(i)}\right) \left(\prod_{\substack{\{i,j\} \in E_3' \\ i \in S}} x_i^{n_i(j)}\right).$$ Call E_3' the subset of cut edges *picked* by such

a monomial/row. Similarly, the non-zero columns of $M_S(f_G)$ are indexed by monomials m' which are characterized by a subset $E_2' \subseteq E_2$ and a subset $E_3' \subseteq E_3$ such that $m' =$

$$\left(\prod_{\{i,j\} \in E_2'} x_i^{n_i(j)} x_j^{n_j(i)}\right) \left(\prod_{\substack{\{i,j\} \in E_3' \\ j \in [n] \setminus S}} x_j^{n_j(i)}\right).$$

Observe the following:

241 ▪ For a row indexed by m and column indexed by m', if the subset of cut edges picked by
242 m and m' are not identical, $M_S(f_G)(m, m') = 0$.
243 ▪ The submatrix induced by row and column monomials that pick the same subset of cut
244 edges has rank 1, since every row in this matrix is all 1's.

245 Therefore $M_S(f_G)$ is a block diagonal matrix with $2^{|\text{cut}(S)|}$ disjoint rank 1 blocks and
246 so $\text{Rank}(M_S(f_G)) = 2^{|\text{cut}(S)|}$. Next, set $l = \lceil \log \alpha \rceil + 1$ and consider the polynomial $f_G^{\otimes l}$.
247 It has degree $\leq (6|E| + 1)^{\lceil \log \alpha \rceil + 1} - 1$, it has a formula of size $O_\alpha(|E|)$ which can be
248 computed from G in polynomial time, and by Lemma 15, for every $S \subseteq [n]$ it satisfies
249 $\text{Rank}(M_S(f_G^{\otimes l})) = 2^{l \cdot |\text{cut}(S)|}$. Therefore, it holds that
250 ▪ If G has cutwidth $\leq k$, then RO-width$(f_G^{\otimes l}) \leq 2^{l \cdot k}$
251 ▪ If G has cutwidth $\geq k + 1$, then RO-width$(f_G^{\otimes l}) \geq 2^l \cdot 2^{l \cdot k} > \alpha 2^{l \cdot k}$.
252 This finishes the proof of Theorem 16. ◄

253 4 Hardness of Equivalence Testing for ROABPs

254 Bhargava et al. [5] demonstrate NP-hardness of order-finding problem for ROABPs via a
255 reduction from the cutwidth problem for graphs. More precisely, given a graph $G = ([n], E)$
256 with maximum degree Δ, the authors of [5] construct the polynomial $f_G \in \mathbb{F}[x_1, \ldots, x_n]$
257 defined as

$$258 \quad f_G = \sum_{\{i,j\} \in E} x_i^{n_i(j)} x_j^{n_j(i)} + \sum_{i=1}^{n} x_i^{\Delta+1} \tag{1}$$

259 where $n_i(j) \in [\Delta]$ is the number of neighbours of i less than or equal to j. The claim ([5],
260 Claim 4.4) central to their reduction is that for every $S \subseteq [n]$, $\text{Rank}(M_S(f_G)) = |\text{cut}(S)| + 2$.
261 This implies that the ROABP width of the polynomial f_G is exactly two more the cutwidth
262 of the graph G and the reduction is *order preserving*, i.e., an optimal arrangement of the
263 vertices in G is exactly an optimal order for an ROABP computing f_G.
264 In this section, we prove that over all fields, testing equivalence to width w ROABPs is
265 NP-hard. Over fields of characteristic 0, we show that this problem is NP-hard even when the
266 input polynomial is *homogeneous*, whereas in positive characteristic, we require inhomogeneity.
267 Our reductions build on the reductions in Bhargava et al. [5] and Baraskar et al. [3]. In
268 particular, given a graph $G = ([n], E)$, we construct a polynomial $f_G \in \mathbb{F}[x_1, \ldots, x_n]$ with
269 the following two properties:
270 **1.** If $A \in \text{GL}_n(\mathbb{F})$ is a permutation matrix times a diagonal matrix, then for every $\mathbf{b} \in \mathbb{F}^n$,
271 the ROABP width of $f(A\mathbf{x} + \mathbf{b})$ is cutwidth$(G) + 2$.
272 **2.** If $A \in \text{GL}_n(\mathbb{F})$ is not a permutation matrix times a diagonal matrix, then for every
273 $\mathbf{b} \in \mathbb{F}^n$, the ROABP width of $f(A\mathbf{x} + \mathbf{b})$ is at least $|E| + 3$ in *every* order.

