A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials

2012 Sb. Math. 203 1411

(http://iopscience.iop.org/1064-5616/203/10/A02)

Sbornik: *Mathematics* **203**:10 1411–1447

Matematicheskiĭ Sbornik **203**:10 33–70 DOI 10.1070/SM2012v203n10ABEH004270

A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials

S. B. Gashkov and I. S. Sergeev

Abstract. This work suggests a method for deriving lower bounds for the complexity of polynomials with positive real coefficients implemented by circuits of functional elements over the monotone arithmetic basis $\{x+y,$ $x\cdot y\}\cup\{a\cdot x \mid a\in\mathbb{R}_+\}$. Using this method, several new results are obtained. In particular, we construct examples of polynomials of degree $m-1$ in each of the n variables with coefficients 0 and 1 having additive monotone complexity $m^{(1-o(1))n}$ and multiplicative monotone complexity $m^{(1/2-o(1))n}$ as $m^n\to\infty$. In this form, the lower bounds derived here are sharp.

Bibliography: 72 titles.

Keywords: lower bounds for complexity, arithmetic circuits, thin sets, monotone complexity, permanent.

§ 1. Introduction

Methods for deriving effective lower bounds for the computational complexity of functions are of keen interest in the context of the widely known problem $P\stackrel{?}{=}NP$, which arose from the works of S. Cook, R. Karp and L. Levin in the 1970s. To solve this problem in the negative (which seems more likely, but is much harder to accomplish), we would need to prove that some computational problems lack efficient solving algorithms. By an efficient algorithm we mean an algorithm whose run-time complexity (that is, the number of computation steps) is on the order of at most n^c, where n denotes the size of the input data in the binary coding and c is some constant independent of n. Algorithms which admit this kind of bound for the run-time complexity are usually called *polynomial-time* algorithms (and the class P of problems which are solvable by such algorithms is referred to as the 'polynomial-time class'). The concept of an algorithm and its complexity, as well as the definition of the classes P and NP, is usually introduced in terms of deterministic and nondeterministic Turing machines (see, for instance, [1]). However, there is a well-known relationship between the time complexity of computations on Turing machines and the complexity of the computation of Boolean functions by

This work was financially supported by the Russian Foundation for Basic Research (grant nos. 11-01-00508 and 11-01-00792-a) and the Department of Mathematical Sciences of the Russian Academy of Sciences (the Fundamental Research Programme "Algebraic and Combinatorial Methods of Mathematical Cybernetics and Information Systems of New Generation," project "Problems of Optimal Synthesis of Control Systems").

AMS 2010 *Mathematics Subject Classification.* Primary 03D15; Secondary 68Q15, 68Q17.

circuits over the standard Boolean basis $\{x\,\&\,y, x\vee y, \neg x\}$ (see, for instance, [2]). In view of this relationship, to solve the problem $P \stackrel{?}{=} NP$ in the negative, it is sufficient to show that certain Boolean functions of n variables (related to some known NP-complete problems) admit no Boolean circuits which compute these functions and contain $n^{O(1)}$ gates. In other words, it is sufficient to derive a *super-polynomial lower bound* for the complexity of these functions.

The current situation is such that not even a *nonlinear* lower bound for the Boolean complexity (that is, an estimate of the form $nf(n)$, where $f(n)\to\infty$, for an n-ary Boolean function) is known so far. In this connection, significant efforts are under way to find nontrivial *linear* lower bounds. At the same time, Lupanov showed in his well-known works (see, for example, his textbook [3], or [2]) that almost all n-ary Boolean functions have computational complexity $(1+o(1))2^n/n$. This is asymptotically equal to the complexity of the most complex function of this class, which Lupanov called a Shannon function. Consequently, the fraction of functions that have, for instance, complexity $2^{n(1-\varepsilon)}$, vanishes as n increases. Hence, there is no doubt in that complex functions do exist. The problem is to specify such function explicitly (that is, effectively in some reasonable sense) and to demonstrate that its complexity is high. There are some not quite effective results establishing high lower bounds for the complexity of Boolean functions (see, for example, [2]), which are of independent interest, but do not provide a solution to the problem of deriving effective lower bounds.

As early as the 1950s (that is, long before the 'theory of NP-completeness' was proposed) Lupanov and Yablonskiĭ realized the importance of the problem of lower bounds. However, for the case of representing Boolean functions by circuits of the general form this problem appeared (and still seems to be) too difficult, and thus methods for deriving lower bounds for the complexity of implementation of Boolean functions by circuits with constraints have been actively developed. Constraints were imposed both on the structure of circuits[1] and on the basis over which the circuits were constructed.[2] In this area significant results were obtained as early as in the 1960s by Lupanov and his students and disciples (see, for example, [2], [4]–[6]). With few exceptions, all estimates derived in that time were polynomial.

In 1984, Razborov and Andreev independently obtained super-polynomial lower bounds for the complexity of the representation of Boolean functions over the monotone basis $\{\&,\vee\}$. In [7] and [8], Razborov derived estimates of the form $n^{\Omega(\log n)}$ for the monotone complexity of the logical analogue of the permanent and for the function that detects a clique of a given size in the graph[3], Andreev's works [11], [12] suggest an almost exponential lower bound of the form $2^{n^{1/8-o(1)}}$ for a specially constructed function. Later Andreev raised his bound to $2^{n^{1/4-o(1)}}$ (the same estimate was obtained in [10]), and in [9] he established an estimate $2^{n^{1/3-o(1)}}$ for

[1] For instance, some works were devoted to representing Boolean functions by a particular kind of circuit, with no branching at the output gate, that is, formulae; also, some other types of circuits were considered — contact networks, gate circuits, contact-rectifier circuits.

