

Lower Bounds for Symmetric Circuits for the Determinant

Anuj Dawar  

Department of Computer Science and Technology, University of Cambridge, UK

Gregory Wilsenach 

Department of Computer Science and Technology, University of Cambridge, UK

Abstract

Dawar and Wilsenach (ICALP 2020) introduce the model of symmetric arithmetic circuits and show an exponential separation between the sizes of symmetric circuits for computing the determinant and the permanent. The symmetry restriction is that the circuits which take a matrix input are unchanged by a permutation applied simultaneously to the rows and columns of the matrix. Under such restrictions we have polynomial-size circuits for computing the determinant but no subexponential size circuits for the permanent. Here, we consider a more stringent symmetry requirement, namely that the circuits are unchanged by arbitrary even permutations applied separately to rows and columns, and prove an exponential lower bound even for circuits computing the determinant. The result requires substantial new machinery. We develop a general framework for proving lower bounds for symmetric circuits with restricted symmetries, based on a new support theorem and new two-player restricted bijection games. These are applied to the determinant problem with a novel construction of matrices that are bi-adjacency matrices of graphs based on the CFI construction. Our general framework opens the way to exploring a variety of symmetry restrictions and studying trade-offs between symmetry and other resources used by arithmetic circuits.

2012 ACM Subject Classification Theory of computation → Circuit complexity; Theory of computation → Algebraic complexity theory

Keywords and phrases arithmetic circuits, symmetric arithmetic circuits, Boolean circuits, symmetric circuits, permanent, determinant, counting width, Weisfeiler-Leman dimension, Cai-Fürer-Immerman constructions

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.52

Related Version *Full Version:* <https://arxiv.org/abs/2107.10986>

Funding Research funded by EPSRC grant EP/S03238X/1.

Acknowledgements We are grateful to Albert Atserias for useful discussions on the construction in Section 5.2

1 Introduction

The central open question in the field of arithmetic circuit complexity is the separation of the complexity classes VP and VNP. Sometimes known as Valiant’s conjecture, this is also described as the algebraic analogue of the P vs. NP question. The conjecture is equivalent to the statement that the permanent of a matrix cannot be expressed by a family of polynomial-size arithmetic circuits. Lower bounds on the size of circuits computing the permanent have been established by imposing certain restrictions on the circuit model. For instance, it is known that there is no subexponential family of *monotone* circuits for the permanent [21] and an exponential lower bound for the permanent is also known for *depth-3* arithmetic circuits [14]. In both these cases, the lower bound obtained for the permanent also



© Anuj Dawar and Gregory Wilsenach;

licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 52; pp. 52:1–52:22

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

applies to the determinant, which is known to be in VP^1 . In that sense, the lower bounds tell us more about the weakness of the model resulting from the restriction than the difficulty of computing the permanent.

In this paper we focus on another restriction on arithmetic circuits introduced relatively recently: that of symmetry [11]. This has been shown to give an exponential separation in the size of circuits computing the permanent and the determinant. We first introduce this restriction. Given a field \mathbb{F} and a set of variables X , let C be a circuit computing a polynomial p in $\mathbb{F}[X]$. For a group G acting on the set X , we say that C is G -symmetric if the action of any element $g \in G$ can be extended to an automorphism of C . Of course, this makes sense only when the polynomial p itself is invariant under the action of G . For example, both the permanent and the determinant are polynomials in a *matrix* of variables $X = \{x_{ij} \mid 1 \leq i, j \leq n\}$. Let G be the group \mathbf{Sym}_n acting on X by the action whereby $\pi \in G$ takes x_{ij} to $x_{\pi(i)\pi(j)}$. We call this the *square symmetric* action. It corresponds to arbitrary permutations applied simultaneously to the rows and columns of the matrix. It is shown in [11] that there are polynomial-size G -symmetric circuits computing the determinant, but any family of G -symmetric circuits for computing the permanent has exponential size. Both results are established for any field of characteristic zero.

The choice of the group action G in these results is natural, but certainly not the only possibility. The lower bound immediately applies to any larger group of symmetries of the polynomial as well. Consider, for instance the action of the group $\mathbf{Sym}_n \times \mathbf{Sym}_n$ on X whereby (π, σ) takes x_{ij} to $x_{\pi(i)\sigma(j)}$. We call this the *matrix symmetric* action. It corresponds to independent permutations applied to the rows and columns. The permanent is invariant under this action and the exponential lower bound for square-symmetric circuits for the permanent applies *a fortiori* to matrix-symmetric circuits as well.

In the case of the determinant, it was left open whether the polynomial upper bound obtained for square symmetric circuits could be improved by requiring larger groups of symmetries on the circuits. The most efficient algorithms for computing the determinant (based on Gaussian elimination) are not square symmetric and the polynomial upper bound is obtained by an application of Le Verrier's method [11]. It is a natural question to ask how much more stringent a symmetry requirement we can impose and still find efficient algorithms. The determinant is not matrix-symmetric like the permanent is. Let us write \mathbf{D}_n for the group of permutations of $X = \{x_{ij} \mid 1 \leq i, j \leq n\}$ which fix the determinant. This can be seen to be $D_n \times T$ where D_n is the subgroup of $\mathbf{Sym}_n \times \mathbf{Sym}_n$ of index 2 consisting of pairs (σ, π) of permutations with $\text{sgn}(\sigma) = \text{sgn}(\pi)$ and $T \cong \mathbb{Z}_2$ represents the transposition of rows and columns. We prove in the present paper that any family of \mathbf{D}_n -symmetric circuits computing the determinant must have exponential size. Indeed, our lower bound is proved even for the subgroup of D_n given by $\mathbf{Alt}_n \times \mathbf{Alt}_n$.

Proving this lower bound requires substantially different methods than those of other results, and developing these methods is a central thrust of this paper. The exponential lower bound for square-symmetric circuits for the permanent is established in [11] by proving a lower bound on the *orbit size* of Boolean circuits computing the permanent of a $\{0, 1\}$ -matrix. Here, the orbit size of a circuit C is the maximal size of an orbit of a gate of C under the action of the automorphism group of C . This lower bound is proved using a connection between the orbit size of circuits computing a graph parameter and the *counting width* of

¹ Note that the determinant is not itself monotone in the usual sense, but there is a suitably adapted notion of monotonicity called *syntactic monotonicity* in [22] with respect to which the determinant does have circuits, but not subexponential size ones.

the parameter as established in [1]. To be precise, it is shown that if a graph parameter has linear counting width, i.e. it distinguishes graphs on n vertices which are not distinguished by $\Omega(n)$ -dimensional Weisfeiler-Leman equivalences, then it cannot be computed by symmetric circuits of subexponential orbit size. The Weisfeiler-Leman equivalences are well-studied approximations of the graph isomorphism relation, graded by dimension (see [15, Section 3.5] for an introduction). The equivalences have many equivalent characterizations arising in combinatorics, algebra, logic and linear optimization. The term counting width comes from the connection with counting logic (see [9]). The main technical ingredient in the lower bound proof in [11] is then a proof of a linear lower bound on the counting width of the number of perfect matchings in a bipartite graph.

We were able to rely on lower bounds on the counting width of graph parameters because a \mathbf{Sym}_n -invariant parameter of a $\{0, 1\}$ -matrix can be seen as a graph parameter. That is, a graph parameter that does not distinguish between isomorphic graphs is necessarily \mathbf{Sym}_n -invariant on the adjacency matrices of graphs. Similarly, the $\mathbf{Sym}_n \times \mathbf{Sym}_n$ action on a matrix can be understood as the natural invariance condition of the biadjacency matrix of a bipartite graph. On the other hand, there seems to be no natural graph structure giving rise to an $\mathbf{Alt}_n \times \mathbf{Alt}_n$ -invariance requirement on the matrices. For this reason, we develop here both a general framework for presenting and studying symmetric circuits and new methods for proving lower bounds under some of these symmetry assumptions.

The generality of this framework allows us to consider a variety of different symmetry conditions, providing both a broad vocabulary for working with these circuits and game-based characterizations of the expressive power of these various symmetric models. This opens up the possibility of studying symmetry as a resource. Our results suggest a spectrum of symmetry restrictions and it would be interesting to establish exactly where on this spectrum the boundary of efficient algorithms for the determinant lies. Similar questions can be asked about other polynomials which admit efficient evaluation. For the permanent, the natural question is how much can we relax the symmetry conditions and still prove lower bounds. This is all to say that, quite apart from the main result, we regard the framework developed here as a contribution in its own right, which lays out a landscape to explore symmetry as a resource in this area.

Table 1 summarizes what is currently known about the power of various symmetric circuit models computing the permanent and determinant. The first column is for unrestricted circuits, i.e. those symmetric under the trivial group action. The upper bound for the determinant is by an adapted Gaussian elimination algorithm [6] and the upper bound for the permanent, which in fact holds for every group in the table, is by Ryser's formula [25]. The lower bound in the first column is the trivial one. The second and fourth column state results established in [11]. There is no result for the determinant in the fourth column as the determinant is not invariant under the $\mathbf{Sym}_n \times \mathbf{Sym}_n$ action. The results in the column for $\mathbf{Alt}_n \times \mathbf{Alt}_n$ are new to this paper. In the last two columns \mathbf{D}_n and \mathbf{P}_n represent the full invariance groups (as subgroups of $\mathbf{Sym}_{n \times n}$) of the determinant and permanent respectively. The lower bounds stated in those columns follow from the ones obtained for their subgroups $\mathbf{Alt}_n \times \mathbf{Alt}_n$ and $\mathbf{Sym}_n \times \mathbf{Sym}_n$ respectively.

A more detailed discussion of some of the main innovations follows.

1. The lower bounds on counting width of graph parameters are proved using the method of *bijection games* applied to graphs based on a construction due to Cai, Fürer and Immerman [7] (we refer to this class of graph constructions as the *CFI construction*). We adapt the bijection games and show that they can be directly used to obtain lower bounds for symmetric circuits without reference to graphs or Weisfeiler-Leman equivalences.

■ **Table 1** Table of upper and lower bounds for G -symmetric circuits for the determinant and permanent, for various group actions G . Here id is meant to denote general circuits (i.e. those symmetric under the action of the trivial group).