274 Property 2 essentially forces the width minimizing A to have a nice form, namely it is a
275 permutation matrix times a diagonal matrix. This is because cutwidth$(G) \leq |E|$. With this
276 overall plan, we proceed with the details of the reduction.

277 4.1 Characteristic Zero

278 Over characteristic 0, we construct a *homogeneous* f_G. In order to show property 2 for a
279 homogeneous f_G, we need the following Lemma from [3] that provides a lower bound on the
280 sparsity of a polynomial divisible by a high power of a linear form with support at least 2.

▶ **Lemma 17** ([3])**.** *Let $\mathbb{F}$ be a field of characteristic 0. Let $l \in \mathbb{F}[x_1, \ldots, x_n]$ be a linear polynomial with support ≥ 2, let $h \in \mathbb{F}[x_1, \ldots, x_n]$ be arbitrary and let $d \in \mathbb{N}$. Then $l^d \times h$ has at least $d + 1$ non-zero monomials.*

In fact, we need a strengthening of this lemma. In the sequel, we strengthen this lemma and show that any polynomial divisible by the dth power of a linear form with support at least 2 has *ROABP width* at least $d + 1$, in every order.

▶ **Lemma 18.** *Let $\mathbb{F}$ be a field of characteristic zero. Let ℓ be a linear polynomial with support at least 2 and $h \in \mathbb{F}[x_1, \ldots, x_n]$ be any non-zero polynomial and $d \in \mathbb{N}$. Let $F = \ell^d \cdot h$. Then for any $\sigma \in S_n$, $\text{RO-width}_\sigma(f) \geq d + 1$.*

Proof. Without loss of generality, let x_1, x_2 be in the support of ℓ, i.e., $\ell = a_1 x_1 + a_2 x_2 + \ell'$ such that $a_1, a_2 \neq 0$. Then, $F = \ell^d \cdot h = (a_1 x_1 + a_2 x_2 + \ell')^d \cdot h$. We can view h as a polynomial in $\mathbb{F}(x_3, \ldots, x_n)[x_1, x_2]$, i.e., a polynomial in x_1, x_2 with coefficients in the field $\mathbb{F}(x_3, \ldots, x_n)$. Let k be the degree of h (over $\mathbb{F}(x_3, \ldots, x_n)$). That is, k is the maximal $i + j$ such that h contains the monomial $c_{i,j} x_1^i x_2^j$ with $c_{i,j} \in \mathbb{F}(x_3, \ldots, x_n)$ and $c_{i,j} \neq 0$. We denote by h_k the homogeneous component of h of degree k. Then, $F = F_1 + F_2$ where $F_1 = (a_1 x_1 + a_2 x_2)^d \cdot h_k$. Every monomial m in F_1 satisfies $\deg_{x_1}(m) + \deg_{x_2}(m) = d + k$. Furthermore, every monomial in F_2 satisfies $\deg_{x_1}(m) + \deg_{x_2}(m) < k + d$. Next, by applying Lemma 17 to $(a_1 x_1 + a_2 x_2)^d \times h_k$ *over the field* $\mathbb{F}(x_3, \ldots, x_n)$, we get $(a_1 x_1 + a_2 x_2)^d \times h_k = \displaystyle\sum_{\substack{i,j \\ i+j=d+k}} c_{i,j} x_1^i x_2^j$

such that $c_{i,j} \in \mathbb{F}[x_3, \ldots, x_n]$ and at least $d + 1$ of the $c_{i,j}$'s non-zero. Let $m_{i,j}$ be the leading monomial of $c_{i,j}$. Observe that:

- There exists a set P of at least $d + 1$ pairs (i, j) with $i + j = d + k$ such that for each pair (i, j) in P, the coefficient of the monomial $x_1^i x_2^j m_{i,j}$ in F_1 is non-zero.
- There is no monomial m in F with non-zero coefficient such that $\deg_{x_1}(m) + \deg_{x_2}(m) > d + k$.