[2] In particular, circuits over incomplete bases were considered.

[3] Andreev [9] and independently Alon and Boppana [10] improved the bound for the function that detects a clique up to $2^{n^{1/6-o(1)}}$.

the complexity of some other function. Apparently being unaware of the results obtained in [9], in [13] Harnik and Raz derived the same estimates.

To some degree problems on Boolean complexity are similar to problems on the complexity of computation of real or complex polynomials by circuits (nonbranching programs) whose elements implement arithmetic operations and constants. At the present time such circuits are often referred to as arithmetic circuits.

Univariate real polynomials of degree n can be evaluated via a Horner scheme. In the early 1960s V. Ya. Pan showed that this method is optimal if the constants used in the scheme are only the coefficients of the polynomial being realized, whereas the number of multiplications can be reduced by almost half if one is allowed to use any other constants in the scheme. At the same time it was demonstrated that almost no polynomial can be calculated appreciably more simply than by Pan's method (see, for instance, [14]). However, it turned out not to be that easy to produce a particular 'intractable' polynomial. Strassen, his students and disciples carried out a series of investigations in this area and suggested in [15]–[18] examples of polynomials of complexity $\Omega(n)$, additive complexity n, multiplicative complexity $n/2 + O(1)$, and nonscalar complexity[4] $\Omega(\sqrt{n})$. In view of the results obtained by Pan and Belaga (see [14]) and by Paterson and Stockmeyer [19] none of these estimates can be improved in order (and some of them are sharp up to an additive constant). A survey of papers from that time devoted to lower bounds in algebraic complexity theory can be found in [20], the present state-of-the-art is described in [21]. However, the polynomials mentioned above have coefficients of rather complex nature (either rational numbers which grow rapidly with the index of the coefficient, or complex roots of unity of rapidly increasing orders).

The existence of polynomials of complexity $\Omega(n/\log n)$ with coefficients 0 and 1 has been proved nonconstructively. Namely, Schnorr and van de Wiele showed in [22] that almost all polynomials have this property. In the same work they derived the estimate $\Omega(\sqrt{n/\log n})$ for multiplicative (and for nonscalar) complexity, and established the estimate $\Omega(\sqrt{n}/\log n)$ for additive complexity. It is known [23] that the complexity of polynomials with coefficients 0, 1 cannot be of order higher than $n/\log n$, even if of all possible constants it is only the constant 1 that is used in the circuit (and thus the circuit is monotone), at the same time the multiplicative complexity is not higher than $O(\sqrt{n})$. We construct a polynomial with coefficients 0 and 1 which has additive monotone complexity $n^{1-o(1)}$ and multiplicative monotone complexity $n^{1/2-o(1)}$ below (thereby solving the open problem 9.3 formulated in [21]).

The complexity of computation of various classes of polynomials whose coefficients belong to a given finite set was also considered in [24]–[26]. It suffices that the basis over which the circuits are designed contain only a finite set of constants. In [25] and [26] it was noted that asymptotically optimal upper bounds can be derived using a modification of Lupanov's method mentioned above. In particular, for polynomials in n variables of degree at most 1 in each of the variables (in [27] such polynomials were called Zhegalkin polynomials[5], whereas in modern works

[4]This term is used here and below for brevity to denote the minimum number of multiplications of the general form not including multiplication by constants.

[5]Named after I. I. Zhegalkin, professor in Moscow State University, who introduced these polynomials in [28].

by non-Russian authors they are called multilinear polynomials) and only having coefficients 0 and 1, the monotone complexity has the asymptotic upper estimate of $2^n/n$, whereas the upper estimate for the multiplicative complexity is $O(2^{n/2})$. Moreover, the first estimate is asymptotically the best possible.

Without altering the set of coefficients a multilinear polynomial in n variables can be reduced by the change of variables $x_i = x^{2^{i-1}}$ to a univariate polynomial of degree at most 2^n-1, and conversely, any univariate polynomial can be transformed into a multilinear one. Therefore, upper estimates for the complexity of multilinear polynomials imply the same estimates for univariate polynomials (hence, the results of [23] follow from [25]), and lower estimates for the complexity of univariate polynomials imply the same estimates for multilinear polynomials.[6] Therefore, from results due to von zur Gathen and Strassen [15], Heintz and Sieveking [16], and Stoss [17] it follows that the aforementioned estimates for multilinear polynomials cannot be essentially improved in order even using circuits over the complete basis.[7] For instance, the multiplicative complexity of the class of all multilinear polynomials with coefficients 0, 1 in n variables has the lower bound $\Omega(2^{n/2}/\sqrt{n})$. One can also explicitly specify multilinear polynomials of additive complexity $2^n - 1$, multiplicative complexity $2^{n-1} + O(n)$, but their coefficients have a very complicated nature.