G	$\{\text{id}\}$	Sym_n	$\text{Alt}_n \times \text{Alt}_n$	$\text{Sym}_n \times \text{Sym}_n$	D_n	P_n
Det	$O(n^3)$	$O(n^4)$ (char 0)	$2^{\Omega(n)}$ (char 0)	N/A	$2^{\Omega(n)}$ (char 0)	N/A
Perm	$O(n^2 2^n)$ $\Omega(n^2)$	$2^{\Omega(n)}$ (char 0)	$2^{\Omega(n)}$ (char $\neq 2$)	$2^{\Omega(n)}$ (char $\neq 2$)	$2^{\Omega(n)}$ (char $\neq 2$)	$2^{\Omega(n)}$ (char $\neq 2$)

2. The support theorem established in [1] and strengthened in [11] is a key tool, which we extend further. We extend the range of group actions for which it can be shown to hold.
3. The original k -pebble bijection games of Hella [18] are two-player games played on a pair of relational structures between two players called *Spoiler* and *Duplicator*. In each move of the game, Duplicator is required to provide a bijection between the two graphs. A winning strategy for Duplicator shows that the two graphs are not distinguishable in the k -dimensional Weisfeiler-Leman equivalences. We refine the games by restricting Duplicator to play bijections from a restricted set. At the same time, we generalize the game so it can be played on a more general notion of structured input rather than a relational structure. We are able to relate Duplicator winning strategies to indistinguishability by G -symmetric circuits taking the adjacency matrices as input.
4. A fourth key ingredient is the construction of matrices with distinct determinants on which we can show Duplicator winning strategies in the $\text{Alt}_n \times \text{Alt}_n$ -restricted bijection game. The two matrices are obtained as pairs of biadjacency matrices of a single bipartite graph given by the CFI construction with differing orders on the columns.
5. An important element of the construction of the matrices in (4) are bipartite 3-regular graphs which are well-connected and have an odd number of perfect matchings. We show the existence of an infinite family of such graphs in Section 5.2. This may be of independent interest. A strengthening of the conditions on the number of perfect matchings could be used to extend our lower bound to fields of positive characteristic other than two. We expand on this in Section 5.4.

Our work may be compared to that of Landsberg and Ressayre [23] who establish an exponential lower bound on the complexity of the permanent (specifically over the complex field \mathbb{C}) under an assumption of symmetry. Their lower bound is for equivariant determinantal representations of the permanent, that is those that preserve all the symmetries of the permanent function. This approach doesn't yield any lower bounds for symmetric circuits in the sense we consider here. On the other hand, lower bounds for equivariant determinantal complexity can be derived from the results in [11], albeit not ones as strong as in [23]. For a more detailed comparison of the two approaches see [11].

This paper is organized as follows. We begin with introducing the notation we need in Section 2. Symmetric circuits working on arbitrary structured inputs are defined in Section 3. The support theorem we need is given in Section 4.3. The bijection games are defined in Section 4.2 where we also establish that Duplicator winning strategies imply indistinguishability by small circuits. The main construction establishing the lower bound for the determinant is presented in Section 5. The corresponding lower bound for the permanent is given in Section 6. Many proofs are sketched or omitted entirely due to lack of space. Full details can be found in [12].

2 Background

We write \mathbb{N} for the positive integers and \mathbb{N}_0 for the non-negative integers. For $m \in \mathbb{N}_0$, $[m]$ denotes the set $\{1, \dots, m\}$. For a set X we write $\mathcal{P}(X)$ to denote the powerset of X . We write id to denote the identity function on some specified set. For $f : X \rightarrow Y$ and $S \subseteq X$ we write $f(S)$ to denote the image of S . Let $\text{Bij}(A, B)$ denote the set of bijections from A to B .

2.1 Groups

Let \mathbf{Sym}_Y and \mathbf{Alt}_Y denote the symmetric group and alternating group on the set Y . We write \mathbf{Sym}_n and \mathbf{Alt}_n to abbreviate $\mathbf{Sym}_{[n]}$ and $\mathbf{Alt}_{[n]}$, respectively. Let $\{\text{id}\}$ denote the trivial group. For groups G and H we write $H \leq G$ to denote that H is a subgroup of G . The *sign* of a permutation $\sigma \in \mathbf{Sym}_Y$ is defined so that if σ is even $\text{sgn}(\sigma) = 1$ and otherwise $\text{sgn}(\sigma) = -1$.

Let G be a group acting on a set X . We denote this as a left action, i.e. σx for $\sigma \in G$, $x \in X$. The action extends in a natural way to powers of X , the power set of X , and functions on X . We refer to all of these as the *natural action* of G on the relevant set.

A set X with the action of group G on it is called a G -set. We do not distinguish notationally between a G -set X and the underlying set of elements. Thus, we can say that if X is a G -set, the collection of functions Y^X is also a G -set with the natural action.

Let X be a G -set. Let $S \subseteq X$. Let $\mathbf{Stab}(S) := \{\sigma \in G \mid \forall x \in S \sigma x = x\}$ denote the *pointwise stabilizer* of S . Let $\mathbf{SetStab}(S) := \{\sigma \in G \mid \sigma(S) = S\}$ denote the *setwise stabilizer* of S . If $S = \{x\}$ is a singleton we omit set braces and write $\mathbf{Stab}(x)$. Note that $\mathbf{SetStab}(S)$ is the pointwise stabilizer of $\{S\}$ in the G -set $\mathcal{P}(X)$. For $x \in X$ let $\mathbf{Orb}(x) := \{\sigma(x) \mid \sigma \in G\}$ denote the *orbit* of x .

2.2 Matrices

Let A and B be finite non-empty sets. We identify matrices with rows indexed by A and columns by B that take values from some set X with functions of the form $M : A \times B \rightarrow X$. So for $a \in A$, $b \in B$, $M_{ab} = M(a, b)$. We also denote M by $(M_{ab})_{a \in A, b \in B}$, or just (M_{ab}) when the index sets are clear from context.

Let R be a commutative ring and $M : A \times B \rightarrow R$ be a matrix with $|A| = |B|$. The *permanent* of M over R is $\text{perm}_R(M) = \sum_{\sigma \in \text{Bij}(A, B)} \prod_{a \in A} M_{a\sigma(a)}$. Suppose $A = B$. The *determinant* of M over R is $\det_R(M) = \sum_{\sigma \in \mathbf{Sym}_A} \text{sgn}(\sigma) \prod_{a \in A} M_{a\sigma(a)}$. The *trace* of M over R is $\text{Tr}_R(M) = \sum_{a \in A} M_{aa}$. We omit reference to the ring when it is obvious from context. When R is a field, we write $\mathbf{rk}(M)$ to denote the *rank* of the matrix M .

We always use \mathbb{F} to denote a field and $\text{char}(\mathbb{F})$ to denote the characteristic of \mathbb{F} . For any prime power q we write \mathbb{F}_q for the finite field of order q . We are often interested in polynomials and circuits defined over a set of variables X with a natural matrix structure, i.e. $X = \{x_{ab} : a \in A, b \in B\}$. We identify X with this matrix. We also identify any function of the form $f : X \rightarrow Y$ with the $A \times B$ matrix with entries in Y defined by replacing each x_{ab} with $f(x_{ab})$.

2.3 Graphs

Given a bipartite graph $\Gamma = (V, E)$ with bipartition $V = U \cup W$, the *biadjacency matrix* A_Γ of Γ is the $U \times W$ $\{0, 1\}$ -matrix with $A_\Gamma(u, v) = 1$ if, and only if, $\{u, v\} \in E$.

A k -factor of a graph Γ is a spanning k -regular subgraph. A *perfect matching* is a 1-factor. It is well known that for a bipartite graph Γ , $\text{perm}(A_\Gamma)$ over any field of characteristic zero counts the number of perfect matchings in Γ [17] and for prime p , $\text{perm}_{\mathbb{F}}(A_\Gamma)$ for a field \mathbb{F} of characteristic p counts the number of perfect matchings in Γ modulo p .

Let $\Gamma = (V, E)$ be a graph. For $S \subseteq V$ let $N^+(S) := \{v \in V \setminus S \mid \exists s \in S, (v, s) \in E\}$. We say Γ is an α -*expander* for $\alpha \in [0, 1]$ if for every $S \subseteq V$ of size at most $|V|/2$ we have $|N^+(S)| \geq \alpha|S|$. For an introduction to expander graphs see [20]. A set S of vertices in a graph Γ is a *balanced separator* if no connected component of $\Gamma \setminus S$ contains more than half the vertices of Γ . It is easy to see that if Γ is an α -expander, then there is a constant τ such that Γ has no balanced separator of size less than $\tau|V|$.

2.4 Circuits

We give a general definition of a circuit that incorporates both Boolean and arithmetic circuits.

► **Definition 1 (Circuit).** *A circuit over the basis \mathbb{B} with variables X and values K is a directed acyclic graph with a labelling where each vertex of in-degree 0 is labelled by an element of $X \cup K$ and each vertex of in-degree greater than 0 is labelled by an element of \mathbb{B} .*

Let $C = (D, W)$, where $W \subset D \times D$, be a circuit with values K . We call the elements of D *gates*, and the elements of W *wires*. We call the gates with in-degree 0 *input gates* and gates with out-degree 0 *output gates*. We call those input gates labelled by elements of K *constant gates*. We call those gates that are not input gates *internal gates*. For $g, h \in D$ we say that h is a *child* of g if $(h, g) \in W$. We write $\text{child}(g)$ to denote the set of children of g . We write C_g to denote the sub-circuit of C rooted at g . Unless otherwise stated we always assume a circuit has exactly one output gate.

We refer the reader to [12] for more detail. For more details on arithmetic circuits see [26] and for Boolean circuits see [27].

3 Symmetric Circuits

Complexity theory is often concerned with computation models that take as input binary strings. In practice these strings are almost always taken to encode some structured input (e.g. graphs, matrices, numbers, etc.). In order to study the symmetries that arise from these structures we forgo this encoding. More precisely, we consider computation models such as circuits whose inputs are themselves functions of type K^X where we think of X as a set of variables and K a domain of values that the variables can take. The set X may have some further structure to reflect the intended structured input, but no more. In particular, we do not assume that X is linearly ordered. For example, if $X = V^2$ and $K = \{0, 1\}$ then the elements of $\{0, 1\}^X$ may be naturally interpreted as directed graphs over the vertex set V . Or, with the same X , if we let $K = \mathbb{F}$, we can think of the elements of K^X as matrices over \mathbb{F} with rows and columns indexed by V .

