Symmetric Determinantal Representation of Weakly-Skew Circuits

Bruno Grenet, Erich Kaltofen, Pascal Koiran, Natacha Portier

Symmetric Determinantal Representation of Weakly-Skew Circuits

Bruno Grenet[1,2], Erich L. Kaltofen*[3], Pascal Koiran[1,2], and Natacha Portier†[1,2]

1 **LIP, UMR 5668, ENS de Lyon – CNRS – UCBL – INRIA**
École Normale Supérieure de Lyon, Université de Lyon
[Bruno.Grenet,Pascal.Koiran,Natacha.Portier]@ens-lyon.fr
2 **Department of Computer Science, University of Toronto**
3 **Dept. of Mathematics, North Carolina State University,**
Raleigh, North Carolina 27695-8205, USA
kaltofen@math.ncsu.edu
http://www.kaltofen.us

Abstract

We deploy algebraic complexity theoretic techniques for constructing symmetric determinantal representations of weakly-skew circuits, which include formulas. Our representations produce matrices of much smaller dimensions than those given in the convex geometry literature when applied to polynomials having a concise representation (as a sum of monomials, or more generally as an arithmetic formula or a weakly-skew circuit). These representations are valid in any field of characteristic different from 2. In characteristic 2 we are led to an almost complete solution to a question of Bürgisser on the VNP-completeness of the partial permanent. In particular, we show that the partial permanent cannot be VNP-complete in a finite field of characteristic 2 unless the polynomial hierarchy collapses.

1998 ACM Subject Classification F.1.1, F.2.1, I.1.1, I.1.2

Keywords and phrases algebraic complexity, determinant and permanent of symmetric matrices, formulas, skew circuits, Valiant's classes

Digital Object Identifier 10.4230/LIPIcs.STACS.2011.543

1 Introduction

1.1 Motivation

A linear matrix expression (symmetric linear matrix form, affine symmetric matrix pencil) is a symmetric matrix with the entries being linear forms in the variables $x_1, \ldots, x_n$ and real number coefficients:

$$A(x_1, \ldots, x_n) = A_0 + x_1 A_1 + \cdots + x_n A_n, \quad A_i \text{ symmetric in } \mathbb{R}^{t \times t}. \tag{1}$$

A linear matrix inequality (LMI) restricts to those values $\xi_i \in \mathbb{R}$ of the x_i such that $A(\xi_1, \ldots, \xi_n) \succeq 0$, i.e., is positive semidefinite. The set of all such values defines a spectrahedron.

* This material is based on work supported in part by the National Science Foundation under Grants CCF-0830347 and CCF-0514585.
† This material is based on work supported in part by the European Community under contract PIOF-GA-2009-236197 of the 7th PCRD.

28th Symposium on Theoretical Aspects of Computer Science (STACS'11).
Editors: Thomas Schwentick, Christoph Dürr; pp. 543–554
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
SYMPOSIUM ON THEORETICAL ASPECTS OF COMPUTER SCIENCE

A *real zero polynomial* is a polynomial p with real coefficients such that for every $x \in \mathbb{R}^n$ and every $\mu \in \mathbb{C}$, $p(\mu x) = 0$ implies $\mu \in \mathbb{R}$. The Lax conjecture and generalized Lax conjecture seek for representations of real zero polynomials $f(x_1, \ldots, x_n)$ (1) with $f = \det(A)$ and $A_0 \succeq 0$. This is in fact an equivalent formulation of the original Lax conjecture which was stated in terms of hyperbolic polynomials (see [11] for this equivalence). Furthermore, the matrices are required to have dimension d where d is the degree of the polynomial. For $n = 2$ such representations always exist while a counting argument shows that this is impossible for $n > 2$ [8] (actually, the authors of [11] give the first proof of the Lax conjecture in its original form based on the results of [8]). Two generalizations have been suggested to avoid this counting argument: first, it was suggested to remove the dimension constraint and allow for bigger matrices, and second, to permit representations of some power of the input polynomial. Counterexamples to both generalizations have recently been constructed [3].

Another relaxation is to drop the condition $A_0 \succeq 0$ and represent any f as $\det(A)$ [7, 16]. However, the purely algebraic construction of [16] leads to exponential matrix dimensions t. Here we continue the line of work initiated by [7, 16] but we proceed differently by symmetrizing the complexity theoretic construction by Valiant [18]. Our construction yields smaller dimensional matrices not only for polynomials represented as sums of monomials but also for polynomials represented by formulas and weakly-skew circuits [14, 9]. Even though in the most general case the bounds we obtained are slightly worse than Quarez's [16], in a lot of interesting cases such as polynomials with a polynomial size formula or weakly-skew circuit, or in the case of the permanent, our constructions yield much smaller matrices [5, Section 4].

