BINARY DETERMINANTAL COMPLEXITY

JESKO HÜTTENHAIN* AND CHRISTIAN IKENMEYER†

Abstract. We prove that for writing the 3 by 3 permanent polynomial as a determinant of a matrix consisting only of zeros, ones, and variables as entries, a 7 by 7 matrix is required. Our proof is computer based and uses the enumeration of bipartite graphs.

Furthermore, we analyze sequences of polynomials that are determinants of polynomially sized matrices consisting only of zeros, ones, and variables. We show that these are exactly the sequences in the complexity class of constant free polynomially sized (weakly) skew circuits.

Keywords: determinant, permanent, computational complexity, arithmetic circuit, constant-free

2010 Mathematics Subject Classification: 68Q05; 68-04.

2012 ACM Computing Classification System: Theory of computation – Models of computation; Theory of computation – Computational complexity and cryptography – Circuit complexity

1. Introduction

Let $\mathfrak{S}_m$ denote the symmetric group on m letters and let $\operatorname{per}_m := \sum_{\pi\in\mathfrak{S}_m}\prod_{i=1}^{m} x_{i,\pi(i)}$ denote the $m\times m$ permanent polynomial in m^2 variables. The flagship problem in algebraic complexity theory is finding superpolynomial lower bounds for the determinantal complexity of the permanent polynomial, a question whose roots date back to Valiant's seminal paper [Val79a], with an additional emphasis on the special role of the permanent in [Val79b].

We call a matrix whose entries are only variables or integers an *integer variable matrix*. One main implication of [Val79a] is the following theorem.

Theorem 1.1. For every polynomial f with rational coefficients one can always find a square matrix A whose entries are variables or rational numbers such that $\det(A) = f$. Moreover, if f has only integer coefficients, then A can be chosen as an integer variable matrix. □

For example,

$$\det\begin{pmatrix} 0 & x_{11} & x_{21} \\ x_{12} & 0 & 1 \\ x_{22} & 1 & 0 \end{pmatrix} = x_{11}x_{22} + x_{12}x_{21} = \operatorname{per}_2. \tag{1.2}$$

For an $n\times n$ square matrix we refer to n as its *size*. What is the minimal size of a matrix whose determinant is per_m and whose entries are only variables and rational numbers? For a given m we take $\operatorname{dc}(\operatorname{per}_m)$ to be this minimal size. It is famously conjectured by Valiant that the sequence $m\mapsto \operatorname{dc}(\operatorname{per}_m)$ of natural numbers grows superpolynomially fast. In modern terms we can concisely phrase this conjecture as $\mathbf{VP_{ws}} \neq \mathbf{VNP}$, see for example [MP08]. A graph construction by Grenet [Gre11], see Section 6.I, has the following consequence.

Theorem 1.3. For every natural number m there exists an integer variable matrix A of size $2^m - 1$ such that $\operatorname{per}_m = \det(A)$. Moreover, A can be chosen such that the entries in A are only variables, zeros, and ones, but no other constants. □

Theorem 1.3 gives rise to the following definition. We call a matrix whose entries are only zeros, ones, or variables, a *binary variable matrix*. We will prove in Corollary 2.4 that every polynomial f with integer coefficients can be written as the determinant of a binary variable matrix and that the size is almost the size of the matrix from Theorem 1.1, see Proposition 2.3 for a precise statement. We

*Technische Universität Berlin, jesko@math.tu-berlin.de.

†Texas A&M University, ciken@math.tamu.edu.

then denote by $\mathrm{bdc}(f)$ the smallest n such that f can be written as a determinant of an $n \times n$ binary variable matrix. It turns out that the complexity class of sequences (f_m) with polynomially bounded binary determinantal complexity $\mathrm{bdc}(f_m)$ is exactly $\mathbf{VP}^0_{\mathbf{ws}}$, the constant free version of $\mathbf{VP}_{\mathbf{ws}}$, see Section 5 for definitions and proofs.

Theorem 1.3 shows that $\mathrm{bdc}(\mathrm{per}_m) \leq 2^m - 1$. It is easy to see that this upper bound is sharp for $m = 1$ and for $m = 2$.

The best known general lower bound is $\mathrm{bdc}(\mathrm{per}_m) \geq \frac{m^2}{2}$ due to [MR04] in a stronger model of computation, see also [LMR10] for the same bound in an even stronger model of computation. This implies that $\mathrm{bdc}(\mathrm{per}_3)$ is either 5, 6, or 7.

The main result of this paper is the following.

Theorem 1.4. $\mathrm{bdc}(\mathrm{per}_3) = 7$.

We use a computer aided proof and enumeration of bipartite graphs in our study. The binary determinantal complexity of per_m is now known to be exactly $2^m - 1$ for $m \in \{1, 2, 3\}$. Unfortunately, determining $\mathrm{bdc}(\mathrm{per}_4)$ is currently out of reach with our methods.

Acknowledgments. We thank Peter Bürgisser, Gordon Royle, and JM Landsberg very much for interesting and helpful discussions. We are very grateful to the Simon's Institute for the Theory of Computing in Berkeley for hosting us during this project.