The symmetries of interest for a given class of structures correspond to group actions on X , which lift to actions on K^X . In this section we introduce the definitions of G -symmetric functions, i.e. functions which are invariant under the action of G on its input, and G -symmetric circuits, which are circuits computing G -symmetric functions but where the structure of the circuit itself and not just the output is invariant under the action of G . The definitions are variations and generalizations of those from [11]. We illustrate them with examples.

3.1 Group Actions and Symmetric Functions

► **Definition 2.** *For a group G acting on the domain of a function F we say F is G -symmetric if for every $\sigma \in G$, $\sigma F = F$. We omit mention of the group when it is obvious from context.*

We are interested in functions of type $K^X \rightarrow K$ with some group G acting on X , which then induces an action on K^X . We think of elements of K^X as “generalized structures”, and define notions of homomorphism and isomorphism below. We first consider some examples. Note that whenever H is a subgroup of G , then any G -symmetric function is also H -symmetric. Every function is $\{\text{id}\}$ -symmetric.

► **Example 3.**

1. The elementary symmetric polynomial of degree k in the set of variables X is the polynomial: $e_k(X) = \sum_{S \in \binom{X}{k}} \prod_{x \in S} x$. For any field \mathbb{F} , $e_k(X)$ defines a function $e_k^{\mathbb{F}} : \mathbb{F}^X \rightarrow \mathbb{F}$ which is \mathbf{Sym}_X -symmetric.
2. If $X = \{x_{ij} \mid 1 \leq i, j \leq n\}$ is a *matrix* of variables, then the trace $\text{tr}(X)$, determinant $\det(X)$ and permanent $\text{perm}(X)$ are polynomials that define, for any field \mathbb{F} , functions of type \mathbb{F}^X which are \mathbf{Sym}_n -symmetric where the group action is defined simultaneously on both coordinates.

Let G and H be groups. An *isomorphism* from the G -set X to H -set Y is a pair of functions (f, ϕ) where $f : X \rightarrow Y$ is a bijection and $\phi : G \rightarrow H$ is a group isomorphism such that for each $x \in X$ and $\pi \in G$, $f(\pi x) = \phi(\pi)f(x)$. Let $M : X \rightarrow K$ with X a G -set and let $N : Y \rightarrow K$ with Y an H -set. An *isomorphism* from (M, G) to (N, H) is an isomorphism $(f, \phi) : (X, G) \rightarrow (Y, H)$ such that $N \circ f = M$. We omit mention of the groups and refer just to an isomorphism from M to N when the groups are clear from context.

Let G be a group acting on X and $F : K^X \rightarrow L$. We are usually interested in such functions up to isomorphism. Let $M : Y \rightarrow Z$ and H be a group acting on Y such that (X, G) and (Y, H) are isomorphic. Then we abuse notation and sometimes write $F(M)$ to denote $F(M \circ f)$ for some isomorphism $f : X \rightarrow Y$.

3.2 Symmetric Circuits

We next define the notion of a symmetric circuit as it appears in [11]. These circuits take as input functions of the form $M : X \rightarrow K$, where X is a G -set, and are symmetric in the sense that the computation itself, not just the value of the output, remains unchanged under the action of G . We first need to formalize what it means for a permutation in G to act on the gates of a circuit, and for this we define the notion of a circuit automorphism extending a permutation.

► **Definition 4 (Circuit Automorphism).** Let $C = (D, W)$ be a circuit over the basis \mathbb{B} with variables X and values K . For $\sigma \in \mathbf{Sym}_X$, we say that a bijection $\pi : D \rightarrow D$ is an automorphism extending σ if for every gate g in D we have that (i) if g is a constant gate then $\pi(g) = g$, (ii) if g is a non-constant input gate then $\pi(g) = \sigma(g)$, (iii) if $(h, g) \in W$ is a wire, then so is $(\pi h, \pi g)$, and (iv) if g is labelled by $b \in \mathbb{B}$, then so is πg .

We say that a circuit C with variables X is *rigid* if for every permutation $\sigma \in \mathbf{Sym}(X)$ there is at most one automorphism of C extending σ . The argument used to prove [10, Lemma 5.5] suffices to show that any symmetric circuit may be transformed into an equivalent rigid one in time polynomial in the size of the circuit. As such, when proving lower bounds we often assume the circuit is rigid without a loss of generality.

We are now ready to define the key notion of a symmetric circuit.

► **Definition 5 (Symmetric Circuit).** Let G be a group acting on a set X and C be a circuit with variables X . We say C is a G -symmetric circuit if for every $\sigma \in G$ the action of σ on X extends to an automorphism of C .

The following can be shown via a straight-forward induction.

► **Proposition 6.** *Let C be a G -symmetric circuit. Then C defines a G -symmetric function.*

4 Games and Supports

Hella's bijection game [18] is a two-player game played on relational structures, such as graphs. It was defined to demonstrate indistinguishability of structures in logics with counting and extensions thereof. The indistinguishability relations it defines on graphs are closely tied to Weisfeiler-Leman equivalences [7]. The games are played on a pair of structures A and B by two players called Spoiler and Duplicator. Spoiler aims to show that the two structures are different while Duplicator pretends they are the same. We associate with each structure a sequence of k pebbles which are placed in the course of the game on elements of the two structures. The game proceeds in a sequence of rounds. The number of rounds can be greater than k and so pebbles can be moved from one element to another during the course of the game. At each round, Spoiler chooses a pebble p_i ($i \in [k]$) from A and the matching pebble q_i from B . Duplicator provides a bijection h between the two structures. Spoiler then chooses an element a of A on which to place p_i and q_i is placed on $h(a)$. In each round, Duplicator must ensure that the partial map between the two structures defined by the placement of the pebbles is a partial isomorphism, otherwise Spoiler wins. For more details on this game see [16].

The connection between bijection games and symmetric circuits is first made in [1] which showed a connection between the expressive power of counting logics and symmetric Boolean circuits in the threshold basis \mathbb{B}_t . This leads to the suggestion (made in [8]) of using bijection games as a tool directly to prove circuit lower bounds. The main contribution of this section is the generalization of these bijection game in two different direction, as well as a series of results establishing how this tool can be used to prove more general circuit lower bounds.

We noted earlier that we may think of functions on G -sets as some sort of generalised structure. The development of the theory of bijection games (and supports) requires us to further restrict our attention to the case where G is a subgroup of some symmetric group. The domain of the symmetric group corresponds in some sense to the universe of the structure in question. We call these *indexed functions*, and discuss them in Section 4.1.

We also develop in Section 4.3 a theory of supports. The support of a gate in a G -symmetric circuit for $G \leq \mathbf{Sym}_A$ is a subset of A which determines both the evaluation of a gate and its orbit. We establish in Section 4.5 the support theorem, which connects the minimum size of these supports with the minimum size of the orbits of a gate (and so the size of the circuit). We show in Section 4.4 that if Duplicator has a winning strategy in the game with $2k$ pebbles on a pair of indexed functions then these functions cannot be distinguished by any pair of G -symmetric circuits with supports of size at most k . In Section 4.5 we combine this result with the support theorem to show that to prove exponential lower bounds it suffices to establish a linear lower bound on the number of pebbles needed by Spoiler.

4.1 Indexed Functions

► **Definition 7.** *Let A be a set, $G \leq \mathbf{Sym}_A$, and X be a G -set. We call the triple (X, A, G) an indexed set. We call a triple (F, A, G) , where F is a function on X , an indexed function.*

Let (X, A, G) and (Y, B, H) be indexed sets. An *isomorphism* from (X, A, G) and (Y, B, H) is a pair of bijections $f : X \rightarrow Y$ and $g : A \rightarrow B$ such that for all $\pi \in G$ and $x \in X$, $f(\pi x) = (g\pi g^{-1})f(x)$.

Let $(M : X \rightarrow K, A, G)$ and $(N : Y \rightarrow K, B, H)$ be indexed functions. An *isomorphism* from (F, A, G) to (G, B, H) is an isomorphism (f, g) from (X, A, G) to (Y, B, H) such that $N \circ f = M$.

All of the structures discussed so far may be identified with indexed functions. We identify a (directed) graph (V, E) with the indexed function $(E : V^2 \rightarrow \{0, 1\}, V, \mathbf{Sym}_V)$ and a bipartitioned graph (V, U, E) with the indexed function $(E : V \times U \rightarrow \{0, 1\}, V \uplus U, \mathbf{Sym}_V \oplus \mathbf{Sym}_U)$. The group actions chosen ensure notions of isomorphism that correspond with the usual notions of isomorphism for graphs and bipartitioned graphs.

We can similarly identify $n \times n$ matrices over a field \mathbb{F} with structured functions of the form $(M : [n] \times [n] \rightarrow \mathbb{F}, [n] \uplus [n], G)$, for some group G . Unlike for structures, there are a number of different matrix similarity notions one might consider, which correspond to different choices for G . If $G = \mathbf{Sym}_n$ then isomorphism corresponds to equivalence under simultaneous row and column permutations and if $G = \mathbf{Sym}_n \times \mathbf{Sym}_n$ then isomorphism corresponds to equivalence under separate row and column permutations.

4.2 Bijection Games

In this subsection we introduce our generalization of Hella's bijection game. We stated previously that the generalization is in two directions. The first is that we allow the game to be played on arbitrary indexed functions, rather than just graphs or relational structures. The second is that we only allow the duplicator to play from a given set of bijections. We usually define this set by composing an initial bijection with a group of permutations. We recover the usual requirement in the bijection game by just taking this group to be the full symmetric group.

So, indexed functions are our notion of structured input and we first introduce a notion of partial isomorphism for such objects. This is necessary for stating the winning condition in the bijection game that follows. We first define the notion of a *lift*.

► **Definition 8.** Let (X, Y, G) be an indexed set. For $S \subseteq Y$ we define the lift of S , denoted X_S , to be the set $\{x \in X \mid \mathbf{Stab}(S) \leq \mathbf{Stab}(x)\}$.