Now, consider any ROABP for F, in an arbitrary order $x_{\pi(1)}, \ldots, x_{\pi(n)}$. Let S be a *prefix* of π that separates 1 and 2. Without loss of generality, assume that $1 \in S$ and $2 \in [n] \setminus S$. Since width of the ROABP is at least $\text{Rank}(M_S)(F)$ we now prove that $\text{Rank}(M_S(F)) \geq d + 1$. For a monomial $m \in \mathbb{F}[x_1, \ldots, x_n]$, let $m[S]$ denote the monomial obtained from m by setting variables outside $\{x_i \mid i \in S\}$ to 1. Consider the submatrix of $M_S(F)$ induced by the row monomials $\{m_{i,j}[S] x_1^i \mid (i, j) \in P\}$ (order the rows by increasing values of i) and the column monomials $\{m_{i,j}[[n] \setminus S] x_2^j \mid (i, j) \in P\}$ (order the columns by increasing value of j). By our observations above, this is a full rank, square, anti-triangular matrix with non-zero entries on the main anti-diagonal. It has at least $d + 1$ rows. Therefore, the rank of this submatrix is at least $|P| \geq d + 1$ and so is the rank of $M_S(F)$. ◀

▶ **Theorem 19.** *The Equivalence to ROABP problem (Problem 4) is* NP-*hard over fields of characteristic 0.* NP-*hardness holds even when the input polynomial f is homogeneous.*

Proof. We reduce from CutWidth. Let $(G = ([n], E), w)$ be an instance of CutWidth. We map it to an instance $(f_G, w + 2)$ of ROABP-Equivalence. To this end, introduce a total order $e_1 < e_2 < \ldots < e_{|E|}$ on the edges of G. For $i \in E$, let $e_i = \{i_1, i_2\}$ such that $i_1 < i_2$. Let $\mathbf{x} = (x_1, \ldots, x_n)$. For $S \subseteq [n]$, define $\Pi_S(\mathbf{x}) \triangleq \left(\prod_{j \in S} x_j^{|E|+2} \right)$ and define the polynomial

$$ f_G(\mathbf{x}) \triangleq \Pi_{[n]}(\mathbf{x}) \left(\sum_{i=1}^{|E|} x_{i_1}^i x_{i_2}^{2|E|-i+1} \right) $$

Clearly, f_G is a homogeneous polynomial of degree $(n+2)|E| + 2n + 1$. We now prove both the forward and reverse directions of the reduction.

Forward Direction: If G has cutwidth at most w, then there exist $A \in \mathrm{GL}_n(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n$ such that $f_G(A\mathbf{x} + \mathbf{b})$ has an ROABP of width at most $w + 2$ in some order.

The proof of the forward direction follows the outline of the corresponding proof in [5]. In particular, we pick $A = I_n$, the $n \times n$ identity matrix, and $\mathbf{b} = 0$. Consider any subset $S \subseteq [n]$ and f_G ca be expressed as

$$
f_G(\mathbf{x}) = \underbrace{\left(\Pi_S(\mathbf{x}) \sum_{\substack{i \in [|E|] \\ i_1, i_2 \in S}} x_{i_1}^i x_{i_2}^{2|E|-i+1} \right) \Pi_{[n]\setminus S}(\mathbf{x})}_{f_1}
$$

$$
+ \underbrace{\left(\Pi_{[n]\setminus S}(\mathbf{x}) \sum_{\substack{i \in [|E|] \\ i_1, i_2 \in [n]\setminus S}} x_{i_1}^i x_{i_2}^{2|E|-i+1} \right) \Pi_S(\mathbf{x})}_{f_2}
$$

$$
+ \underbrace{\left(\sum_{\substack{i \in [|E|] \\ \{i_1, i_2\} \in \mathrm{cut}(S)}} \Pi_S(\mathbf{x}) \Pi_{[n]\setminus S}(\mathbf{x}) x_{i_1}^i x_{i_2}^{2|E|-i+1} \right)}_{f_3}
$$

Observe that f_1 and f_2 are non-zero polynomials of the form $g(\mathbf{x}_S) \times h(\mathbf{x}_{[n]\setminus S})$, where for a subset S of $[n]$, $\mathbf{x}_S$ are the x variables indexed by S. Therefore, we have that $\mathrm{Rank}(M_S(f_1)) = \mathrm{Rank}(M_S(f_2)) = 1$. Finally, notice that f_3 can be written as a *sum of* $|\mathrm{cut}(S)|$ monomials. For every monomial m, $\mathrm{Rank}(M_S(m)) = 1$ for each S. Since $M_S(f_G) = M_S(f_1) + M_S(f_2) + M_S(f_3)$, by subadditivity of rank, we have that $\mathrm{Rank}(M_S(f_G)) \leq |\mathrm{cut}(S)| + 2$. Consider a linear arrangement $\pi : [n] \to [n]$ that witnesses $\mathrm{cutwidth}(G) \leq w$. Due to the above reasoning, combined with Nisan's characterization, we have that f_G has an ROABP in order π, of width $\leq w + 2$.

