HAL
open science

Symmetric Determinantal Representation of Formulas and Weakly Skew Circuits

Bruno Grenet, Erich Kaltofen, Pascal Koiran, Natacha Portier

▶ **To cite this version:**

Bruno Grenet, Erich Kaltofen, Pascal Koiran, Natacha Portier. Symmetric Determinantal Representation of Formulas and Weakly Skew Circuits. 2010. ensl-00504925v2

HAL Id: ensl-00504925

https://ens-lyon.hal.science/ensl-00504925v2

Preprint submitted on 26 Jul 2010 (v2), last revised 24 Oct 2011 (v4)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Symmetric Determinantal Representation of Formulas and Weakly Skew Circuits

Bruno Grenet[*] Erich L. Kaltofen[†] Pascal Koiran[*]
Natacha Portier[*‡]

July 26, 2010

Rapport de Recherche RRLIP20010-24

Abstract

We deploy algebraic complexity theoretic techniques for constructing symmetric determinantal representations of formulas and weakly skew circuits. 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.

[*]LIP, UMR 5668, ENS de Lyon – cnrs – UCBL – INRIA, École Normale Supérieure de Lyon, Université de Lyon and Department of Computer Science, University of Toronto
{Bruno.Grenet,Pascal.Koiran,Natacha.Portier}@ens-lyon.fr

[†] Dept. of Mathematics, North Carolina State University, Raleigh, North Carolina 27695-8205, USA
kaltofen@math.ncsu.edu; http://www.kaltofen.us

This material is based on work supported in part by the National Science Foundation under Grants CCF-0830347 and CCF-0514585.

[‡] partially funded by European Community under contract PIOF-GA-2009-236197 of the 7th PCRD.

1 Introduction

1.1 Motivation

A linear matrix expression 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.

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 real zero polynomials $f(x_1, \ldots, x_n)$ representations (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 [Lewis et al. 2005] 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 $n > 2$ [Helton and Vinnikov 2006] (actually, [Lewis et al. 2005] give the first proof of the Lax conjecture in its original form based on the results of [Helton and Vinnikov 2006]). Two relaxations have been suggested to avoid this counting argument: At first it was suggested to remove the dimension constraint and seek for bigger matrices, and this was further relaxed by seeking for representations of some power of the input polynomial. Counterexamples to both relaxations have recently been constructed [Brändén 2010].

Another relaxation is to drop the condition $A_0 \succeq 0$ and represent any f as $\det(A)$ [Helton et al. 2006; Quarez 2008]. However, the purely algebraic construction of [Quarez 2008] leads to exponential matrix dimensions t. Here we continue the line of work initiated by [Helton et al. 2006; Quarez 2008] but we proceed differently by symmetrizing the complexity theoretic construction by Valiant [1979]. 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 [Malod and Portier 2008; Kaltofen and Koiran 2008]. Even though in the most general case the bounds we obtained are slightly worse than Quarez's [2008], 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 (see Section 4). Our constructions are valid for any field of characteristic different from 2. For fields of characteristic 2, we conjecture that some polynomials cannot be represented as determinants of symmetric matrices. A simple candidate to prove this is the polynomial $xy + z$. This is related to a question of Bürgisser [2000]: Is the partial permanent VNP-complete over fields of characteristic 2? We give an almost complete negative answer to this question. Beyond a proof or a disproof that the polynomial $xy + z$ (or any other polynomial) cannot be represented as a determinant of a symmetric matrix, it would be interesting to exactly characterize which polynomials admit such a representation in characteristic 2. It is

shown in the paper that for every polynomial p, p^2 admits a symmetric determinantal representation in characteristic 2.

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 $O(n^5)$ which entries are the inderminates 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 [Berkowitz 1984; Malod and Portier 2008], and this weakly-skew circuit can be represented by a determinant of a symmetric matrix as proved in this paper. Note that the conjecture that $xy + z$ has no symmetric determinantal representation in characteristic 2 means that the matrix $\left(\begin{smallmatrix} x & z \\ 1 & y \end{smallmatrix}\right)$ cannot be "symmetrized."

Organization. Section 1.2 is devoted to an introduction to the algebraic complexity theoretic used in our constructions, as well as a reminder of the existing related constructions in algebraic complexity. Section 2 deals with symmetric representations of formulas while Section 3 focuses on weakly-skew circuits. Table 2 page 34 gives an overview of all the different constructions used in this paper. Section 4 then proceeds to the comparisons between the results obtained so far and Quarez's [2008]. The special case of fields of characteristic 2 is studied in Section 5.

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.

1.2 Known results and definitions

In his seminal paper Valiant [1979] 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 [Nisan 1991; Beimel and Gál 1999]. 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 [1987] gives another way to express a formula as a determinant: his proof does not use digraphs and his bound is $2e + 2$. Refining his techniques, Liu and Regan [2006] gave a construction leading to a $e + 1$ bound and an extra property: multiplications by constant are free and do not count into the size of the formula.

Our purpose here is to express a formula as a determinant of a symmetric matrix. Multiplications by constant are also given for free. Our construction uses paths in graphs, similar to the paths in digraphs in original Valiant's proof. In fact, this original

construction appears to have a little flaw in it. Interestingly enough, this flaw has never been mentioned in the literature to the authors' knowledge. A slight change in the proof is given in [Bürgisser et al. 1997, Exercise 21.7 (p570)] that settles a part of the problem. And the same flaw appears in the proof of the universality of the permanent in [Bürgisser 2000]. When adding two formulas, the resulting digraph can have two arcs between the source and the target, which can lead to the sum of two variables being an entry of the matrix, and this is not allowed in this model. The first idea to correct the proof is to keep the same parity for all s-t-path as in Valiant's original proof, adding two new vertices and replacing one of the arcs by a length-three path. This method is very simple but its disadvantage is that it increases the size of the final matrix to $2e + 3$. In the symmetric case we will use -1 coefficient to correct the parity differences between paths instead of adding new vertices. Using this technique in the non-symmetric case allows us to prove Valiant's theorem with $(e + 1)$ instead of $(e + 2)$. Our technique also gives for free multiplications by constants as in [Liu and Regan 2006]. It uses digraphs and is to our opinion more intuitive than direct work on matrices.

In [Toda 1992; Malod and Portier 2008], results of the same flavor were proved for a more general class of circuits, namely the *weakly-skew* circuits. Malod and Portier [2008] 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 restriction on the degree of the polynomials) for which the determinant is complete under p-projection. 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 constraint 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 by the only 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 specifically computed for this gate.

Toda [1992] 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 [2008]: 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 gates). Note that for a circuit in general and for a weakly-skew circuit in particular $m \leq 2e + 1$. The latter construction uses negated variables in the matrix. It is actually possible to get rid of them [Kaltofen and Koiran 2008]. Although the skinny size is well suited for the formulas, the fat size appears more appropriate for weakly-skew circuits. In Section 3, 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. In fact, this can be refined as well as the non-symmetric construction. An even more appropriate size for a weakly-skew circuit

is $(e+i)$ where e is the skinny size and i the number of inputs labelled by a variable (clearly $e+i \leq m$). We can show that the bounds are still valid if we replace m by $(e+i)$ and even when multiplications by constants are free as in [Liu and Regan 2006] (see Section 3.2).

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 *gates* and its arcs *arrows*.

An arithmetic circuit with constant inputs in a field k and variables in a set $\bar{x}$ naturally computes a polynomial $f \in k[\bar{x}]$.

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. A gate α receiving arrows from β and γ is said to be *disjoint* if the sub-circuits associated to β and γ are disjoint from one another. The gates β and γ are called the *arguments* of α.

A *formula* is an arithmetic circuit in which all the gates are disjoint.

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. For instance, in Fig. 1, the weakly-skew circuit on the left has two closed sub-circuits. The input x_1 is in the left closed sub-circuit and is therefore not reusable. But inside this closed sub-circuit, it is reusable. On the right of the same figure is an equivalent formula, that is both the circuit and the formula compute the polynomial $2x_1x_2 + 2x_1y + x_2z + yz$. Let us remark

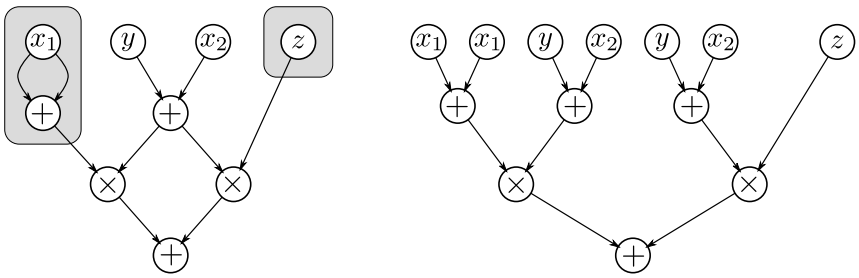


Figure 1: A weakly-skew circuit (left) and an equivalent arithmetic formula.

a fact that will be useful later: all the multiplication gates of a weakly-skew circuit are disjoint (but it is not a sufficient condition).

In our constructions, we shall use *graphs* and *digraphs*. In particular, the improved construction based on Valiant's represents formulas by paths in a digraph. On the

other hand, to obtain symmetric determinantal representations the digraphs have to be symmetric. These correspond to graphs. In order to avoid any confusion between directed and undirected graphs, we shall exclusively use the term graph for undirected ones, and use digraphs else. 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 1. *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 $\{1, \ldots, n\}$ 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 $A_{1,\sigma(1)} \cdots A_{n,\sigma(n)}$, whence 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 sequel, 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 the sequel as the weight of the corresponding cycle cover (with length-2 cycles). This means that this 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 $1 \leq i \leq k-1$, there exists an arc from u_i to u_{i+1} with nonzero weight. The size $|P|$ of such a path is k.