For the purposes of the next definition, we introduce some notation. Suppose A is a G -set and $S \subseteq A$. Let $P = \mathbf{Stab}(A \setminus S)$ be the pointwise stabilizer of the complement of S and note that $P \leq \mathbf{SetStab}(S)$. We can identify P with a subgroup \hat{P} of \mathbf{Sym}_S , namely the group of permutations $\pi \in \mathbf{Sym}_S$ which, when extended with the identity on $A \setminus S$ are in P . We call this subgroup of \mathbf{Sym}_S the S -restriction of G and denote it $\mathbf{Rest}_G(S)$. We drop the subscript G when it is clear from context.

► **Definition 9.** Let $(M : X \rightarrow K, A, G)$ and $(N : Y \rightarrow K, B, H)$ be indexed functions. Let $C \subseteq A$, $D \subseteq B$, and $g : C \rightarrow D$ be a bijection. We say that g induces a partial isomorphism if there exists f such that (f, g) is an isomorphism from $(M|_{X_C}, C, \mathbf{Rest}(C))$ to $(N|_{X_D}, D, \mathbf{Rest}(D))$.

We can recover the usual notion of a partial isomorphism between graphs as a special case. Let $\Gamma = (V, E)$ and $\Delta = (U, F)$ be directed graphs and $(E : V^2 \rightarrow \{0, 1\}, V, \mathbf{Sym}_V)$ and $(F : U^2 \rightarrow \{0, 1\}, U, \mathbf{Sym}_U)$ be their respective indexed functions. Let $A \subseteq V$ and $B \subseteq U$. The lifts of A and B are $X_A = \{(x, y) \mid x, y \in A\}$ and $X_B = \{(x, y) \mid x, y \in B\}$. Also, $\mathbf{Rest}(A) \cong \mathbf{Sym}_A$ and $\mathbf{Rest}(B) \cong \mathbf{Sym}_B$. Then $E|_{X_A}$ is just the indexed function representing the induced subgraph $\Gamma[A]$ and $F|_{X_B}$ the indexed function representing $\Delta[B]$. The bijection $g : A \rightarrow B$ induces a partial isomorphism from E to F if, and only if, g is an isomorphism from $\Gamma[A]$ to $\Delta[B]$.

With this, we are ready to define the bijection game on indexed functions. We define it very generally, parameterized by some set of bijections. We then specialize this to the case of symmetry groups in order to apply it. The game is played by two players Spoiler and Duplicator on a pair of indexed functions, using a set of *pebbles*. During the course of the game, the pebbles are placed on elements of the indexing sets. Where it does not cause confusion, we do not distinguish notationally between the pebbles and the elements on which they are placed.

► **Definition 10.** *Let $(M : X \rightarrow K, A, G)$ and $(N : Y \rightarrow K, B, H)$ be indexed functions. Let T be a set of bijections from A to B and let $k \in \mathbb{N}$. The (T, k) -bijection game on (M, N) is defined as follows. The game is played between two players called the Spoiler and Duplicator using two sequences of pebbles a_1, \dots, a_k and b_1, \dots, b_k . A round of the game is defined as follows:*

1. *Spoiler picks a pair of pebbles a_i and b_i ,*
2. *Duplicator picks a bijection $\gamma \in T$ such that for each $j \neq i$, $\gamma(a_j) = b_j$, and*
3. *Spoiler chooses some $a \in A$ and places a_i on a and b_i on $\gamma(a)$.*

Spoiler has won the game at the end of the round if the bijection taking a_1, \dots, a_k to b_1, \dots, b_k does not induce a partial isomorphism. We say that Duplicator has a winning strategy for the (T, k) -bijection game if it has a strategy to play the game forever without Spoiler winning.

We are interested in the case when the set of bijections is generated by composing a single bijection with all of the permutations of a group. For a group $G \leq \mathbf{Sym}_A$ and bijection $\alpha : A \rightarrow B$ let $T(G, \alpha) := \{\alpha \circ \pi \mid \pi \in G\}$.

We recover the ordinary bijection game on graphs by taking $X = Y = [n]^2$, $G = H = \mathbf{Sym}_n$, and α to be id, for instance. Note, in this case it does not matter which permutation we take α to be, as composition with G yields all permutations. The presence of α is significant when G is a proper subgroup of \mathbf{Sym}_n . In this case, T is a coset of G and the choice of α determines which coset. This is noteworthy when we play the game on isomorphic graphs. In the ordinary bijection game, if two graphs are isomorphic, then Duplicator has a winning strategy by always playing the isomorphism. In the $(T(G, \alpha), k)$ bijection game, the existence of an isomorphism does not guarantee a Duplicator winning strategy, as the isomorphism may not be present in the set $T(G, \alpha)$. This is just the case in the application in Section 5.

4.3 Supports

Lower bounds for symmetric circuits rely on the notion of a *support*. We define the notion formally below but it is worthwhile developing an intuition. If we have a G -symmetric circuit C then the function computed by C is invariant under permutations in G . This is not the case for individual gates g in C other than the output gate: applying a permutation $\pi \in G$ might yield a different function at g . But, by the symmetry condition, there is then another gate g^π which computes this other function. If the circuit is small, the orbit of g is small and thus the stabilizer group of g is large. That is, for many π we have $g = g^\pi$. What the support theorem tells us is that in this case, there is a small subset S (which we call the *support* of g) of the permutation domain of G such that the function computed at g only depends on S . This is in the sense that permutations that only move elements of the permutation domain outside of S do not change the function computed at g . This support theorem can be proved as long as the group G is, in a sense, large enough. We now define the notion of a support formally and prove the relationship between support size and orbit size in Section 4.4.

► **Definition 11.** Let X be a G -set. We say that $S \subseteq X$ is a support of G if $\mathbf{Stab}(S) \leq G$.

We extend this notion to group actions. That is, we consider a group G , which is defined as a permutation group on some domain Y to act on a set X possibly different from Y . A key example is the action of \mathbf{Sym}_n on the set $X = [n] \times [n]$ or on the collection of matrices $M : X \rightarrow \{0, 1\}$. We want to define the support of an object $x \in X$ as a collection of elements in Y such that fixing those elements under the action of G , fixes x . This is formalized below.

► **Definition 12.** Let (X, Y, G) be an indexed set. We say that a set $S \subseteq Y$ is a support of $x \in X$ if it is a support of $\mathbf{Stab}(x)$.

Note that S is a support of x just in case x is in the lift of S .

Let (X, Y, G) be an indexed set. Let $\mathbf{max-orbit}(X)$ be the maximum size of the orbit of x over all $x \in X$. For $x \in X$ let $\mathbf{min-supp}(x)$ be the minimum size of a support of x . Let $\mathbf{max-supp}(X)$ be the maximum of $\mathbf{min-supp}(x)$ over all $x \in X$.

We note the following general result on supports.

► **Lemma 13** ([3, Lemma 26]). Let $G \leq \mathbf{Sym}_Y$ and let $A, B \subseteq Y$ be supports of G . If $A \cup B \neq Y$ then $A \cap B$ is a support of G .

Let (X, Y, G) be an indexed set. From Lemma 13 we have for $x \in X$ that if $\mathbf{min-supp}(x) < |Y|/2$ then x has a unique minimal size support. We call this the *canonical support* of x and denote it by $\mathbf{sp}(x)$.

We now specialise our discussion to circuits. Let $C = (D, W)$ be a rigid G -symmetric circuits, where $G \leq \mathbf{Sym}_n$ for some natural number n . Then $(D, [n], G)$ is an indexed set. In this way we can speak of the supports and orbits of a gate. We abuse notation slightly and write $\mathbf{max-orbit}(C)$ and $\mathbf{max-supp}(C)$ to denote $\mathbf{max-orbit}(D)$ and $\mathbf{max-supp}(D)$, respectively.

4.4 Playing Games on Circuits

We are now ready to prove the first major theorem of this section. This links the number of pebbles in a bijection game with the size of the support. Structures in which Duplicator has a $2k$ -pebble winning strategy cannot be distinguished by symmetric circuits with supports limited to size k . The statement of the theorem and argument used generalize that in [8].

► **Theorem 14.** Let (X, A, G) be an indexed set. Let C be a G -symmetric circuit with values from K and variables X . Let $M : X \rightarrow K$ and $N : X \rightarrow K$. Let k be the maximum size of a support in C . If Duplicator has a winning strategy for the $(T(G, \text{id}), 2k)$ -bijection game played on (M, A, G) and (N, A, G) then $C[M] = C[N]$.

4.5 Bounds on Supports

The main result of this subsection establishes that if a family of G -symmetric circuits has subexponential size orbits than it has sublinear size supports. We prove this specifically for the case when G is an alternating group. The argument extends easily to cases where G contains a large alternating group, and we derive one such instance in Corollary 17. The proof relies on a standard fact about permutation groups, attributed to Jordan and Liebeck, that translates a bound on orbit size to a bound on support size. To understand this, suppose g is a gate with orbit size (relative to \mathbf{Alt}_n) bounded by $\binom{n}{k}$. Then by the orbit-stabilizer theorem, this is equivalent to $[\mathbf{Alt}_n : \mathbf{Stab}(g)] \leq \binom{n}{k}$. One way for $\mathbf{Stab}(g)$ to have small index in this way is for it to always contain a large alternating group. That is $\mathbf{Stab}(g)$ contains the alternating group restricted to $n - k$ elements, or equivalently g has a support of size at most k . Theorem 15 asserts that indeed this is the only way.

► **Theorem 15** ([13], Theorem 5.2B). *Let Y be a set such that $n := |Y| > 8$, and let k be an integer with $1 \leq k \leq \frac{n}{4}$. Suppose that $G \leq \mathbf{Alt}_Y$ has index $[\mathbf{Alt}_Y : G] < \binom{n}{k}$ then there exists $X \subset Y$ with $|X| < k$ such that $\mathbf{Stab}_{\mathbf{Alt}_Y}(X) \leq G$.*

We derive from Theorem 15 the following asymptotic relationship between orbit and support size. An analogous version of this with respect to the symmetric group is stated in [11] and the proof is essentially the same.