2. Binary Algebraic Branching Programs and the Cost of Computing Integers

The main purpose of this section is to prove that even though we only allow the constants 0 and 1, *all* polynomials with integer coefficients can be obtained as the determinant of a binary variable matrix, see Corollary 2.4. Moreover, the size of the matrices is not much larger than the size of matrices from Theorem 1.1, see Proposition 2.3. We use standard techniques from algebraic complexity theory, heavily based on [Val79a], but a certain attention to the signs has to be taken.

In what follows, a *digraph* is always a finite directed graph which may possibly have loops, but which has no parallel edges. We label the edges of a digraph by polynomials. We will almost exclusively be concerned with digraphs whose labels are only variables or the constant 1. Note that we consider only labeled digraphs.

A cycle cover of a digraph G is a set of cycles in G such that each vertex of G is contained in exactly one of these cycles. If a cycle in G has i edges with labels $e_1, \ldots, e_i$, then its *weight* is defined as $(-1)^{i-1} \cdot e_1 \cdots e_i$. The weight of a cycle cover is the product of the weights of its cycles. The *value* of G is the polynomial that arises as the sum over the weights of all cycle covers in G. We then define the *directed adjacency matrix* A of a digraph G as the matrix whose entry A_{ij} is the label of the edge (i, j) or 0 if that edge does not exist.

In what follows, we will often construct matrices as the directed adjacency matrices of digraphs. The reason is the following well-known observation, see for example [Val79a].

Observation 2.1. The value of a digraph G equals the determinant of its directed adjacency matrix.

As an intermediate step, we will often construct a *binary algebraic branching program*: This is an acyclic digraph $\Gamma = (\Gamma, s, t)$ where every edge is labeled by either 1 or a variable. The digraph Γ has two distinguished vertices, the *source* s and the *target* t, where s has no incoming and t has no outgoing edges. If an s-t-path in Γ has i edges with labels $e_1, \ldots, e_i$, then its *path weight* is defined as the value $(-1)^{i-1} \cdot e_1 \cdots e_i$. The *path value* of Γ is the polynomial that arises as the sum over the path weights of all s-t-paths in Γ. We remark that this notion of weight differs from the literature by a sign.

Proposition 2.2. For a nonzero constant $c \in \mathbb{Z}$, there is a binary algebraic branching program Γ with at most $\mathcal{O}(\log |c|)$ vertices whose path value is c.

Proof. We can assume without loss of generality that $c > 0$: Given a binary algebraic branching program Γ with path value $c > 0$ and at most $\mathcal{O}(\log c)$ vertices, we can add a single vertex t' and an edge from t to t' with label 1 to obtain a new program (Γ', s, t') with path value $-c$.

For a natural number c, an *addition chain* of length ℓ is a sequence of distinct natural numbers $1 = c_0, c_1, \ldots, c_\ell = c$ together with a sequence of tuples $(j_1, k_1), \ldots, (j_\ell, k_\ell)$ such that $c_i = c_{j_i} + c_{k_i}$ and $j_i, k_i < i$ for all $1 \leq i \leq \ell$. However, we will think of this data as a digraph $\tilde{\Gamma}$ on the vertices $\{c_0, \ldots, c_\ell\}$ with edges (c_{j_i}, c_i) and (c_{k_i}, c_i) for all $1 \leq i \leq \ell$. The labels of all edges are equal to 1. Note that we allow double edges in these digraphs temporarily. We set $s := c_0$ and $t := c_\ell$. Thus, we view an addition chain as an acyclic digraph where every vertex except for c_0 has indegree two. This already strongly resembles a binary algebraic branching program, but $\tilde{\Gamma}$ might have parallel edges. Observe that there are exactly c_i many paths from c_0 to c_i in the digraph $\tilde{\Gamma}$. In particular, there are exactly c paths from s to t in $\tilde{\Gamma}$.

Using the algorithm of repeated squaring [Knu97, Sec. 4.6.3, eq. (10)] one can construct an addition chain $\tilde{\Gamma}$ as above with at most $\mathcal{O}(\log c)$ vertices and such that there are exactly c paths from s to t in $\tilde{\Gamma}$. For every edge (v, w) in $\tilde{\Gamma}$ we add a new vertex u and replace the edge (v, w) by two new edges (v, u) and (u, w). We call the resulting digraph $\Gamma = (\Gamma, s, t)$. Observe that the binary algebraic branching program Γ has no parallel edges any more and all s-t-paths in Γ have even length. Also, the digraph Γ still has $\mathcal{O}(\log c)$ many vertices. Labelling all edges in Γ with 1, the path value of Γ is equal to c. □

Proposition 2.3. Let C be an $n \times n$ matrix whose entries are variables and *arbitrary* integer entries. Let $c_{\max}$ be the integer entry of C with the largest absolute value. Then there is a binary variable matrix A of size $\mathcal{O}(n^2 \cdot \log |c_{\max}|)$ with $\det(A) = \det(C)$.

