Complexity of Linear Boolean Operators

Stasys Jukna
Vilnius University, Lithuania and Frankfurt University, Germany
jukna@online.de

Igor Sergeev
Lomonosov Moscow State University, Russia
isserg@gmail.com

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Jukna and I. Sergeev. *Complexity of Linear Boolean Operators*. Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 1, pp. 1–123, 2013.

This Foundations and Trends® issue was typeset in LaTeX using a class file designed by Neal Parikh. Printed on acid-free paper.

ISBN: 978-1-60198-727-3

Foundations and Trends® in Theoretical Computer Science
Volume 9, Issue 1, 2013

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Theoretical Computer Science publishes surveys and tutorials on the foundations of computer science. The scope of the series is broad. Articles in this series focus on mathematical approaches to topics revolving around the theme of efficiency in computing. The list of topics below is meant to illustrate some of the coverage, and is not intended to be an exhaustive list.

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations research
- Parallel algorithms
- Quantum computation
- Randomness in computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2013, Volume 9, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 9, No. 1 (2013) 1–123

DOI: 10.1561/0400000063

now
the essence of knowledge

Complexity of Linear Boolean Operators

Stasys Jukna
Vilnius University, Lithuania and Frankfurt University, Germany
jukna@online.de

Igor Sergeev
Lomonosov Moscow State University, Russia
isserg@gmail.com

Contents

Abstract

How to compute a linear Boolean operator by a small circuit using only unbounded fanin addition gates? Because this question is about one of the simplest and most basic circuit models, it has been considered by many authors since the early 1950s. This has led to a variety of upper and lower bound arguments—ranging from algebraic (determinant and matrix rigidity), to combinatorial (Ramsey properties, coverings, and decompositions) to graph-theoretic (the superconcentrator method). We provide a thorough survey of the research in this direction, and prove some new results to fill out the picture. The focus is on the cases in which the addition operation is either the boolean OR or XOR, but the model in which arbitrary boolean functions are allowed as gates is considered as well.

S. Jukna and I. Sergeev. *Complexity of Linear Boolean Operators*. Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 1, pp. 1–123, 2013.

DOI: 10.1561/0400000063.

1

Introduction

Let $(S, +)$ be a commutative semigroup, that is, a set S closed under a binary "sum" operation $+$ which is associative and commutative. Our goal is to simultaneously compute a given system

$$y_i = \sum_{j \in T_i} x_j, \qquad i = 1, \ldots, m \tag{1.1}$$

of m sums by only using the sum operation of the semigroup. By identifying the subsets T_i with their characteristic 0/1 vectors, this system turns to a linear operator $y = Ax$ for a boolean matrix A.

A natural computational model towards this goal is that of *addition circuits* over $(S, +)$. Such a circuit is a directed acyclic graph with n input nodes $x_1, \ldots, x_n$ of zero fanin, and m output nodes $y_1, \ldots, y_m$ of zero fanout. Each non-input node computes the sum of its inputs over $(S, +)$. There are no restrictions on the fanin or fanout of gates. The *size* of a circuit is the total number of edges in it, and the *depth* is the length of (the number of edges in) a longest path.

We will concentrate on the most basic semigroups—the OR semigroup $(\{0, 1\}, \vee)$, and the XOR group $(\{0, 1\}, \oplus)$. Thus, OR circuits allow "cancellations" $x + x = x$ (partial sums can be "merged"), whereas XOR circuits allow cancellations $x + x = 0$ (partial sums can be "anni-

hilated"). We also consider a restricted model of SUM circuits where the system of sums (1.1) is computed over the semiring $(\mathbb{N}, +)$. In this model none of these two types of cancellations can be used. Note that the XOR and OR (and its "dual" AND) are the only commutative semigroups over $S = \{0, 1\}$.

We stress that, given a boolean matrix A, the goal of all these three types of circuits is the *same*: to compute the system of sums (1.1) defined by A. The only difference is in what type of cancellations a circuit can use to achieve this goal. OR circuits constitute the simplest *monotone* model, whereas XOR circuits constitute the simplest group model (necessarily non-monotone since the group is finite). SUM circuits are "universal" in the sense that every such circuit for A is an addition circuit for A over any semigroup $(S, +)$.

The model of OR circuits was first considered by Lupanov [62] by inventing the model of rectifier circuits. XOR circuits were first considered by Nechiporuk in [70]. SUM circuits were first explicitly introduced by Pippenger [81]. SUM circuits of fanin-2 are also known as "vector addition chains" (see, for example, Knuth [55, Sect. 4.6.3]).

It is important to note that computing an operator $y = Ax$ for a boolean matrix $A = (a_{ij})$ by an addition circuit actually means to "encode" the matrix A by paths in a directed acyclic graph. Namely, if p_{ij} denotes the number of paths from the input node x_j to the output node y_i in such a circuit for A then the circuit *implements* (or *encodes*) the matrix A in the following sense:

- SUM circuit: $p_{ij} = a_{ij}$.
- OR circuit: $p_{ij} > 0$ if $a_{ij} = 1$, and $p_{ij} = 0$ if $a_{ij} = 0$.
- XOR circuit: p_{ij} is odd if $a_{ij} = 1$, and p_{ij} is even if $a_{ij} = 0$.

Thus, SUM circuits constitute the most restricted model in which there cannot be more than one path between the same pair of input and output nodes. Also, unlike XOR circuits, SUM and OR circuits are *monotone* models: increasing values of inputs cannot decrease the values of outputs. For these circuits, large (almost quadratic) explicit[1] lower bounds, without any restriction on the circuit-depth are known.

[1]Intuitively, a matrix or a boolean function being "explicit" means being "explic-

However, XOR circuits are a "Waterloo" of circuit complexity: here superlinear lower bounds are only known for constant-depth circuits (and these are barely-superlinear even for depth 5, say).

In this text we survey the most important complexity-theoretic questions about the addition circuit model:

Q1: What is the maximum complexity of implementing a boolean $n \times n$ matrix? Answer: it is about $n^2/\log n$ in all three models (Chapter 2).

Q2: What are the best known explicit lower bounds for the three complexity measures? Answer: for SUM and OR circuits, we have near-optimal explicit examples of boolean $n \times n$ matrices with a lower bound of $n^{2-o(1)}$ (§ 3.4). On the other hand, we have nothing super-linear for XOR circuits, except for constant depth d, and these degrade badly as d grows. For depth 2, the strongest known lower bound is about $n(\ln n/\ln\ln n)^2$, and is about $n \ln\ln n$ for depth 3 (§ 3.7, § 3.8 and Chapter 6).