Our constructions are valid for any field of characteristic different from 2. For fields of characteristic 2, it can be shown that some polynomials (such as e.g. the polynomial $xy + z$) cannot be represented as determinants of symmetric matrices [6]. Note as a result that the 2-dimensional permanent $xw + yz$ cannot be "symmetrized" over characteristic 2 with any dimension. It would be interesting to exactly characterize which polynomials admit such a representation in characteristic 2. For the polynomial $x + y$, we have

$$x + y = \det\left(\begin{bmatrix} 0 & x & 0 & y & -1 \\ x & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ y & 0 & -1 & 0 & 1/2 \\ -1 & 0 & 0 & 1/2 & 0 \end{bmatrix}\right) = \det\left(\begin{bmatrix} x & 0 & 0 & 1 \\ 0 & y & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}\right),$$

where the first matrix is derived from our construction, but the second is valid over any commutative ring. It is easily shown that for every polynomial p, p^2 admits a symmetric determinantal representation in characteristic 2. This is related to a question of Bürgisser [4]: Is the partial permanent VNP-complete over fields of characteristic 2? We give an almost complete negative answer to this question.

Our results give as a by-product an interesting result, which was not known to the authors' knowledge: Let A be an $(n \times n)$ matrix with indeterminate coefficients (ranging over a field of characteristic different from 2); then there exists a symmetric matrix B of size $0(n^5)$ whose entries are the indeterminates from A and constants from the field such that $\det A = \det B$. This relies on the existence of a size-$O(n^5)$ weakly-skew circuit to compute the determinant of an $(n \times n)$ matrix [2, 14]. The size of B can be reduced to $O(n^4)$ if we replace the weakly-skew circuits from [2, 14] by the skew circuits of size $O(n^4)$ constructed by Mahajan and Vinay [13]. These authors construct an arithmetic branching program for

the determinant with $O(n^4)$ edges,[1] and the arithmetic branching program can be evaluated by a skew circuit of size $O(n^4)$. After learning of our result, Meena Mahajan and Prajakta Nimbhorkar have noticed that the arithmetic branching program for the determinant can be transformed directly into a symmetric determinant of size $O(n^3)$ with techniques similar to the ones used in this paper. A detailed proof will appear in the full version of this paper.

Acknowledgments: We learned of the symmetric representation problem from Markus Schweighofer's ISSAC 2009 Tutorial
`http://www.math.uni-konstanz.de/~schweigh/presentations/dcssblmi.pdf`.

We thank Meena Mahajan for pointing out [13] and sketching the construction of a symmetric determinant of size $O(n^3)$ from a determinant of size n.

1.2 Known results and definitions

In his seminal paper Valiant [18] expressed the polynomial computed by an arithmetic formula as the determinant of a matrix whose entries are constants or variables. If we define the *skinny size* e of the formula as its number of arithmetic operations then the size of the matrix is at most $e + 2$. The proof uses a weighted digraph construction where the formula is encoded into paths from a source vertex to a target, sometimes known as an Algebraic or Arithmetic Branching Program [15, 1]. This theorem shows that every polynomial with a sub-exponential size formula can be expressed as a determinant with sub-exponential size formula, enhancing the prominence of linear algebra. A slight variation of the theorem is also used to prove the universality of the permanent for formulas which is one of the steps in the proof of its VNP-completeness. In a tutorial, von zur Gathen [21] gives another way to express a formula as a determinant: his proof does not use digraphs and his bound is $2e + 2$. Refining von zur Gathen's techniques, Liu and Regan [12] gave a construction leading to a $e + 1$ bound and an extra property: multiplications by constant are not counted in e.

In [17, 14], results of the same flavor were proved for a more general class of circuits, namely the *weakly-skew* circuits. Malod and Portier [14] can deduce from those results a fairly simple proof of the VQP-completeness of the determinant (under *qp*-projection). Moreover, they define a new class VP_{ws} of polynomials represented by polynomial-size weakly-skew circuits (with no explicit restriction on the degree of the polynomials) for which the determinant is complete under *p*-projection. (See [4, 14] for the definitions.) A formula is a circuit in which every vertex has out-degree 1 (but the output). This means in particular that the underlying digraph is a tree. A weakly-skew circuit is a kind of generalization of a formula, with a less constrained structure on the underlying digraph. For an arithmetic circuit, the only restriction on the digraph is the absence of directed cycles (that is the underlying digraph is a directed acyclic graph). A circuit is said weakly-skew if every multiplication gate α has the following property: the sub-circuit associated with one of its arguments β is connected to the rest of the circuit only by the arrow going from β to α. This means that the underlying digraph is disconnected as soon as the multiplication gate α is removed. In a sense, one of the arguments of the multiplication gate was separately computed for this gate.

Toda [17] proved that the polynomial computed by a weakly-skew circuit of skinny size e can be represented by the determinant of a matrix of size $(2e + 2)$. This result was improved by Malod and Portier [14]: The construction leads to a matrix of size $(m + 1)$ where m is the *fat size* of the circuit (*i.e.* its total number of gates, including the input nodes). Note that for a circuit in general and for a weakly-skew circuit in particular $m \leq 2e + 1$. The

[1] This bound can be found on p.11 of their paper.

latter construction uses negated variables in the matrix. It is actually possible to get rid of them [9]. Although the skinny size is well suited for the formulas, the fat size appears more appropriate for weakly-skew circuits. In Section 2, we symmetrize this construction so that a polynomial expressed by a weakly-skew circuit equals the determinant of a symmetric matrix. Our construction yields a size-$(2m + 1)$ symmetric matrix.

Let us now give some formal definitions of the arithmetic circuits and related notions.