2 Formulas

2.1 Non-symmetric case

In this section, as in Sections 2.2 and 3, a field k of characteristic different from 2 is fixed and the constant inputs of the formulas and the weakly-skew circuits are taken from k. The variables are supposed to belong to a countable set $\bar{x} = \{x_1, x_2, \dots\}$. Following [Liu and Regan 2006], we define a formula size that does not take into account multiplications by constants.

Definition 4. Consider formulas with inputs being variables or constants from k. The green size $\mathrm{gsize}(\varphi)$ of a formula φ is defined inductively as follows:

- The green size of a constant or a variable is 0;
- If c is a constant then the green size of $c \times \varphi$ is equal to the green size of φ;
- If φ_1 and φ_2 are formulas, then $\mathrm{gsize}(\varphi_1 + \varphi_2) = \mathrm{gsize}(\varphi_1) + \mathrm{gsize}(\varphi_2) + 1$.
- If φ_1 and φ_2 are non-constant formulas, then $\mathrm{gsize}(\varphi_1 \times \varphi_2) = \mathrm{gsize}(\varphi_1) + \mathrm{gsize}(\varphi_2) + 1$

An even smaller size can be defined by deciding that every variable-free formula has size zero and Theorem 1 can easily be extended to this case. A formal definition of this size is given is Section 3.2 in the context of weakly-skew circuits.

Theorem 1 ([Liu and Regan 2006])**.** *For every formula φ of green size e with at least one addition there is a square matrix A of size $e+1$ whose entries are inputs of the formula and elements of $\{0, 1, -1, 1/2\}$ such that $\varphi = \det(A)$.*

Remark that if φ has no addition it is of the form $cx_1 \dots x_n$ and it has size $(n-1)$. Then a suitable matrix is the $(n+1) \times (n+1)$ diagonal matrix made of the n variables and the constant c. Thus the size is at most $n+1 = e+2$, and is $n = e+1$ if $c = 1$. Note that this latter bound is minimal as the determinant of a $(d \times d)$ matrix is a degree-d polynomial. The size $(n+1)$ is not minimal when $c \neq 1$ as shown by the (3×3) matrix

$$\begin{pmatrix} 0 & x & y \\ x & 0 & z \\ y & z & 0 \end{pmatrix}$$

representing $2xyz$. One can also see that the n bound cannot be general as there is no (2×2) matrix representing the polynomial $2xy$.

Lemma 2. *Let φ be an arithmetic formula of green size e. Then there exists a constant c_0 and an edge-weighted digraph G with at most $e+2$ vertices and two distinct vertices s and t such that*

$$c_0 \cdot \sum_{s\text{-}t\text{-path } P} (-1)^{|P|}\ w(P) = \varphi.$$

Proof of Lemma 2. We prove the lemma by induction on formulas. If φ is equal to a variable x (resp. a constant c) then G has two vertices s and t and an edge (s,t) labelled by x (resp. c) and the constant c_0 is equal to 1.

If $\varphi = c \times \varphi'$ let G' be the digraph and c'_0 the constant satisfying the lemma for the formula φ'. Then obviously $G = G'$ and $c_0 = c'_0 c$ satisfy the lemma for φ.

If $\varphi = \varphi_1 \times \varphi_2$, let G_1 and c_1 (resp. G_2 and c_2) satisfying the lemma for φ_1 (resp. φ_2). Then let $c = c_1 c_2$ and G be the disjoint union of G_1 and G_2, except for t_1 and s_2 which are merged (see Fig 2). The size of G is equal to $|G_1| + |G_2| - 1 \leq \text{gsize}(\varphi_1) + \text{gsize}(\varphi_2) + 3 =$

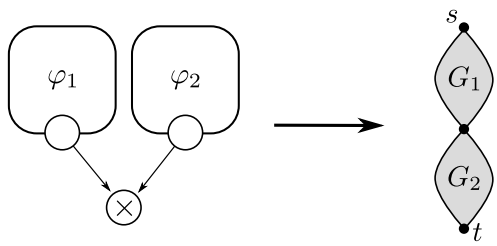


Figure 2: G_1, c_1 and G_2, c_2 are respectively associated to φ_1 and φ_2; $\varphi = \varphi_1 \times \varphi_2$.

$\text{gsize}(\varphi) + 2$. A s-t-path P in G is a s_1-t_1-path P_1 in G_1 followed by a s_2-t_2-path P_2 in G_2 and we have $|P| = |P_1| + |P_2| - 1$ and $w(P) = w(P_1) \times w(P_2)$, hence the result.

If $\varphi = \varphi_1 + \varphi_2$, let G_1 and c_1 (resp. G_2 and c_2) satisfying the lemma for φ_1 (resp. φ_2). If $c_1 = 0$ then φ and φ_2 compute the same polynomial and we just have to take $G = G_2$ and $c = c_2$. Suppose now $c_1 \neq 0$. Then we define G as the disjoint union of G_1 and G_2, except for s_1 and s_2 which are merged, and with an edge (t_2, t_1) of weight $-c_2/c_1$ (see Fig 3). The size of G satisfies the same relation as in the multiplication

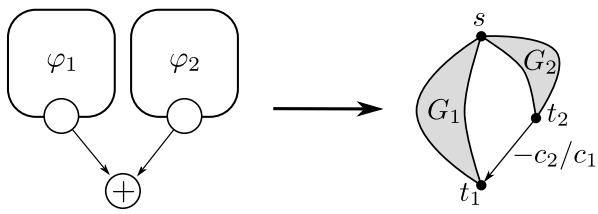


Figure 3: G_1, c_1 and G_2, c_2 are respectively associated to φ_1 and φ_2; $\varphi = \varphi_1 + \varphi_2$.

case. Let $c_0 = c_1$. A s-t-path P in G is a s_1-t_1-path in G_1 or a s_2-t_2-path P_2 in G_2 followed by the edge (t_2, t_1), and in the second case we have $w(P) = w(P_2)(-c_2/c_1)$ and $|P| = |P_2| + 1$, hence the result. Remark that t_2 has only one outgoing edge and

its weight is a constant, and that this property will not be changed in the inductive construction. This property will be useful to prove the bound in the theorem. □

Proof of Theorem 1. Let φ be an arithmetic formula of green size e and let G and c_0 be given by Lemma 2. Let $\bar{G}$ be the digraph obtained from G in the following way. We merge s and t. As remarked in the proof of Lemma 2 there is a vertex v that has only one outgoing edge and its weight is a constant c (as φ is supposed to have at least one addition). We change its weight to c_0c and add a loop weighted by c_0 on v. We put a loop with weight 1 on every other vertex than v and s.

Let $\{1, \ldots, e+1\}$ be the vertices of $\bar{G}$ and A its adjacency matrix. Let us have a closer look at cycle covers of $\bar{G}$. The cycles in $\bar{G}$ are cycles containing s (which are in bijection with s-t-paths in G) and loops. In a cycle cover C the vertex s belongs to a cycle S. Its weight $w(s)$ is the weight of the corresponding s-t-path P in G and its cardinal is $|S| = |P| - 1$. If the vertex v appears in S then $w(S) = c_0 w(P)$ and every other cycle in C is a loop of weight 1. Otherwise $w(S) = w(P)$ and C contains the loop v of weight c_0. In both case $w(C) = c_0 w(P)$. Let us recall that $\mathrm{sgn}(C)$ is the signature of the underlying permutation: here it is -1 if S is even and 1 otherwise, and so it is equal to $(-1)^{|P|}$. Using Lemma 1 we get

$$\det(A) = \sum_{\substack{\text{cycle cover} \\ C \text{ of } \bar{G}}} \mathrm{sgn}(C) w(C) = c_0 \cdot \sum_{\substack{s\text{-}t\text{-path} \\ P \in G}} (-1)^{|P|}\, w(P) = \varphi.$$

□

2.2 Symmetric case

The aim of this section is to write an arithmetic formula as a determinant of a symmetric matrix, whose entries are constants or variables. Recall that in this section as in Section 3, a field k of characteristic different from 2 is fixed, and the input constants are taken from this field. In the sequel, every constructed graph is undirected. At first, the result is proved for the skinny size of the formula. We recall that the skinny size of φ is the number of arithmetic operators it contains.

Theorem 2. *Let φ be an arithmetic formula of skinny size e. Then there exists a matrix A of size at most $2e+3$ whose entries are inputs of the formula and elements of $\{0, 1, -1, 1/2\}$ such that $\varphi = \det A$.*

This theorem is a corollary of the following lemma.

Lemma 3. *Let φ be an arithmetic formula of skinny size e. Then there exists a graph G with at most $2e+2$ vertices and two distinct vertices s and t such that*

1. *The graph G has an even number of vertices, every cycle in G is even and every s-t-path has an even number of vertices.*

2. *The subgraph $G \setminus \{s,t\}$ is empty if $e = 0$ and for $e \geq 1$ it has only one cycle cover: it is a perfect matching of weight 1. For every s-t-path P in G, the subgraph $G \setminus P$ is empty or has only one cycle cover: as above it is a perfect matching of weight 1.*

3. *The following equality holds in G:*

$$\sum_{s\text{-}t\text{-path } P} (-1)^{|P|/2+1}\ w(P) = \varphi$$

The graph G is called the graph associated to φ.

The first property of the lemma ensures that because of a parity argument every cycle cover of the final constructed graph $\bar{G}$ used in the proof of Theorem 2 (see Fig. 4) includes exactly one path between s and t. The second property ensures that the weight of the cycle cover is the weight of the cycle involving s and t, that is every other cycle has weight 1, and that other cycles of the cover are of length 2. The third property gives the relation between the graph and the formula.