Proof. We will interpret C as the directed adjacency matrix of a digraph. Any edge that has an integer label which is neither 1 nor 0 will be replaced by a subgraph of size $\mathcal{O}(\log |c_{\max}|)$ arising from

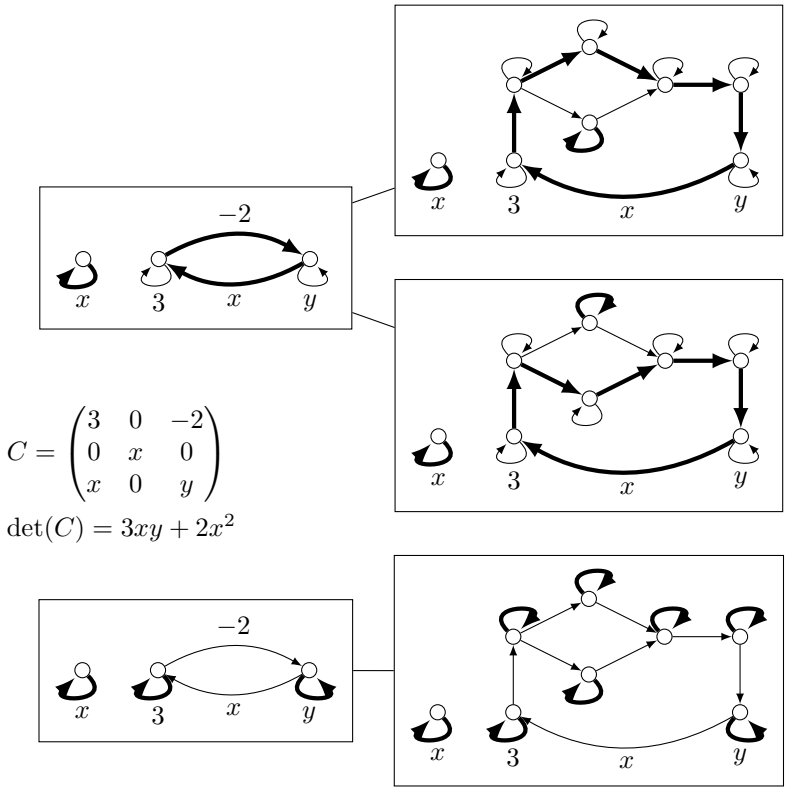

FIGURE 1. Given a matrix C we construct a digraph H with directed adjacency matrix C (left hand side) and the digraph G (right hand side) by replacing the edge with label -2 in H by a binary algebraic branching program. We omit the labels for edges that have label 1. The right hand side depicts the cycle covers K of G and the left hand side shows the corresponding cycle covers K^H of H.

the construction of the previous Lemma 2.2. The directed adjacency matrix of the resulting graph will be the desired matrix A. Formally, we proceed by induction.

Denote by q the number of integer entries in the matrix C that are neither equal to 0 nor 1. By induction on q, we will prove the slightly stronger statement that there is a binary variable matrix A of size $n + q \cdot \mathcal{O}(\log |c_{\max}|)$ with $\det(A) = \det(C)$. Since $q \leq n^2$, this implies the statement. Note that the case $q = 0$ is trivial, so we assume $q \geq 1$ and perform the induction step.

Let H be the digraph whose directed adjacency matrix is C. Recall that this means the following: H is a digraph on the vertices $1, \dots, n$ and there is an edge (i, j) with label C_{ij} if $C_{ij} \neq 0$ and otherwise no such edge exists. Let $e = (i, j)$ be the edge corresponding to an integer entry $c = C_{ij}$ which is neither 0 nor 1. Let $\Gamma = (\Gamma, s, t)$ be a binary algebraic branching program with path value c and $\mathcal{O}(\log |c|)$ many vertices, which exists by Proposition 2.2.

We will now replace the edge (i, j) by Γ (see Figure 1): Let G be the digraph that arises from $H \cup \Gamma$ by removing the edge (i, j), adding edges (i, s) and (t, j) with label 1 and adding loops with label 1 to all vertices of Γ. The directed adjacency matrix of G has size $n + \mathcal{O}(\log |c|) \leq n + \mathcal{O}(\log |c_{\max}|)$ and contains $q - 1$ integer entries which are neither 0 nor 1. By applying the induction hypothesis to the directed adjacency matrix of G, we obtain a matrix A of size

$$n + \mathcal{O}(\log |c_{\max}|) + (q - 1) \cdot \mathcal{O}(\log |c_{\max}|) = n + q \cdot \mathcal{O}(\log |c_{\max}|)$$

whose determinant equals the value of G. We are left to show that the value of G is equal to $\det(C)$, i.e., the value of H.

For this purpose, we will analyze the relation between cycle covers of G and H, which is straightforward (see Figure 1): Consider a cycle cover K of G. Any vertex of Γ which is not covered by its loop must be part of a cycle whose intersection with Γ is a path from s to t. To K we can therefore associate a cycle cover K^H of H as follows: If every vertex of Γ is covered by its loop in K, let K^H be K without these loops. Otherwise, there is unique cycle κ_K in K that restricts to an s-t-path π_K in Γ. Let κ_K^H be the intersection $\kappa_K \cap H$ together with the edge (i, j) and note that κ_K^H is a cycle in H. We obtain K^H from K by replacing κ_K with κ_K^H and removing all remaining loops from inside Γ.