▶ **Definition 1.** An *arithmetic circuit* is a directed acyclic graph with vertices of in-degree 0 or 2 and exactly one vertex of out-degree 0. Vertices of in-degree 0 are called *inputs* and labelled by a constant or a variable. The other vertices, of in-degree 2, are labeled by $\times$ or $+$ and called *computation gates*. The vertex of out-degree 0 is called the *output*. The vertices of a circuit are commonly called *arithmetic gates* and its arcs *arrows*.

A (division-free) arithmetic circuit with constants in a field k and input variables $x_1, \ldots, x_n$ naturally computes a polynomial $f \in k[x_1, \ldots, x_n]$.

If α is a gate of a circuit C, the *sub-circuit associated to* α is the subgraph of C made of all the gates β such that there exists a oriented path from β to α in C, including α. The gates β and γ are called the *arguments* of α.

An arithmetic circuit is said *weakly-skew* if for any multiplication gate α, the sub-circuit associated to one of its arguments β is only connected to the rest of the circuit by the arrow going from β to α: it is called the *closed* sub-circuit of α. A gate which does not belong to a closed sub-circuit of C is said to be *reusable* in C. The reusability of a gate depends, of course, on the considered circuit C.

In our constructions, we shall use *graphs* and *digraphs*. In order to avoid any confusion between directed and undirected graphs, we shall exclusively use the term graph for undirected ones, and otherwise use the term digraph. It is well-known that cycle covers in digraphs are in one-to-one correspondence with permutations of the vertices and therefore that the permanent of the adjacency matrix of a digraph can be defined in terms of cycle covers of the graph. Let us now give some definitions for those facts, and see how it can be extended to graphs.

▶ **Definition 2.** A *cycle cover* of a digraph $G = (V, A)$ is a set of cycles such that each vertex appears in exactly one cycle. The *weight* of a cycle cover is defined to be the product of the weights of the arcs used in the cover. Let the *sign* of a vertex cover be the sign of the corresponding permutation of the vertices, that is $(-1)^N$ where N is the number of even cycles. Finally, let the *signed weight* of a cycle cover be the product of its weight and sign.

For a graph $G = (V, E)$, let $G^d = (V, A)$ be the corresponding symmetric digraph. Then a cycle cover of G is a cycle cover of G^d, and the definitions of weight and sign are extended to this case. In particular, if there is a cycle cover of G with a cycle $C = (u_1, \ldots, u_k)$, then a new cycle cover is defined if C is replaced by the cycle $(u_k, \ldots, u_1)$. Those two cycle covers are considered as different cycle covers of G.

▶ **Definition 3.** Let G be a digraph. Its *adjacency matrix* is the $(n \times n)$ matrix A such that $A_{i,j}$ is equal to the weight of the arc from i to j ($A_{i,j} = 0$ is there is no such arc). The definition is extended to the case of graphs, seen as symmetric digraphs. In particular, the adjacency matrix of a graph is symmetric.

▶ **Lemma 4.** *Let G be a (di)graph, and A its adjacency matrix. Then the permanent of A equals the sum of the weights of all the cycle covers of G, and the determinant of A is equal to the sum of the signed weights of all the cycle covers of G.*

Proof. The cycle covers are obviously in one-to-one correspondence with the permutations of the set of vertices, and the sign of a cycle cover is defined to match the sign of the corresponding permutation. Suppose that the vertices of V are $\{1,\dots,n\}$ and let $A_{i,j}$ be the weight of the arc (i,j) in G. Let C a cycle cover and σ the corresponding permutation. Then it is clear that the weight of C is $A_{1,\sigma(1)}\cdots A_{n,\sigma(n)}$, hence the result. ◀

The validity of this proof for graphs follows from the definition of the cycle covers of a graph in terms of the cycle covers of the corresponding symmetric digraph. In the following, the notion of perfect matching is used. A *perfect matching* in a graph G is a set M of edges of G such that every vertex is incident to exactly one edge of M. The weight of a perfect matching is defined in this paper as the weight of the corresponding cycle cover (with length-2 cycles). This means that it is the product of the weights of the arcs it uses, or equivalently it is the square of the product of the weights of the edges it uses. Note that this is the square of the usual definition.

A *path* P in a digraph is a subset of vertices $\{u_1,\dots,u_k\}$ such that for $1 \le i \le k-1$, there exists an arc from u_i to u_{i+1} with nonzero weight. The size $|P|$ of such a path is k.

2 Weakly-skew circuits

In this section, we extend the construction of [14] to the case of symmetric matrices: given a weakly-skew circuit computing a polynomial p, a symmetric matrix M which entries are variables and constants is built such that $p = \det M$. Malod and Portier [14] express a polynomial as a determinant of a non-symmetric matrix. Their construction relies on the construction of a digraph whereas ours relies on the construction of a (non-directed) graph. Recall that a weakly-skew circuit has several *reusable* gates. This means that when a weakly-skew circuit is recursively turned into a (di)graph, some vertices have to be *reusable*. This is ensured in [14] by the property that the digraph is acyclic. As we are dealing with a graph instead of a digraph, this cannot be used anymore. A solution to this problem is given in Lemma 6 by introducing the notion of acceptable paths: A path P in a graph G is said *acceptable* if $G \setminus P$ admits a cycle cover.

As in [14], the size bounds of the constructed matrix and graph are given in terms of the fat size of the weakly-skew circuit: the *fat size* of a circuit is its total number of gates, including the input gates. Note that one can refine these bounds using the notion of *green size* defined in the long version of this paper [5, Section 3.2]. Furthermore, if the polynomial is given as a formula instead of a weakly-skew circuit, it is possible to get tighter bounds [5, Section 2].