As in Valiant's construction for the non necessarily symmetric case, the formula φ will be encoded in the weights of paths between s and t, but in a slightly different way. In Valiant's construction, a cycle cover of the digraph is made of a cycle including a s-t-path, other cycles being loops. Moreover every s-t-path has the same parity and so every cycle cover has the same parity of odd cycles and the underlying permutation has the same signature. With this property of the digraph the determinant of its adjacency matrix is equal to its permanent up to the sign. In our construction a cycle cover of the graph is made of a cycle including a s-t-path, other cycles being length-2 cycles. A length-2 cycle has a negative signature and every s-t-path of the graph has an even cardinality, so the sign of the cycle permutation is -1 to the number of length 2 cycles. This shows that the sign of the cycle permutation is a function of the length of the involved s-t-path *modulo* 4. There is a way to ensure that this sign does not depend on the chosen s-t-path: replace the graph G associated to a size-0 formula x in the proof of Lemma 3 by a 4-vertices path with weight x on its first edge, and replace weights -1 (Fig. 4, Fig. 6 and Fig. 7) by weights 1. This yields a matrix with entries in $k \cup \bar{x}$ whose determinant and permanent are equal to φ, but its size can be $4e + 5$. To achieve the $2e + 3$ bound, we construct a matrix A whose determinant can be very different from the permanent: For example, the permanent of the matrix associated to $\varphi = x + x$ is 0 when its determinant is $2x$. Nonetheless we can very easily obtain a matrix B having the same size that A and such that $\operatorname{perm} B = \varphi$ by replacing every -1 entry in A by 1.

Proof of Theorem 2. Let G be the graph associated to φ and let $\bar{G}$ be the graph G augmented with a new vertex c and the edges tc of weight $1/2$ and cs of weight $(-1)^{|G|/2-1}$ (see Fig. 4).

Conditions (1) and (2) imply that there is a bijection between paths from s to t or t to s and cycle covers in $\bar{G}$. More precisely, every cycle cover in $\bar{G}$ has a unique odd cycle and it is of the form cPc where P is a s-t-path or a t-s-path. Indeed, the graph $\bar{G}$ has

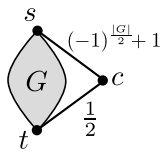


Figure 4: Construction of $\bar{G}$ from G.

an odd number of vertices. Suppose there is a cycle cover of $\bar{G}$ involving the length-2 cycle tct. Other cycles of this cover are cycles of G and thus by (1) they are all even. This is not possible as an odd set can not be partitioned into even subsets. For the same reason, there is no cycle cover of $\bar{G}$ involving the cycle scs. Thus every cycle cover of $\bar{G}$ has a cycle including c and a path P between s and t.

Let us recall that the sign of a cycle cover is the sign of the underlying permutation, i.e. -1 if it has an odd number of even cycles and 1 otherwise, and let us define the signed weight of a cycle cover as the product of its weight and sign. Let C be a cycle cover of $\bar{G}$ involving the s-t-path P. By property (2) there is only one way to complete the cover. Thus the weight of the cycle cover is the weight of P multiplied by $(1/2\ (-1)^{|G|/2+1})$ and its sign is the sign of a perfect matching of cardinality $|G \setminus P|$, so it is $(-1)^{(|G\setminus P|)/2}$. By symmetry, the inverse cycle cover has the same signed weight. So the sum of the signed weights of all cycle covers of $\bar{G}$ is equal to twice the sum over all s-t-path P of $(1/2\ (-1)^{|P|/2+1}\ w(P))$. According to Lemma 3 it is equal to φ. The result follows from Lemma 1.

□

Proof of Lemma 3. Let $\varphi = x$ be an arithmetic formula of size 0. Then the graph G associated to φ by definition has two vertices s and t and an edge st of weight x. It verifies trivially properties (1) and (2) and its only s-t-path is st and we have: $(-1)^{2/2+1}x = \varphi$.

Let $\varphi = \varphi_1 + \varphi_2$ and G_1 and G_2 be the graphs associated to φ_1 and φ_2. First let us suppose s_1t_1 or s_2t_2 has weight 0. It means in particular that φ_1 or φ_2 is of size at least 1. Let $s = s_1 = s_2$ and $t = t_1 = t_2$. Suppose $G_1 \setminus \{s_1, t_1\}$ and $G_2 \setminus \{s_2, t_2\}$ have disjoints sets of vertices and let $G = G_1 \cup G_2$ (see Fig. 5). Then $|G| = |G_1| + |G_2| - 2 \leq 2|\varphi_1| + 2|\varphi_2| + 2 = 2|\varphi|$.

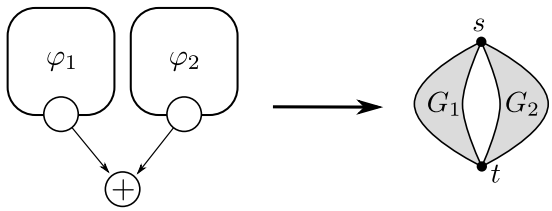


Figure 5: Graph associated to $\varphi = \varphi_1 + \varphi_2$.

If s_1t_1 is an edge in G_1 and s_2t_2 is an edge in G_2 then the preceding construction

would lead to two edges between s and t. They could be transformed into a single edge if adding the two weights, but then the weight could be a sum of two variables, and it is something that is not allowed in this context. So the graph G_1 is transformed into a graph G_1' by adding two vertices u and v, removing the edge s_1t_1 with weight x and adding the edges s_1u with weight x, uv with weight 1 and vt_1 with weight -1 (see Fig. 6). We can verify easily that G_1' verifies the three conditions of Lemma 3. In

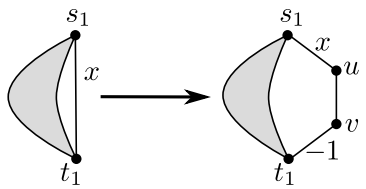


Figure 6: Transformation of G_1 into G_1'.

particular for the third condition, the term x corresponding to the path s_1t_1 in G_1 in the sum is replaced by the term corresponding to the path s_1uvt_1 in G_1': $-(-1)^{4/2+1}x = x$. We then construct the graph G associated to φ as above but with G_1' replacing G_1. It size is at most $2|\varphi| + 2$.

Now let us prove that the graph associated to φ satisfies the three properties of the lemma.

1. G has an even number of vertices and the cardinality of every s-t-path is even. A cycle in G is a cycle in G_1, or a cycle in G_2, or a path from s to t in G_1 or G_2 followed by path from t to s in G_1 or G_2, and consequently every cycle in G is even.

2. If $G_1 \setminus \{s_1, t_1\}$ and $G_2 \setminus \{s_2, t_2\}$ are non-empty they are disconnected, and a cycle cover of the subgraph $G \setminus \{s, t\}$ is constituted by a cycle cover of $G_1 \setminus \{s_1, t_1\}$ and a cycle cover of $G_2 \setminus \{s_2, t_2\}$. So $G \setminus \{s, t\}$ has only one cycle cover and it is a perfect matching of weight 1. If $G_1 \setminus \{s_1, t_1\}$ is empty then $G \setminus \{s, t\} = G_2 \setminus \{s_2, t_2\}$ and has only one cycle cover and it is a perfect matching of weight 1.

   Let P be a path between s and t in G. We can suppose wlog that the subgraph $G \setminus P$ is the union of the two graphs $G_1 \setminus P$ and $G_2 \setminus \{s_2, t_2\}$, which are disconnected from one another. The property to prove is then straightforward from the induction hypothesis.

3. A path of G is a path of G_1 or a path of G_2, which proves the equality.

Let $\varphi = \varphi_1 \times \varphi_2$ and G_1 and G_2 be the graphs associated to φ_1 and φ_2. Suppose G_1 and G_2 have disjoints sets of vertices and let G be $G_1 \cup G_2$ with an additional edge t_1s_2 of weight -1, and let $s = s_1$ and $t = t_2$ (see Fig.7). Then $|G| = |G_1| + |G_2| \leq 2|\varphi_1| + 2|\varphi_2| + 4 = 2|\varphi| + 2$. Let us prove that G satisfies the three properties of the lemma.

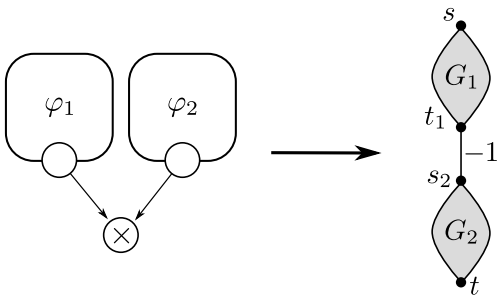


Figure 7: Graph associated to $\varphi = \varphi_1 \times \varphi_2$.

1. G has an even number of vertices and every path from s to t has an even cardinality. A cycle in G is either a cycle in G_1, or a cycle in G_2 or the length-2 cycle $t_1 s_2$, and consequently every cycle in G is even.

2. Let us consider a cycle cover of $G \setminus \{s, t\}$. The vertex t_1 can be in a cycle of G_1 or in the cycle $t_1 s_2$. If it is in a cycle of G_1 then we have a cycle cover of $G_1 \setminus \{s_1\}$, which is not possible because it is an odd set and all its cycles are even. Thus the cycle cover of $G \setminus \{s, t\}$ can be partitioned into $t_1 s_2$ of weight $(-1)^2$, a cycle cover of $G_1 \setminus \{s_1, t_1\}$ and a cycle cover of $G_2 \setminus \{s_2, t_2\}$. Those cycle covers are unique and so there is only one cycle cover of $G \setminus \{x, y\}$ and it is a perfect matching of weight 1.