For monotone arithmetic circuits the first almost exponential effective lower bound was established by Schnorr [29]. This estimate was of the order of $2^{\sqrt{n}}/\sqrt[4]{n}$; more precisely, for some polynomial of degree n^2 in $4n^2$ variables (associated with the clique problem [1]) the additive monotone complexity was actually shown to coincide with the binomial coefficient $C_{2n}^n - 1$.

Almost exponential lower bounds of the form $2^{\Omega(\sqrt{n})}$ for the monotone complexity of polynomials were also obtained by Jerrum and Snir in [30] and Valiant in [31]. The work [30] suggests an asymptotically sharp estimate $(1 - o(1))2^{n-1}n$ for the monotone multiplicative complexity of computation of the permanent[8] of a real $(n \times n)$-matrix; the corresponding upper bound was established by H. J. Ryser and W. B. Jurkat in 1967 (see, for instance, [14]). As is known, in the complete basis, the determinant[9] has complexity $O(n^{\omega+o(1)})$, where ω is the exponent of matrix multiplication, which is currently known to satisfy the inequality $2 \leqslant \omega < 2,4$.

In [32] and [33] Valiant suggested that it is difficult to derive almost exponential lower bounds for the complexity of computation of some monotone polynomials in the complete basis. Namely, he showed that the existence of such an estimate for the permanent of a real matrix would imply $VNP \neq VP$, where $VNP \stackrel{?}{=} VP$ denotes

[6] To transform a circuit S that realizes a multilinear polynomial in n variables into a circuit that realizes the corresponding univariate polynomial, one has to attach the inputs of the circuit S to the outputs of a circuit that computes the n-tuple of powers x^{2^i}, $i = 0, \ldots, n-1$; such a circuit can be designed using $n - 1$ product gates.

[7] That is, in the basis that contains subtraction or all possible constants, including negative ones.

[8] The permanent is a multilinear monotone polynomial of degree n in n^2 variables with coefficients $0, 1$.

[9] The determinant is a multilinear non-monotone polynomial of degree n in n^2 variables with coefficients $0, \pm 1$.

some algebraic analogue of the conventional (Boolean) problem $P \stackrel{?}{=} NP$. In the same paper he demonstrated that the permanent of a matrix with integer entries can be computed modulo 2^k using Boolean circuits with complexity $O(n^{4k-3})$.

For reasons explained in [34], for instance, in the theory of algebraic complexity classes developed by Valiant, it is more convenient to consider the multilinear polynomial

$$HC_n = \sum_{\sigma} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

instead of the permanent; this is used to determine whether a graph on n vertices is Hamiltonian, and summation is taken over all cyclic permutations $\sigma \in S_n$. A detailed account of Valiant's theory can be found in [21]. We also note that an analogue of the problem $P \stackrel{?}{=} NP$ for the field of complex numbers was studied in [35].

Investigation of the complexity of the permanent attracted further interest. In [36] the methods of [30] were applied to obtain the same lower estimates for the monotone complexity of the $(0,1)$-permanent.[10] Another approach, under which the permanent of a matrix is expressed in terms of the determinant of a larger matrix, was put forward in [37]. In [38] both the permanent and the determinant were shown to have super-polynomial complexity when realized by *multilinear formulae* [11] in the complete basis.

The theory of complexity classes underlies certain methods for introducing the concept of *effectiveness*. Effectiveness may be used to formalize the intuitive idea of concreteness, explicit specification (what does it mean to say that a function is specified explicitly?).

For instance, the effectiveness of (sequences of) Boolean functions is often treated as their belonging to the class NP. This definition appears ill-chosen, at least while the problem $P \stackrel{?}{=} NP$ remains unsolved. Indeed, in the case $P = NP$, attempts to derive effective super-polynomial lower bounds for complexity in the complete basis would turn out to be meaningless.

Polynomials can be specified explicitly in a number of ways. For instance, one could actually specify (or suggest an easy procedure for calculating) the coefficients of the monomials or the roots. Examples of intractable polynomials which we construct later on in this work have coefficients 0 and 1. In particular, they come within the scope of the following definition of effectiveness. A polynomial is *effective* if the Boolean function that calculates the coefficient of the polynomial by the degree of the corresponding monomial (the degree is given in binary representation) is implemented by a Boolean circuit of polynomial complexity over the standard basis. It follows from a result in [33] that polynomials which are effective in this sense belong to the class VNP (an algebraic analogue of the class NP).

However, even being in the class VNP is not an entirely satisfactory criterion for the effectiveness of a polynomial. For instance, it is hard to say whether a particular

[10] That is, the permanent of a $(0,1)$-matrix was computed using monotone polynomials which always evaluate (as the variables take values 0 or 1) to the permanent of the corresponding $(0,1)$-matrix.

[11] In multilinear formulae all subformulae realize multilinear polynomials.

specified polynomial such as the multilinear analogue of the polynomial $\sum 2^{2^k} x^k$ (an example suggested by Strassen) belongs to VNP or not. If it does (which seems unlikely), then $VP \neq VNP$, since the complexity of this polynomial in the complete arithmetic basis is super-polynomial. If not, then, perhaps, effectiveness should be defined in some other way.