Q3: How large a gap can occur between the SUM, OR and XOR complexities of a given boolean $n \times n$ matrix A? Answer: the largest possible gap in each of the three models is $O(n/\log n)$ (Chapter 2). The largest known SUM/OR gap is $\Omega(\sqrt{n}/\log^2 n)$, OR/XOR gap is $\Omega(n/\log^2 n)$, and the largest known gap between the OR complexity of a matrix A and its complement is $\Omega(n/\log^3 n)$ (Chapter 5).

Q4: What are the most important known lower bound techniques for handling specific matrices, what are their limitations? A variety of techniques are described in Chapter 3 and Chapter 6. They give a flexible toolkit for lower-bounding the SUM and OR complexities, their bounded-depth analogues, and the depth-2 XOR complexity. Each of presented lower-bound techniques uses some property of matrices and gives some lower bound based on only these properties. Is the technique "optimal" in the sense that one cannot derive a larger bound by only using the same properties? We show various examples of this kind, indicating where progress on lower bounds gets stuck (Table 4.1, § 6.1 and § 6.2).

itly constructed", not just being "shown to exist". A more rigorous definition of the term "explicit" can be found, for example, in the book [50, Section 1.5.1].

Q5: XOR circuits are the "natural" way to compute linear operators over $\mathbb{F}_2$; but are they the "best" way? To address this question, we consider *general* circuits that allow *arbitrary* boolean functions at its gates. Despite this model's crazy power, we still don't know if there is any example where it computes an $\mathbb{F}_2$-linear operator more efficiently than XOR circuits do. Moreover, some of our lower bound techniques apply also to this stronger model, and we describe some of this work in Chapter 6.

For general circuits computing *linear* $\mathbb{F}_2$-operators, the strongest known explicit lower bounds have the form $\Theta(n(\ln n/\ln\ln n)^2)$ in depth 2, and the form $\Theta(n\ln\ln n)$ in depth 3; these bounds are tight and are achievable even by XOR circuits (see Chapter 6). This highlights the power of XOR circuits and difficulties of dealing with them. In larger depths, the known lower bounds for XOR circuits are only barely superlinear.

If we consider *non-linear* operators in the arbitrary gates model, then we have explicit $\Omega(n^{3/2})$ bounds in depth 2, and $\Omega(n\ln n)$ in depth 3. These bounds were proved by Cherukhin [18, 19] and Jukna [48] using entropy arguments which do not work for linear operators. In larger depths, the known bounds are only barely better than those known for linear operators.

Though organized as a survey, the text also contains some new, previously unpublished results. These include:

1. Hansel–Krichevski type lower bound (Theorem 3.5).
2. Rectangle-area lower bounds (Theorem 3.12).
3. Depth-2 lower bound for block matrices (Theorem 3.18(iii)).
4. Lower bound for Kronecker products (Theorem 3.20(ii)).
5. Bounds for the Kneser–Sierpinski matrix (Lemma 4.2).
6. Upper bounds for the Sylvester matrix (Theorem 4.3).
7. Balanced decomposition of the triangular matrix (Lemma 5.3).
8. Coverings vs. decompositions in depth 2 (Theorem 5.4).
9. An XOR/OR gap in depth 2 (Theorem 5.12).
10. Matrix/complement gaps (Theorem 5.13, items (i) and (iii)).
11. Linearization of half-linear depth-2 circuits (Lemma 7.17).

Most of the remaining (known) results are given with proofs—in most

cases, substantially simplified—or at least with detailed proof sketches. The subject of this survey previously found an only fragmentary exposition in the books by Wegener [108], Dunne [24], Jukna [50], and in an earlier very short survey by Lupanov [63].

What we do not cover To compute linear operators over fields $(S, +, \cdot)$, and in particular over infinite fields, it is natural to allow multiplication by arbitrary field elements as a basic circuit operation. Such circuits are called *linear circuits*. If $S = \{0, 1\}$, then these are just the addition circuits considered in this survey. However, the ability to use "for free" arbitrarily complex coefficients of arbitrary magnitude is one of the central "mysteries" in arithmetic circuit complexity over infinite fields.

Research in this direction also has long history, starting with the seminal works of Morgenstern [67, 68], Grigoriev [37] and Valiant [106]. In this case, gates may compute arbitrary linear combinations of their inputs, not just 0/1 combinations. It is still an open problem to prove more than linear lower bounds on circuits computing a linear form Ax defined by an explicit 0/1 matrix A—such bounds are only known when either the matrix A has very "complicated" entries (say, square roots of the first n^2 distinct primes) or when the circuit is not allowed to use large coefficients; see, for example, the book by Bürgisser, Clausen, and Shokrollahi [13], or the more recent survey by Lokam [61].

1.1 Concepts used

We first recall some (mostly basic) concepts concerning boolean matrices which we will use later. A matrix is *boolean* if it only has entries 0 and 1. If not otherwise stated,

by a "matrix" we will always mean a "boolean matrix".

For such a matrix A, $|A|$ denotes the number of 1-entries in A. A *rectangle* in a matrix is an all-1 submatrix. If this is an $a \times b$ rectangle, then we define its *weight* as $a + b$, its *area* as $a \cdot b$, and its *density* as $a \cdot b/(a+b)$. For a positive integer r, $[r] = \{1, \ldots, r\}$ will always denote the set of the first r positive integers.

The *Kronecker product* $A \otimes B$ of a $p \times q$ matrix $A = (a_{i,j})$ and an $n \times m$ matrix B is an $np \times mq$ block-matrix obtained by replacing 1-entries of A by copies of B. The *direct sum* of matrices A and B is the matrix $A \boxplus B = \left[\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right]$.

We can view a rectangle R in an $n \times n$ matrix A as an $n \times n$ matrix $\hat{R}$ with all entries outside R filled by 0s. A set $R_1, \ldots, R_s$ of rectangles in a matrix A is a:

- SUM covering (or a *decomposition*) of A if $A = \sum_{i=1}^{s} \hat{R}_i$;
- OR covering (or just a *covering*) of A if $A = \bigvee_{i=1}^{s} \hat{R}_i$;
- XOR covering of A if $A = \bigoplus_{i=1}^{s} \hat{R}_i$.