All cycle covers L of H are of the form $L = K^H$ for some cycle cover K of G. If L is a cycle cover of H containing the edge (i, j) then the cycle covers K of G with $L = K^H$ are in bijection with the s-t-paths in Γ. We now fix such a cycle cover L. By definition of the value of a digraph, it suffices to show that

$$\sum_{\substack{K \text{ cycle cover of } G \\ \text{such that } L = K^H}} \text{weight}(K) = \text{weight}(L).$$

Note that K and $L = K^H$ differ only in loops and in the cycles κ_K and κ_K^H, respectively. Since loops contribute a factor of 1 to the weight of a cycle cover, we are left to prove that

$$\sum_{\substack{K \text{ cycle cover of } G \\ \text{such that } L = K^H}} \text{weight}(\kappa_K) = \text{weight}(\kappa_K^H).$$

Let $e_1, \dots, e_r$ be the labels of the edges of $\kappa_K \cap H$. These are the edges shared by κ_K and κ_K^H. Thus,

$$\begin{aligned}
\text{weight}(\kappa_K^H) &= (-1)^r \cdot c \cdot e_1 \cdots e_r \\
&= \left(\sum_{\substack{\pi \text{ is } s\text{-}t\text{-path} \\ \text{inside } P}} \text{weight}(\pi) \right) \cdot (-1)^r \cdot e_1 \cdots e_r = \left(\sum_{\substack{K \text{ cycle cover of } G \\ \text{such that } L = K^H}} \text{weight}(\pi_K) \right) \cdot (-1)^r \cdot e_1 \cdots e_r \\
&= \left(\sum_{\substack{K \text{ cycle cover of } G \\ \text{such that } L = K^H}} \text{weight}(\pi_K) \cdot (-1)^r \cdot e_1 \cdots e_r \right) = \sum_{\substack{K \text{ cycle cover of } G \\ \text{such that } L = K^H}} \text{weight}(\kappa_K)
\end{aligned}$$

is precisely the desired equality. □

Corollary 2.4. For every polynomial f with integer coefficients there exists a binary variable matrix whose determinant is f.

Proof. Combine Theorem 1.1 and Proposition 2.3. □

3. Lower Bounds

This section is dedicated to the proof of Theorem 1.4. Let $\mathbb{B} := \{0, 1\}$. A sequential numbering makes the proof much easier to read, so we think of the variables as arranged in a 3×3 matrix

$$x = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}.$$

In this section, we will understand $\mathrm{per}_3 = \mathrm{per}(x)$ as a polynomial in the variables $x_1, \ldots, x_9$ instead of the variables x_{ij} with $1 \leq i, j \leq 3$.

Proof Outline. Let $n \in \mathbb{N}$ and A an $n \times n$ binary variable matrix. The binary matrix $B(A) \in \mathbb{B}^{n\times n}$ is defined as the matrix arising from A by setting all variables to 1. We call $B(A)$ the *support matrix* of A. If we set all variables to 1 in per_3, we obtain the value 6, so if $\mathrm{per}_3 = \det(A)$, then substituting 1 for all variables on both sides of the equation, we obtain the condition

$$6 = \det(B(A)). \tag{3.1}$$

In [EZ62, Slo14], the maximal values of determinants of binary matrices are computed for small values of n. Since

$$\forall B \in \mathbb{B}^{5\times 5}\colon\ \det(B) \leq 5, \tag{3.2}$$

we immediately obtain the lower bound $\mathrm{bdc}(\mathrm{per}_3) \geq 6$.

Unfortunately, there are several matrices $B \in \mathbb{B}^{6\times 6}$ that satisfy $\det(B) = 6$. We proceed in two steps to verify that nevertheless, none of these matrices B is the support matrix $B(A)$ of a candidate matrix A with $\mathrm{per}_3 = \det(A)$. A rough outline is the following:

(a) Enumerate all matrices $B \in \mathbb{B}^{6\times 6}$ with $\det(B) = 6$ up to symmetries.
(b) For all those matrices B prove that B is not the support matrix $B(A)$ of a binary variable matrix A with $\det(A) = \mathrm{per}_3$. We describe this process in the next subsection.

3.I. **Stepwise Reconstruction.** Let us make part (b) precise. In the hope of failing, we attempt to reconstruct a binary variable matrix A that has support B and which also satisfies $\det(A) = \mathrm{per}_3$. During the reconstruction process, we successively replace 1's in B by the next variable. The process is as follows:

Given a binary matrix $B \in \mathbb{B}^{6\times 6}$, let $S := \{(i, j) \mid B_{ij} = 1\}$ be the set of possible variable positions. For any set of positions $I \subseteq S$, we consider the matrix B_I that arises from B by placing a variable y in every position in I. If B is the support of a binary variable matrix A with $\det(A) = \mathrm{per}_3$ and I contains exactly the positions where $y := x_1$ occurs in A, then $\det(B_I)$ must be equal to

$$\mathrm{per}_3 \begin{pmatrix} y & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 2y + 4. \tag{3.3}$$

We define the set $\mathcal{S} := \{I \subseteq S \mid \det(B_I) = 2y + 4\}$.

Claim 3.4. Let A be a binary variable matrix with support B and $\det(A) = \mathrm{per}_3$. Let $k \in \{1, \ldots, 9\}$ and define $I_k := \{(i, j) \mid A_{ij} = x_k\}$ as the set of positions where the variable x_k occurs in A. Then, we have $I_k \in \mathcal{S}$.

Proof. By the symmetry of the permanent, we may assume that $k = 1$. In the matrix A, setting every variable except $y := x_1$ to 1 yields the matrix B_I and therefore, $\det(B_I) = 2y + 4$ as in (3.3), because $\det(A) = \mathrm{per}_3$. This means $I_k \in \mathcal{S}$ by definition. □

Therefore, if B is the support matrix $B(A)$ of a binary variable matrix A with $\det(A) = \mathrm{per}_3$, we can find 9 pairwise disjoint sets in $\mathcal{S}$, one for each variable x_k, that specify precisely where to place these variables in A.