In 1983 Kasim-Zade [39], [40] constructed a multilinear polynomial in n variables with coefficients $0, 1$ having additive monotone complexity $2^{\lfloor n/2 \rfloor} - 1$, and thereby derived the first effective exponential lower bound for this measure of complexity. Exponential lower bounds for the complexity of monotone polynomials were also obtained in 1984 by Kuznetsov [41] (as is noted in [39]–[41], estimates of this kind can also be derived from Kuznetsov's earlier work [42]). In 1987, in [43] a method for deriving lower bounds for monotone complexity was presented, based on ideas in [39], [40] and [29]. Using that method, in particular, the author effectively specified a multilinear polynomial in n variables with coefficients $0, 1$ having additive monotone complexity of order at least $2^{2n/3}$ and multiplicative monotone complexity of order at least 2^{cn}, where the constant $c > 1/3$.

In [40] Kasim-Zade also constructed a sequence of multilinear polynomials in n variables with rational coefficients having complexity $\Omega(2^{c_1 n})$ over the monotone arithmetic basis and complexity $O(n^{c_2})$ over the basis augmented by subtraction.[12]

Apparently being unaware of the works [39]–[43], in their recent paper [44] Raz and Yehudayoff derived a lower bound of the form $2^{\Omega(n)}$ for the monotone complexity of some multilinear polynomial in n variables. In [44] they also obtained some results on the complexity of various types of multilinear formulae (that is, formulae in multilinear bases).[13]

Some methods for deriving lower bounds for the monotone complexity of Boolean functions also apply to the case of representing Boolean functions by *monotone circuits over the field of real numbers*[14] — this was the subject of study, for example, in the works by Haken and Cook [48] and Pudlák [49]. The latter work suggests a lower bound $2^{n^{1/6-o(1)}}$ for the monotone Boolean function of n variables which determines whether a given graph contains a clique of a given size.

Because of space limitations, [43] contained only sketches of the proofs of the main theorems. In this work we present (in a somewhat generalized form) the method for deriving lower bounds suggested in [43] with a detailed proof and present some new results.

[12] The results of Schnorr [29] and Kasim-Zade [39], [40] were formulated for calculations over the field $\mathbb{Q}$, rather than $\mathbb{R}$, but it makes no difference.

[13] According to [44] the model of multilinear circuits and formulae was first introduced in 1995 in [45]. However, we note that these concepts appeared in [27] and [46] as early as 1980; these papers also contain some results concerning the complexity of the realization of Boolean functions by multilinear circuits and formulae. The ideas in [27] and [46] were developed further in [47], which also used the terms multilinear polynomial and multilinear formula. The works [47] and [27] were cited in [35].

[14] Such circuits are composed of elements that realize monotone functions of real variables. A circuit implements a Boolean function if it returns 0 or 1 whenever the value supplied at the inputs of the circuit is 0 or 1. Note that this definition of implementation of Boolean functions by circuits over continuous bases was proposed by Lupanov; it was investigated in [27], [46] in the late 1970s.

In particular, we combine the aforementioned method with an interesting combinatorial result obtained by Kóllar, Rónyai and Szabó [50] and on the way we derive the lower bound $m^{n(1-o(1))}$ for the additive monotone complexity and the lower bound $m^{n(1/2-o(1))}$ for the multiplicative monotone complexity (as $m^n \to \infty$) for particular polynomials in n variables of degree $m-1$ in each of the variables with unit coefficients. In this form the estimates obtained are best possible. This example incorporates important special cases of multilinear polynomials ($m = 2$) and univariate polynomials ($n = 1$).

Also, we effectively construct a multilinear polynomial in n variables of degree $m-1$ in each of the variables with unit coefficients for which the ratio between the complexity of the realization in the monotone basis and the complexity of the realization in the complete basis is not less than $m^{(0,5-o(1))n}$ as $m^n \to \infty$. Earlier, in [31] Valiant considered the case $m = 2$ of multilinear polynomials and estimated the same ratio from below by $2^{\Omega(\sqrt{n})}$; Kasim-Zade obtained the exponential estimate 2^{cn} (see above).

As another application of our method we derive the lower bound $\Omega(2^n\sqrt{n})$ for the additive monotone complexity of the permanent of order n. The lower bound $\Omega(2^n/\sqrt{n})$ for the polynomial HC_n mentioned above can be obtained similarly. (The authors are unaware of any other results concerning the additive monotone complexity of these polynomials.)

We also show that the lower bounds derived using the method suggested in this work cannot be essentially improved.

§ 2. Main definitions

We consider polynomials computed by circuits which are composed of sum gates, product gates, and positive real constants. For any polynomial f of this kind, by $L_+(f)$ we denote the minimum number of additions, and by $L_\times(f)$ the minimum number of nonscalar multiplications required for its computation. As usual, the semiring of monotone polynomials in the variables $x_1, \dots, x_n$ with respect to the operations of addition and multiplication is denoted by $\mathbb{R}_+[x_1, \dots, x_n]$. We let $P(N^n)$ denote the semiring of finite subsets of the set N^n (where $N = \mathbb{N} \cup \{0\}$) with respect to the operations of disjunction $\vee$ and multiplication $\times$: if $A, B \in P(N^n)$, then $A, B \subset N^n$,

$$A \vee B = A \cup B, \qquad A \times B = \{a + b \mid a \in A,\ b \in B\}.^{15}$$

By mon we denote the homomorphism from the semiring $\mathbb{R}_+[x_1, \dots, x_n]$ to the semiring $P(N^n)$ defined as follows: $a = (a_1, \dots, a_n) \in \operatorname{mon} f$ if and only if the polynomial f contains a monomial $c_a x_1^{a_1} \cdots x_n^{a_n}$.