   Let P be a path between s and t in G. It is a path P_1 from s_1 to t_1 in G_1 followed by $t_1 s_2$ and a path P_2 from s_2 to t_2 in G_2. So $G \setminus P$ is the union of the two graphs $G_1 \setminus P_1$ and $G_2 \setminus P_2$, which are disconnected (if non empty) from one another. The property to prove is then straightforward from the induction hypothesis.

3. A s-t-path P in G can be decomposed into three paths: a s_1-t_1-path P_1, $t_1 s_2$ which is of weight -1 and a s_2-t_2-path P_2.

   Thus

$$\begin{aligned}(-1)^{\frac{|P|}{2}+1}\ w(P) &= (-1)^{\frac{|P_1|+|P_2|}{2}+1} w(P_1)(-1)w(P_2) \\ &= (-1)^{\frac{|P_1|}{2}+1}\ w(P_1) \times (-1)^{\frac{|P_2|}{2}+1}\ w(P_2)\end{aligned}$$

   and so

$$\begin{aligned}\sum_P (-1)^{\frac{|P|}{2}+1}\ w(P) &= \sum_{P_1} (-1)^{\frac{|P1|}{2}+1} w(P_1) \times \sum_{P_2} (-1)^{\frac{|P_2|}{2}+1} w(P_2) \\ &= \varphi_1 \times \varphi_2 \\ &= \varphi.\end{aligned}$$

$\square$

The upper bound $(2e+2)$ of Lemma 3 is tight as shown by Fig. 8. It can be shown easily that this construction yields a graph of size at least $|\varphi|+2$, and this lower bound is tight as shown by Fig. 9.

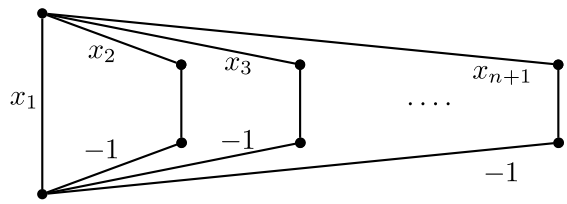


Figure 8: Graph associated to $\varphi = x_1 + \cdots + x_{n+1}$: $|\varphi| = n$ and $|G| = 2n+2$.

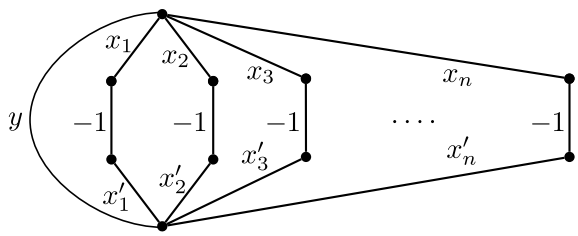


Figure 9: Graph associated to $\varphi = x_1x'_1 + x_2x'_2 \cdots + x_nx'_n + y$: $|\varphi| = 2n$ and $|G| = 2n+2$.

In fact, as in the non-symmetric case, the skinny size can be replaced by the green size of the formula defined in Definition 4.

Theorem 3. *For every formula φ of green size e there is a square matrix A of size $2e+3$ whose entries are inputs of the formula and elements of $\{0, 1, -1, 1/2\}$ such that $\varphi = \det A$.*

Proof. It is sufficient to show how to have the constants for free in the construction of Lemma 3. In fact, the construction remains almost the same but with the last property changed. For an arithmetic formula φ of green size e, there exists a graph G that satisfies the conditions of Lemma 3 but the third one is replaced by the existence of a constant c_0 such that

$$c_0 \cdot \sum_{s\text{-}t\text{-path } P} (-1)^{|P|/2+1}\, w(P) = \varphi.$$

Let $\varphi = x$ be an arithmetic formula of size 0. Then the graph G associated to φ by definition has two vertices s and t and an edge st of weight x. The associated constant is $c_0 = 1$.

Let $\varphi = c\psi$ and G, c_0 be associated to ψ. Then G, cc_0 is associated to φ.

Let $\varphi = \varphi_1 \times \varphi_2$ and G_1, c_1 (resp. G_2, c_2) be associated to φ_1 (resp. φ_2). The graph G associated to φ is exactly the same as in the proof of Lemma 3 and the constant is c_1c_2.

Let $\varphi = \varphi_1 + \varphi_2$ and G_1, c_1 (resp. G_2, c_2) be the graph and constant associated to φ_1 (resp. φ_2). We suppose that G_1 and G_2 have distinct sets of vertices except for $s_1 = s_2$. The graph G is obtained by adding a new vertex u, an edge t_2u with weight 1 and an edge ut_1 with weight $-c_2/c_1$, and the associated constant is c_1 (see Fig. 10).

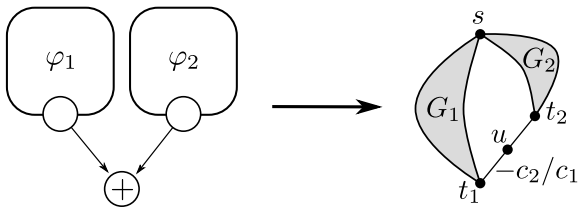


Figure 10: $\varphi = \varphi_1 + \varphi_2$; G_1, c_1 and G_2, c_2 are respectively associated to φ_1 and φ_2.

This defines a size-$(2e+2)$ graph G associated to a green size-e formula φ. It remains to turn this graph into a matrix. Let $\bar{G}$ be the graph G augmented with a new vertex c and the edges tc of weight $c_0/2$ and cs of weight $(-1)^{|G|/2-1}$. The adjacency matrix A of $\bar{G}$ satisfies $\varphi = \det(A)$ and the proof is similar to the one of Theorem 2. $\square$

The bound obtained in Theorem 3 can be sharpened when $k = \mathbb{R}$ or $\mathbb{C}$. The idea is to build $\bar{G}$ by merging s and t instead of adding a new vertex. Suppose that φ has at least one addition gate. Let $w = \sqrt{|c_0|/2}$. In the construction for this addition gate (see Fig. 10), multiply the weights of t_2u and ut_1 by w. A cycle cover of the graph either goes through the path t_2ut_1, or contains the edge ut_2 in its perfect matching part. In both cases, its weight is multiplied by w^2. Now if $(-1)^{|G|/2+1}c_0/2 > 0$, then the graph obtained has the satisfying properties, and the new bound is $2e+1$. If it is negative, two solutions can be applied. Either k is the field of complex numbers and it is sufficient to replace w by iw (where $i^2 = -1$) to get the same bound $2e+1$. Otherwise, if k is the field of real numbers, it is sufficient to add a new vertex with a loop of weight -1 (this corresponds to adding a new line and a new column, filled with zeroes but the diagonal element with -1) to get the bound $(2e+2)$.

3 Weakly skew circuits

In this section, we extend the previous results to the case of weakly-skew circuits. Recall that those circuits are defined from arithmetic circuits by a restriction on the multiplication gate: the sub-circuit associated to one of the arguments of a multiplication gate α has to be closed, that is only connected to the rest of the circuit by the arrow going to α. A gate that is not in any such closed sub-circuit is said to be *reusable*.

The main difficulty to extend the results in the existence of several reusable gates. In the case of formulas, there is a single output. Therefore, there is a single vertex t in the graph for which the sum of the weights of the s-t-paths has to equal a given expression. This is no longer the case for weakly-skew circuits. If the matrix we wish to construct is not symmetric, that is if the graph is oriented, this difficulty is overcome by ensuring

that the graph is a directed acyclic graph. In that way, adding a new vertex cannot change the expressions computed at previously added vertices. But in the symmetric case, adding a new vertex, for example in the case of an addition gate, creates some new paths in the graph. Thus it changes the sum of the weights of the s-t_α-paths for some vertex t_α.

A solution to this problem is given in Lemma 4 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.

3.1 Symmetric determinantal representation

For the weakly-skew circuits, the green size is no longer appropriate. Hence, the results of this section are expressed in terms of the fat size of the circuits: the *fat size* of a circuit is its total number of gates, including the input gates. This measure of the size of the circuits is refined in Section 3.2.

Theorem 4. *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 4. *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 has an odd number of vertices (even if not acceptable);*
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. The graph G is built by induction on the (fat) size of the circuit, the required properties being verified at each step of the induction. 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. It is straightforward to check that G satisfy the conditions of the lemma.

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. 11). The vertex s is the distinguished vertex of G. The size

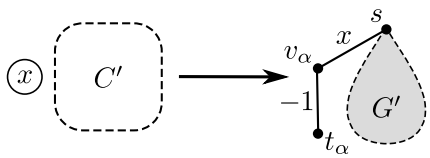


Figure 11: Induction step when α is an input gate.

of G is $|G| = |G'| + 2 \leq (2(m-1)+1)+2 = 2m+1$. Thus $|G|$ is odd. A cycle in G is either a cycle in G' or one of the two cycles sv_α or $v_\alpha t_\alpha$, so every cycle in G is even. The size-3 path from s to t_α is acceptable (as $G' \setminus \{s\}$ has a unique cycle cover of weight 1) and satisfies (2). Now, any other reusable gate β belongs to C', so the conditions are satisfied by induction hypothesis (it is sufficient to remark that when s is removed, v_α and t_α are disconnected from the rest of the circuit, and a cycle cover has to match those two vertices).