By a recursive search and backtracking, we now look for sets $I_1, \ldots, I_k \in \mathcal{S}$ such that

(i) $I_1, \ldots, I_k$ are pairwise disjoint.
(ii) Placing x_i into B at every position from I_i for $1 \leq i \leq k$ yields a matrix A_k such that $\det(A_k)$ is equal to $\mathrm{per}_3(x_1, \ldots, x_k, 1, \ldots, 1)$.

The search is recursive in the following sense: First, the possible choices at depth $k = 1$ are given by $\mathcal{S}$. Enumerating the possible choices for depth $k+1$ works as follows: For each choice $I_1, \ldots, I_k \in \mathcal{S}$ with the above two properties, we enumerate all $I_{k+1} \in \mathcal{S}$ that have empty intersection with $I_1 \cup \cdots \cup I_k$ and check whether condition (b) is satisfied.

If the recursive search never reaches $k = 9$ or fails there, then B is not the support of a binary variable matrix A with $\det(A) = \mathrm{per}_3$. If we reach level 9 however and do not fail there, we have found such an A.

In practice, the process is sped up significantly by working over a large finite field $\mathbb{F}_p$ and choosing random elements $x_1, \ldots, x_9 \in \mathbb{F}_p \setminus \{0, 1\}$.

3.II. **Exploiting Symmetries in Enumeration.** Let us call two matrices *equivalent* if they arise from each other by transposition and/or permutation of rows and/or columns. A key observation is that equivalent matrices have the same determinant up to sign. Therefore we do not have to list all binary matrices $B \in \mathbb{B}^{6\times 6}$ with $\det(B) = 6$, but it suffices to list one representative matrix B with $\det(B) = \pm 6$ for each equivalence class. It happens to be the case that the equivalence classes of 6×6 binary matrices are in bijection to graph isomorphy classes of undirected bipartite graphs $G = (V \cup W, E)$ with $|V| = |W| = 6$, $V \cap W = \emptyset$ as follows: For $V = \{v_1, \ldots, v_6\}$ and $W = \{w_1, \ldots, w_6\}$, the bipartite adjacency matrix $B(G) \in \mathbb{B}^{6\times 6}$ of G is defined via $B(G)_{i,j} = 1$ if and only if $\{v_i, w_j\} \in E$. Row and column permutations in $B(G)$ are reflected by renaming vertices in G. Transposition of $B(G)$ amounts to switching V and W in G.

The computer software nauty [MP13] can enumerate all 251 610 of these bipartite graphs, which is already a significant improvement over the $2^{36} = 68\,719\,476\,736$ elements of $\mathbb{B}^{6\times 6}$. To further limit the number of bipartite graphs that have to be considered, we make the following observations:

- We need not consider binary matrices B containing a row i with only a single entry B_{ij} equal to 1. Indeed, Laplace expansion over the i-th row yields that $\det(B)$ is equal to the determinant of a 5×5 binary matrix, which can at most be 5, see (3.2). Translating to bipartite graphs, we only need to consider those bipartite graphs where all vertices have at least two neighbours.
- If two distinct vertices in G have the same neighbourhood, then the bipartite adjacency matrix $B(G)$ has two identical rows (or columns) which would imply $\det(B(G)) = 0$. Hence, we only need to enumerate bipartite graphs where all vertices have distinct neighbourhoods. Unfortunately nauty can impose this restriction only on rows and not on columns.

With these restrictions, the nauty command

```
genbg -d2:2 -z 6 6
```

generates 44 384 bipartite graphs, only 263 of which have a bipartite adjacency matrix with determinant equal to ± 6. We then preprocess this list by swapping the first two rows of any matrix with negative determinant.

Finally, the stepwise reconstruction (section 3.I) fails for all of these 263 matrices, proving that $\mathrm{bdc}(\mathrm{per}_3) \geq 7$. The algorithm takes 28 seconds on an Intel Core$^{\mathrm{TM}}$ i7-4500U CPU (2.4 GHz) to finish.

Unfortunately, $\mathrm{bdc}(\mathrm{per}_4)$ can currently not be determined in this fashion because the enumeration of all apropriate bipartite graphs, already on $9 + 9$ vertices, is infeasible.

4. Uniqueness of the Grenet construction in the 7×7 case

The methods from Section 3 can be used to determine all 7×7 binary variable matrices A with the property that $\det(A) = \mathrm{per}_3$. By means of a cluster computation over the course of one week, we determined all 463 binary variable matrices with this property and made some noteworthy discoveries.

The Grenet construction (see Section 6.I) yields the matrix

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & x_{32} & x_{33} & 0 & 0 \\ 0 & 1 & 0 & x_{31} & 0 & x_{33} & 0 \\ 0 & 0 & 1 & 0 & x_{31} & x_{32} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & x_{23} \\ 0 & 0 & 0 & 0 & 1 & 0 & x_{22} \\ 0 & 0 & 0 & 0 & 0 & 1 & x_{21} \end{pmatrix}. \tag{4.1}$$

It is the unique "sparse" 7×7 binary variable matrix from among the 463, in the sense that every other matrix from the list has more than three nonzero entries in some row or column.