The *weight* of a covering is the sum of weights of its rectangles. For

$$\mathsf{L} \in \{\text{SUM,OR,XOR}\}\,,$$

the L-*rank* of A is the smallest number of rectangles in an L-covering of A. The L-*product* of two matrices is their product over the corresponding semiring. Thus, the L-rank of A is the smallest number r such that A can be written as an L-product $A = PQ^\top$, where P and Q are $n \times r$ matrices. To visually better distinguish the three ranks, we will use $\mathrm{rk}_+(A)$, $\mathrm{rk}_\vee(A)$ and $\mathrm{rk}(A)$ to denote, respectively, the SUM-, OR- and XOR-rank of A. In communication complexity,[2] $\log \mathrm{rk}_\vee(A)$ is exactly the *nondeterministic* communication complexity of A (see, e.g. [50, § 4.2]).

The *term rank*, $\mathrm{tr}(B)$, of a boolean matrix B is the largest number of its 1s, no two of which lie in the same row or column. By the König–Egerváry theorem, this is exactly the smallest number of rows and columns covering all 1s of B. It is easy to see that

$$\mathrm{tr}(B) \geqslant \mathrm{rk}_+(B) \geqslant \mathrm{rk}_\vee(B)\,.$$

Indeed, $\mathrm{tr}(B)$ is the smallest number $a+b$ such that, after some permutation of rows and columns, the matrix B can be written in the form $B = \left[\begin{smallmatrix} C & D \\ F & 0 \end{smallmatrix}\right]$, where C is an $a \times b$ matrix. We can therefore write B as a sum of $a + b$ pairwise disjoint rectangles, each corresponding to one row or column of B.

[2] If not specified otherwise, $\log n$ will always stand for $\log_2 n$.

A matrix A is (k,l)-*free* ($k,l \geqslant 1$) if it does not contain a $k \times l$ rectangle; being k-*free* means being (k,k)-free. Known upper bounds for the Zarankiewicz problem (see, for example, [58] or the book [8]) state that, if A is a (k,l)-*free* matrix of dimension $m \times n$, then

$$|A| \leqslant (k-1)^{1/l}(n-l+1)m^{1-1/l} + (l-1)m\,. \tag{1.2}$$

A matrix is (k,l)-*Ramsey matrix* if both the matrix and its complement are (k,l)-free.

We will often use the arithmetic-geometric mean inequality

$$\frac{1}{n}\sum_{i=1}^{n} x_i \geqslant \Big(\prod_{i=1}^{n} x_i\Big)^{1/n}, \tag{1.3}$$

as well as a special version of the Jensen inequality for a convex function f:

$$\sum_{i=1}^{n} f(x_i) \geqslant n \cdot f\Big(\frac{X}{n}\Big), \tag{1.4}$$

where $X = \sum_{i=1}^{n} x_i$ and all $x_i \geqslant 0$. In particular, by taking $f(x) = x\log x$, we obtain

$$\sum_{i=1}^{n} x_i \log x_i \geqslant X \log \frac{X}{n}\,, \tag{1.5}$$

In some estimates we will also use the binary entropy function

$$H(\alpha) = \alpha \log \frac{1}{\alpha} + (1-\alpha)\log\frac{1}{1-\alpha}\,.$$

Asymptotic notation To spare parenthesis (in larger expressions), we will occasionally write $f \succcurlyeq g$ instead of $f = \Omega(g)$, $f \preccurlyeq g$ instead of $f = O(g)$, and $f \asymp g$ instead of $f = \Theta(g)$. Also, $f \ll g$ stands for $f = o(g)$. Notation $f \sim g$ means the usual (tight) asymptotic $f/g \to 1$. By saying "the $n \times n$ matrix A has complexity $\succcurlyeq g(n)$" we will actually mean that we have an infinite sequence $\{A_n\}$ of $n \times n$ matrices ($n = 1, 2, \ldots$) for which there exists a constant $\epsilon > 0$ such that "complexity of A_n is $\geqslant \epsilon g(n)$" holds for infinitely many n. By writing "A has complexity $\geqslant g(n)$", we will mean that this holds for all large enough dimensions n.

1.2 Simple observations

We denote the minimum number of edges in an OR, XOR and SUM circuit implementing a given matrix A by $\mathsf{OR}(A)$, $\mathsf{XOR}(A)$ and $\mathsf{SUM}(A)$. If we speak only about circuits of depth $\leqslant d$, then the corresponding measures are denoted by $\mathsf{OR}_d(A)$, $\mathsf{XOR}_d(A)$ and $\mathsf{SUM}_d(A)$.

As we noted above, SUM circuits constitute the weakest model: each such circuit can be turned into an OR circuit or an XOR circuit just by replacing the operations computed at their nodes. So, for every matrix A, we have that

$$\mathsf{OR}(A) \leqslant \mathsf{SUM}(A) \quad \text{and} \quad \mathsf{XOR}(A) \leqslant \mathsf{SUM}(A)\,.$$

In the case of depth-d circuits, we will assume that the underlying graph is "leveled" in the following sense. We have $d+1$ levels of nodes. The first level consists of input nodes, the last consists of output nodes, and each edge goes from one level to the next one. Thus, if A_i is the boolean adjacency matrix of the bipartite graph between the $(i+1)$-th and i-th levels, then these measures give the smallest weight $\sum_{i=1}^{d} |A_i|$ of the presentation of A as a product $A = A_d \cdot A_{d-1} \cdots A_1$ of boolean matrices over the corresponding semirings, where $|A_i|$ is the number of 1s in A_i. That is,

L-complexity of A = smallest weight of an L-factorization of A.

Observation 1.1 (Transposition principle)**.** The complexities of a matrix A and its transpose $A^\top$ are the same.

Proof. Given any circuit for A, one may reverse the direction of all edges to obtain a circuit for $A^\top$. □

Observation 1.2. The complexity of a submatrix is at most the complexity of the entire matrix.

Proof. Given a circuit for a matrix, we can remove all input and output nodes that are not in the submatrix. □

For counting reasons, it is sometimes convenient to transform the circuit so that every inner node (non-input node) has fanin at most 2,

and then count the nodes in a new circuit rather than the edges in the original one.

Observation 1.3. An unbounded fanin circuit with e edges and v non-input nodes can be turned into an equivalent fanin-2 circuit with $e - v$ nodes.

Proof. Just replace every node of fanin $d > 2$ by a binary tree with $d - 1$ inner nodes. The difference $e' - v'$ in the new circuit equals $e - v$ in the original circuit. See [50, Section 1.8] for more details. □

Depth-1 complexity is a trivial measure: we have $\mathsf{SUM}(A) \leqslant \mathsf{SUM}_1(A) = |A| \leqslant n^2$ for every $n \times n$ matrix A. Depth-2 circuits constitute the first non-trivial model. We already know that $\mathsf{L}_2(A) = \min\{|B| + |C| \colon A = B \cdot C\}$. Here and in what follows, $\mathsf{L}(A)$ stands for the SUM, OR or XOR complexity, and the matrix product is over the corresponding semiring. On the other hand, depth-2 circuits have also a *combinatorial* description in terms of coverings.