Reverse Direction: If there exist $A \in \mathrm{GL}_n(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n$ such that $f_G(A\mathbf{x} + \mathbf{b})$ has an ROABP of width at most $w + 2$ in some order, then G has cutwidth at most w.

In order to prove the reverse direction, we need the following key lemma.

▶ **Lemma 20.** *Suppose $A \in \mathrm{GL}_n(\mathbb{F})$ is not the product of a permutation matrix and a diagonal matrix, then for every $\mathbf{b} \in \mathbb{F}^n$, every ROABP computing $f_G(A\mathbf{x} + \mathbf{b})$ must have width at least $|E| + 3$.*

Proof. If A is not the product of a permutation matrix and a diagonal matrix, then $A\mathbf{x} + \mathbf{b}$ must send at least one x variable to a linear polynomial with support *at least* 2. We may then write $f_G(A\mathbf{x} + \mathbf{b}) = l(\mathbf{x})^{|E|+2} \times h$ for a nonzero polynomial h. By Lemma 18, for any $\sigma \in S_n$, $\mathrm{RO\text{-}width}_\sigma(f_G(A\mathbf{x} + \mathbf{b})) \geq |E| + 3$. ◀

348 We use Lemma 20 to complete the reverse direction of the reduction. First, we observe that if A
349 is the product of a diagonal matrix and a permutation matrix, then RO-width$_\sigma(f_G(A\mathbf{x}+b)) =$
350 RO-width$_\sigma(f_G(\mathbf{x}))$: Suppose A has this form. Then there exist $a_1, \ldots, a_n \in \mathbb{F}$, all non-zero,
351 and a permutation $\pi : [n] \to [n]$ such that $A\mathbf{x}+\mathbf{b} = (a_1 x_{\pi(1)}+b_1, a_2 x_{\pi(2)}+b_2, \ldots, a_n x_{\pi(n)}+b_n)$.
352 We can obtain an ROABP for $f_G(\mathbf{x})$ from an ROABP for $f_G(a_1 x_{\pi(1)} + b_1, \ldots, a_n x_{\pi(n)} + b_n)$
353 by replacing each $x_{\pi(i)}$ with $(x_i - b_i)/a_i$. The resulting ABP is still an ROABP, with the
354 same width as before. Also, this process is clearly reversible.