Motivated by the above observation, we wrote a program that would attempt to reduce the other matrices by elementary row and column operations. And indeed, all of the 463 matrices reduce to (4.1):

Proposition 4.2. Every 7×7 binary variable matrix A with $\det(A) = \mathrm{per}_3$ is equivalent to the Grenet construction (4.1) under the following two group actions:

(1) The action of $\{(g,h) \mid \det(g) = \det(h)\} \subseteq \mathrm{GL}_7(\mathbb{Z}) \times \mathrm{GL}_7(\mathbb{Z})$ on 7×7 matrices via left and right multiplication, together with transposition of 7×7 matrices.
(2) The action of $\mathfrak{S}_3 \times \mathfrak{S}_3$ on the variables x_{ij} with $1 \le i, j \le 3$, and the corresponding transposition (i.e. the map $x_{ij} \mapsto x_{ji}$.)

Note that (1) leaves the determinant of any 7×7 binary variable matrix invariant and (2) leaves the permanent polynomial invariant. □

Example 4.3. One of the matrices that occur in our enumeration is the matrix

$$A := \begin{pmatrix} x_{31} & x_{32} & x_{31} & 0 & x_{32} & 1 & x_{23} \\ 1 & x_{33} & 0 & x_{31} & x_{33} & x_{31} & x_{22} \\ x_{33} & 0 & x_{33} & x_{32} & 1 & x_{32} & x_{21} \\ 1 & 0 & 1 & 0 & 0 & 0 & x_{22} \\ 0 & x_{11} & x_{12} & x_{13} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & x_{21} \\ 0 & 0 & 0 & 1 & 0 & 1 & x_{23} \end{pmatrix}.$$

One can check that indeed $\det(A) = \mathrm{per}_3$. In this case, the matrices

$$g := \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \qquad h := \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

are both invertible over $\mathbb{Z}$ and gAh is precisely (4.1).

5. Algebraic Complexity Classes

In this section we relate binary determinantal complexity to classical complexity measures. An *algebraic circuit* $\mathcal{C}$ over the rational numbers is a directed acyclic digraph whose vertices have indegree 0 or 2 with a single vertex having outdegree 0. Those with indegree 0 are labeled with an integer or a variable, and are called *input gates*. Those with indegree 2 are labeled with either $+$ or $\times$ and are called *addition gates* and *multiplication gates*, respectively. At each addition or multiplication gate the circuit $\mathcal{C}$ defines a polynomial with rational coefficients via adding/multiplying the polynomials of its two parents. For the polynomial f which is defined at the unique vertex with outdegree 0 we say that the circuit $\mathcal{C}$ *computes* f. If all input gates are labeled with either 1, -1, or a variable, the circuit is called *constant-free*. Note that every constant-free circuit computes a polynomial that has integer coefficients. An algebraic circuit is called *skew* if for every multiplication gate at least one of its two parents is an input gate. An algebraic circuit is called *weakly skew* if for every multiplication gate

α there is at least one of its two parents β for which the circuit graph splits into disjoint connected components if we remove the edge between α and β. The *skew complexity* of f is defined as the minimal number of vertices required for a skew algebraic circuit to compute f. Analogously, the *weakly skew complexity* of f is defined as the minimal number of vertices required for a weakly skew algebraic circuit to compute f. Moreover, the *constant-free skew complexity* of f is defined as the minimal number of vertices required for a constant-free skew algebraic circuit to compute f and the *constant-free weakly skew complexity* of f is defined as the minimal number of vertices required for a constant-free weakly skew algebraic circuit to compute f. The complexity class $\mathbf{VP_s}$ is defined as the set of sequences of polynomials with polynomially bounded skew complexity. Analogously, the complexity class $\mathbf{VP_{ws}}$ is defined as the set of sequences of polynomials with polynomially bounded weakly skew complexity, the complexity class $\mathbf{VP_s^0}$ is defined as the set of sequences of polynomials with polynomially bounded constant-free skew complexity, and the complexity class $\mathbf{VP_{ws}^0}$ is defined as the set of sequences of polynomials with polynomially bounded constant-free weakly skew complexity, see also [Mal03]. A fundamental result in [Tod92] (see also [MP08]) is that $\mathbf{VP_{ws}} = \mathbf{VP_s}$. Analyzing the constants which appear in the proof of $\mathbf{VP_{ws}} = \mathbf{VP_s}$ in [Tod92], we see that the proof immediately yields $\mathbf{VP_{ws}^0} = \mathbf{VP_s^0}$. For the sake of comparison with $\mathbf{VP_s^0}$, let us make the following definition.

Definition 5.1. The complexity class $\mathbf{DETP}^0$ consists of all sequences of polynomials that have polynomially bounded binary determinantal complexity bdc.

The main purpose of this section is to show the following statement.

Proposition 5.2. $\mathbf{VP_s^0} = \mathbf{DETP}^0$.