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. 12). 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. Then $|G| = |G'| + 2 \leq 2m+1$, and $|G|$ remains odd. Every s-t_δ-path for some reusable

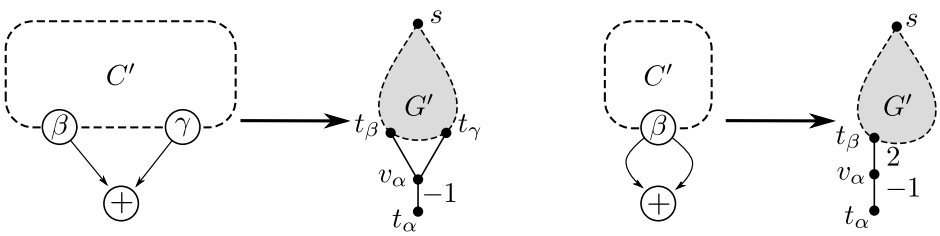


Figure 12: Induction step when α is an addition gate.

gate δ in C' is even. A cycle in G is either a cycle in G', or the cycle $v_\alpha t_\alpha$, or is made of a t_β-t_γ-path P in G' plus the vertex v_α. Let P' be q s-t_β-path and u the first vertex of P' belonging to P. Then, $P' = s, \ldots, u, \ldots, t_\beta$ and $P'' = s, \ldots, u, \ldots, t_\gamma$ are both even-size path. In particular the sizes of $u, \ldots, t_\beta$ and $u, \ldots, t_\gamma$ are of same parity. Thus P is of odd size and $P \cup \{v_\alpha\}$ is an even-size cycle. Hence, every cycle in G is even. An acceptable path in G is either an acceptable path in G' or a path from s to t_α. Indeed, the only way to cover t_α in a cycle cover is to match it with v_α. Therefore, no acceptable path goes through t_β, v_α and t_γ. So, the reusable gates in C' satisfy the conditions of the lemma by induction. Any acceptable path P from s to t_α is an acceptable path P' from s to t_β or t_γ followed by a path from t_β or t_γ to t_α. Thus $|P| = |P'| + 2$ is odd and $G \setminus P = G' \setminus P'$ has a unique cycle cover which is a perfect matching of weight 1. Finally,

$$\begin{aligned}
&\sum_{\substack{\text{acceptable}\\ s\text{-}t_\alpha\text{-path } P}} (-1)^{\frac{|P|-1}{2}} w(P) \\
=&\sum_{\substack{\text{acceptable}\\ s\text{-}t_\beta\text{-path } P_\beta}} (-1)^{\frac{|P_\beta|+2-1}{2}} (-1 \cdot w(P_\beta)) + \sum_{\substack{\text{acceptable}\\ s\text{-}t_\gamma\text{-path } P_\gamma}} (-1)^{\frac{|P_\gamma|+2-1}{2}} (-1 \cdot w(P_\gamma)) \\
=&\sum_{P_\beta} (-1)^{\frac{|P_\beta|-1}{2}} w(P_\beta) + \sum_{P_\gamma} (-1)^{\frac{|P_\gamma|-1}{2}} w(P_\gamma) \\
=&f_\beta + f_\gamma = f_\alpha.
\end{aligned}$$

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. 13 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. Then $|G| = |G_1| + |G_2| - 1$, so $|G|$ is odd,

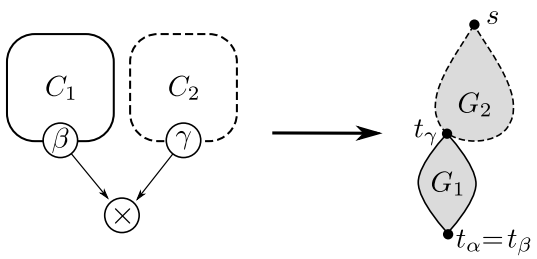


Figure 13: Induction step when α is a multiplication gate.

and if m_1 and m_2 are the respective sizes of C_1 and C_2 ($m = m_1 + m_2 + 1$), then $|G| \leq 2m_1 + 1 + 2m_2 + 1 - 1 = 2m - 1$. A cycle in G is either a cycle in G_1 or a cycle

in G_2 and is therefore even. The reusable gates of C are α and the reusable gates of C_2 (by definition, C_1 is closed and in particular t_β is not reusable). A path (in G) from s to a reusable gate of G_2 cannot enter G_1 so the reusable gates of G_2 satisfy the first and the third conditions in the lemma. Furthermore, if such a path P is removed from G, the only cycle cover of $G \setminus P$ has to be made of a cycle cover of $G_2 \setminus P$ and a cycle cover of $G_1 \setminus s_1$. Indeed, the vertex $s_1 = t_\gamma$ has to be either in a cycle cover of G_1 or in a cycle cover of G_2. But $G_2 \setminus (P \cup \{t_\gamma\})$ is a graph of odd size and cannot be covered by cycles of even size and G_1 is also of odd size. Thus, the reusable gates in G_2 also satisfy the second condition of the lemma. It remains to prove that the reusable gate α satisfies the conditions of the lemma:

1. A s-t_α-path P is a s-t_γ-path P_γ followed by a s_1-t_β-path P_β. Thus $|P| = |P_\gamma| + |P_\beta| - 1$ as $t_\gamma = s_1$ and $|P|$ is odd.

2. The graph $G \setminus P$ is the disjoint union of $(G_2 \setminus P_\gamma)$ and $(G_1 \setminus P_\beta)$, so by induction $G \setminus P$ is either empty or has a unique cycle cover which is a perfect matching of weight 1.

3. As $w(P) = w(P_\gamma)w(P_\beta)$, we have

$$\begin{aligned}(-1)^{\frac{|P|-1}{2}} w(P) &= (-1)^{\frac{|P_\gamma|+|P_\beta|-2}{2}} w(P_\gamma)w(P_\beta) \\ &= (-1)^{\frac{|P_\gamma|-1}{2}} w(P_\gamma) \times (-1)^{\frac{|P_\beta|-1}{2}} w(P_\beta),\end{aligned}$$

   whence

$$\begin{aligned}\sum_P (-1)^{\frac{|P|-1}{2}} w(P) &= \sum_{P_\gamma} (-1)^{\frac{|P_\gamma|-1}{2}} w(P_\gamma) \times \sum_{P_\beta} (-1)^{\frac{|P_\beta|-1}{2}} w(P_\beta) \\ &= f_\gamma \times f_\beta \\ &= f_\alpha.\end{aligned}$$

Finally, the only way to cover $G \setminus \{s\}$ is to cover $G_2 \setminus \{s_2\}$ on one hand and $G_1 \setminus \{s_1\}$ on the other hand for parity reasons as before. The weight of this cover is the product of the weights of the covers of G_1 and G_2, that is 1. □

Proof of Theorem 4. Let C be a weakly-skew circuit computing the polynomial f, and G be the graph built from C in Lemma 4. 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 4, 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 4, this equals f and Lemma 1 concludes the proof.

□

3.2 Minimization

The aim of this section is to refine the bound we obtained in Section 3.1, using the notion of green size that was defined in Section 2.1 (and matches the notion of size used in [Liu and Regan 2006]). As mentioned before, one can refine this notion of green size. It relies on the idea already mentioned by Liu and Regan for the formulas: One can add weights on the arrows of the circuit. If there is an arrow from a gate α to a gate β with weight c, then β receives as argument the value cf_α where f_α is the polynomial computed by α. Such a circuit is called a *weighted circuit*. Of course, a classical circuit is a weighted one with all weights equal to 1.

To refine the notion of green size, the idea is to avoid counting the variable-free sub-circuit. The next lemma shows that it is possible to do this in a very simple way.

Lemma 5. *If C is a weighted circuit, then there exists an equivalent weighted circuit C' with the same number of inputs labelled by a variable and at most the same number of computation gates such that:*

1. *An input gate is labelled either by a variable or the constant 1, and the constant inputs have out-degree 1;*
2. *An addition gate has at most one constant argument and this argument is an input gate;*
3. *A multiplication gate has both arguments non-constant.*

Proof. One can suppose that there exists some input gate labelled by a variable, otherwise the polynomial computed by C would be constant. To obtain the three points, each of the four following rules is recursively applied to C. Each rule is applied as long as possible before we apply the next one. We never go back to a previous rule.

1. Every input gate labelled by a constant c is replaced by an input gate labelled by 1, and the weight of an arrow going from it is multiplied by c. If there are several arrows going from this input gate, it is duplicated so that each copy has out-degree 1.

2. Every computation gate α that has both arguments constant is replaced by an input gate labelled by 1, and the weight of every arrow going from it is multiplied by the value α computed. As in previous step, the new input gates are duplicated to have out-degree 1.

3. If a multiplication gate α with positive out-degree has one constant argument β labelled by 1 and with an arrow from β to α of weight c_1, and another argument γ, non-constant, with an arrow of weight c_2, then α and β are deleted, and every arrow going from α of weight c is replaced by an arrow going from γ of weight cc_1c_2 (see Fig. 14).

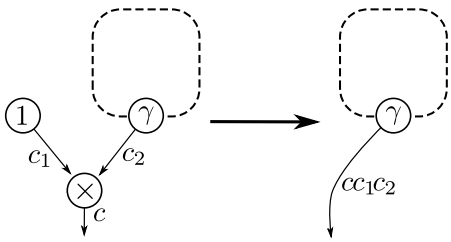


Figure 14: Minimization for a multiplication gate.

4. If the output gate α is a multiplication with one constant argument β with an arrow of weight c_1 going from β to α and the other argument γ, non-constant, with an arrow from γ to α of weight c_2, then α and β are deleted, γ becomes the new output gate, and the weight of every arrow coming to γ is multiplied by c_1c_2 (see Fig. 15).