The fact that the mapping mon is indeed a homomorphism follows from the easily verifiable identities

$$\operatorname{mon}(f_1 + f_2) = \operatorname{mon} f_1 \vee \operatorname{mon} f_2, \qquad \operatorname{mon}(f_1 f_2) = \operatorname{mon} f_1 \times \operatorname{mon} f_2,$$
$$\operatorname{mon} 0 = \varnothing, \qquad \operatorname{mon} 1 = \{(0, \dots, 0)\}.$$

[15] The set $A \times B$ is the Minkowski sum of the sets A and B. In this work we have to use the symbol '$\times$' for Minkowski addition since it plays the role of multiplication (this is the way the degrees of monomials are transformed as monotone polynomials are multiplied).

A subset H of the semigroup $(G, +)$ is said to be (k, l)-*thin* if it contains no subset of the form $A \times B = \{a+b \mid a \in A,\ b \in B\}$, where $|A| = k$ and $|B| = l$ (here and below the cardinality of a finite set M is denoted by $|M|$).

In the case where $(G, +)$ is a group, this definition admits an equivalent formulation: a subset H of the group $(G, +)$ is said to be (k, l)-thin if for any distinct elements $g_1, \dots, g_k \in G$ the following inequality holds:

$$\left|\bigcap_{i=1}^{k} g_i H\right| < l, \qquad g_i H = \{g_i\} \times H.$$

Proving these two definitions are equivalent is straightforward. Indeed, suppose that for some elements $g_1, \dots, g_k \in G$ the inequality $|\bigcap_{i=1}^{k} g_i H| \geqslant l$ holds true. Since $\{-g_1, \dots, -g_k\} \times \bigcap_{i=1}^{k} g_i H \subset H$, the subset H is not (k, l)-thin in the sense of the first definition.

Conversely, suppose that $A \times B \subset H$, $A = \{g_1, \dots, g_k\}$, $|B| = l$. Since $B \subset \bigcap_{i=1}^{k}(-g_i)H$, we have $|\bigcap_{i=1}^{k}(-g_i)H| \geqslant l$. Consequently, H is not (k, l)-thin in the sense of the second definition.

In what follows, when using the notion of a (k, l)-thin subset in a commutative semigroup, in particular, in $(N^n, +)$, we always assume that $k \leqslant l$. In addition, we call a (k, k)-thin subset k-thin for short.

§ 3. Main theorem

Denote by $\alpha(k)$ the maximum number of distinct Boolean $(k-1)$-tuples of which none is equal to the disjunction of any two other $(k-1)$-tuples. It is easily verified that $\alpha(2) = 2$, $\alpha(3) = 3$, $\alpha(4) = 5$, $\alpha(5) = 9$, and $\alpha(k) < 2^{k-2}$ for $k > 5$. In [51] Kleitman showed that $\alpha(k) \sim C_{k-1}^{\lfloor (k-1)/2 \rfloor}$.

The following theorem was formulated and proved in [43] for the case $k = l$.

Theorem 1. *Let $k > 1$ and $\operatorname{mon} f$ be a (k, l)-thin subset of the set $(N^n, +)$. Set $h = \max\{|A| \mid A = A_1 \times \dots \times A_p \subset \operatorname{mon} f,\ |A_i| < l\}$ and $H = h^{-1}|\operatorname{mon} f|$. Then the following inequalities are valid*:

(i) $L_+(f) \geqslant H - 1$;

(ii) $L_\times(f) \geqslant 2\sqrt{H} - n - 2$;

(iii) *if* $\log H/(\alpha(k)\log\alpha(l)) \to \infty$, *then*

$$L_\times(f) \geqslant (2 - o(1))\big(\alpha(l) - \alpha(k) + 1\big)^{-1/(2\alpha(k)-1)} H^{\alpha(k)/(2\alpha(k)-1)} - n - 2.$$

In what follows, apart from the next section which is devoted to the additive complexity of the permanent, when we refer to this theorem we shall always replace h with another quantity h^*; the estimate $h^* \geqslant h$ is established in the following simple lemma.

Lemma 1. *The following inequality is valid*: $h \leqslant h^* = \max\{(k-1)^3, (l-1)^2\}$.

Proof. We will show that for any set $A = A_1 \times \dots \times A_p \subset \operatorname{mon} f$, $|A_i| < l$, the estimate $|A| \leqslant h^*$ holds.

In the case $p = 2$ we obviously have $|A_1 \times A_2| \leqslant (l-1)^2$. For $p = 3$ we renumber the sets A_i in order of nondecreasing cardinality, so that $|A_1| \leqslant |A_2| \leqslant |A_3|$.

If $|A_1 \times A_2| \geqslant l$, then $|A_3| \leqslant k-1$, whence it follows that $|A_1 \times A_2 \times A_3| \leqslant |A_3|^3 \leqslant (k-1)^3$. Otherwise, if $|A_1 \times A_2| \leqslant l-1$, then $|(A_1 \times A_2) \times A_3| \leqslant (l-1)^2$.