Proof. The proof of [Tod92, Lemma 3.4] immediately shows that $\mathbf{DETP}^0 \subseteq \mathbf{VP_s^0}$. To show that $\mathbf{VP_s^0} \subseteq \mathbf{DETP}^0$ we want to adapt the proof of [Tod92, Lemma 3.5 or Theorem 4.3], but a subtlety arises: The proof shows that from a weakly skew or skew circuit $\mathcal{C}$ we can construct a matrix A' of size polynomially bounded in the number of vertices in $\mathcal{C}$ such that $\det(A')$ is the polynomial compute by $\mathcal{C}$ with the drawback that A' is not a binary variable matrix, but A' has as entries variables and constants 0, 1, and -1. Fortunately Proposition 2.3 establishes $\mathbf{DETP}^0 = \mathbf{VP_s^0} = \mathbf{VP_{ws}^0}$. □

Remark 5.3. In the past, other models of computation with bounded coefficients have already given way to stronger lower bounds than their corresponding unrestricted models: [Mor73] on the fast fourier transform, [Raz03] on matrix multiplication, and [BL04] on arithmetic operations on polynomials.

From Valiant's completeness result [Val79a] we deduce that $\mathbf{VP} \neq \mathbf{VNP}$ implies $\mathrm{per}_m \notin \mathbf{VP_{ws}^0}$. A main goal is to prove $\mathrm{per}_m \notin \mathbf{VP_{ws}^0}$ unconditionally. This could be a simpler question than $\mathbf{VP} \neq \mathbf{VNP}$ or even $\mathbf{VP}^0 \neq \mathbf{VNP}^0$, because with what is known today, from $\mathrm{per}_m \in \mathbf{VP_{ws}^0}$ we cannot conclude $\mathbf{VP}^0 = \mathbf{VNP}^0$, see [Koi04, Thm. 4.3]. If we replace the permanent polynomial by the Hamiltonian Cycle polynomial

$$\mathrm{HC}_m := \sum_{\substack{\pi \in \mathfrak{S}_m \\ \pi \text{ is } m\text{-cycle}}} \prod_{i=1}^{m} x_{i,\pi(i)},$$

then the question $\mathrm{HC}_m \notin \mathbf{VP_{ws}}$ is indeed equivalent to separating $\mathbf{VP_{ws}^0}$ from $\mathbf{VNP}^0$, see [Koi04, Thm. 2.5], mutatis mutandis. We ran our analysis for HC_m, $m \leq 4$ and proved $\mathrm{bdc}(\mathrm{HC}_1) = 1$, $\mathrm{bdc}(\mathrm{HC}_2) = 2$, $\mathrm{bdc}(\mathrm{HC}_3) = 3$, $\mathrm{bdc}(\mathrm{HC}_4) \geq 7$. This means that $7 \leq \mathrm{bdc}(\mathrm{HC}_4) \leq 13$, where the upper bound follows from considerations analogous to Grenet's construction, see Section 6.II.

6. Graph Constructions for Polynomials

In this section, we review the proof of Theorem 1.3 from [Gre11]. Furthermore, we use the same methods to prove the following result about the Hamiltonian Cycle polynomial:

Theorem 6.1. For all natural numbers $m \in \mathbb{N}$, we have $\mathrm{bdc}(\mathrm{HC}_{m+1}) \leq m \cdot 2^{m-1} + 1$.

In this section, we denote by $[m] := \{1, \ldots, m\}$ the set of numbers between 1 and m.

6.I. **Grenet's Construction for the Permanent.** In this subsection, we prove Theorem 1.3. The construction of Grenet is a digraph Γ whose vertices $V := \{v_I \mid I \subseteq [m]\}$ are indexed by the subsets of $[m]$. Hence, $|V| = 2^m$. We partition $V = V_0 \cup \cdots \cup V_m$ such that V_i contains the vertices belonging to subsets of size i. We set $s := v_\emptyset$ and $t := v_{[m]}$, so $V_0 = \{s\}$ and $V_m = \{t\}$. Edges will go exclusively from V_{i-1} to V_i for $i \in [m]$. In fact, we insert an edge from v_I to v_J if and only if there is some $j \in [m]$ with $J = I \cup \{j\}$. This edge is then labeled with the variable x_{ij}, where $i = |J|$. For example, there are m edges going from V_0 to V_1, one for each variable x_{1j} with $1 \leq j \leq m$. It is clear that for each permutation $\pi \in \mathfrak{S}_m$, there is precisely one s-t-path in Γ whose path weight is $(-1)^{m-1} \cdot x_{1,\pi(1)} \cdots x_{m,\pi(m)}$. Consequently, the path value of the algebraic branching program $\Gamma = (\Gamma, s, t)$ is equal to $(-1)^{m-1} \cdot \mathrm{per}_m$. Theorem 1.3 then follows from the following lemma:

Lemma 6.2. Let $\Gamma = (\Gamma, s, t)$ be a binary algebraic branching program on $n \geq 3$ vertices with path value $\pm f$. Then, there is a binary variable matrix of size $n-1$ whose determinant is equal to f.