Observation 1.4. For every matrix A, $\mathsf{L}_2(A)$ is the minimum weight of an L-covering of A.

Proof. The paths going through one node on the middle level of a circuit for A define a rectangle in A. □

Let again $\mathsf{L}(A)$ stand for the SUM, OR or XOR complexity, and let $A + B$ and $A \cdot B$ denote the matrix sum and the matrix product over the corresponding semiring. Then we have:

1. $\mathsf{L}(A + B) \leqslant \mathsf{L}(A) + \mathsf{L}(B)$, if the matrices can be added;
2. $\mathsf{L}(A \cdot B) \leqslant \mathsf{L}(A) + \mathsf{L}(B)$, if the matrices can be multiplied;
3. $\mathsf{L}(A \boxplus B) \leqslant \mathsf{L}(A) + \mathsf{L}(B)$;
4. $\mathsf{L}(A \otimes B) \leqslant a \cdot \mathsf{L}(B) + b \cdot \mathsf{L}(A)$, if A has a rows, and B has b columns.

Only (4) needs a proof. First, we rewrite the Kronecker product as $A \otimes B = (I_a \otimes B)(A \otimes I_b)$, and observe that $A \otimes I_b = P(I_b \otimes A)Q$ for particular permutation matrices P and Q. Since, $I_a \otimes B = B \boxplus B \boxplus \cdots \boxplus B$ is a direct sum (a times), the desired inequality (4) follows from (2) and (3).

1.3 Some basic matrices

Let us recall the definitions of some basic matrices whose complexities we will investigate later. These matrices are well-suited to demonstrate known lower bound techniques. This section is just for later reference, so that the reader can safely skip it, and proceed with the next section.

Full triangular matrix The *full triangular* matrix T_n, known also as the *prefix matrix*, is an $n \times n$ matrix with 1s on the main diagonal and below it, and zeroes elsewhere. For $n = 2^r$, these matrices can be defined recursively as follows:

$$T_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad T_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad T_{2n} = \begin{bmatrix} T_n & 0 \\ 1 & T_n \end{bmatrix}.$$

This gives the recursion $\mathsf{SUM}_2(T_n) \leqslant 2 \cdot \mathsf{SUM}_2(T_{n/2}) + n$, which results to

$$\mathsf{SUM}_2(T_n) \leqslant n \log n + n\,. \tag{1.6}$$

Complement of identity matrix To demonstrate some bounds, we will also use the complement $\overline{I}_n = T_n \oplus T_n^\top$ of the identity matrix I_n for $n = 2^r$. For this matrix, we have that

$$\mathrm{rk}_\vee(\overline{I}_n) \leqslant 2r = 2\log n \quad \text{and} \quad \mathsf{OR}_2(\overline{I}_n) \leqslant 2r2^r = 2n \log n\,. \tag{1.7}$$

To see this, label the rows and columns of $\overline{I}_n$ by vectors $u \in \{0,1\}^r$. For each position $i \in \{1,\ldots,r\}$, we have two rectangles: one consists of all pairs (u,v) such that $u_i = 0$ and $v_i = 1$, and the other consists of all pairs (u,v) such that $u_i = 1$ and $v_i = 0$. This way, we obtain a covering of $\overline{I}_n$ by $2r$ rectangles of total weight $4r2^{r-1} = 2n \log n$.

A general construction of some important $n \times n$ matrices, for $n = 2^r$ being a power of two, is the following. Label the rows and columns by distinct subsets u of $[r]$. The $n \times n$ matrix M_f induced by a function $f : \{0,1,\ldots,r\} \to \{0,1\}$ is then defined by: $M_f[u,v] := f(|u \cap v|)$.

Kneser–Sierpinski (disjointness) matrix In graph theory, the Kneser graph is the graph whose nodes correspond to the k-element subsets of a set of r elements, and where two nodes are adjacent if and only if the two corresponding sets are disjoint. Kneser graphs are named after Martin Kneser, who first investigated them in 1955.

By analogy, the *Kneser-Sierpinski* $n \times n$ *matrix* (known also as the *disjointness matrix*) $D = D_n$ is the f-intersection matrix induced by the function $f(x) = 1$ if and only if $x = 0$. That is, the rows and columns of $D = D_n$ with $n = 2^r$ are labeled by distinct subsets u of $[r]$, and $D[u, v] = 1$ if and only if $u \cap v = \emptyset$. These matrices can be defined inductively as follows:

$$D_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad D_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad D_{2n} = \begin{bmatrix} D_n & 0 \\ D_n & D_n \end{bmatrix}. \tag{1.8}$$

The Kneser–Sierpinski matrix D is an important object. This matrix is also sometimes called the Sierpinski matrix, since it resembles the well-known "Sierpinski gasket". In particular, it gives a linear transformation between the vector of the values of a boolean function f and the vector of coefficients of its unique representation as multilinear polynomial over the 2-element field. This polynomial is also known as the *Zhegalkin polynomial* for f.

To see this, consider a boolean function $f : 2^{[r]} \to \{0, 1\}$ and its XOR-polynomial $f(X) = \bigoplus_{u \subseteq [r]} g(u) X_u$ with boolean coefficients $g(u)$, and $X_u = \prod_{i \in u} x_i$. Then the $2^r \times 2^r$ matrix D induces a linear mapping from the vector $(g(u) \colon u \subseteq [r])$ to the vector $(f(v) \colon v \subseteq [r])$: just note that $X_u(v) = 1$ if and only if $u \subseteq v$, or, in other words, if and only if $u \cap \overline{v} = \emptyset$. Moreover, the inverse map is also given by the matrix D, since $D = D^{-1}$ (easy to check).