Let us fix a field k of characteristic different from 2 and a countable set $\bar{x} = \{x_1, x_2, \dots\}$ of variables. The circuits we consider are supposed to have inputs in $k \cup \bar{x}$.

▶ **Theorem 5.** *Let f be a polynomial computable by a weakly-skew circuit of fat size m. Then there exists a symmetric matrix A of size at most $2m+1$ whose entries are inputs of the circuit and elements from $\{0, 1, -1, 1/2\}$ such that $f = \det A$.*

The proof relies on the following lemma. It applies to so-called *multiple-output* weakly-skew circuits. This generalization just consists in circuits for which there exist several out-degree-0 gates.

▶ **Lemma 6.** *Let C be a multiple-output weakly-skew circuit of fat size m. There exists a graph G with at most $2m+1$ vertices and a distinguished vertex s such that $|G|$ is odd, every cycle in G is even, and for every reusable gate $\alpha \in C$ there exists a vertex $t_\alpha \in G$ such that*

1. *Every s-t_α-path (whether acceptable or not) has an odd number of vertices;*
2. *For every acceptable s-t_α-path P in G, the subgraph $G \setminus P$ is either empty or has a unique cycle cover, which is a perfect matching of weight* 1*;*
3. *The following equality holds in G:*

$$\sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-path } P}} (-1)^{\frac{|P|-1}{2}} w(P) = f_\alpha \tag{2}$$

where f_α is the polynomial computed by the gate α.

Furthermore, the graph $G \setminus \{s\}$ has a unique cycle cover which is a perfect matching of weight 1.

Proof sketch. The graph G is built by induction on the (fat) size of the circuit. We only sketch here its construction. For a proof that G satisfies the conditions of the lemma, refer to [5, Lemma 4]. If α is a reusable gate of C, then t_α is said to be a reusable vertex of G.

A size-1 circuit is an input gate α with label x. The corresponding graph G has three vertices: s, t_α and an additional vertex v_α. There is an edge between s and v_α of weight x, and an edge between v_α and t_α of weight -1.

Let $m > 1$ and suppose that the lemma holds for any multiple-output weakly-skew circuit of size less than m. Let C be a multiple output weakly-skew circuit of size m, and α be any of its outputs.

If α is an input gate with label x, let $C' = C \setminus \{\alpha\}$ and G' the corresponding graph with a distinguished vertex s. The graph G is obtained from G' by adding two new vertices v_α and t_α, an edge of weight x between s and v_α and an edge of weight -1 between v_α and t_α (see Fig. 1). The vertex s is the distinguished vertex of G.

If α is an addition gate, let $C' = C \setminus \{\alpha\}$ and suppose that α receives arrows from gates β and γ. Note that β and γ are reusable. Let G' be the graph corresponding to C', and s be its distinguished vertex. G' contains two reusable vertices t_β and t_γ. The graph G is obtained by adding two vertices v_α and t_α, and the following edges: $t_\beta v_\alpha$ and $t_\gamma v_\alpha$ of weight 1, and $v_\alpha t_\alpha$ of weight -1 (see Fig. 3). If $\beta = \gamma$, then G' contains a vertex t_β, and we merge the two edges adjacent to t_β and t_γ into an edge $t_\beta v_\alpha$ of weight 2.

If α is a multiplication gate, α receives arrows from two distinct gates β and γ. Exactly one of those gates, say β, is not reusable and removing the gate α yields two disjoint circuits C_1 and C_2 (say β belongs to C_1 and γ to C_2). Let G_1 and G_2 be the respective graphs obtained by induction from C_1 and C_2, with distinguished vertices s_1 and s_2 respectively. The graph G is obtained as in Fig. 2 as the union of G_1 and G_2 where t_γ and s_1 are merged, the distinguished vertex s of G being the distinguished vertex s_2 of G_2, and t_α being equal to t_β. ◀

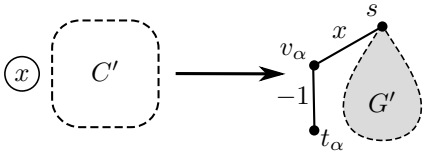

Figure 1 Input gate

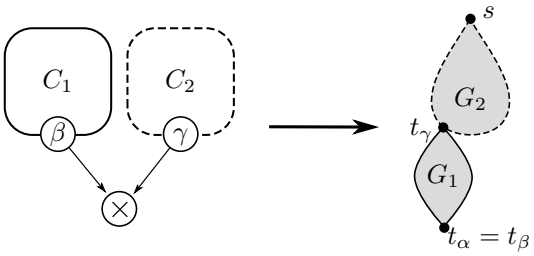

Figure 2 Multiplication gate

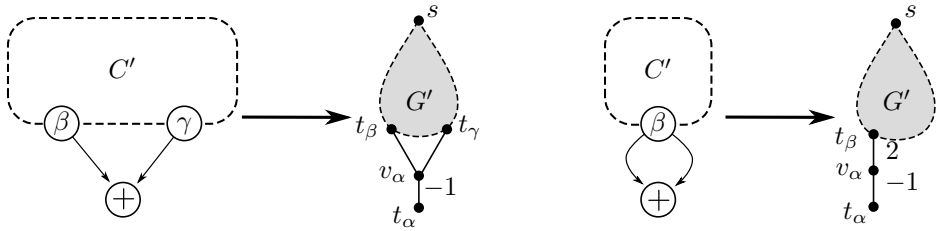

Figure 3 Both cases for an addition gate

Proof of Theorem 5. Let C be a weakly-skew circuit computing the polynomial f, and G be the graph built from C in Lemma 6. The circuit C has a unique output, and there exists in G a vertex t corresponding to this output. Let G' be the graph obtained from G by adding an edge between t and s of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}}$.