► **Theorem 16.** *Let (C_n) be a family of rigid \mathbf{Alt}_n -symmetric circuits. If $\mathbf{max-orbit}(C_n) = 2^{o(n)}$ then $\mathbf{max-supp}(C_n) = o(n)$.*

The following corollary establishes the analogue of Theorem 16 needed to prove our lower bounds for $\mathbf{Alt}_n \times \mathbf{Alt}_n$ -symmetric circuits.

► **Corollary 17.** *Let $(C_n)_{n \in \mathbb{N}}$ be such that for each n , C_n is defined over the matrix of variables $X_n = \{x_{i,j} \mid i, j \in [n]\}$ and C_n is a rigid $\mathbf{Alt}_n \times \mathbf{Alt}_n$ -symmetric circuit. If $\mathbf{max-orbit}(C_n) = 2^{o(n)}$ then $\mathbf{max-supp}(C_n) = o(n)$.*

We now combine these results along with Theorem 14 to establish the crucial connection between bijection games and exponential lower bounds for symmetric circuits. We prove the result for the particular case of interest to us in this paper, namely for $\mathbf{Alt}_n \times \mathbf{Alt}_n$ -symmetric circuits taking as input $n \times n$ -matrices, but note that it holds more generally.

► **Theorem 18.** *Let K be a set. For each $n \in \mathbb{N}$ let $G_n = \mathbf{Alt}_n \times \mathbf{Alt}_n$, and X_n be a G_n -set. Let $P : K^X \rightarrow K$ be a G -symmetric function. Suppose there exists a function $t(n) = O(n)$ such that for all $n \in \mathbb{N}$ there exists $M_{t(n)}, N_{t(n)} : X_{t(n)} \rightarrow K$ such that $P(M_{t(n)}) \neq P(N_{t(n)})$ and Duplicator has a strategy to win the $(T(G_n, \text{id}), n)$ -bijection game played on $(M_n, [n] \uplus [n], G_n)$ and $(N_n, [n] \uplus [n], G_n)$. Then there is no family of G_n -symmetric circuits that computes P and has size $2^{o(n)}$.*

Proof. From Theorem 14 any G_n -symmetric circuit C_n that has $\mathbf{max-supp}(C_n) \leq n/2$ must have that $C[M_{t(n)}] = C[N_{t(n)}]$, and so cannot compute P . It follows then that any family of G_n -symmetric circuits that computes P must have $\mathbf{max-supp}(C_n) = \Omega(n)$ and so from Corollary 17 cannot have orbits of size $2^{o(n)}$, and hence cannot have size $2^{o(n)}$. ◀

These games on matrices are very similar to the ordinary bijection games played on graphs. If we restrict our attention to $\{0, 1\}$ -valued functions on some domain $\{x_{ij} \mid i, j \in [n]\}$ then we may think of these games as being played on bipartite graphs, and differing from Hella's game in two respects. First, the existence of the partial isomorphism condition in this game is equivalent to the existence of an ordinary partial isomorphism between graphs except with the additional requirement that the bipartition is preserved. Second, Duplicator is restricted to choose only those bijections that preserve the parts and correspond to a pair of even permutations acting on each part separately.

Notice that both the definition of the bijection games and Theorem 14 place almost no restriction on the group actions considered. The link between the number of pebbles in the game and the size of the support is robust. However, the application in Theorem 18 is for a severely limited group action. This is because the link between support size and orbit size proved in Theorem 16 requires the presence of a large alternating group.

5 Lower Bound for the Determinant

We now deploy the machinery we have developed to prove the main lower bound result of this paper.

► **Theorem 19** (Main Theorem). *Let \mathbb{F} be a field of characteristic 0. There is no family of $\mathbf{Alt}_n \times \mathbf{Alt}_n$ -symmetric circuits $(C_n)_{n \in \mathbb{N}}$ over \mathbb{F} of size $2^{o(n)}$ computing the determinant over \mathbb{F} .*

To prove Theorem 19 we need to construct for each k , a pair of $n \times n$ $\{0, 1\}$ -matrices M_k and N_k with $n = O(k)$, $\det(M_k) \neq \det(N_k)$ and such that Duplicator has a winning strategy in the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \text{id}), k)$ -bijection game played on the matrices.

We construct the matrix M_k as the biadjacency matrix of a bipartite graph Γ . The matrix N_k is obtained from M_k by interchanging a pair of columns of M_k . Hence, N_k is also a biadjacency matrix of Γ and $\det(M_k) = -\det(N_k)$ by construction. Thus, as long as $\det(M_k) \neq 0$ the two determinants are different.

In Section 5.1 we describe the construction of the graph which gives rise to the biadjacency matrix M_k . This graph is obtained by a CFI construction from a base graph Γ satisfying a number of conditions. We show the existence of graphs Γ satisfying these conditions in Section 5.2. Then, in Section 5.3 we argue that Duplicator has a winning strategy in the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \text{id}), k)$ -bijection game played on M_k and N_k . Since N_k is obtained from M_k by swapping a single pair of columns, this is equivalent to showing that Duplicator has a winning strategy in the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \alpha), k)$ -bijection game played on two copies of M_k , where α is a permutation swapping two columns. We bring it all together in Section 5.4 for a proof of Theorem 19.

5.1 Constructing the Graph

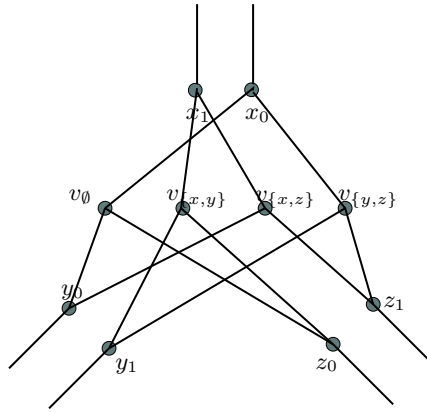
In proving the lower bound for symmetric circuits computing the permanent in [11], we adapted a construction due to Cai, Fürer and Immerman [7] of pairs of graphs not distinguished by the k -dimensional Weisfeiler-Leman algorithm. We showed that we could obtain such a pair of bipartite graphs with different numbers of perfect matchings. Note that saying a pair of graphs are not distinguished by the k -dimensional Weisfeiler-Leman algorithm is the same as saying that Duplicator has a winning strategy in the $(k + 1)$ -pebble bijection game, using arbitrary bijections. In the present construction, we consider a game played on a pair of isomorphic bipartite graphs but where the set of permissible bijections does not include any isomorphisms between them. Equivalently, we play the game on two distinct biadjacency matrices for the same graph. The graphs we consider are, indeed, exactly the graphs used in [7] except that we have to ensure they are bipartite.

CFI graphs and Determinants

Let $\Gamma = (U \cup V, E)$ be a 3-regular bipartite graph with bipartition U, V . We obtain the graph $\hat{\Gamma}$ by replacing each vertex v , with neighbours x, y, z with the ten-vertex gadget depicted in Figure 1. This gadget is described as follows. There is a set denoted I_v of four *inner vertices*: a vertex v_S for each set $S \subseteq \{x, y, z\}$ of even size. There is a set denoted O_v of six *outer vertices*: two u_0, u_1 for each $u \in \{x, y, z\}$. There is an edge between v_S and u_1 if $u \in S$ and an edge between v_S and u_0 if $u \notin S$.

Corresponding to each edge $e = \{u, v\} \in E$ there is a pair of edges that we denote e_0 and e_1 in $\hat{\Gamma}$: e_0 connects the vertex $u_0 \in O_v$ with $v_0 \in O_u$ and e_1 connects the vertex $u_1 \in O_v$ with $v_1 \in O_u$.

Note that the graph $\hat{\Gamma}$ is bipartite. Indeed, if we let $X := \bigcup_{v \in U} I_v \cup \bigcup_{v \in V} O_v$ and we let $Y := \bigcup_{v \in V} I_v \cup \bigcup_{v \in U} O_v$ then it is easily seen that all edges in $\hat{\Gamma}$ are between X and Y . Since Γ is a 3-regular bipartite graph, it follows that $|U| = |V|$ and therefore $|X| = |Y|$. Writing m for $|U|$ and n for $|X| = 10m$, we obtain a biadjacency $n \times n$ matrix representing



■ **Figure 1** A gadget in $\hat{\Gamma}$ corresponding to vertex v with neighbours x, y, z .

the graph $\hat{\Gamma}$ by fixing a pair of bijections $\eta : X \rightarrow [n]$ and $\eta' : Y \rightarrow [n]$. The action of the group D_n divides the collection of all such matrices into two orbits. Letting M and N be representatives of the two orbits, we have $\det(M) = -\det(N)$. We next aim to show that $\det(M) \neq 0$, provided that Γ has an odd number of perfect matchings.

Suppose we are given bijections $\eta : X \rightarrow [n]$ and $\eta' : Y \rightarrow [n]$ which determine a biadjacency matrix M representation of $\hat{\Gamma}$. We can also identify each perfect matching in $\hat{\Gamma}$ with a bijection $\mu : X \rightarrow Y$ such that $\mu(x)$ is a neighbour of x for all $x \in X$. We write $\text{match}(\hat{\Gamma})$ for the collection of all perfect matchings of $\hat{\Gamma}$. Then, the determinant of M is given by:

$$\det(M) = |\{\mu \mid \mu \in \text{match}(\hat{\Gamma}) \text{ with } \text{sgn}(\eta' \mu \eta^{-1}) = 1\}| - |\{\mu \mid \mu \in \text{match}(\hat{\Gamma}) \text{ with } \text{sgn}(\eta' \mu \eta^{-1}) = -1\}|.$$

From now on, we take η and η' to be fixed and write $\text{sgn}(\mu)$ and talk of the sign of a matching μ as short hand for $\text{sgn}(\eta' \mu \eta^{-1})$.

To show that this determinant is non-zero, we analyze the structure of the set $\text{match}(\hat{\Gamma})$. In what follows, we assume that η and η' are fixed and note that this imposes a linear order on the sets X and Y . It also induces a linear order on the sets U and V . We make use of this order without further elaboration.