355

356   By the proof of the forward direction, we know that RO-width$(f_G) \leq$ cutwidth$(G) + 2 \leq$
357 $|E| + 2$. Now suppose there exist $A \in \mathrm{GL}_n$ and $\mathbf{b} \in \mathbb{F}^n$ such that $f_G(A\mathbf{x} + \mathbf{b})$ has ROABP
358 width at most $w + 2$ in some order. Due to Lemma 20 and the observation above, we may
359 assume that A is the identity matrix and $\mathbf{b} = \mathbf{0}$. Next, we show that for each $S \subseteq [n]$,
360 Rank$(M_S(f_G)) \geq |\mathrm{cut}(S)| + 2$ by a proof similar to the NP hardness in [5] by exhibiting a
361 submatrix of $M_S(f_G)$ that is a $|\mathrm{cut}(S)| \times |\mathrm{cut}(S)|$ permutation matrix, along with two rows
362 that lie in disjoint spaces.
363   This suffices for the reverse direction, for if f_G has an ROABP of width $\leq w + 2$ in order
364 π, then due to Nisan's characterization (Theorem 10), we would have that cutwidth$(G) \leq w$,
365 witnessed by the linear arrangement π.
366   Define $E_1 \triangleq \{e_i \mid e_i \in \mathrm{cut}(S), i_1 \in S, i_2 \in [n] \setminus S\}$ and $E_2 \triangleq \{e_i \mid e_i \in \mathrm{cut}(S), i_1 \in$
367 $[n] \setminus S, i_2 \in S\}$. We look at the submatrix of $M_S(f_G)$ induced by the row monomials
368 $R = \{\Pi_S(\mathbf{x})x_{i_1}^i \mid e_i \in E_1\} \cup \{\Pi_S(\mathbf{x})x_{i_2}^{2|E|+1-i} \mid e_i \in E_2\}$ and column monomials $C =$
369 $\{\Pi_{[n]\setminus S}(\mathbf{x})x_{i_1}^i \mid e_i \in E_2\} \cup \{\Pi_{[n]\setminus S}(\mathbf{x})x_{i_2}^{2|E|+1} \mid e_i \in E_1\}$. This is a permutation matrix, since
370 each monomoial labeling both the rows an columns can be associated with a unique end
371 point of an edge in cut(S), and the only non-zero entry (in the entirety of $M_S(f_G)$, not just
372 the submatrix) in that row/column corresponds to the monomial labeling the column/row
373 associated with the other end point of that edge. On the other hand, consider the row
374 labeled by $\Pi_S(\mathbf{x})$. This has non-zero entries in the columns labeled by the monomials
375 $\Pi_{[n]\setminus S}(\mathbf{x})x_i^{2|E|+1}$, for each $i \in [n] \setminus S$ (note that these monomials are *not* contained in C),
376 and a zero entry in the column labeled by $x_{[n]\setminus S}$. Also, a row labeled by $\Pi_S(\mathbf{x})x_i^{2|E|+1}$ for
377 an $i \in [S]$ (again, note that this monomial is *not* contained in R) has a non-zero entry in the
378 column labeled by $\Pi_{[n]\setminus S}$. This gives us that Rank$(M_S(f_G)) \geq |\mathrm{cut}(S)| + 2$.   ◀

379   4.2   Characteristic p

380 In this section, we prove hardness of testing equivalence to width w ROABPs, over charac-
381 teristic p. In this setting, we resort to inhomogeneity to prove hardness. This is because
382 Lemma 17, and therefore, Lemma 20 fail to hold over small characteristic. In particular, we
383 show that a skewed version of the polynomial in Equation (1) gives us hardness, even over
384 characteristic p. Recall the polynomial $f_G = \sum_{\{i,j\}\in E} x_i^{n_i(j)} x_j^{n_j(i)} + \sum_{i=1}^n x_i^{\Delta+1}$ constructed
385 in [5]. Instead of the term $\sum_{i=1}^n x_i^{\Delta+1}$, we introduce the asymmetric $\sum_{i=1}^n x_i^{D_j}$. We carefully
386 choose distinct exponents D_j such that they are polynomial in the size of the graph while
387 also allowing us to prove NP-hardness.
388   We will use the following well known result of Lucas.

▶ **Theorem 21.** *Let p be a prime and m, n be integers such that $m = \sum_{k=0}^t m_k p^k$ and
$n = \sum_{k=0}^t n_k p^k$ are the base p expansions of m and n respectively. Then,*

$$\binom{m}{n} \equiv \prod_{k=0}^t \binom{m_k}{n_k} \mod p$$

where we use the convention that $\binom{m_k}{n_k} = 0$ if $m_k < n_k$.

▶ **Theorem 22.** *Let p be a prime and let $\mathbb{F}$ be a field of characteristic p. The Equivalence to ROABP problem (Problem 4) is* NP-*hard over $\mathbb{F}$.*

Proof. Let $(G = ([n], E), w)$ be an instance of the CutWidth problem with maximum degree of G is ≤ 3. We map it to an instance $(f_G, w + 2)$ of ROABP-Equivalence.

Let $M = \max\{|E| + 4, 7\}$. Let L be the smallest integer such that $p^L > M$. For each $j \in [n]$, define the exponent

$$D_j := (p^L - 1) + (j - 1)p^L.$$

Note that each D_j is $\mathsf{poly}(n, |E|)$. For each vertex i, let $n_i(j) \in [\deg(i)]$, as before, be number of neighbours of i less than or equal to j. Note that $n_i(j) \leq 3$ for each $\{i, j\} \in E$. Let $\mathbf{x} = (x_1, \ldots, x_n)$. Define the polynomial

$$f_G(\mathbf{x}) \triangleq \sum_{\{i,j\} \in E} x_i^{n_i(j)} x_j^{n_j(i)} + \sum_{j=1}^{n} x_j^{D_j}. \qquad (2)$$

First, we check that a statement analogous to Claim 4.4 in [5] continues to hold for the f_G we have defined. The proof in [5] works for our f_G as well, we include a proof here for completeness.