There is no cycle cover of G' containing the 2-cycle st. Indeed, $|G' \setminus \{s,t\}|$ is odd and G contains only even cycles. This means that a cycle cover of G' contains a cycle made of a s-t-path plus (t,s) or a t-s-path plus (s,t). Let P be such a path. Then $G' \setminus P = G \setminus P$. Hence, by Lemma 6, there is exactly one cycle cover of $G' \setminus P$ and it is a perfect matching of weight 1. This means that there is a one-to-one correspondence between the cycle covers of G' and the paths from s to t or from t to s. There is also a one-to-one correspondence between the paths from s to t and the paths from t to s.

Let us recall that the sign of a cycle cover is the sign of the underlying permutation and its signed weight is the product of its sign and weight. Let C be a cycle cover of G' involving the s-t-path P. The previous paragraph shows that the weight of C equals $\frac{1}{2}(-1)^{\frac{|G|-1}{2}}w(P)$. As C has an odd cycle and a perfect matching, its sign is $(-1)^{|G\setminus P|/2}$, that is the number of couples in the perfect matching. The inverse cycle cover $\bar{C}$ of G' has the same signed weight as C. Hence the sum of the signed weights of all cycle covers of G' equals twice the sum over all s-t-paths P of $\frac{1}{2}(-1)^{\frac{|G|-1}{2}}(-1)^{\frac{|G\setminus P|}{2}}w(P) = \frac{1}{2}(-1)^{\frac{|P|-1}{2}}w(P)$. By Lemma 6, this equals f and Lemma 4 concludes the proof.

◀

3 Characteristic 2

In characteristic 2, the construction of Section 2 fails because of the scalar 1/2 it uses. Nevertheless, for a polynomial computable by a weakly-skew circuit, it is possible to represent, by the usual symmetrization, its square as the determinant of a symmetric matrix. On the other hand, as pointed out in the introduction representing the polynomial itself is not always possible. Related to these problems, the VNP-completeness of the partial permanent is also studied. Actually, we give an almost complete answer to an open question of Bürgisser [4, Problem 3.1] showing that if the partial permanent is complete in finite fields of characteristic 2, then the (boolean) polynomial hierarchy collapses. For any field of characteristic 2 (finite or infinite), we show that the VNP-completeness of this family would imply that every VNP family of polynomials has its square in VP_{ws}. This also seems unlikely to happen unless $\mathsf{VP}_{ws} = \mathsf{VNP}$.

Let G be an edge-weighted graph with vertices $\{v_1, \ldots, v_n\}$. Recall that the adjacency matrix A of G is the $(n \times n)$ symmetric matrix defined by $A_{ij} = A_{ji} = w_{ij}$ where w_{ij} is the weight of the edge $v_i v_j$. Suppose now that G is bipartite with two independent sets of vertices V_r and V_c of cardinality m and n respectively. Let $V_r = \{r_1, \ldots, r_m\}$ and $V_c = \{c_1, \ldots, c_n\}$.

The *biadjacency matrix* of G (also known as the *bipartite adjacency matrix*) is the $(m \times n)$ matrix B such that B_{ij} is the weight of the edge between r_i and c_j. This means that the rows of B are indexed by V_r and its columns by V_c. For a bipartite graph G of adjacency and biadjacency matrices A and B respectively,

$$A = \begin{pmatrix} 0 & B \\ B^t & 0 \end{pmatrix}.$$

Throughout this section, we shall use the usual definition of the weight of a partial matching: it is the product of the weights of the edges it uses.

3.1 Symmetric determinantal representation of the square of a polynomial

▶ **Lemma 7.** *Let G be an edge-weighted graph and A its adjacency matrix. In characteristic 2, the determinant of A is the sum of the weights of the cycle covers with cycles of length at most 2.*

Proof. Let us consider G as a symmetric digraph (that is an edge uv is seen as both arcs (u, v) and (v, u)). In Lemma 4, the signs of the cycle covers are considered. In characteristic 2, this is irrelevant. Therefore, the determinant of A is the sum of the weights of the cycle covers of G.