Perfect Matchings

In any perfect matching μ of $\hat{\Gamma}$, all four vertices in I_v for any $v \in U \cup V$ must be matched to vertices in O_v . Thus, exactly two of the vertices of O_v are matched to vertices in other gadgets. These two could be two vertices in a pair, e.g. $\{x_0, x_1\}$ in Figure 1 or they could be from different pairs, e.g. $\{x_0, y_0\}$. It is easily checked that in either case, removing the two vertices of O_v from the gadget results in an 8-vertex graph that admits a perfect matching. Indeed, if we remove two vertices in a pair, such as $\{x_0, x_1\}$ the resulting graph is an 8-cycle. On the other hand, removing two vertices of O_v from different pairs results in a graph which is a 6-cycle with a path of length 2 attached to one of its vertices. We now classify perfect matchings in $\text{match}(\hat{\Gamma})$ according to which edges *between* gadgets are included in the matching.

Say that a matching $\mu \in \text{match}(\hat{\Gamma})$ is *uniform* if for each edge $e \in E$, at most one of the two edges e_0 and e_1 is included in μ . Thus, μ is *non-uniform* if for some $e \in E$ both e_0 and e_1 are included in μ . The non-uniform matchings contribute a net zero to the determinant of

M . We can prove this by showing that these matchings can be paired off into matchings of opposite sign, where two matchings in a pair differ only in a single gadget. Writing $\text{uni-match}(\hat{\Gamma})$ to denote the set of uniform matchings of $\hat{\Gamma}$, this gives us the following lemma.

► **Lemma 20.**

$$\det(M) = |\{\mu \mid \mu \in \text{uni-match}(\hat{\Gamma}) \text{ with } \text{sgn}(\mu) = 1\}| \\ - |\{\mu \mid \mu \in \text{uni-match}(\hat{\Gamma}) \text{ with } \text{sgn}(\mu) = -1\}|.$$

Uniform Perfect Matchings

Our next aim is to count uniform perfect matchings in $\hat{\Gamma}$ and classify them by sign. Suppose then that μ is a perfect matching that includes for each $e \in E$ at most one of the two edges e_0 and e_1 . Let $F_\mu \subseteq E$ be the set of those $e \in E$ such that *exactly* one of e_0 and e_1 is in μ . Furthermore, let $f_\mu : F_\mu \rightarrow \{0, 1\}$ be the function given by $f_\mu(e) = i$ if, and only if, e_i is in μ .

Since for each $v \in U \cup V$, exactly two of the vertices of O_v are matched to vertices in other gadgets we can see that F_μ includes exactly two edges incident on every vertex v . In other words, F_μ is a 2-factor of Γ and therefore has exactly $2m$ edges.

For a 2-factor F of Γ and a function $f : F \rightarrow \{0, 1\}$, write $\mu(F, f)$ for the collection of all matchings μ of $\hat{\Gamma}$ with $F_\mu = F$ and $f_\mu = f$. We can prove that there are exactly 2^{2m} such matchings for every F and f and they all have the same sign. This is shown by considering the 8-vertex graph obtained from the gadget in Fig. 1 by deleting two vertices in different pairs, say x_0 and y_0 . As we noted, the resulting graph is a 6-cycle with a path of length 2 attached at a vertex. This graph has exactly two perfect matchings, and they are related to each other by an *even* permutation. The 2^{2m} matchings in $\mu(F, f)$ are obtained by independently selecting one such matching in each gadget.

► **Lemma 21.** *There are exactly 2^{2m} perfect matchings in $\mu(F, f)$, for any 2-factor F of Γ and any function $f : F \rightarrow \{0, 1\}$ and they all have the same sign.*

Furthermore, we can show that the sign of the matchings in $\mu(F, f)$ does not depend on the choice of f .

► **Lemma 22.** *For any 2-factor F of Γ , any functions $f, g : F \rightarrow \{0, 1\}$ and any matchings $\mu_1 \in \mu(F, f)$ and $\mu_2 \in \mu(F, g)$, $\text{sgn}(\mu_1) = \text{sgn}(\mu_2)$.*

With this, we are now ready to establish the main result of this section.

► **Lemma 23.** *If Γ has an odd number of perfect matchings, then $\det(M) \neq 0$.*

Proof. By Lemma 20, we have

$$\det(M) = |\{\mu \mid \mu \in \text{uni-match}(\hat{\Gamma}) \text{ with } \text{sgn}(\mu) = 1\}| \\ - |\{\mu \mid \mu \in \text{uni-match}(\hat{\Gamma}) \text{ with } \text{sgn}(\mu) = -1\}|.$$

For any 2-factor F of Γ write $\mu(F)$ for $\bigcup_{f:F \rightarrow \{0,1\}} \mu(F, f)$ and note that by Lemma 21 $\mu(F) = 2^{2m}$ for all F . Moreover, by Lemma 22 all matchings in $\mu(F)$ have the same sign. Thus, we define $\text{sgn}(F)$ to be the sign of $\eta' \mu \eta^{-1}$ for any $\mu \in \mu(F)$. Hence, we have that

$$\det(M) = 2^{4m} \sum_F \text{sgn}(F),$$

where the sum is over all 2-factors of Γ .

Since Γ is 3-regular, the number of 2-factors of Γ is exactly the number of perfect matchings. Indeed, the complement of any 2-factor is a perfect matching and this gives a bijection between the collection of perfect matchings and 2-factors. Thus, since the number of perfect matchings of Γ is odd, so is the number of 2-factors and we conclude that the sum $\sum_F \text{sgn}(F)$ cannot be zero, proving the result. \blacktriangleleft

5.2 Graphs with Odd Number of Perfect Matchings

We have seen that if Γ has an odd number of perfect matchings, then the matrices M and N have different determinant. In order to play the bijection game on M and N we also need Γ to be well connected. We now show that we can find suitable graphs that satisfy both of these conditions simultaneously.

For a positive integer k , say that Γ is *k-well-connected* if any balanced separator of Γ has size greater than k . For our construction, we need 3-regular bipartite graphs on $2n$ vertices which are *k-well-connected* for $k = \Omega(n)$ and which have an odd number of perfect matchings. The main purpose of this section is to establish the existence of such a family of graphs.

► **Theorem 24.** *For all positive integers n there is a bipartite graph $\Gamma_n = (U, V, E)$ satisfying the following conditions: (i) $|U| = |V| = n$, (ii) Γ_n is 3-regular, (iii) Γ_n is *k-well-connected* for $k = \Omega(n)$, and (iv) Γ_n has an odd number of perfect matchings.*

We prove the existence by showing that a random 3-regular bipartite graph on $2n$ vertices satisfies the third condition with high probability. We show that it can be modified to satisfy the fourth condition while keeping the connectivity high. To do this, we need some facts about the distribution of random 3-regular bipartite graphs.

Fix U and V to be two disjoint sets of n vertices, and we are interested in the uniform distribution on 3-regular bipartite graphs on the vertices U and V . This distribution is not easy to sample from but it is known to be well-approximated by a number of other random models, including the union of disjoint random matchings, which we now describe. We say that a pair of bijections $\pi, \sigma : U \rightarrow V$ is *disjoint* if there is no $u \in U$ with $\pi(u) = \sigma(u)$. Now consider a random graph \mathcal{G} obtained by the following process: (i) choose, uniformly at random, three bijections $\pi_1, \pi_2, \pi_3 : U \rightarrow V$; (ii) if for some $j \in \{1, 2, 3\}$ with $i \neq j$, π_i and π_j are not disjoint discard this choice of bijections; otherwise (iii) let \mathcal{G} be the bipartite graph with parts U and V edges $\{\{u, \pi_i(u)\} \mid i \in \{1, 2, 3\}\}$.

The random graph model obtained in this way is known to be *contiguous* to the uniform distribution on 3-regular bipartite graphs [24]. This means that any property that holds asymptotically almost surely in one also holds so in the other. The property we are interested in is that of being an expander. It is known [5] that a random 3-regular bipartite graph is an expander with probability tending to 1. This result is, in fact, proved in the configuration model of Bollobas [4] but this is also known to be contiguous to the uniform distribution. We can therefore conclude that the same is true for the random graph \mathcal{G} .

► **Lemma 25.** *There is a constant $\alpha > 0$ such that with probability tending to 1, \mathcal{G} is an α -expander.*

An immediate consequence of this is that with high probability, \mathcal{G} is ϵn -well-connected for some constant ϵ . We now describe how we can obtain from \mathcal{G} a graph which also has an odd number of perfect matchings.

Let A_Γ denote the biadjacency matrix of $\Gamma = (U, V, E)$ with rows indexed by U and columns by V . Then the permanent of A_Γ over a field of characteristic p is exactly the number of perfect matchings in Γ modulo p . In particular, when $p = 2$, since the permanent

is the same as the determinant, we have that the number of perfect matchings in Γ is odd if, and only if, $\det(A_\Gamma) \neq 0$, where the determinant is over \mathbb{F}_2 . We do not expect that $\det(A_G) \neq 0$ with high probability. To prove Theorem 24 it would suffice to show that this is the case with positive probability and this does seem likely to be true. However, we adopt an indirect approach. We show that with probability bounded away from zero $\mathbf{rk}(A_G)$ is at least $n - o(n)$. And, we then show that we can transform any graph Γ with $\mathbf{rk}(A_\Gamma) < n$ to a graph Γ' so that $\mathbf{rk}(A_{\Gamma'}) > \mathbf{rk}(A_\Gamma) + 1$ and Γ' is still well-connected if Γ is. Together these give us the graphs we want.

In what follows, we treat the biadjacency matrix A_Γ of a graph Γ as being a matrix over \mathbb{F}_2 and so all arithmetic operations on elements of the matrix should be taken as being over this field. We are able to show that for the random graph \mathcal{G} , the matrix A_G has nearly full rank with probability bounded away from 0. To be precise, we show that the size of the null-set of A_G is at most linear in n with probability $1/2$.

► **Lemma 26.** *There is a constant ϵ such that for all sufficiently large n , $\Pr[\mathbf{rk}(A_G) \geq n - \epsilon \log n] \geq 1/2$.*

To complete the construction, we show that if Γ is a 3-regular bipartite graph with $n \times n$ biadjacency matrix A_Γ and $\mathbf{rk}(A) < n$, then under mild assumptions satisfied by almost all such graphs, we can edit Γ to get Γ' so that $\mathbf{rk}(A_{\Gamma'}) > \mathbf{rk}(A_\Gamma)$ and Γ' is at least $(k - 4)$ -well-connected if Γ is k -well-connected.