Proof. We first construct a graph G from Γ by identifying the two vertices s and t and adding loops with label 1 to every other vertex. The s-t-paths in Γ are then in one-to-one correspondence with the cycle covers of G: Indeed, any cycle cover in G must cover the vertex $s = t$ and this cycle corresponds to an s-t-path in Γ. Every other vertex can only be covered by its loop because Γ is acyclic. The graph G now has the value $\pm f$ by definition and its directed adjacency matrix A has size $n-1$. Since $n - 1 \geq 2$, we can exchange the first two rows of A to change the sign of its determinant. □

6.II. **Hamiltonian Cycle Polynomial.** In this subsection, we prove Theorem 6.1 using Lemma 6.2. In order to construct a binary algebraic branching program $\Gamma = (\Gamma, s, t)$ with path value HC_{m+1}, we proceed similar to subsection 6.I. We will refer to cyclic permutations in $\mathfrak{S}_{m+1}$ of order $m+1$ simply as *cycles* because no cyclic permutations of lower order will be considered. Observe that the cycles in $\mathfrak{S}_{m+1}$ are in bijection with the permutations in $\mathfrak{S}_m$. This can be seen by associating to $\pi \in \mathfrak{S}_m$ the cycle $\sigma = (\pi(1), \ldots, \pi(m), m+1) \in \mathfrak{S}_{m+1}$. In other words, σ maps $m+1$ to $\pi(1)$, it maps $\pi(1)$ to $\pi(2)$ and so on.

In addition to two vertices s and t, our binary algebraic branching program will have a vertex $v_{(I,i)}$ for every nonempty subset $I \subseteq [m]$ and $i \in I$. By our above Lemma 6.2, the resulting binary variable matrix will have a size of

$$1 + \sum_{i=1}^{m} \binom{m}{i} \cdot i = m \cdot 2^{m-1} + 1.$$

For $m = 3$, this is equal to $3 \cdot 2^2 + 1 = 13$.

We will construct the edges in Γ in such a way that every cycle $\sigma = (a_1, \ldots, a_m, m+1)$ corresponds to an s-t-path which has $v_{(I,i)}$ as its k-th vertex if and only if $I = \{a_1, \ldots, a_k\}$ and $i = a_k$. We insert the following edges:

- from s to $v_{(\{i\},i)}$ for each $i \in [m]$ with label $x_{m+1,i}$
- from $v_{(I,i)}$ to $v_{(I\cup\{j\},j)}$ for each $i \in I \subseteq [m]$ and $j \in [m] \setminus I$ with label $x_{i,j}$
- from $v_{([m],i)}$ to t for each $i \in [m]$ with label $x_{i,m+1}$.

We can again partition the set of vertices as $V = V_0 \cup V_1 \cup \cdots \cup V_{m+1}$ where $V_0 = \{s\}$, $V_{m+1} = \{t\}$ and for $k \in [m]$, the set V_k consists of all vertices $v_{(I,i)}$ with $|I| = k$. Then, edges go only from V_k to V_{k+1}, in particular Γ is acyclic. Furthermore, all s-t-paths in Γ have the same lengths and correspond uniquely to cycles in $\mathfrak{S}_{m+1}$. This concludes the proof of Theorem 6.1.

We know no better construction for arbitrary m, but for small m we have

$$\mathrm{HC}_2 = \det \begin{pmatrix} x_{12} & 0 \\ 0 & x_{21} \end{pmatrix} \qquad \mathrm{HC}_3 = \det \begin{pmatrix} 0 & x_{12} & x_{13} \\ x_{21} & 0 & x_{23} \\ x_{31} & x_{32} & 0 \end{pmatrix}.$$

References

[BL04] P. Bürgisser and M. Lotz. Lower Bounds on the Bounded Coefficient Complexity of Bilinear Maps. Journal of the ACM, 51(3):464–482, 2004.

[EZ62] H. Ehlich and K. Zeller. Binäre Matrizen. *Zeitschrift für Angewandte Mathematik und Mechanik*, 42(S1):T20–T21, 1962.

[Gre11] B. Grenet. An upper bound for the permanent versus determinant problem. 2011. Manuscript, accepted for publication in Theory of Computing.

[Knu97] D. E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[Koi04] P. Koiran. Valiant's model and the cost of computing integers. *Computational Complexity*, 13:131–146, 2004.

[LMR10] J. M. Landsberg, L. Manivel, and N. Ressayre. Hypersurfaces with degenerate duals and the geometric complexity theory program. arXiv:1004.4802, 2010.

[Mal03] G. Malod. *Polynômes et coefficients*. PhD thesis, L'Université Claude Bernard Lyon 1, 2003.

[Mor73] J. Morgenstern, Note on a lower bound of the linear complexity of the fast Fourier transform. J. Assoc. Comput. Mach., 20, 305-306, 1973.

[MP08] G. Malod and N. Portier. Characterizing Valiant's algebraic complexity classes. *J. Complexity*, 24(1):16–38, 2008.

[MP13] B. D. McKay and A. Piperno. Practical graph isomorphism, ii. *J. Symbolic Computation*, 60:94–112, 2013.

[MR04] T. Mignon and N. Ressayre. A quadratic bound for the determinant and permanent problem. *Int. Math. Res. Not.*, (79):4241–4253, 2004.

[Raz03] R. Raz. On the complexity of matrix product. SIAM J. Comput. 32(5):1356–1369, 2003.

[Slo14] N. Sloane. The on-line encyclopedia of integer sequences, sequence A003432. Published electronically at http://oeis.org/A003432.

[Tod92] S. Toda. Classes of Arithmetic Circuits Capturing the Complexity of the Determinant. *IEICE TRANS. INF. & SYST.*, E75-D(1):116–124, 1992.

[Val79a] L. G. Valiant. Completeness classes in algebra. In *Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing (Atlanta, Ga., 1979)*, pages 249–261. ACM, New York, 1979.

[Val79b] L. G Valiant. The complexity of computing the permanent. *Theor. Comput. Sci.*, 8:189–201, 1979.