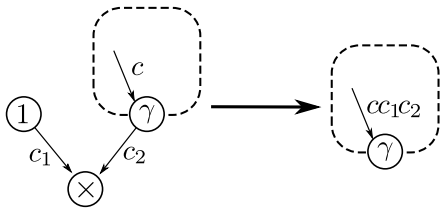


Figure 15: Minimization for the output gate.

The first two rules ensure that all the constant input gates are labelled by 1 and have out-degree 1. After the second rule, each computation gate has at most one constant argument, and that it is an input gate. Then rules 3 and 4 delete all multiplication gates that have a constant argument. □

Note that the above lemma is valid for any kind of arithmetic circuit, and that the construction does not change the nature of the circuit. So this can be applied to a formula to get a formula, or to a weakly-skew circuit to get a weakly-skew circuit.

Definition 5. Let C be an arithmetic circuit. Then the circuit C' obtained in Lemma 5 is the *minimized* circuit associated to C, and written $\min(C)$. The *green size* of C is equal to the skinny size of $\min(C)$, that is the number of computation gates in $\min(C)$.

Note that this definition does not exactly match Definition 4 in the case of formulas, but is equivalent to the size mentioned right after the definition. In fact, the way of defining the green size we use here yields a smaller size. Nevertheless, it is easy to see that the results obtained in Section 2.2 remain true with this new definition.

Theorem 5. *Let f be a polynomial computable by a weighted weakly skew circuit of green size e and with i inputs labelled by a variable. Then there exists a symmetric matrix A of size at most $2(e+i)+1$ whose entries are inputs of the circuit and elements of $\{0, 1, -1, 1/2\}$ such that $f = \det A$.*

Proof. The first step is to use Lemma 5 to minimize the circuit. Thus in the sequel the circuit is supposed to be a minimized weighted weakly-skew circuit. It is sufficient to show how to manage the constants in the construction of Lemma 4.

The idea is to have the same construction as in Lemma 4 but with the last property changed: for every reusable gate α, there exists a constant c_α such that

$$c_\alpha \cdot \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-path } P}} (-1)^{\frac{|P|-1}{2}} w(P) = f_\alpha. \tag{3}$$

The changes in the construction only concern the induction steps for computation gates (that is for multiplication and addition gates).

Suppose that α is an addition gate with one constant argument, say β, with an arrow from β to α of weight c_1. Suppose the second argument of α is a non-constant gate γ with an arrow from γ to α of weight c_2. By induction, there exists a graph G_γ of size $2((e-1)+i)+1$ that satisfies the conditions. In particular, there exists a distinguished vertex s, and a vertex t_γ with the required properties (let c_γ be the associated constant). Then G is obtained by adding two new vertices v_α and t_α and the following edges: an edge $t_\gamma v_\alpha$ of weight $c_2 c_\gamma$, an edge $v_\alpha t_\alpha$ of weight -1, and an edge $s v_\alpha$ of weight c_1 (see Fig. 16). One can check that G satisfies the required properties. In particular, t_α satisfies (3) with the constant 1, and $|G| = |G_\gamma| + 2 = 2((e-1)+i)+1+2 = 2(e+i)+1$.

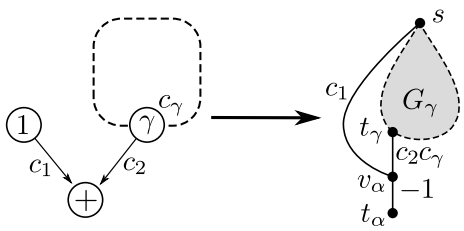


Figure 16: Graph obtained for the sum of a constant and a sub-circuit.

Suppose that α is an addition gate, receiving arrows from non-constant gates β and γ. There exist constants c_β and c_γ such that (3) holds for β and γ. Suppose that the arrows from β and γ to α have respective weights c_1 and c_2. The construction for the induction step in the same as in the proof of Lemma 4, on Fig. 12, with the following changes: the edges $t_\beta v_\alpha$ and $t_\gamma v_\alpha$ are respectively weighted $c_\beta c_1$ and $c_\gamma c_2$. Note that this does not change the weight of the perfect matching as those edges never belong to those matchings. As in that case, $f_\alpha = c_1 f_\beta + c_2 f_\gamma$, we obtain

$$\begin{aligned}
&\sum_{\substack{\text{acceptable}\\ s\text{-}t_\alpha\text{-path } P}} (-1)^{\frac{|P|-1}{2}} w(P)\\
=&\sum_{\substack{\text{acceptable}\\ s\text{-}t_\beta\text{-path } P_\beta}} (-1)^{\frac{|P_\beta|+2-1}{2}} (-c_1 c_\beta \cdot w(P_\beta)) + \sum_{\substack{\text{acceptable}\\ s\text{-}t_\gamma\text{-path } P_\gamma}} (-1)^{\frac{|P_\gamma|+2-1}{2}} (-c_2 c_\gamma \cdot w(P_\gamma))\\
=&c_1 \cdot \left(c_\beta \cdot \sum_{P_\beta} (-1)^{\frac{|P_\beta|-1}{2}} w(P_\beta) \right) + c_2 \cdot \left(c_\gamma \cdot \sum_{P_\gamma} (-1)^{\frac{|P_\gamma|-1}{2}} w(P_\gamma) \right)\\
=&c_1 f_\beta + c_2 f_\gamma = f_\alpha.
\end{aligned}$$

Note that the constant c_α associated to t_α is equal to 1 in that case. If $\beta = \gamma$, with the same notations as above, it is sufficient to replace the weight-2 edge $t_\beta v_\alpha$ by an edge of weight $2c_1 c_\beta$.

In the case of a multiplication gate, the construction (shown in Fig. 13) has no available edge to put the constants. But here, if the arrows from β and γ to α are still labelled by c_1 and c_2 respectively, then $f_\alpha = c_1 c_2 f_\beta f_\gamma$. Thus, the same construction is kept, and the constant c_α associated to α is defined to be $c_\alpha = c_1 c_2 c_\beta c_\gamma$ (where c_β and c_γ are respectively associated to β and γ).

It remains to adapt the proof of Theorem 4 to this case. This is easily done by multiplying the weight of the edge between s and t by the constant associated to the output gate. □

4 Comparison with Quarez's results

In this section, a comparison between our results and those in [Quarez 2008] is made. While Quarez builds matrices of fixed dimensions (depending only on the degree of the polynomial and its number of variables), we build matrices whose dimensions are polynomial in the size of the input formula or weakly-skew circuit. Consequently, if a polynomial can be represented as a formula or a weakly-skew circuit of small size (say polynomial in the number of variables and in the degree), then our constructions yield much smaller matrices than Quarez's. This is for example the case for the determinant polynomial (that is the determinant of a matrix of indeterminates) which is known to have a polynomial size weakly-skew circuit, or of the polynomial defined as the sum of all possible monomials of degree at most d (for this, see below). On the other hand, some polynomials are not known to have such polynomial size formulas or weakly-skew

circuits. A famous example among those is the permanent. We shall see that our constructions also yield better bounds in that interesting case. In the most general case though, our constructions may yield bigger matrices. The next theorem quantifies this.

Theorem 6. *Let p be a degree-d polynomial in n variables over a field k of characteristic different from 2. Then p admits a formula of skinny size*

$$F(n,d) \leq \binom{n+d+1}{n+1} - \binom{n+d-1}{n+1} - 2.$$

This yields a symmetric determinantal representation of size

$$S(n,d) \leq 4\binom{n+d-1}{n} - 2.$$

Proof. Let $P_{n,d}$ a degree-d polynomial in n variables $\{x_1, \ldots, x_n\}$. We shall build a *weighted formula* in the sense of Section 3.2, that is a formula with inputs in $\{1, x_1, \ldots, x_n\}$ and with weights on the wires. In a first time, a algorithm to build such a formula is explained, and then a bound on the size of the formula is given.

In order to clarify the construction, let us homogenize the polynomial $P_{n,d}$ with a new variable x_0. There exists two homogeneous polynomials $P_{n,d-1}$ and $P_{n-1,d}$ such that $P_{n,d-1}$ is a polynomial of degree at most $(d-1)$ in $(n+1)$ variables and $P_{n-1,d}$ is a polynomial of degree at most d in variables $x_0, \ldots, x_{n-1}$ which satisfy

$$P_{n,d} = x_n \cdot P_{n,d-1} + P_{n-1,d}. \tag{4}$$

Along with the equations $P_{k,1} = a_0x_0 + a_1x_1 + \cdots + a_kx_k$ and $P_{0,\delta} = p_0x_0^\delta$, this gives a formula for the polynomial $P_{n,d}$. Clearly, some $P_{k,\delta}$ may be the zero polynomial.

The rest of the proof is devoted to compute a bound on the size of the formula obtained by Equation (4). Let $F(n,d)$ denote the bound on the size of the formula computing $P_{n,d}$: $F(n,d) \leq F(n-1,d) + F(n,d-1) + 2$. For the base cases, $F(k,1) \leq k$ for all k, $F(0,\delta) \leq \delta - 1$. Let $G(N,d) = F(N-d-1,d) + 2$ (for $N > d$ and $d \geq 1$). Then $G(N,d)$ satisfies Pascal's formula

$$G(N,d) \leq G(N-1,d) + G(N-1,d-1) \tag{5}$$

and $G(\delta+1,\delta) \leq \delta+1$, $G(k+2,1) \leq k+2$. Thus it is exactly the binomial coefficient: $G(N,d) \leq \binom{N}{d}$ and

$$F(n,d) \leq \binom{n+d+1}{d} - 2. \tag{6}$$

This gives a first bound on $F(n,d)$, somewhat bigger than the announced one. This comes from the fact that the base case bound $F(0,\delta) \leq \delta - 1$ is too large: As the new variable x_0 is for homogenization, the actual formula is obtained by replacing it by 1 and therefore the formula for $P_{0,\delta} = p_0x_0^\delta$ is made of a single input labelled by 1 with the constant p_0 on the wire going from it. So $F(0,\delta) = 0$.