In the general case $p > 3$ we take s to be the largest integer such that $|A_1 \times \cdots \times A_s| < l$. If $s = p$, then there is nothing to prove. If $s = p-1$, then we have $|(A_1 \times \cdots \times A_{p-1}) \times A_p| \leqslant (l-1)^2$. Otherwise, set $A'_1 = A_1 \times \cdots \times A_s$, $A'_2 = A_{s+1}$, $A'_3 = A_{s+2} \times \cdots \times A_p$. We have $A_1 \times \cdots \times A_p = A'_1 \times A'_2 \times A'_3$, where $|A'_1|, |A'_2| \leqslant l-1$ and $|A'_3| \leqslant k-1 \leqslant l-1$. Thus, the argument for the case $p = 3$ examined above applies to the subset $A'_1 \times A'_2 \times A'_3$. The proof of the lemma is complete.

Before we prove the theorem we shall make some remarks in which we establish a relationship between it and the results in [39], [40] and [29] mentioned in the introduction.

Suppose that the group $(G, +)$ has no elements of order 2.

A subset H of the group $(G, +)$ is called *a semidifference* if for any elements $a, b, c, d \in H$ the following implication holds:

$$0 \neq a - b = c - d \quad \Longrightarrow \quad (a = c)\ \&\ (b = d).$$

It is easy to see that H is a semidifference subset of the Abelian group $(G, +)$ if and only if any quadruple of elements $a, b, c, d \in H$ obeys the implication

$$a + b = c + d \quad \Longrightarrow \quad \big((a = c)\ \&\ (b = d)\big) \vee \big((a = d)\ \&\ (b = c)\big).$$

Such a subset is also called a *Sidon set*, see [52].

In the method used in [39] and [40] the role of $\operatorname{mon} f$ is played by the semidifference subsets $\{0,1\}^n \subset (\mathbb{Z}^n, +)$.

We shall show that in an Abelian group the definitions of a semidifference and a 2-thin subset are equivalent. Suppose that $H \subset G$ is not 2-thin, which is to say that for some elements $a \neq b$, $c \neq d$ we have $a + c, a + d, b + c, b + d \in H$. Then $0 \neq (b + c) - (a + c) = (b + d) - (a + d)$, but $b + c \neq b + d$, which means that H is not a semidifference subset.

Now suppose that H is not a semidifference subset, that is, for some elements $a, b, c, d \in H$ we have $a + b = c + d$, where $a \neq c$, $a \neq d$. Then $\{a, d\} \times \{c - a, 0\} = \{a, b, c, d\} \subset H$, which means that H is not 2-thin.

For this reason the result in [39], [40] follows from Theorem 1, (i) (provided we can produce 2-thin subset $H \subset \{0,1\}^n$ of cardinality $2^{\lfloor n/2 \rfloor}$, see Theorem 3, (i.b) below).

In [29] a set $M \subset N^n$ is called *separated* if any $r, s, t \in M$ and $u \in N^n$ obey the following implication:

$$r + u = s + t \quad \Longrightarrow \quad (r = s) \vee (r = t).$$

It is clear that any separated subset is a semidifference subset and therefore it is 2-thin. Consequently Theorem 1, (i) yields all results in Section 4 in [29].

Proof of Theorem 1. We will go from circuits realizing f to circuits that realize $\operatorname{mon} f$ over the basis $\{\vee, \times\}$. We shall utilize the following lemma. (The minimum number of $\vee$ gates and $\times$ gates required to realize the set $\operatorname{mon} f$ by such circuits are denoted by $L_\vee(\operatorname{mon} f)$ and $L_\times(\operatorname{mon} f)$, respectively.)

Lemma 2. *The following inequalities hold*:

$$L_{\times}(f) \geqslant L_{\times}(\operatorname{mon} f), \qquad L_{+}(f) \geqslant L_{\vee}(\operatorname{mon} f).$$

Proof. Let $\widetilde{S}$ be an arbitrary circuit realizing some polynomial f. In this circuit we replace the product gates with $\times$ gates, and the sum gates with $\vee$ gates. We replace the inputs x_i with the constants

$$a_i = \{(\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots, 0)\} \in P(N^n), \qquad i = 1, \ldots, n,$$

and the constants from $\mathbb{R}_+$ with the constant $\{(0, \ldots, 0)\} \in P(N^n)$. As a result we obtain a circuit S that computes the set $\operatorname{mon} f$ in the semiring $P(N^n)$ (this follows because mon is a homomorphism) and contains as many $\times$ gates (and $\vee$ gates) as the circuit $\widetilde{S}$ contains product gates (sum gates, respectively). The proof of the lemma is complete.

Now we introduce some definitions and notation. An arbitrary gate of circuit S will be denoted by the symbol e. By $\varphi(e)$ we denote the element of the semiring $P(N^n)$ realized at the output of the gate e. The *weight* of the gate e is the cardinality of the set $\varphi(e)$. Without loss of generality we shall assume that the circuit S contains no gates which are not connected to the output by at least one directed path (any such gate can be removed from the circuit). The *predecessors* of the gate e are the gates that have outgoing edges entering into e.