Let C be a cycle cover of G containing a (directed) cycle of length at least 3 denoted by $(v_1, v_2, \ldots, v_k, v_1)$. One can change the direction of this cycle (as G is symmetric) and obtain a new cycle cover C' containing the same cycles as C, but $(v_k, v_{k-1}, \ldots, v_1, v_k)$ instead of $(v_1, v_2, \ldots, v_k, v_1)$. Clearly, the weights of C and C' are the same as the graph is symmetric. Therefore, when the determinant of A is computed in characteristic 2, the contributions of those two cycle covers to the sum cancel out. This shows that the determinant of a matrix in characteristic two is obtained as the sum of the weights of cycle covers with cycles of length 1 (loops) or 2. ◀

▶ **Proposition 8.** *Let p be a polynomial over a field of characteristic 2, represented by a weakly-skew circuit of fat size m. Then there exists a symmetric matrix A of size $(2m + 2)$ such that $p^2 = \det(A)$.*

Proof. Let C be a weakly-skew circuit representing a polynomial p over a field of characteristic 2. Let M be the matrix obtained by Malod and Portier's construction [14] such that $p = \det(M)$. Let G be the digraph represented by M, and let G' be the bipartite graph obtained from G by the two following operations: Each vertex v of G is turned into two vertices v^s and v^t in G', and each arc (u, v) is turned into the edge $\{u^s, v^t\}$. A loop on a vertex u is simply represented as the edge $\{u^s, u^t\}$. Let A be the symmetric adjacency matrix of G' (when the vertices are ordered $v_0^s, v_1^s, \ldots, v_m^s, v_0^t, \ldots, v_m^t$).

It is well-known that cycle covers of G and perfect matchings of G' are in one-to-one correspondence. This one-to-one correspondence shows that the determinant of M equals the sum of the weights of the perfect matchings in G'. If a perfect matching in G' is considered as a cycle cover with length-2 cycles, the weight of the cycle cover is the square of the weight of the perfect matching. Indeed, in the cycle cover, all the arcs of the length-2 cycles have to be considered, that is each edge contributes twice to the product. Lemma 7 and the fact that there is no loop in G' show that

$$\det(A) = \sum_{\mu} w(\mu)^2 = \Big(\sum_{\mu} w(\mu)\Big)^2,$$

where μ ranges over all perfect matchings of G' and $w(\mu)$ is the weight of the perfect matching μ. The second equality holds as the field has characteristic 2.

Finally, it is shown in [14] that $p = \det(M)$, and we showed that $\det(M) = \sum_\mu w(\mu)$ and $\det(A) = \left(\sum_\mu w(\mu)\right)^2$. Therefore, $\det(A) = \det(M)^2 = p^2$. ◀

This proposition raises the following question: Let f be a family of polynomials such that $f^2 \in \mathsf{VP}_{ws}$. Does f belong to VP_{ws}? This question is discussed with more details in the next section.

3.2 Is the partial permanent complete in characteristic 2?

▶ **Definition 9.** Let $X = (X_{ij})$ be an $(n \times n)$ matrix. The partial permanent of X, as defined by Bürgisser [4], is

$$\mathrm{per}^*(X) = \sum_\pi \prod_{i \in \mathrm{def}(\pi)} X_{i\pi(i)},$$

where the sum ranges over the injective partial maps from $[n] = \{1, \ldots, n\}$ to $[n]$ and $\mathrm{def}(\pi)$ is the domain of the partial map π.

The family (PER^*_n) is the family of polynomials such that PER^*_n is the partial permanent of the $(n \times n)$ matrix whose coefficients are the indeterminates X_{ij}.

▶ **Lemma 10.** *Let G be the complete bipartite graph with two independent sets of vertices V_r and V_c such that the edge between r_i and c_j is labelled by B_{ij} (the matrix B is the biadjacency matrix of G). Then the partial permanent of B is equal to the sum of the weights of the partial matchings of G.*

A partial matching in a graph G is a set of pairs of vertices connected by an edge such that no vertex appears in more than a pair. Equivalently, a partial matching can be seen as a set of disjoint edges. The weight of a partial matching is the product of the weights of its edges.

The proof of the lemma is quite straightforward as a injective partial map π from $[n]$ to $[n]$ exactly defines a partial matching in G such that for $i \in \mathrm{def}(\pi)$, r_i is matched with $c_{\pi(i)}$.

▶ **Lemma 11.** *Let G be the complete bipartite graph with two independent sets of vertices V_r and V_c such that the edge between r_i and c_j is labelled by B_{ij} (the matrix B is the biadjacency matrix of G). Let A be its adjacency matrix. Then in characteristic 2,*

$$\det(A + I_{2n}) = (\mathrm{per}^*(B))^2,$$

where I_{2n} is the identity matrix of size $2n$.

Proof. By Lemma 7, to compute a determinant in characteristic 2, one can focus only on cycles of length at most 2. A cycle cover with such cycles actually is a partial matching when the graph is symmetric (length-2 cycles define the pairs of vertices, and length-1 cycles are isolated vertices). Considering G as a symmetric digraph, the weight of a cycle cover is equal to the product of the weights of its loops and the square of the weights of the edges it uses (a length-2 cycle corresponds to an edge).

Consider the graph G' obtained from G by adding weight-1 loops on all its vertices. In other words, G' is the graph whose adjacency matrix is $A + I_{2n}$. By the previous remark, and by the fact that the loops have weight 1, the determinant of $A + I_{2n}$ is

$$\det(A + I_{2n}) = \sum_\mu w(\mu)^2 = \left(\sum_\mu w(\mu)\right)^2$$

where μ ranges over the partial matchings of G' and $w(\mu)$ is the weight of the partial matching μ. The second equality is true as the characteristic of the field is 2.