▷ **Claim 23** (Analogous to Claim 4.4 in [5]). For each $S \subseteq [n]$, we have $\mathrm{Rank}(M_S(f_G)) = |\mathrm{cut}(S)| + 2$.

Proof. The nonzero rows of $M_S(f_G)$ are of at most three types:
(1) Row indexed by the constant monomial 1;
(2) Rows indexed by $x_i^{n_i(j)}$ for $i \in S$ and $j \in [n] \setminus S$;
(3) Rows indexed by $x_i^{n_i(j)} x_j^{n_j(i)}$ for $i, j \in S$ or by $x_i^{D_i}$ for $i \in S$.
Similarly, columns of $M_S(f_G)$ are of at most three types:
(1) Column indexed by the constant monomial 1;
(2) Columns indexed by $x_j^{n_j(i)}$ for $j \in [n] \setminus$ and $i \in S$;
(3) Columns indexed by $x_i^{n_i(j)} x_j^{n_j(i)}$ for $i, j \in [n] \setminus S$ or by $x_j^{D_j}$ for $j \in [n] \setminus S$.
Let $M_{i,j}$ denote the submatrix of $M_S(f_G)$ induced by rows of type (i) and columns of type (j) from the possibilities mentioned above. By construction, $M_{2,2}$ is a $|\mathrm{cut}(S)| \times |\mathrm{cut}(S)|$ permutation matrix. On the other hand, $M_{1,3}$ and $M_{3,1}$ are non-zero row and column matrices respectively (due to the presence of the $\sum x_j^{D_j}$ monomials in f_G). All the other submatrices $M_{i,j}$ are zero matrices. Therefore, $\mathrm{Rank}(M_S(f_G)) = \mathrm{Rank}(M_{2,2}) + \mathrm{Rank}(M_{1,3}) + \mathrm{Rank}(M_{3,1}) = |\mathrm{cut}(S)| + 2$. ◀

Forward Direction: If G has cutwidth at most w, then there exist $A \in \mathrm{GL}_n(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n$ such that $f_G(A\mathbf{x} + \mathbf{b})$ has an ROABP of width at most $w + 2$ in some order.
We pick $A = I_n$ and $\mathbf{b} = 0$. By Claim 23, we have for each $S \subseteq [n]$, that $\mathrm{Rank}(M_S(f_G)) = |\mathrm{cut}(S)| + 2$. If there is a linear arrangement π that witnesses $\mathrm{cutwidth}(G) \leq w$, then by Nisan's characterization (Theorem 10), f_G has an ROABP in order π of width $\leq w + 2$.

Reverse Direction: If there exist $A \in \mathrm{GL}_n(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n$ such that $f_G(A\mathbf{x} + \mathbf{b})$ has an ROABP of width at most $w + 2$ in some order, then G has cutwidth at most w.
We first prove the following key lemma which is the analogue of Lemma 20 in the case of characteristic p:

▶ **Lemma 24.** *Suppose $A \in \mathrm{GL}_n(\mathbb{F})$ is not the product of a permutation matrix and a diagonal matrix. Then for every $\mathbf{b} \in \mathbb{F}^n$, every ROABP computing $f_G(A\mathbf{x} + \mathbf{b})$ must have width at least $|E| + 3$.*

Proof. If A is not the product of a permutation matrix and a diagonal matrix, there is a row of A, say A_j, with at least two non-zero entries. Let j be the largest index for which this holds. The linear form $l_j(\mathbf{x}) = A_j\mathbf{x} + b_j$ has support at least 2. Assume, without loss of generality, that $l_j(\mathbf{x}) = a_{jk_1}x_{k_1} + a_{jk_2}x_{k_2} + \ldots$ with $k_1 \neq k_2$ and $a_{jk_1}, a_{jk_2} \neq 0$.