Intersection matrix The *intersection* $n \times n$ *matrix* is the f-intersection matrix induced by the function $f(x) = 1$ if and only if $x > 0$. That is, the intersection matrix is just the complement $Đ_n = \overline{D_n}$ of the Kneser–Sierpinski matrix with $n = 2^r$. The rows and columns are labeled by distinct subsets u of $[r]$, and $Đ[u, v] = 1$ if and only if

$u \cap v \neq \emptyset$. These matrices also have a recursive definition:

$$\mathcal{D}_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \mathcal{D}_4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathcal{D}_{2n} = \begin{bmatrix} \mathcal{D}_n & 1 \\ \mathcal{D}_n & \mathcal{D}_n \end{bmatrix}.$$

By identifying subsets u with their characteristic vectors, we see that $\mathcal{D}[u,v] = \bigvee_{i=1}^{r} u_i \wedge v_i$. Thus, over the boolean semiring, we have that $\mathcal{D} = B \cdot B^\top$ for the $n \times r$ matrix B whose rows are all vectors of length r. This yields

$$\mathsf{OR}_2(\mathcal{D}_n) \leqslant 2r2^{r-1} = n \log n\,. \tag{1.9}$$

In the *unique intersection matrix* $\mathcal{D}^u$ we have a stronger condition for 1s: $\mathcal{D}^u[u,v] = 1$ if and only if $|u \cap v| = 1$.

Sylvester matrices The Sylvester $n \times n$ matrix H_n for $n = 2^r$ is the $n \times n$ f-intersection matrix induced by the function $f(x) = x \mod 2$. That is, the rows and columns of H are labeled by distinct subsets u of $[r]$, and $H[u,v] = 1$ if and only if $|u \cap v|$ is odd. Sylvester matrices can be defined inductively as follows:

$$H_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & \overline{H}_n \end{bmatrix}. \tag{1.10}$$

By identifying subsets of $[r]$ with their characteristic vectors $u \in \{0,1\}^r$, we see that $H[u,v] = \langle u, v \rangle = u_1 v_1 \oplus u_2 v_2 \oplus \cdots \oplus u_r v_r$ is the scalar product of u and v over $\mathbb{F}_2$. Thus, H is just a "counting version" of the intersection matrix, and we have $H = B \cdot B^\top$ over $\mathbb{F}_2$ for the $n \times r$ matrix B whose rows are all n binary vectors of length r. This yields

$$\mathsf{XOR}_2(H_n) \leqslant 2r2^{r-1} = n \log n\,. \tag{1.11}$$

A basic property of Sylvester matrices is expressed by the following lemma, whose simple proof can be found, say, in [28, p. 88].

Lindsey's Lemma. The Sylvester $n \times n$ matrix contains no monochromatic $a \times b$ submatrices, unless $ab \leqslant \sqrt{n}$.

We will show in § 3.3 that $\mathsf{OR}(A) \geqslant |A|/k^2$ holds for every k-free matrix A. Here we give some examples of such matrices.

Random matrices A random $n \times n$ matrix A, where each entry is drawn uniformly and independently from $\{0,1\}$, has $\Omega(n^2)$ ones, and is k-free for relatively small k. This holds because A fails to be k-free with probability at most $\binom{n}{k}^2 2^{-k^2} \ll \mathrm{e}^{2k\ln n - k^2}$: there are $\binom{n}{k}^2$ $k \times k$ submatrices, and the probability that all k^2 entries of a given $k \times k$ submatrix are 0s is 2^{-k^2}. For $k \geqslant 2\ln n$, this probability tends to 0 as $n \to \infty$. Thus, k-free $n \times n$ matrices A with $k = O(\log n)$ and $|A| = \Omega(n^2)$ exist.

Singer matrix [100] The upper bound (1.2) for the Zarankiewicz problem implies that no 2-free $n \times n$ matrix can have more than $n^{3/2}+n$ ones. On the other hand, there are several *explicit* constructions of 2-matrices with almost this number of 1s. One of the oldest construction is due to Singer [100].

For a prime power q, a projective plane $PG(2,q)$ has $n = q^2+q+1$ points and n subsets of points (called lines). Every point lies in $q+1$ lines, every line has $q+1$ points, any two points lie on a unique line, and any two lines meet in the unique point.

The point-line incidence matrix of a finite projective plane P was introduced by Singer [100]. Label rows by points x, columns by lines L, and let $P[x,L] = 1$ if and only if $x \in L$, then the obtained matrix is 2-free. The number of 1s is $|P| = (q+1)n > n^{3/2}$.

A 2-free matrix similar in spirit to Singer's was constructed by Kövari–Sós—Turán [58] and Nechiporuk [74]. This matrix is related to the point-line incidences in a finite *affine* plane. Here rows and columns correspond to pairs of numbers in $\mathbb{F}_q$, and each row (a,b) has 1s in positions $(x, ax-b)$ with $x \in \mathbb{F}_q$. Thus, $|A| = nq = q^3 = n^{3/2}$. The matrix is 2-free because every system of two equations $ax = b+y$ and $cx = d+y$ has at most one solution.

Circulant matrices A matrix is *circulant* if each its row is a cyclic shift (by one position to the left) of the previous one. Singer [100]

proved that his $n \times n$ matrices P with $n = q^2 + q + 1$ and q a prime power are circulant: there exists a subset $S \subseteq \{0, 1, \ldots, n-1\}$ of size $|S| = q+1$ such that (after permutation of rows and columns) we have that $P[x, y] = 1$ if and only if $y = x + a \mod n$ for some $a \in S$. The circulant property is significant for us because such matrices have small XOR complexity (see § 5.4).

We can define a circulant matrix by giving a subset $S = \{s_1, \ldots, s_k\}$ of $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$: these are the positions of 1s in the first row. The resulting circulant matrix A has $|A| = kn$ ones. Such a set is called a *Sidon set* if all differences modulo n of two its elements are distinct. It is well known (and not difficult to show) that, if the support S of a circulant matrix A is a Sidon set, then the matrix A is 2-free: the 1s of A stay on $|S|$ diagonals determined by position in S. It is known that no Sidon set can have more than $\sqrt{n} + 1$ elements. Explicit examples of Sidon sets S with $|S| \sim \sqrt{n}$ were given by Alexeev [1], Bose [9], Ruzsa [94], and other authors; see a survey by O'Bryant [77].

Norm matrices Let q be a prime-power, $t \geqslant 2$ an integer, and consider the field $\mathbb{F}_{q^t}$ with q^t elements. The norm of an element a of this field is defined as the element $\|a\| := a \cdot a^q \cdots a^{q^{t-1}} = a^{(q^t-1)/(q-1)}$ of this field. Now let $n = q^t$, and construct an $n \times n$ matrix $N = N_{n,t}$ whose rows and columns are labeled by elements of $\mathbb{F}_{q^t}$. The entries are defined by letting $N[a, b] = 1$ if and only if $\|a + b\| = 1$.