Recall now that G is bipartite. Of course, the partial matchings of G and G' are the same. So

$$\mathrm{per}^*(B) = \sum_{\mu} w(\mu),$$

where μ ranges over the partial matchings of G. This proves the lemma. ◀

This lemma shows in particular that for computing the parity of the number of partial matchings in a bipartite graph, it is sufficient to compute a determinant (this is the case where G is not edge-weighted). Therefore, this problem is solvable in polynomial time. This was already mentioned by Valiant [19] but without any proof or reference.

▶ **Theorem 12.** *In characteristic* 2*, the family* $((\mathrm{PER}^*)_n^2)$ *is in* VP_{ws}*.*

Proof. The previous lemma shows that the polynomial $(\mathrm{PER}^*)_n^2$ is a p-projection of DET_{2n} in characteristic 2. Thus, $((\mathrm{PER}^*)_n^2)$ is in VP_{ws} as $(\mathrm{DET}_n) \in \mathsf{VP}_{ws}$ [14]. ◀

Suppose that (PER_n^*) is VNP-complete. Then every VNP family (f_n) is a p-projection of (PER_n^*), and thus (f_n^2) is a p-projection of $((\mathrm{PER}^*)_n^2)$. Let $\mathsf{VNP}^2 = \{(f_n^2) : (f_n) \in \mathsf{VNP}\}$ be the class of *squares of* VNP *families*. This implies the following corollary of the theorem:

▶ **Corollary 13.** *In any field of characteristic* 2*, if* (PER_n^*) *is* VNP*-complete, then* $\mathsf{VNP}^2 \subseteq \mathsf{VP}_{ws}$*.*

This situation is unlikely to happen. In particular, it would be interesting to investigate whether this inclusion implies that $\mathsf{VP}_{ws} = \mathsf{VNP}$ in characteristic 2. Let us now give another consequence of (PER_n^*) being VNP-complete. This only holds for finite fields of characteristic 2 but may give a stronger evidence that (PER_n^*) is unlikely to be VNP-complete.

▶ **Theorem 14.** *If the partial permanent family is* VNP*-complete in a finite field of characteristic* 2*, then* $\oplus\mathsf{P}/\mathsf{poly} = \mathsf{NC}^2/\mathsf{poly}$*, and the polynomial hierarchy collapses to the second level.*

The proof of this theorem uses the *boolean parts* of Valiant's complexity classes defined in [4]. In the context of finite fields of characteristic 2, the boolean part of a family (f_n) of polynomials with coefficients in the ground field $\mathbb{F}_2$ is the function $bp_f : \{0,1\}^* \to \{0,1\}$ such that for $x \in \{0,1\}^n$, $bp_f(x) = f_n(x) \pmod 2$. The boolean part $\mathrm{BP}(C)$ of a Valiant's class C is the set of boolean parts of all $f \in C$.

Proof. Let (f_n) be a VNP family and (φ_n) its boolean part. As $\varphi_n(x) \in \{0,1\}$ for all $x \in \{0,1\}^n$, (φ_n) is the boolean part of (f_n^2) too. This shows that $\mathrm{BP}(\mathsf{VNP}) \subseteq \mathrm{BP}(\mathsf{VNP}^2)$. By Corollary 13, $\mathsf{VNP}^2 \subseteq \mathsf{VP}_{ws} \subseteq \mathsf{VP}$. Thus, $\mathrm{BP}(\mathsf{VNP}) \subseteq \mathrm{BP}(\mathsf{VNP}^2) \subseteq \mathrm{BP}(\mathsf{VP})$ and as $\mathsf{VP} \subseteq \mathsf{VNP}$

$$\mathrm{BP}(\mathsf{VP}) = \mathrm{BP}(\mathsf{VNP}).$$

Bürgisser [4] shows that in a finite field of characteristic 2, $\oplus\mathsf{P}/\mathsf{poly} = \mathrm{BP}(\mathsf{VNP})$, and $\mathrm{BP}(\mathsf{VP}) \subseteq \mathsf{NC}^2/\mathsf{poly}$. Hence, $\oplus\mathsf{P}/\mathsf{poly} \subseteq \mathsf{NC}^2/\mathsf{poly}$. Moreover, $\mathsf{NC}^2/\mathsf{poly} \subseteq \mathsf{P}/\mathsf{poly} \subseteq \oplus\mathsf{P}/\mathsf{poly}$ hence we conclude that

$$\oplus\mathsf{P}/\mathsf{poly} = \mathsf{NC}^2/\mathsf{poly}.$$

The collapse of the polynomial hierarchy follows from a non uniform version of the Valiant-Vazirani Theorem [20]: Theorem 4.10 in [4] states that $\mathsf{NP/poly} \subseteq \oplus\mathsf{P/poly}$. Therefore,

$$\mathsf{NC}^2\mathsf{/poly} \subseteq \mathsf{NP/poly} \subseteq \oplus\mathsf{P/poly} = \mathsf{NC}^2\mathsf{/poly}.$$

In particular, $\mathsf{P/poly} = \mathsf{NP/poly}$ and Karp and Lipton [10] showed that this implies the collapse of the polynomial hierarchy to the second level. ◀

4 Conclusion

As was already mentioned, our results can be refined by using a modified version of the skinny size in which multiplications by constants do not count (this is the size considered in [12]). Let us call *green size* this variant. Furthermore, if the polynomial is given as a formula rather than as a weakly-skew circuits, some better bounds can be obtained. These two improvements are detailed in [5, Sections 2 and 3]. Table 1 compares the results obtained, in this paper and in previous ones. The bounds are given for a formula of green size e and for a weakly-skew circuit of green size e with i input gates labelled by a variable, and take into account the improvements explained in the long version.