Assume then, that Γ is a 3-regular graph on two sets U and V of n vertices each and A is its biadjacency matrix. As before, we write r_u^A to denote the row of A indexed by $u \in U$. We drop the superscript A where it is clear from context. We always treat these rows as vectors in \mathbb{F}_2^V .

We say that a pair of edges $e_1 = \{u_1, v_1\}$ and $e_2 = \{u_2, v_2\}$ of Γ with $u_1, u_2 \in U$ and $v_1, v_2 \in V$ are *switchable* if they are disjoint and neither of $\{u_2, v_1\}$ nor $\{u_1, v_2\}$ is an edge. For a switchable pair e_1, e_2 we denote by $\tilde{\Gamma}_{e_1, e_2}$ the graph obtained from Γ by exchanging the two edges e_1 and e_2 . That is, $\tilde{\Gamma}_{e_1, e_2}$ is the bipartite graph on the vertices U, V with edge set

$$E(\Gamma) \setminus \{e_1, e_2\} \cup \{\{u_1, v_2\}, \{u_2, v_1\}\}.$$

Note that $\tilde{\Gamma}_{e_1, e_2}$ is also a 3-regular bipartite graph. We write \tilde{A}_{e_1, e_2} for the biadjacency matrix of $\tilde{\Gamma}_{e_1, e_2}$.

Assume now that $\mathbf{rk}(A) < n$. Then A has a *zero-sum set*, i.e. a set $S \subseteq U$ such that $\sum_{u \in S} r_u = 0$. Moreover, by the 3-regularity of Γ , we have $2 \leq |S| \leq 2n/3$. We are able to show that if $|S| < 2n/3$, then we can find a pair of edges switching which increases the rank of the matrix.

► **Lemma 27.** *If A has a zero-sum set S with $|S| < 2n/3$, then there are switchable edges $e_1, e_2 \in E(\Gamma)$ so that $\mathbf{rk}(\tilde{A}_{e_1, e_2}) > \mathbf{rk}(A)$.*

Proof of Theorem 24 (sketch). By Lemma 25, for large enough values of n , the random 3-regular graph \mathcal{G} is τn -well-connected for some constant $\tau > 0$ with probability tending to 1. Thus, with high probability, the first three conditions are satisfied. If the biadjacency matrix A_Γ of the resulting graph Γ has rank n , we are done.

It can be shown from Lemma 26 that with high probability, A_Γ satisfies the pre-conditions of Lemma 27. The result then follows by repeated application of Lemma 27. Note that each iteration switches exactly two edges, so decreases the size of the minimum balanced separator by at most 4. ◀

5.3 Playing the Game

Suppose Γ is a bipartite 3-regular graph on two sets U and V of m vertices each that is $(k+3)$ -well-connected. Let $\hat{\Gamma}$ be the CFI-graph constructed from Γ as described in Section 5.1, and M and N be two biadjacency matrices for $\hat{\Gamma}$ where N is obtained from M by interchanging exactly one pair of columns. We aim to prove that Duplicator has a winning strategy in the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \text{id}), k)$ -bijection game played on M and N .

To say that Duplicator has a winning strategy in the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \text{id}), k)$ -bijection game played on M and N is the same as saying that Duplicator has a winning strategy in the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \alpha), k)$ -bijection game played on two copies of M where α is a permutation swapping two columns of M . Equivalently, we say Duplicator has a winning strategy in the $(T(\mathbf{Alt}_X \times \mathbf{Alt}_Y, \alpha), k)$ -bijection game played on two copies of the graph $\hat{\Gamma}$ where α is a permutation of Y consisting of a single swap (yy') of two elements $y, y' \in Y$. It also does not matter which two elements y, y' we choose as any swap can be obtained from (yy') by composing with a permutation in \mathbf{Alt}_Y . This is then the formulation we prove. For some $u \in U$, fix two vertices $x_0, x_1 \in O_u$ which form a single pair in the gadget corresponding to u and let $\alpha = (x_0x_1)$.

► **Lemma 28.** *Duplicator has a winning strategy in the $(T(\mathbf{Alt}_X \times \mathbf{Alt}_Y, \alpha), k)$ -bijection game played on two copies of the graph $\hat{\Gamma}$.*

Proof (sketch). The key property of the gadget in Figure 1 is that for any two of the three sets $\{x_0, x_1\}$, $\{y_0, y_1\}$ and $\{z_0, z_1\}$, there is an automorphism of the gadget swapping the two elements within those two sets while fixing the two in the third. Moreover, it can be checked that this automorphism, seen as a permutation on the vertices of $\hat{\Gamma}$ is in $\mathbf{Alt}_X \times \mathbf{Alt}_Y$. Given a cycle C in the graph Γ , we can chain together these permutations of $\hat{\Gamma}$: for each vertex v in C , swap the vertices in the pairs corresponding to the two edges that are in the cycle. This gives an automorphism of $\hat{\Gamma}$ we call β_C . Since all cycles in $\hat{\Gamma}$ are of even length, this automorphism is also in $\mathbf{Alt}_X \times \mathbf{Alt}_Y$.

Duplicator's strategy can now be described as follows. At any point in the game, at most k vertices of $\hat{\Gamma}$ are pebbled and these are from gadgets corresponding to at most k vertices $\{p_1, \dots, p_k\}$ of Γ . By the connecteness assumption, $\Gamma \setminus \{p_1, \dots, p_k\}$ has a component Δ which contains more than half of the vertices of Γ , and Δ is 2-connected. We call Δ the *large* component at this game position. Duplicator ensures that the bijection at any stage of the game is an automorphism of $\hat{\Gamma}$ composed with a swap (v_0v_1) of a pair of vertices in O_u for some edge $\{u, v\} \subseteq \Delta$. We call $\{u, v\}$ the *twisted* edge. The condition is clearly satisfied in the initial position as Δ is the whole graph. At each subsequent move, after Spoiler has placed a pebble on a vertex x , Duplicator chooses an edge $\{u', v'\}$ in the new large component to twist. This must be combined with an untwisting of $\{u, v\}$ while ensuring that the entire bijection is obtained from the previous one by composing with a permutation in $\mathbf{Alt}_X \times \mathbf{Alt}_Y$. If x is not in $\{v_0, v_1\}$ this is easy, as we can simply apply the two swaps (v_0v_1) and $(v'_0v'_1)$. However, if $x \in \{v_0, v_1\}$ we must find a permutation that fixes the pair $\{v_0, v_1\}$ pointwise. We do this by finding a cycle C within the large component before x is chosen containing the edge $\{u, v\}$ and composing the swaps (v_0v_1) and $(v'_0v'_1)$ with the automorphism β_C of $\hat{\Gamma}$. ◀

5.4 Bringing it Together

We pull things together to prove Theorem 19

Proof of Theorem 19. We have from Theorem 24 that for each $n \in \mathbb{N}$ there exists a 3-regular balanced bipartite graph Γ_n with $2n$ vertices that is $k(n)$ -well-connected for $k(n) = \Omega(n)$ and has an odd number of perfect matchings. Let $\hat{\Gamma}_n$ be the CFI-graph constructed from Γ_n as described in Section 5.1, and M_n and N_n be two biadjacency matrices for $\hat{\Gamma}_n$ where N_n is obtained from M_n by interchanging exactly one pair of columns. From Lemma 28 we have that Duplicator has a winning strategy for the $(T(\mathbf{Alt}_n \times \mathbf{Alt}_n, \text{id}), k(n) - 3)$ -bijection game on M_n and N_n . From Lemma 23 and the fact that Γ_n has an odd number of perfect matchings, it follows that $\det(M_n) \neq 0$ and so, since $\det(M_n) = -\det(N_n)$, we have $\det(M_n) \neq \det(N_n)$. The result now follows from Theorem 18. \blacktriangleleft

Theorem 19 is stated and proved specifically for fields of characteristic zero and we leave an extension to finite fields for future work.

6 Lower Bound for the Permanent

We previously established in [11] lower bounds on symmetric circuits for the permanent showing that there are no subexponential square-symmetric circuits computing the permanent of an $n \times n$ matrix in any field of characteristic zero, along with a similar result for matrix-symmetric circuits in any field of characteristic other than two.

These bounds are consequences of the same construction: we give, for each k , a pair of bipartite graphs X_k and \tilde{X}_k on which Duplicator has a winning strategy in the k -pebble bijection game which have different numbers of perfect matchings. The graphs X_k and \tilde{X}_k are on two sets A and B of $n = O(k)$ vertices each and the difference between the number of perfect matchings in X_k and \tilde{X}_k is a power of 2. The k -pebble bijection game for which a Duplicator winning strategy is shown is essentially the $(T(\mathbf{Sym}_A \times \mathbf{Sym}_B, \text{id}), k)$ game. This shows that the biadjacency matrices of X_k and \tilde{X}_k cannot be distinguished by $\mathbf{Sym}_A \times \mathbf{Sym}_B$ -symmetric circuits of subexponential size and also that the adjacency matrices of X_k and \tilde{X}_k cannot be distinguished by $\mathbf{Sym}_{A \cup B}$ -symmetric circuits of subexponential size. Since X_k and \tilde{X}_k have different numbers of perfect matchings, their biadjacency matrices have distinct permanents. Since the number of perfect matchings differ by a power of 2, they have distinct permanents modulo p for any odd prime p . Moreover, since the permanent of the adjacency matrix of a bipartite graph is the square of the permanent of its biadjacency matrix, we have that the adjacency matrices have distinct permanents. Together, these give us the stated lower bounds for circuits computing the permanent in the second and fourth columns of Table 1. To establish the lower bound in the third column, it suffices to observe that Duplicator has a winning strategy on X_k and \tilde{X}_k even in the restricted game $(T(\mathbf{Alt}_A \times \mathbf{Alt}_B, \text{id}), k)$.