The polynomial $f_G(A\mathbf{x} + \mathbf{b})$ contains the term $(l_j(\mathbf{x}))^{D_j}$. By our choice of $D_j = (p^L - 1) + (j-1)p^L$, Lucas's Theorem (Theorem 21) guarantees that $\binom{D_j}{i} \not\equiv 0 \pmod{p}$ for all $1 \leq i \leq M < D_j$. This ensures that in the expansion of $(l_j(\mathbf{x}))^{D_j}$, the coefficient of $x_{k_1}^i x_{k_2}^{D_j - i}$ is non-zero for all $1 \leq i \leq M - 1$. Note that the support of these monomials is at least 2.

The other terms in $f_G(A\mathbf{x} + \mathbf{b})$ have lower total degree or have support at most 1: For $l > j$, the term $(A_l\mathbf{x} + b_l)^{D_l}$ only involves one variable. For $l < j$, the term $(A_l\mathbf{x} + b_l)^{D_l}$ has total degree $D_l < D_j$. The edge terms have total degree at most $6 < D_j$. Thus, the analysis is dominated by $(l_j(\mathbf{x}))^{D_j}$.

Now, consider any ROABP for $f_G(A\mathbf{x} + \mathbf{b})$ in an arbitrary order π. Pick a prefix S of π that separates k_1 and k_2. The width of the ROABP is at least $\mathrm{Rank}(M_S(f_G(A\mathbf{x} + \mathbf{b})))$. The submatrix of M_S corresponding to row monomials $\{x_{k_1}^i\}_{i=1}^{M-1}$ and column monomials $\{x_{k_2}^{D_j - i}\}_{i=1}^{M-1}$ is an anti-triangular matrix of size $(M-1) \times (M-1)$ with non-zero entries on its anti-diagonal. Its rank is therefore $M - 1 \geq |E| + 3$. Since π was arbitrary, this holds for any order. ◀

We use Lemma 24 to prove the reverse direction. Suppose there exist $A \in \mathrm{GL}_n(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n$ such that $f_G(A\mathbf{x} + \mathbf{b})$ has ROABP width at most $w + 2$. Combining with Lemma 24 the reasoning provided in the proof of Theorem 19 we may assume that A is the identity matrix and that $\mathbf{b} = \mathbf{0}$. By Claim 23, we have

$$\mathrm{cutwidth}(G) + 2 = \mathrm{RO\text{-}width}(f_G(\mathbf{x})) \leq w + 2,$$

which implies $\mathrm{cutwidth}(G) \leq w$. This completes the soundness argument and the proof of the theorem. ◀

5 Hardness of Order-Finding for Quadratic Forms

The NP hardness reduction for ROABP order finding provided by [5] embeds the cut sizes of the graph into the ranks of the corresponding Nisan matrices. Instead, we can also embed the *cut-rank* information into the Nisan matrices. Let G be a graph and S be a subset of it's vertices. For a field $\mathbb{F}$, cut-rank$_{\mathbb{F}}(S)$ is defined as the rank over $\mathbb{F}$ of the $0 - 1$ matrix whose rows are indexed by vertices of G in S, columns by vertices not in S, and the (u, v)-th entry is 1 iff $\{u, v\}$ is an edge of G. This leads us to our next reduction, which gives NP-Hardness of order finding for quadratic forms. This is an improvement over [5], who give hardness for degree 6 polynomials).

▶ **Theorem 25.** *DenseROwidth-2 is NP-hard over any field $\mathbb{F}$.*

Proof. We reduce from the linear rank-width problem over $\mathbb{F}$. Let $(G = ([n], E), w)$ be an instance of the linear rank-width problem. Construct the polynomial f_G over $\mathbb{F}$ defined as

$$f_G = \sum_{\{i,j\} \in E} x_i x_j + \sum_{i=1}^{n} x_i^2$$

The proof of NP-hardness follows from the next claim.