	Non-symmetric matrix	Symmetric matrix
Formula	$e+1$	$2e+1$[a]
Weakly-skew circuit	$(e+i)+1$	$2(e+i)+1$

[a] The bound is achieved if and only if the entries can be complex numbers. Else, the bound is $2e+2$.

Table 1 Bounds for determinantal representations of formulas and weakly-skew circuits. The bounds for symmetric representations are new, and the bound for a non-symmetric representation of a weakly-skew circuit is a slight improvement of known bounds.

The $(e+1)$ bound for the representation of a formula by a (non-symmetric) matrix determinant was given in [12] by a method purely based on matrices. We show in [5, Section 2.1] that this bound can also be obtained directly from Valiant's original proof [18]. Along the way, we show that Valiant's proof contained a little flaw that was surprisingly never pointed out in the literature (and is present in more recent texts such as [4]). The $(e+i+1)$ bound for the representation of a polynomial computed by a weakly-skew circuit can be obtained from the $(m+1)$ bound (where m is the fat size of the circuit) obtained in [14] if we use our minimization lemma [5, Lemma 15] as well as a similar trick as in the proof of [5, Theorem 5]. Both bounds for the symmetric cases are given in the long version of this paper.

All of these results are valid for any field of characteristic different from 2. We showed that there are some important differences in fields of characteristic 2 for the complexity of polynomials. The open question of characterizing which polynomials can be represented as determinants of symmetric matrices is quite intriguing. Note that a lot of *variants* of the irreprensentable polynomial $xy+z$ (such as $xy+z+xyz+1$ and $xy+1$) do admit symmetric determinantal representations.

References

1 Amos Beimel and Anna Gál. On arithmetic branching programs. *J. Comput. Syst. Sci.*, 59(2):195–220, 1999.

2 Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inform. Process. Letters*, 18:147–150, 1984.

3 P. Brändén. Obstructions to determinantal representability. *ArXiv e-prints*, April 2010. http://adsabs.harvard.edu/abs/2010arXiv1004.1382B.

4 Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Algorithms and Computation in Mathematics. Springer, 2000.

5 Bruno Grenet, Erich L. Kaltofen, Pascal Koiran, and Natacha Portier. Symmetric Determinantal Representation of Formulas and Weakly Skew Circuits. http://arxiv.org/abs/1007.3804v2, 2010.

6 Bruno Grenet, Thierry Monteil, and Stephan Thomassé. Symmetric determinantal representations in characteristic 2. In preparation.

7 J. William Helton, Scott A. McCullough, and Victor Vinnikov. Noncommutative convexity arises from linear matrix inequalities. *J. Funct. Anal.*, 240(1):105–191, November 2006. http://math.ucsd.edu/~helton/osiris/NONCOMMINEQ/convRat.ps.

8 J.W. Helton and V. Vinnikov. Linear matrix inequality representation of sets. *Communications on Pure and Applied Mathematics*, 60(5):654–674, 2006. http://arxiv.org/pdf/math.OC/0306180.

9 Erich Kaltofen and Pascal Koiran. Expressing a fraction of two determinants as a determinant. In David Jeffrey, editor, *ISSAC 2008*, pages 141–146, New York, N. Y., 2008. ACM Press. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/08/KaKoi08.pdf.

10 R.M. Karp and R.J. Lipton. Turing machines that take advice. *L'Enseignement Mathématique*, 28:191–209, 1982.

11 A.S. Lewis, P.A. Parrilo, and M.V. Ramana. The Lax conjecture is true. *Proceedings of the American Mathematical Society*, 133(9):2495–2500, 2005. http://arxiv.org/pdf/math.OC/0304104.

12 H. Liu and K.W. Regan. Improved construction for universality of determinant and permanent. *Inf. Process. Lett.*, 100(6):233–237, 2006.

13 M. Mahajan and V. Vinay. Determinant: Combinatorics, algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, 5(1997):730–738, 1997.

14 G. Malod and N. Portier. Characterizing Valiant's algebraic complexity classes. *J. Complexity*, 24(1):16–38, 2008. Presented at MFCS'06.

15 Noam Nisan. Lower bounds for non-commutative computation. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 410–418. ACM, 1991.

16 Ronan Quarez. Symmetric determinantal representation of polynomials. http://hal.archives-ouvertes.fr/hal-00275615/en/, April 2008.

17 S. Toda. Classes of arithmetic circuits capturing the complexity of computing the determinant. *IEICE T. Inf. Syst.*, 75(1):116–124, 1992.

18 L. G. Valiant. Completeness classes in algebra. In *Proc. 11th STOC*, pages 249–261, New York, N.Y., 1979. ACM.

19 L.G. Valiant. Completeness for parity problems. *Computing and Combinatorics*, pages 1–8, 2005.

20 L.G. Valiant and V.V. Vazirani. NP is as easy as detecting unique solutions. *Theor. Comput. Sci.*, 47:85–93, 1986.

21 J. von zur Gathen. Feasible arithmetic computations: Valiant's hypothesis. *J. Symb. Comput.*, 4(2):137–172, 1987.