For each product gate $\times$ we distinguish one of the predecessors and call the edge that connects them *prohibited*. Below we shall demonstrate that it is always possible to distinguish a predecessor whose weight is less than l. Let $\psi(e)$ be an element of the semiring $P(N^n)$ calculated by the aforementioned predecessor of the gate e. In what follows we consider only (directed) paths that visit no prohibited edges. Let C be some path that joins the gate e with the output of the circuit S and let $e_1, \ldots, e_m$ be all the product gates involved in the path C excluding e (it may be that $m = 0$). We set $\Psi(C) = \psi(e_1) \times \cdots \times \psi(e_m)$; if $m = 0$ we define $\Psi(C) = \{(0, \ldots, 0)\}$. The disjunction $\bigvee_C \Psi(C)$ taken over all paths C that join the gate e with the output of circuit S will be denoted by $\Psi(e)$ (if there are no such paths we set $\Psi(e) = \varnothing$).

A set of gates or constants of the circuit is called a *cut* if any path that connects a constant with the output of the circuit goes through at least one gate of this set.

Lemma 3. *For any cut E of the circuit the following relation is satisfied*:

$$\operatorname{mon} f = \bigvee_{e \in E} \varphi(e) \times \Psi(e).$$

Proof. The inclusion $\operatorname{mon} f \supset \bigvee_{e \in E} \varphi(e) \times \Psi(e)$ follows since $\operatorname{mon} f \supset \varphi(e) \times \Psi(C)$ which is obvious for any path C joining the gate e with the output of the circuit.

The reverse inclusion $\operatorname{mon} f \subset \bigvee_{e \in E} \varphi(e) \times \Psi(e)$ is established by induction on the complexity of the circuit S. The base case, which corresponds to a circuit that involves a single constant, is evident.

Let us perform the inductive step. Denote the output of the circuit by e'. We shall assume that $e' \notin E$ (otherwise, the inclusion is clearly satisfied).

Consider the case where e' is an OR gate. Let e'_1 and e'_2 be its predecessors and denote by S_i the circuit obtained by eliminating the gate e' from S and specifying the output gate e'_i, $i = 1, 2$. If $e'_1 = e'_2$, then the required relation follows immediately as we pass to the subcircuit S_1. Therefore, we shall assume below that $e'_1 \neq e'_2$.

Let C be an arbitrary path that connects an internal gate of the circuit S with the gate e'. The direct predecessor of this gate in the path C is one of the gates e'_i, and the path C can be obtained by adding the gate e' to the corresponding path C' of the subcircuit S_i. It is evident that $\Psi(C) = \Psi(C')$.

Set $E_i = E \cap S_i$. For any gate $e_i \in E_i$ and subcircuit S_i we define $\Psi_i(e)$ in the same way as $\Psi(e)$. Then $\Psi(e) = \Psi_i(e)$ for any $e \in E_i \setminus E_{3-i}$ and $\Psi(e) = \Psi_1(e) \vee \Psi_2(e)$ for any $e \in E_1 \cap E_2$. Applying the inductive hypothesis to the subcircuits S_i and using distributivity we obtain the required inclusion

$$\begin{aligned}\operatorname{mon} f = \varphi(e') = \varphi(e'_1) \vee \varphi(e'_2) &\subset \Big(\bigvee_{e\in E_1} \varphi(e) \times \Psi_1(e)\Big) \vee \Big(\bigvee_{e\in E_2} \varphi(e) \times \Psi_2(e)\Big) \\ &= \Big(\bigvee_{e\in E_1\setminus E_2} \varphi(e) \times \Psi_1(e)\Big) \vee \Big(\bigvee_{e\in E_2\setminus E_1} \varphi(e) \times \Psi_2(e)\Big) \\ &\quad \vee \Big(\bigvee_{e\in E_1\cap E_2} \varphi(e) \times (\Psi_1(e) \vee \Psi_2(e))\Big) = \bigvee_{e\in E} \varphi(e) \times \Psi(e).\end{aligned}$$

It remains to consider the case when e' is a product gate. Then $\operatorname{mon} f = \varphi(e') = \varphi(e'_1) \times \psi(e')$, where e'_1 is the only gate connected with e' by an unforbidden edge. Let S_1 denote the circuit obtained from S by eliminating the gate e' and specifying the output gate e'_1.

Any path C in the circuit S that connects an internal gate with the gate e' can be obtained by adding the gate e' to some path C' that lies in the subcircuit S_1 and ends with the gate e'_1. Since $\Psi(C) = \Psi(C') \times \psi(e')$, we apply the inductive hypothesis to the subcircuit S_1 and use the distributive property to obtain the relation $\Psi(e) = \Psi_1(e) \times \psi(e')$ for any $e \in E$ (where $\Psi_1(e)$ is defined in the same way as in the previous case). This gives the required inclusion

$$\begin{aligned}\operatorname{mon} f = \varphi(e') = \varphi(e'_1) \times \psi(e') &\subset \Big(\bigvee_{e\in E} \varphi(e) \times \Psi_1(e)\Big) \times \psi(e') \\ &= \bigvee_{e\in E} \varphi(e) \times \Psi_1(e) \times \psi(e') = \bigvee_{e\in E} \varphi(e) \times \Psi(e).\end{aligned}$$

The proof of the lemma is complete.