It is known that the number of solutions in $\mathbb{F}_{q^t}$ of the equation $\|x\| = 1$ is $(q^t - 1)/(q - 1)$; see e. g., the book by Lidl and Niederreiter [60]. Hence, each row of N has $r = (q^t - 1)/(q - 1)$ ones, implying that the total number of ones is $|N| = rq^t \geqslant q^{2t-1} = n^{2-1/t}$.

Kollár, Rónyai and Szabó [57] proved that, for every t distinct elements $a_1, \ldots, a_t$ of $\mathbb{F}_{q^t}$, the system of equations $\|a_1 + x\| = 1, \|a_2 + x\| = 1, \ldots, \|a_t + x\| = 1$ has at most $t!$ solutions $x \in \mathbb{F}_{q^t}$. This implies that the constructed matrix N has no $t \times (t! + 1)$ all-1 submatrix. Hence, the constructed matrix A is $(t, t! + 1)$-free. Explicit matrices with slightly worse parameters were constructed earlier by Andreev [7].

References

[1] V.E. Alexeev. Two constructions of difference sets. *Problemy Kibernetiki*, 38:259–262, 1981 (in Russian).

[2] N. Alon. Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory. *Combinatorica*, 6(3):207–219, 1986.

[3] N. Alon, M. Karchmer, and A. Wigderson. Linear circuits over GF(2). *SIAM J. Comput.*, 19(6):1064–1067, 1990.

[4] N. Alon and W. Maass. Meanders and their applications in lower bounds arguments. *J. Comput. Syst. Sci.*, 37(2):118–129, 1988.

[5] N. Alon and P. Pudlák. Superconcentrators of depths 2 and 3; odd levels help (rarely). *J. Comput. Syst. Sci.*, 48(1):194–202, 1994.

[6] A.E. Andreev. On the complexity of realization of transitivity relations by rectifier circuits. In *Physical and mathematical modeling of discrete systems*, volume 56, pages 11–21. MEI, Moscow, 1985 (in Russian).

[7] A.E. Andreev. On a family of Boolean matrices. *Vestnik Moskow Univ.*, (2):97–100, 1986. Engl. transl. in: Moscow. Univ. Math. Bull. 1986. 41, 79–82.

[8] B. Bollobás. *Extremal graph theory.* Academic Press, 1978.

[9] R.C. Bose. An affine analogue of Singer's theorem. *J. Indian Math. Soc.*, 6:1–15, 1942.

[10] J. Boyar and M. Find. Cancellation-free circuits: An approach for proving superlinear lower bounds for linear boolean operators. Technical report, arXiv:1207.5321, 2012.

[11] J. Boyar and M. Find. Cancellation-free circuits in unbounded and bounded depth. Technical report, arXiv:1305:3041, 2013.

[12] S. Bublitz. Decomposition of graphs and monotone formula size of homogeneous functions. *Acta Inf.*, 23(6):689–696, 1986.

[13] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic complexity theory*. Springer, 1997.

[14] A.K. Chandra, S. Fortune, and R.J. Lipton. Unbounded fan-in circuits and associative functions. *J. Comput. Syst. Sci.*, 30(2):222–234, 1985.

[15] A.K. Chandra, S. Fortune, and R.L. Lipton. Lower bounds for constant depth circuits for prefix problems. In *Proc. in 10th Int. Colloq. on Automata, Languages and Programming (ICALP)*, volume 154 of *Springer Lect. Notes in Comput. Sci*, pages 109–117, 1983.

[16] A.V. Chashkin. Perfect linear hashing in boolean cube. In *Transactions on Discrete Mathematics and its Applications*, volume 5, pages 56–67. Keldysh Institute of Applied Mathematics, 2009 (in Russian).

[17] A.V. Chashkin. On linear operators injective on subsets of the space $\mathrm{GF}^n(p)$. *Discrete Mathematics and Applications*, 2013 (to appear).

[18] D.Yu. Cherukhin. On complexity of linear operators on the class of circuits of depth 2. *Diskretnaya Matematika*, 20(1):109–119, 2008. Engl. transl. in: Discrete Mathematics and Applications. 2008. 18(2), 143–154.

[19] D.Yu. Cherukhin. Lower bounds for complexity of boolean circuits of finite depth with arbitrary elements. *Discrete Mathematics and Applications*, 21(4):499–508, 2011.

[20] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, 17(2):230–261, 1988.

[21] F.R.K. Chung, P. Erdős, and J. Spencer. On the decomposition of graphs into complete bipartite graphs. In *Studies in Pure Mathematics, To the Memory of Paul Turán*, pages 95–101. Akadémiai Kiadó, 1983.

[22] D. Dolev, C. Dwork, N. Pippenger, and A. Wigderson. Superconcentrators, generalizers and generalized connectors with limited depth (preliminary version). In *Proc. of 15th Ann. ACM Symp. on Theory of Computing*, pages 42–51, 1983.

[23] A. Drucker. Limitations of lower-bound methods for the wire complexity of boolean operators. In *IEEE Conference on Computational Complexity*, pages 170–180, 2012. Full version in ECCC Report Nr. 125, 2011.

[24] P.E. Dunne. *The complexity of Boolean networks*. Academic Press Professional, Inc., San Diego, CA, 1988.

[25] C. Dutta and J. Radhakrishnan. More on a problem of Zarankiewicz. In *Proc. of 23rd Int. Symp. on Algorithms and Computation, ISAAC 2012*, volume 7676 of *Springer Lect. Notes in Comput. Sci.*, pages 257–266, 2012. arXiv.1201.1377.

[26] P. Erdős, R.L. Graham, and E. Szemerédi. On sparse graphs with dense long paths. In *Computers and Math. with Appl.*, pages 365–369. Pergamon, Oxford, 1976.

[27] P. Erdős and R. Rado. Intersection theorems for systems of sets. *J. London Math. Soc*, 35:85–90, 1960.

[28] P. Erdős and J. Spencer. *Probabilistic methods in combinatorics*. Academic Press, 1974.

[29] T. Feder and R. Motwani. Clique partitions, graph compression and speeding-up algorithms. *J. Comput. Syst. Sci.*, 51(2):261–272, 1995.

[30] M. Find, M. Göös, P. Kaski, J. Korhonen, M. Koivisto, and J.H. Korhonen. Separating OR, SUM, and XOR circuits. Technical report, arXiv.1304.0513, 2013.

[31] J. Friedman. A note on matrix rigidity. *Combinatorica*, 13(2):235–239, 1993.

[32] A. Gál. On the complexity of realization of some classes of matrices by rectifier networks. *Matematicheskije Voprosy Kibernetiki*, 1:234–235, 1988 (in Russian).