▷ **Claim 26.** Let $S \subseteq [n]$ be such that $1 \leq |S| \leq n-1$. Then $\text{Rank}(M_S(f_G)) = \text{cut-rank}_{\mathbb{F}}(S) + 2$

Proof. The proof follows by inspecting the structure of the matrix $M_S(f_G)$. Since f_G is a quadratic form, we only need to consider monomials of degree at most 2. We partition the rows and columns of the Nisan matrix $M_S(f_G)$ by the degree of the indexing monomials and obtain the following block structure for $M_S(f_G)$

$$M_S(f_G) \cong \begin{pmatrix} M_{0,0} & M_{0,1} & M_{0,2} \\ M_{1,0} & M_{1,1} & M_{1,2} \\ M_{2,0} & M_{2,1} & M_{2,2} \end{pmatrix}$$

Here, $M_{i,j}$ is the submatrix induced by row monomials of degree i and column monomials of degree j. First, note that $M_{1,1}$ is exactly the cut-rank matrix for the subset S. Also, note that $M_{2,0}$ and $M_{0,2}$ are non-zero (because of the x_i^2 terms) column and row matrices respectively, and so they have rank 1. Finally, note that the rest of the $M_{i,j}$ are all $\mathbf{0}$. Therefore, $\text{Rank}(M_S(f_G)) = \text{Rank}(M_{0,2}) + \text{Rank}(M_{2,0}) + \text{Rank}(M_{1,1}) = \text{cut-rank}_{\mathbb{F}}(S) + 2$ ◄

In particular, this implies that RO-width(f_G) is linear rank-width of G plus 2. ◄

---- **References** ----

1 Christoph Ambühl, Monaldo Mastrolilli, and Ola Svensson. Inapproximability results for maximum edge biclique, minimum linear arrangement, and sparsest cut. *SIAM Journal on Computing*, 40(2):567–596, 2011. `arXiv:https://doi.org/10.1137/080729256`, `doi:10.1137/080729256`.

2 Per Austrin, Toniann Pitassi, and Yu Wu. Inapproximability of treewidth, one-shot pebbling, and related layout problems. In Anupam Gupta, Klaus Jansen, José Rolim, and Rocco Servedio, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 13–24, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

3 O. Baraskar, A. Dewan, C. Saha, and P. Sinha. NP-hardness of testing equivalence to sparse polynomials and to constant-support polynomials. In *Proceedings of the 51st International Colloquium on Automata, Languages, and Programming (ICALP)*, 2024.

4 Omkar Baraskar, Agrim Dewan, and Chandan Saha. Testing equivalence to design polynomials. In Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov, editors, *41st International Symposium on Theoretical Aspects of Computer Science, STACS 2024, March 12-14, 2024, Clermont-Ferrand, France*, volume 289 of *LIPIcs*, pages 9:1–9:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. URL: `https://doi.org/10.4230/LIPIcs.STACS.2024.9`, `doi:10.4230/LIPICS.STACS.2024.9`.

5 V. Bhargava, P. Dutta, S. Ghosh, and A. Tengse. The complexity of order-finding for roabps. arXiv preprint arXiv:2411.18981, 2024. `arXiv:2411.18981`.

6 Vishwas Bhargava and Sumanta Ghosh. Improved hitting set for orbit of roabps. *computational complexity*, 31(2):15, Oct 2022. `doi:10.1007/s00037-022-00230-9`.

7 J. Díaz, J. Petit, and M. Serna. A survey of graph layout problems. *ACM Computing Surveys*, 34(3):313–356, 2002.

8 Nikhil Gupta, Chandan Saha, and Bhargav Thankey. *Equivalence Test for Read-Once Arithmetic Formulas*, pages 4205–4272. URL: `https://epubs.siam.org/doi/abs/10.1137/1.9781611977554.ch162`, `arXiv:https://epubs.siam.org/doi/pdf/10.1137/1.9781611977554.ch162`, `doi:10.1137/1.9781611977554.ch162`.

9   Dori Medini and Amir Shpilka. Hitting sets and reconstruction for dense orbits in vp_{e}
       and ΣΠΣ circuits. In Valentine Kabanets, editor, *36th Computational Complexity Conference,*
       CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference), volume 200
       of *LIPIcs*, pages 19:1–19:27. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. URL:
       `https://doi.org/10.4230/LIPIcs.CCC.2021.19`, `doi:10.4230/LIPICS.CCC.2021.19`.

10   N. Nisan. Lower bounds for non-commutative computation. In *Proceedings of the 23rd Annual*
       ACM Symposium on Theory of Computing (STOC), pages 410–418, 1991.

11   S. Oum. Rank-width: Algorithmic and structural results. *Discrete Applied Mathematics*,
       231:15–24, 2017.

12   Chandan Saha and Bhargav Thankey. Hitting sets for orbits of circuit classes and polynomial
       families. *ACM Trans. Comput. Theory*, 16(3), September 2024. `doi:10.1145/3665800`.