The construction of the graph $\hat{\Gamma}$ from Γ given in Section 5.1 gives from Γ a pair of non-isomorphic graphs which are not distinguishable by k -dimensional Weisfeiler-Leman equivalence. We use only one graph $\hat{\Gamma}$ from the pair, as our game is played on two different biadjacency matrices of the same graph and our main concern is that this matrix has non-zero determinant. Of course, the different biadjacency matrices have the same permanent, and for a lower bound for the latter, we do need to play the game on a pair of non-isomorphic graphs. It turns out that the other graph in the pair has the same number of perfect matchings as $\hat{\Gamma}$ and therefore the bi-adjacency matrix has the same permanent. Instead, we can use the construction we presented in [11] where we adapted the CFI construction in two ways. The

graph $X(\Gamma)$ is obtained from $\hat{\Gamma}$ by first, for each edge $e = \{u, v\}$ of Γ , contracting the two edges $e_0 = \{u_0, v_0\}$ and $e_1 = \{u_1, v_1\}$ in $\hat{\Gamma}$ and secondly, for each vertex v of Γ , adding a new vertex v_b to $\hat{\Gamma}$ which is adjacent to all four vertices in I_v . The resulting graph $X(\Gamma)$ is a 4-regular bipartite graph and $\tilde{X}(\Gamma)$ is obtained from it by taking one vertex v of Γ and in the corresponding gadget, for one edge e incident on v , interchanging the connections of e_0 and e_1 . The fact that $X(\Gamma)$ and $\tilde{X}(\Gamma)$ have biadjacency matrices with different permanents is proved in [11]. What we are able to show is that Duplicator has a winning strategy in a pebble game (with a linear number of pebbles) played on these two graphs, even when restricted to bijections from $\mathbf{Alt}_A \times \mathbf{Alt}_B$, which suffices to establish the following.

► **Theorem 29.** *Let \mathbb{F} be a field of characteristic other than 2. There is no family of $\mathbf{Alt}_n \times \mathbf{Alt}_n$ -symmetric circuits $(C_n)_{n \in \mathbb{N}}$ over \mathbb{F} of size $2^{o(n)}$ computing the permanent over \mathbb{F} .*

7 Concluding Discussion

The study of the complexity of symmetric circuits began in the context of logic. Specifications of decision problems on graphs (or similar structures) formulated in formal logic translate naturally into algorithms that respect the symmetries of the graphs. This yields a restricted model of computation based on symmetric circuits for which we are able to prove concrete lower bounds, in a fashion similar to the restriction to monotone circuits. Methods developed in the realm of logic for proving inexpressibility results can be reinterpreted as circuit lower bound results.

One step in this direction was the connection established in [1] between polynomial-size Boolean threshold circuits on the one hand and fixed-point logic with counting on the other. This shows that the power of symmetric Boolean threshold circuits to decide graph properties is delimited by the counting width of those properties. In particular, this shows that a number of NP-complete graph problems including 3-colourability and Hamiltonicity cannot be decided by polynomial-size symmetric Boolean threshold circuits. This is particularly interesting as the power of such symmetric circuits has been shown to encompass many strong algorithmic methods based on linear and semidefinite programming (see, for instance, [2]). This methodology was extended to graph parameters beyond decision problems, and to arithmetic circuits rather than Boolean circuits in [11]. Together these extensions established that no subexponential size square symmetric (i.e. unchanged by simultaneous row and column permutations) arithmetic circuits could compute the permanent.

The permanent of a $\{0, 1\}$ matrix M has a natural interpretation as a graph invariant and so lends itself easily to methods for proving lower bounds on graph parameters. The situation with the determinant of M is more subtle. If M is a symmetric $n \times n$ matrix, then we can see at as the adjacency matrix of a graph Γ on n vertices and the determinant is a graph invariant, that is to say it only depends on the isomorphism class of Γ . Moreover, it is a graph invariant that can be computed efficiently by symmetric circuits (at least in characteristic zero) as was shown for Boolean circuits in [19] and for arithmetic circuits in [11]. When M is not a symmetric matrix, we could think of it as the adjacency matrix of a directed graph. In this case, the symmetries that a circuit must preserve are still the permutations of n , so simultaneous permutations of the rows and columns of M and the upper bounds obtained still apply. But, we can also think of M as a biadjacency matrix of a bipartite graph Γ , and now the determinant of M is not an invariant of Γ . We have a richer set of symmetries, and methods for proving bounds on the complexity of graph parameters do not directly apply.

What we have sought to do in the present paper is to develop the methods for proving lower bounds on the counting width of graph parameters to a general methodology for proving circuit lower bounds for polynomials or more generally functions invariant under certain permutations of their input variables. To do this, we prove a support theorem for circuits which is for a more general collection of symmetry groups than proved in prior literature; we adapt the Spoiler-Duplicator bijection game to work for more general invariance groups and more general structured inputs than those arising as symmetries of graph matrices; and we show a direct relationship between these games and orbit size of circuits that bypasses connections with width measures on graphs. This methodology is then applied to arithmetic circuits computing the determinant and we are able to prove an exponential lower bound for circuits symmetric under the full permutation group $D_n \leq \mathbf{Sym}_n \times \mathbf{Sym}_n$ that fixes the determinant of M . Indeed, we do this for the smaller group $\mathbf{Alt}_n \times \mathbf{Alt}_n$. The application requires considerable work in constructing the example matrices and applying the bijection games.

We see one main contribution to be establishing the general methodology for proving circuit lower bounds under various notions of symmetry. There are many ways in which this could be pushed further. First, our proof of the support theorem requires the presence of large alternating groups in the symmetry group under consideration. Perhaps more sophisticated notions of support could be developed which would allow us to consider smaller groups. Secondly, while we state our main result for the group $\mathbf{Alt}_n \times \mathbf{Alt}_n$, the bijection game itself uses rather fewer symmetries. It would be interesting to establish tighter bounds on the symmetry group for which we get exponential lower bounds. Indeed, the results can be seen as giving a trade-off between circuit size and symmetries and this suggests an interesting terrain in which to explore the symmetry requirements of the circuit as a resource.

References

- 1 M. Anderson and A. Dawar. On symmetric circuits and fixed-point logics. *Theory Comput. Syst.*, 60(3):521–551, 2017.
- 2 A. Atserias, A. Dawar, and J. Ochremiak. On the power of symmetric linear programs. *J.ACM*, 2021. to appear. arxiv:1901.07825.
- 3 A. Blass, Y. Gurevich, and S. Shelah. Choiceless polynomial time. *Annals of Pure and Applied Logic*, 100(1):141–187, 1999. doi:10.1016/S0168-0072(99)00005-6.
- 4 Béla Bollobás. The distribution of the maximum degree of a random graph. *Discret. Math.*, 32:201–203, 1980. doi:10.1016/0012-365X(80)90054-0.
- 5 G. Brito, I. Dumitriu, and K. D. Harris. Spectral gap in random bipartite biregular graphs and applications. *Combinatorics, Probability and Computing*, 2021. to appear. arXiv:1804.07808.
- 6 P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*. Springer, Berlin, Heidelberg, 1 edition, 1997.
- 7 J-Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.
- 8 A. Dawar. On symmetric and choiceless computation. In Mohammad Taghi Hajiaghayi and Mohammad Reza Mousavi, editors, *Topics in Theoretical Computer Science*, pages 23–29, Cham, 2016. Springer International Publishing.
- 9 A. Dawar. Symmetric computation (invited talk). In *28th EACSL Annual Conference on Computer Science Logic, CSL 2020*, 2020. doi:10.4230/LIPIcs.CSL.2020.2.
- 10 A. Dawar and G. Wilsenach. Symmetric circuits for rank logic. In *27th EACSL Annual Conference on Computer Science Logic, CSL 2018*, pages 20:1–20:16, 2018. Full version at arXiv:1804.02939. doi:10.4230/LIPIcs.CSL.2018.20.

- 11 A. Dawar and G. Wilsenach. Symmetric Arithmetic Circuits. In *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:18, 2020. Full version at arXiv:2002.06451.
- 12 A. Dawar and G. Wilsenach. Lower bounds for symmetric circuits for the determinant, 2021. arXiv:2107.10986.
- 13 J.D. Dixon and B. Mortimer. *Permutation Groups*. Graduate Texts in Mathematics. Springer New York, 1996. URL: <https://books.google.co.uk/books?id=4QDpFN6k61EC>.
- 14 D. Grigoriev and M. Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, pages 577–582, 1998. doi:10.1145/276698.276872.
- 15 M. Grohe. *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*, volume 47 of *Lecture Notes in Logic*. Cambridge University Press, 2017.
- 16 M. Grohe. *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*. Lecture Notes in Logic. Cambridge University Press, 2017.
- 17 F. Harary. Determinants, permanents and bipartite graphs. *Mathematics Magazine*, 42:146–148, 1969. doi:10.1080/0025570X.1969.11975950.
- 18 L. Hella. Logical hierarchies in PTIME. *Information and Computation*, 129(1):1–19, 1996.
- 19 B. Holm. *Descriptive Complexity of Linear Algebra*. PhD thesis, University of Cambridge, 2010.
- 20 S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.
- 21 M. Jerrum and M. Snir. Some exact complexity results for straight-line computations over semirings. *J. ACM*, 29:874–897, 1982. doi:10.1145/322326.322341.
- 22 N. Kayal and R. Saptharishi. A selection of lower bounds for arithmetic circuits. In M. Agrawal and V. Arvind, editors, *Perspectives in Computational Complexity*. Birkhäuser Basel, 2014.
- 23 J.M. Landsberg and N. Ressayre. Permanent v. determinant: An exponential lower bound assuming symmetry. In *Proc. ACM Conference on Innovations in Theoretical Computer Science*, pages 29–35. ACM, 2016. doi:10.1145/2840728.2840735.
- 24 M. Molloy, H. D. Robalewska, R. W. Robinson, and N. C. Wormald. 1-factorizations of random regular graphs. *Random Struct. Algorithms*, 10:305–321, 1997.
- 25 H.J. Ryser. *Combinatorial Mathematics*, volume 14. Mathematical Association of America, 1 edition, 1963.
- 26 A. Shpilka and A. Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3–4):207–388, 2010. doi:10.1561/04000000039.
- 27 H. Vollmer. *Introduction to Circuit Complexity - A Uniform Approach*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 1999. doi:10.1007/978-3-662-03927-4.