This remark yields the same equation as Equation (5) for G but with a new base case $G(\delta+1,\delta)=2$. A general form for such recurrences is

$$G(N,d)=\sum_{j=0}^{d} a_j \binom{N}{d-j}$$

for some a_j. Nevertheless, the values we get for the a_j if we apply this equation to the base cases are not really explicit. Therefore, we shall proceed in a different way: the new bound for $G(N,d)$ is computed as the difference between the bigger bound $\binom{N}{d}$ and the number of $P_{0,\delta}$ that were counted. In the recurrence (4), consider the recursion tree: Suppose that the vertex corresponding to $P_{n,d-1}$ is the left child of the vertex corresponding to $P_{n,d}$, and $P_{n-1,d}$ its right child. The root of the recursion tree corresponds to the output of the formula, and its leaves to some $P_{k,1}$ or some $P_{0,\delta}$. The quantity to count is the number of leaves corresponding to some $P_{0,\delta}$. A path from the root $P_{n,d}$ to $P_{0,\delta}$ has to decrease the first argument from n to 0 and the second from d to δ. In the recursion tree, this corresponds to a path going n times to the right and $(d-\delta)$ times to the left. Moreover, such a path finishes by a move from $P_{1,\delta}$ to its right child $P_{0,\delta}$, as $P_{0,\delta+1}$ has no child. Let us define the set of strings $W_{i,j}$ as

$$W_{i,j}=\{w\in\{L,R\}^* : |w|_R=i \text{ and } |w|_L=j\}\,.$$

The cardinality of $W_{i,j}$ is $\binom{i+j}{i}$ as an element of this set is determined by the i places for the letters R in a length-$(i+j)$ word. As the path from $P_{n,d}$ to $P_{0,\delta}$ finishes by a right move, the number of $P_{0,\delta}$ occurring in the recursion tree is equal to the cardinality of $W_{n-1,d-\delta}$, that is $\binom{n+d-\delta-1}{n-1}$. And for each $P_{0,\delta}$, the original bound counted $(\delta-1)$ operations instead of zero. Thus, to get a tighter bound we have to subtract

$$\sum_{\delta=1}^{d}(\delta-1)\binom{n+d-\delta-1}{n-1}=\sum_{j=0}^{d-1}(d-j-1)\binom{n+j-1}{j}.$$

Let Mon_n^j (resp. $\mathrm{Mon}_n^{\leq j}$) be the set of all monomials in n variables of degree j (resp. at most j). Then Mon_n^j has cardinality $\binom{n+j-1}{j}$, and $(d-j-1)\binom{n+j-1}{j}$ is the cardinality of the set $\{x^p\,\mathrm{Mon}_n^j : 0\leq p\leq d-j-2\}$ where x is a fresh variable. Thus, the sum over j of those quantities is the cardinality of $\mathrm{Mon}_{n+1}^{\leq d-2}$, that is $\binom{n+d-1}{n+1}$. This gives the first part of the theorem:

$$F(n,d)\leq\binom{n+d+1}{n+1}-\binom{n+d-1}{n+1}-2.$$

In the rest of the proof, we shall give a bound on the size of the matrix obtained by our construction of Section 2.

In [Quarez 2008], the symmetric matrix that is built contains linear functions as entries (and not only variables and constants). Therefore, we give a bound in that case for the size of the matrix to permit a tighter comparison between both methods. Authorizing

linear functions in the matrix corresponds to defining the size of the arithmetic formula $a_0x_0 + a_1x_1 + \cdots + a_kx_k$ as 0 instead of k. In other words, we can suppose that the inputs of the formula are not only constants and variables, but also linear functions. As in the previous paragraph, a direct computation where the bounds on the base cases are changed can be done but yields non explicit formulas. Therefore, we use the same technique as before: The size of the formula when inputs can be linear functions is the difference between the size of the classical formula and the number of linear functions that appear. Those linear functions are the $P_{k,1}$ and appear as leaves in the recursion tree. A leaf labelled by $P_{k,1}$ is reachable by a path going $(n-k)$ times to the right and $(d-1)$ times to the left. As above, the path finishes by a move from $P_{k,2}$ to its left child $P_{k,1}$. Therefore the number of leaves labelled by $P_{k,1}$ is the cardinality of $W_{n-k,d-2}$, that is $\binom{n+d-k-2}{n-k}$. All those leaves count for k additions, thus the total number of saved additions is

$$\sum_{k=1}^{n} k\binom{n+d-k-2}{n-k} = \sum_{j=0}^{n-1}(n-j)\binom{j+d-2}{j}.$$

The computation is now the same as above and this sum equals $\binom{n+d-1}{d}$. Using now Theorem 3, we get a symmetric matrix of size

$$S(n,d) \leq 2\left[\binom{n+d+1}{n+1} - \binom{n+d-1}{n+1} - \binom{n+d-1}{n-1} - 1\right].$$

To complete the proof, it is sufficient to use twice Pascal's formula:

$$\begin{aligned}\binom{n+d+1}{n+1} &= \binom{n+d}{n+1} + \binom{n+d}{n} \\ &= \left[\binom{n+d-1}{n+1} + \binom{n+d-1}{n}\right] + \left[\binom{n+d-1}{n} + \binom{n+d-1}{n-1}\right] \\ &= 2\binom{n+d-1}{n} + \binom{n+d-1}{n+1} + \binom{n+d-1}{n-1}.\end{aligned}$$

□

Note that the bound $F(n,d)$ we obtain with this construction is only better by a linear factor in n than the obvious formula consisting in summing all the monomials. Indeed, for any $j \leq d$, there are at most $\binom{n+j-1}{j}$ monomials of degree j which use $(j-1)$ multiplications, and there are at most $(\binom{n+d}{d} - 1)$ additions. Therefore the size of the formula we get in this way is

$$\sum_{j=1}^{d}(j-1)\binom{n+j-1}{j} + \binom{n+d}{d} - 1 = n\binom{n+d}{n+1} = \frac{n(n+d)}{n+1}\binom{n+d-1}{n}.$$

The first equality comes from similar techniques as in the previous proof and the second one is a straightforward computation. This yields a matrix of size $\frac{n(n+d)}{2(n+1)}S(n,d)$ approximately.

Nevertheless, this is a bound in the worst case, that is for a polynomial $M_{n,d}$ in which all the monomials of degree at most d appear. But in this special case one can change this construction if the aim is to have the polynomial $M_{n,d}$ itself. Indeed, the recurrence given by Equation (4) can be change in the following manner:

$$\begin{aligned} M_{n,d} &= x_n M_{n,d-1} + M_{n-1,d} \\ &= x_n M_{n,d-1} + x_{n-1} M_{n-1,d-1} + M_{n-2,d} \\ &= x_n M_{n,d-1} + \cdots + x_0 M_{0,d-1}. \end{aligned}$$

This gives an inductive construction of a skew circuit to compute $M_{n,d}$. At step 1, $M_{n,1}$ is built, and it is clear that every $M_{n-k,1}$ is represented by a gate in the circuit. At step $\delta \leq d$, suppose that we have a circuit such that every $M_{n-k,\delta-1}$ is represented by a gate. Then one can build a circuit with $(n+1)$ new variable inputs, $(n+1)$ multiplication gates and n addition gates such that every $M_{n-k,\delta}$ is represented by a gate. At each step, the circuit size increases by $(2n+1)$ and $(n+1)$ inputs are added. As the size of the circuit for degree 1 is n with $(n+1)$ inputs, the circuit for $M_{n,d}$ has size $(2nd - n + d - 1)$ and has $(n+1)d$ inputs. This yields a polynomial (in n and d) size matrix, much smaller than with Quarez's construction.

Let us now compare the bounds of Theorem 6 in the worst case with Quarez's. To this end let us consider a polynomial with n variables and of degree $2d$. Then Quarez builds a symmetric matrix of size $2\binom{n+d}{n}$ whereas our construction yields a matrix of size $4\binom{n+2d-1}{n} - 2$. A bound on the quotient of those quantities can be given using the inequalities (see e.g. [Knuth 1997])

$$\binom{n+d}{n} \leq \left(\frac{e(n+d)}{n}\right)^n \text{ and } \binom{n+2d-1}{n} \geq \left(\frac{n+2d-1}{n}\right)^n.$$

So, the quotient is bounded by

$$\left(\frac{e(n+d)}{n}\right)^n \cdot \left(\frac{n}{n+2d-1}\right)^n = e^n \cdot \left(\frac{n+d}{n+2d-1}\right)^n \leq e^n.$$

This means that Quarez's construction is exponentially better in the general case even though our construction yields much smaller matrices when the polynomial has a polynomial size formula or weakly-skew circuit.

We now compare Quarez's results and ours for the special case of the permanent. This is an important example of a polynomial for which no polynomial size circuit is known (even non weakly-skew). Nevertheless, there exists a formula for computing it of much smaller size than the bounds for the general case. Ryser's formula [Ryser 1963] to compute the permanent of a matrix M is

$$\operatorname{per}(A) = \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \notin S} M_{ij}.$$

As the sums of variables are not counted, this gives a size-$O(n2^n)$ formula, and hence yields a size-$O(n2^n)$ symmetric matrix to represent the permanent. Let us consider the

permanent of a $(2n \times 2n)$ matrix. This is a polynomial of degree $2n$ with $4n^2$ variables. Therefore, Quarez's construction yields a matrix of size $2\binom{4n^2+n}{n}$. This quantity can be bounded as above and therefore we get the following bound (up to a constant factor) for the quotient:

$$\frac{\binom{4n^2+n}{n}}{n2^{2n}} \geq \frac{\left((4n^2+n)/n\right)^n}{n4^n} \geq \frac{4^n n^n}{n4^n} = n^{n-1}.$$

A more careful computation shows that this quotient is equal to $O(n^{n-1/2}(4e)^n)$ when n tends to infinity.

