Linear Algebra and its Applications 504 (2016) 559–573

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Binary determinantal complexity

Jesko Hüttenhain [a], Christian Ikenmeyer [b,*]

[a] Technische Universität Berlin, Germany
[b] Texas A&M University, United States

ARTICLE INFO

Article history:
Received 27 January 2015
Accepted 17 April 2016
Available online 26 April 2016
Submitted by R. Brualdi

MSC:
68Q05
68-04

Keywords:
Determinant
Permanent
Computational complexity
Arithmetic circuit
Constant-free

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.

1. Introduction

Let $\mathfrak{S}_m$ denote the symmetric group on m letters and let $\mathrm{per}_m := \sum_{\pi \in \mathfrak{S}_m} \prod_{i=1}^{m} x_{i,\pi(i)}$ 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

* Corresponding author.
E-mail addresses: jesko@math.tu-berlin.de (J. Hüttenhain), ciken@math.tamu.edu (C. Ikenmeyer).

http://dx.doi.org/10.1016/j.laa.2016.04.027

seminal paper [16], with an additional emphasis on the special role of the permanent in [17].

We call a matrix whose entries are only variables or integers an *integer variable matrix*. One main implication of [16] 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,

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

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 $\mathrm{dc}(\mathrm{per}_m)$ to be this minimal size. It is famously conjectured by Valiant that the sequence $m \mapsto \mathrm{dc}(\mathrm{per}_m)$ 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 [10]. A graph construction by Grenet [4], see Section 6.1, 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* $\mathrm{per}_m = \det(A)$*. 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 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 $\mathbf{VP^0_{ws}}$, the constant free version of $\mathbf{VP_{ws}}$, 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 [12] in a stronger model of computation, see also [7] 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.