[33] A. Gál, K.A. Hansen, M. Koucký, P. Pudlák, and E. Viola. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates. In *STOC 2012*, pages 479–494, 2012. Full preliminary version in ECCC Report Nr. 150, 2011.

[34] S.B. Gashkov and I.S. Sergeev. On the complexity of linear boolean operators with thin matrices. *Diskretn. Anal. Issled. Oper.*, 17(3):3–18, 2010. Engl. transl.: J. Applied and Industrial Math. 2011. 5(2), 202–211.

[35] S.B. Gashkov and I.S. Sergeev. A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials. *Matematicheskii Sbornik*, 203(10):33–70, 2012. Engl. transl. in: Sbornik: Mathematics. 2012. 203(10), 1411–1447.

[36] O. Goldreich and A. Wigderson. On the circuit complexity of perfect hashing. In *Studies in Complexity and Cryptography*, pages 26–29. 2011. Preliminary version in ECCC Report Nr. 41, 1996.

[37] D.Yu. Grigoriev. An application of separability and independence notions for proving lower bounds of circuit complexity. In *Notes of the Scientific Seminar Leningrad branch of the Steklov Institute*, volume 60, pages 38–48. 1976. English translation in J. Soviet Math. 14:5 (1980), 1450–1456.

[38] D.Yu. Grigoriev. On a nonlinear lower bound for circuit complexity of a set of disjunctions in monotone boolean basis. In *Notes of the Scientific Seminar Leningrad branch of the Steklov Institute*, volume 68, pages 19–25. 1977. English translation in J. Soviet Math. 15:1 (1981), 11–13.

[39] D.Yu. Grigoriev. Additive complexity in directed computations. *Theoret. Comput Sci.*, 19:39–87, 1982.

[40] D.Yu. Grigoriev. Lower bounds in algebraic complexity. In *Notes of the Scientific Seminar Leningrad branch of the Steklov Institute*, volume 118, pages 25–82. 1982. English translation in J. Soviet Math. 29 (1985), 1388–1425.

[41] M.I. Grinchuk. On the complexity of realization of boolean triangular matrices by rectifier schemes of various depths. *Metody Diskretnogo Analiza*, 4:3–23, 1986 (in Russian).

[42] M.I. Grinchuk. Complexity of the realization of cyclic boolean matrices by gate circuits. *Izvestija VUZov. Matematika*, 7:39–44, 1988. English translation in Soviet Math. 32:7 (1988), 65–72.

[43] M.I. Grinchuk and I.S. Sergeev. Thin circulant matrices and lower bounds on the complexity of some boolean operators. *Diskretn. Anal. Issled. Oper.*, 18(5):38–53, 2011 (in Russian).

[44] G. Hansel. Nombre minimal de contacts de fermeture nécessaires pour réaliser une fonction booléenne symétrique de n variables. *C. R. Acad. Sci.*, 258(25):6037–6040, 1964 (in French).

[45] G.H. Hardy, J.E. Littlewood, and G. Polya. *Inequalities*. University Press Cambridge, 1934.

[46] A.P. Hiltgen. Towards a better understanding of one-wayness: facing linear permutations. In *EUROCRYPT*, volume 1403 of *Springer Lect. Notes in Comput. Sci.*, pages 319–333, 1998.

[47] S. Jukna. Disproving the single level conjecture. *SIAM J. Comput.*, 36(1):83–98, 2006.

[48] S. Jukna. Entropy of operators or why matrix multiplication is hard for depth-two circuits. *Theory of Computing Systems*, 46(2):301–310, 2010.

[49] S. Jukna. Representing (0,1)-matrices by depth-2 circuits with arbitrary gates. *Discrete Mathematics*, 310:184–187, 2010.

[50] S. Jukna. *Boolean Function Complexity.* Springer, 2012.

[51] S. Jukna and G. Schnitger. Min-rank conjecture for log-depth circuits. *J. Comput. Syst. Sci.*, 77(6):1023–1038, 2011.

[52] G. Katona and E. Szemerédy. On a problem of graph theory. *Studia Scientiarum Mathematicarum Hungarica*, 2:23–28, 1967.

[53] N.H. Katz. On the CNF-complexity of bipartite graphs containing no squares. *Lithuanian Math. Journal*, 52(4):385–389, 2012.

[54] M.M. Klawe. Shallow grates. *Theor. Comput. Sci.*, 123(2):389–395, 1994.

[55] D.E. Knuth. *Art of programming: seminumerical algorithms*, volume 2. Reading, Massachusetts: Addison-Wesley, 1997. Third Edition.

[56] V.V. Kochergin. On the complexity of rectifier networks with multiple number of paths. In *Materials of the 18-th International School on Synthesis and Complexity of Control Systems (Penza, 2009)*, pages 51–56, 2009 (in Russian).

[57] J. Kollár, L. Rónyai, and T. Szabó. Norm-graphs and bipartite Turán numbers. *Combinatorica*, 16(3):399–406, 1996.

[58] T. Kövari, V.T. Sós, and P. Turán. On a problem of K. Zarankiewicz. *Colloq. Math.*, 3:50–57, 1954.

[59] R.E. Krichevski. Complexity of contact circuits realizing a function of logical algebra. *Doklady Akad. Nauk SSSR*, 151(4):803–806, 1963. English translation in Soviet Physics Doklady 8 (1963), 770–772.

[60] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, 1986.

[61] S.V. Lokam. Complexity lower bounds using linear algebra. *Foundations and Trends in Theoretical Computer Science*, 4(1-2):1–155, 2009.

[62] O.B. Lupanov. On rectifier and switching-and-rectifier schemes. *Doklady Akad. Nauk SSSR*, 111:1171–1174, 1956 (in Russian).

[63] O.B. Lupanov. On rectifier schemes. *Acta Cybernetica*, 4(4):311—315, 1980 (in Russian).

[64] K. Mehlhorn. Some remarks on Boolean sums. *Acta Informatica*, 12:371–375, 1979.

[65] P. Miltersen. Error correcting codes, perfect hashing circuits, and deterministic dynamic dictionaries. In *SODA*, pages 556–563, 1998.

[66] B.S. Mitiagin and B.N. Sadovskiy. On linear Boolean operators. *Doklady Akad. Nauk SSSR*, 165(4):773–776, 1965 (in Russian).

[67] J. Morgenstern. Note on a lower bound of the linear complexity of the Fast Fourier Transform. *J. of the ACM*, 20(2):305–306, 1973.