5 Characteristic 2

In characteristic 2, the constructions of Sections 2 and 3 are not valid anymore because of the coefficients 1/2 they use. Nevertheless, for a polynomial computable by a weakly-skew circuit, it is possible to represent its square as the determinant of a symmetric matrix. On the other hand, representing the polynomial itself seems to be a challenging problem. For instance, it is not clear if it is possible to represent the polynomial $xy + z$ in this way. 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 [2000] (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. This also seems unlikely to happen unless VP = 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.

5.1 Symmetric determinantal representation of the square of a polynomial

Lemma 6. *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 1, 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 1. *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 [2008] such that $\operatorname{per} M = p$. 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. If there is a cycle cover of G, then each vertex v belongs to a cycle, and thus has both a predecessor v and a successor w. This means that u^t and u^s are matched to v^s and w^t respectively (if u is covered by a loop, then u^s and u^t are matched). Conversely, suppose that G' has a perfect matching. Let u^s be any vertex. Then it is matched to some v^t. In the same way, v^s is matched to some w^t. As the set of vertices is finite, as some point we go back to u^t. Thus it defines a cycle in G, and by doing the same process with other vertices not in this cycle this eventually defines a cycle cover in G.

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 6 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 [Malod and Portier 2008] 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, $\det(A) = \det(M)^2 = p^2$. $\square$

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

5.2 Is the partial permanent complete in characteristic 2?

Definition 6. Let $X = (X_{ij})$ be an $(n \times n)$ matrix. The partial permanent of X, as defined by Bürgisser [2000], 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 7. *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 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 partial injective 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 8. *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 6, 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. Otherwise stated, 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

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

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 [2005] but without any proof or reference.

Theorem 7. *In characteristic* 2*, the family* $((\mathrm{PER}^*)^2_n)$ *is in* VP*.*

Proof. The previous lemma shows that the polynomial $(\mathrm{PER}^*)^2_n$ is a p-projection of DET_{2n} in characteristic 2. Thus, $((\mathrm{PER}^*)^2_n)$ is in VP. □

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

Corollary 1. *In any field of characteristic* 2*, if* (PER^*_n) *is* VNP*-complete, then* $\mathsf{VNP}^2 \subseteq \mathsf{VP}$*.*

This situation is unlikely to happen. In particular, it would be interesting to investigate whether this inclusion implies that $\mathsf{VP} = \mathsf{VNP}$ 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 8. *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 [Bürgisser 2000]. 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 1, $\mathsf{VNP}^2 \subseteq \mathsf{VP}$. 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 [2000] 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, $\mathsf{NC}^2/\mathsf{poly} \subseteq \mathsf{P}/\mathsf{poly} \subseteq \oplus\mathsf{P}/\mathsf{poly}$ whence 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 [1986]: Theorem 4.10 in [Bürgisser 2000] states that $\mathsf{NP}/\mathsf{poly} \subseteq \oplus\mathsf{P}/\mathsf{poly}$. Therefore,

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

In particular, $\mathsf{P}/\mathsf{poly} = \mathsf{NP}/\mathsf{poly}$ and Karp and Lipton [1982] showed that this implies the collapse of the polynomial hierarchy to the second level. □

6 Conclusion

Figure 17 show the graphs obtained from the weakly-skew circuit and the formula of Fig. 1 for a field of characteristic different from 2, and Table 2 recalls all the constructions used in this paper.

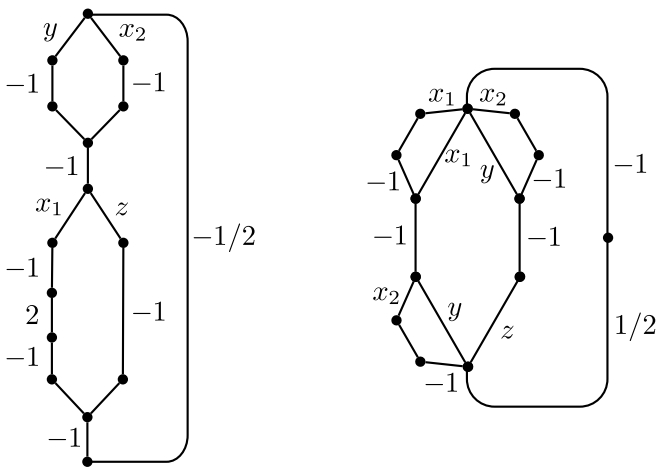


Figure 17: Graphs obtained from the circuit and formula of Fig. 1.

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.

	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 $(e+1)$ bound for the representation of a formula by a (non-symmetric) matrix determinant was given in [Liu and Regan 2006] by a method purely based on matrices. We show in Section 2.1 that this bound can also be obtained directly from Valiant's original proof when we remove the little flaw it contains. 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 [Malod and Portier 2008] if we use our minimization lemma (Lemma 5) as well as a similar trick as in the proof of Theorem 5. Both bounds for the symmetric cases are given in this paper.

A formula is a special case of weakly-skew circuit. If our construction for weakly-skew circuits is applied to a formula, this yields a matrix that can be as large as twice the size of the matrix obtained with the specific constructions for the formulas. In the converse way, one could turn a weakly-skew circuit into a formula and then apply the construction for the formula. Yet, turning a weakly-skew circuit into a formula of polynomial size is not known to be possible. In fact, this would give a polynomial size formula for the determinant, and hence a parallel time $O(\log n)$ for computing the determinant.

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, all the more so since we do not know whether the very simple polynomial $xy+z$ admits such a representation. Note that a lot of *variants* of this polynomial (such as $xy+z+xyz+1$) admit symmetric determinantal representations.

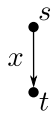
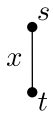
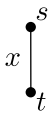
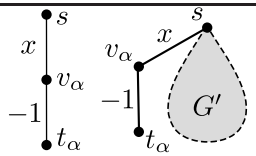
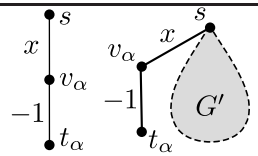
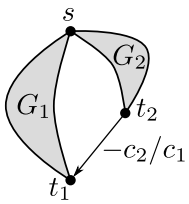
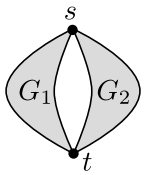
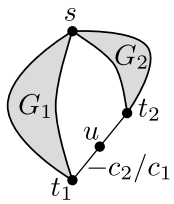
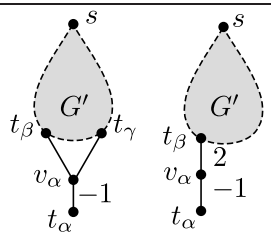
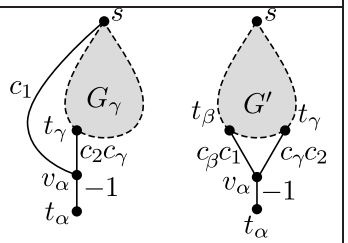
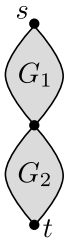
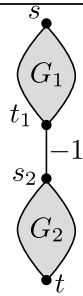
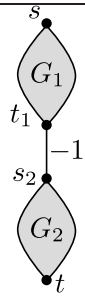
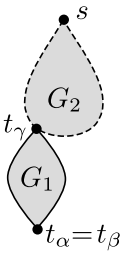
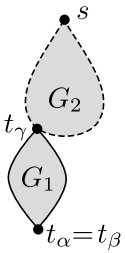
	Valiant's construction with constants (Section 2.1)	Formulas (Section 2.2)	Formulas with constants (Section 2.2)	Weakly skew circuits (Section 3.1)	Weakly skew circuits with constants (Section 3.2)
Input gate	 constant 1	 no constant	 constant 1	 no constant	 constants 1
Addition gate	 constant c_1	 no constant	 constant c_1	 no constant	 constants 1
Multiplication gate	 constant c_1c_2	 no constant	 constant c_1c_2	 no constant	 constant $c_1c_2c_\beta c_\gamma$

Table 2: Summary of the constructions

References

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

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

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

Bürgisser, Peter. *Completeness and Reduction in Algebraic Complexity Theory*. Algorithms and Computation in Mathematics. Springer, 2000. ISBN 9783540667520.

Bürgisser, Peter, Clausen, Michael, and Shokrollahi, Mohammad A. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997. ISBN 3540605827.

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

Helton, J. William, McCullough, Scott A., and Vinnikov, Victor. 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.

Kaltofen, Erich and Koiran, Pascal. Expressing a fraction of two determinants as a determinant. In Jeffrey, David, editor, *ISSAC 2008*, pages 141–146, New York, N. Y., 2008. ACM Press. ISBN 978-1-59593-904-3. URL: EKbib/08/KaKoi08.pdf.

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

Knuth, Donald E. *The Art of Computer Programming, Volume 1: Fundamental Algorithms (3rd Edition)*. Addison-Wesley Professional, 3rd edition, 1997. ISBN 9780201896831.

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

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

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

Nisan, Noam. 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.

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

Ryser, Herbert J. *Combinatorial Mathematics*, volume 14 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, 1963. ISBN 0883850141.

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

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

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

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

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