[68] J. Morgenstern. The linear complexity of computation. *J. of the ACM*, 22(2):184–194, 1974.

[69] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[70] E.I. Nechiporuk. On multipolar switching circuits realizing functions of multi-valued logics. *Problemy Kybernetiki*, 5:49–60, 1961 (in Russian).

[71] E.I. Nechiporuk. Rectifier networks. *Doklady Akad. Nauk SSSR*, 148(1):50–53, 1963. English translation in: Soviet Physics Doklady 8 (1963), 5–7.

[72] E.I. Nechiporuk. On the synthesis of rectifier networks. *Problemy Kibernetiki*, 9:37–44, 1963 (in Russian).

[73] E.I. Nechiporuk. Self-correcting diode networks. *Doklady Akad. Nauk SSSR*, 156(5):1045–1048, 1964. English translation in: Soviet Physics Doklady 9(6) (1964), 422–425.

[74] E.I. Nechiporuk. On a boolean matrix. *Problemy Kibernetiki*, 21:237—240, 1969. English translation in: Systems Theory Res. 21 (1970), 236–239.

[75] E.I. Nechiporuk. On the topological principles of self-correction. *Problemy Kibernetiki*, 21:5–102, 1969. English translation in: Systems Theory Res. 21 (1970), 1–99.

[76] I. Newman and A. Wigderson. Lower bounds on formula size of boolean functions using hypergraph entropy. *SIAM J. Discrete Math.*, 8(4):536–542, 1995.

[77] K. O'Bryant. A complete annotated bibliography of work related to Sidon sequences. *Electronic Journal of Combinatorics*, 11:1–39, 2004.

[78] V.A. Orlov. Realization of "narrow" matrices by rectifier networks. *Problemy Kybernetiki*, 22:45–52, 1970. English translation in: *Systems Theory Research*, 22, 42–50, 1972.

[79] H. Perfect. Applications of Menger's graph theorem. *Journal of Mathematical Analysis and Applications*, 22:96–111, 1968.

[80] T. Pinto. Biclique covers and partitions. Technical report, arXiv:1307.6363, 2013.

[81] N. Pippenger. On the evaluation of powers and related problems. In *FOCS*, pages 258–263, 1976.

[82] N. Pippenger. Superconcentrators. *SIAM J. Comput.*, 6(2):298–304, 1977.

[83] N. Pippenger. The minimum number of edges in graphs with prescribed paths. *Math. Syst. Theory*, 12(1):325–346, 1979.

[84] N. Pippenger. On another Boolean matrix. *Theor. Comput. Sci.*, 11:49–56, 1980.

[85] N. Pippenger. Superconcentrators of depth 2. *J. Comput. Syst. Sci.*, 24(1):82–90, 1982.

[86] P. Pudlák. Communication in bounded depth circuits. *Combinatorica*, 14(2):203–216, 1994.

[87] P. Pudlák. A note on the use of determinant for proving lower bounds on the size of linear circuits. *Inf. Process. Letters*, 74:197–201, 2000.

[88] P. Pudlák and V. Rödl. Some combinatorial-algebraic problems from complexity theory. *Discrete Math.*, 136(1-3):253–279, 1994.

[89] P. Pudlák, V. Rödl, and P. Savický. Graph complexity. *Acta Inf.*, 25(5):515–535, 1988.

[90] P. Pudlák and Z. Vavrín. Computation of rigidity of order n^2/r for one simple matrix. *Comm. Math. Univ. Carol.*, 32(2):213–218, 1991.

[91] J. Radhakrishnan. Entropy and counting. Manuscript, available at http://www.tcs.tifr.res.in/∼jaikumar/mypage.html, 2001.

[92] J. Radhakrishnan and A. Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. Discrete Math.*, 13(1):2–24, 2000.

[93] A.A. Razborov. Lower bounds on the size of bounded-depth networks over a complete basis with logical addition. *Mat. Zametki*, 41(4):598–607, 1987. Engl. transl. in: Math. Notes of the Acad. of Sci. of the USSR 41 (1987), 333–338.

[94] I.Z. Ruzsa. Solving a linear equation in a set of integers. I. *Acta Arith.*, 65:259–282, 1993.

[95] G. Schnitger. A family of graphs with expensive depth-reduction. *Theor. Comput. Sci.*, 18:89–93, 1982.

[96] G. Schnitger. On depth-reduction and grates. In *24th IEEE Ann. Symp. on Foundations of Comput. Sci.*, pages 323–328, 1983.

[97] A. Schönhage. Schnelle multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf.*, 7:395–398, 1977 (in German).

[98] S.N. Selezneva. Lower bound on the complexity of finding polynomials of Boolean functions in the class of circuits with separated variables. In *Proc. of 11-th Int. Seminar on Discrete Math. and Its Appl. (Moscow, June 2012)*, pages 216–218, 2012. Journal version in: Computational Mathematics and Modeling, Consultants Bureau (United States), 24(1), 146–152, 2013.

[99] I.S. Sergeev. Implementation of linear maps with circulant matrices via modulo 2 rectifier circuits of bounded depth. Technical report, arXiv.1305.4389, 2013.

[100] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.

[101] D.A. Spielman. Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory*, 42(6):1723–1731, 1996.

[102] M. Sudan. Essential coding theory, 2002. Manuscript, available at http://research.microsoft.com/en-us/um/people/madhu/.

[103] T.G. Tarjan. Complexity of lattice-configurations. *Stud. Sci. Math. Hung.*, 10:203–211, 1975.

[104] Z. Tuza. Covering of graphs by complete bipartite subgraphs; complexity of 0-1 matrices. *Combinatorica*, 4(1):111–116, 1984.

[105] L.G. Valiant. Graph-theoretic properties in computational complexity. *J. Comput. Syst. Sci.*, 13(3):278–285, 1976.

[106] L.G. Valiant. Graph-theoretic methods in low-level complexity. In *Springer Lect. Notes in Comput. Sci.*, volume 53, pages 162–176, 1977.

[107] I. Wegener. A new lower bound on the monotone network complexity of Boolean sums. *Acta Inform.*, 15:147–152, 1980.

[108] I. Wegener. *The complexity of Boolean functions*. Wiley-Teubner, 1987.

[109] D.J. Welsh. *Matroid theory*. Academic Press, London, 1976.

[110] A. Wigderson. P, NP and mathematics - a computational complexity perspective. In *Proceedings of the ICM 06 (Madrid)*, volume 1, pages 665–712. EMS Publishing House, Zurich, 2007.