Lemma 4. *Let the product gate e in the circuit S implement a (k, l)-thin subset* $\operatorname{mon} f$ *of the set N^n. Then the weight of one of the predecessors of the gate e is less than l.*

Proof. Suppose the contrary. Then $\varphi(e) = \varphi_1 \times \varphi_2$, where $|\varphi_i| \geqslant l$. Consider a cut of the circuit that contains the gate e (it may be added to any cut). Applying the result

of the previous lemma to this cut we derive the inclusion $\operatorname{mon} f \supset \varphi(e) \times \Psi(e) = \varphi_1 \times (\varphi_2 \times \Psi(e))$. But $|\varphi_2 \times \Psi(e)| \geqslant |\varphi_2| \geqslant l$, contradicting the assumption that the set $\operatorname{mon} f$ is (k, l)-thin.

In deriving these relations we have used the associativity of multiplication and the inequality $|A \times B| \geqslant \max\{|A|, |B|\}$, which follows from the inclusions $\{a\} \times B \subset A \times B$ and $A \times \{b\} \subset A \times B$, where $a \in A$ and $b \in B$, which are obvious (in fact, a stronger inequality $|A \times B| \geqslant |A| + |B| - 1$ is valid). The proof of the lemma is complete.

From now on we will assume that for each product gate in the circuit S the forbidden edge is chosen to come out of a predecessor whose weight is less than l. With this convention we may assume that for any product gate e the estimate $|\psi(e)| < l$ is satisfied. Otherwise we may replace each product gate e with a single-input gate that implements multiplication by $\psi(e)$.

On every path of the circuit S that goes from the input to the output of this circuit, consider the OR gate having weight at least l and located closest to the input (if there is such a gate) together with its preceding gate (or constant) along this path. Denote the set of the distinguished OR gates by $V = \{v_1, \ldots, v_m\}$, and the set of their direct predecessors by $U = \{u_1, \ldots, u_t\}$ (it may happen that $m = 0$).

The case $m = 0$ means that there are no OR gates in the circuit S whose weights are higher than $l - 1$. We will show that in this case the theorem holds. In such a circuit any path that joins a constant with the output of the circuit ends up with a (possibly empty) series of product gates preceded by a constant or an OR gate of weight less than l. Therefore, such a circuit implements a set of the form $A_1 \times \cdots \times A_p$, where $|A_i| < l$ for all i. Consequently, $|\operatorname{mon} f| \leqslant h$ (by the definition of h), and under this condition the statement of the theorem is satisfied.

From now on we shall assume that $m > 0$.

Lemma 5. *The sets V and U are cuts of the circuit S.*

Proof. We will show that V is a cut. Suppose that some path C does not go through elements of V, which means that it contains no OR gates of weight higher than $l - 1$. Consider an arbitrary path C' that meets V. The paths C and C' share a common gate e', the output of the circuit, and consequently they have a common subpath C'' which ends up at the gate e'. Let e be the first node of this subpath counted from the inputs.

The elements of the set $V \cap C'$ do not occur in the subpath C''; hence, they appear along the path C' before the gate e, which implies that the weight of e is less than l. Since $e \in C$, it cannot be an OR gate. Then e is a product gate. However, a product gate has a single input and then its direct predecessor also lies on $C \cap C'$, which contradicts the choice of e as the first gate on the common subpath of C and C'.

We have shown above that any path in the circuit contains an element of the set V. Consequently, by construction, it also contains an element (or constant) of the set U. The proof of the lemma is complete.

Now we will transform the circuit S as follows. Replace each gate u_i with the corresponding constant that implements $\varphi(u_i)$; this constant will also be denoted by u_i. Then eliminate from the circuit all the edges that enter into the gates u_i.

If all the edges issuing from some gate are eliminated, then we remove this gate together with all the edges that enter into it, and so on.

After this transformation, the set implemented by the circuit remains unchanged and neither the number of OR gates, nor the number of all other types of gates, has increased. We shall denote the resulting circuit by $\widehat{S}$.

Now we define a matrix $(\beta_{i,j})$ in the following way: we set $\beta_{i,j} = 1$ if and only if the edge (u_i, v_j) occurs in $\widehat{S}$, and $\beta_{i,j} = 0$ otherwise.

Lemma 6. *The following relation holds*:

$$\operatorname{mon} f = \bigvee_{\substack{i,j \\ \beta_{i,j}=1}} \varphi(u_i) \times \Psi(v_j).$$

Proof. It follows from Lemma 5 that the set $U \cap \widehat{S}$ is a cut of the circuit $\widehat{S}$. Applying Lemma 3 and the definition of the function $\Psi(e)$ to $\widehat{S}$, we obtain

$$\operatorname{mon} f = \bigvee_{i=1}^{t} \varphi(u_i) \times \Psi(u_i) = \bigvee_{\substack{i,C \\ u_i \in C}} \varphi(u_i) \times \Psi(C),$$

where $\{C\}$ denotes the set of paths going from the outputs of constants u_j to the output of the circuit $\widehat{S}$ (if $u_i \notin \widehat{S}$, then we set $\Psi(u_i) = \varnothing$). Let C be an arbitrary path of this kind issued from constant u_i.

Let us show that the gate that follows u_i in this path belongs to V. First, we shall prove that $V \cap \widehat{S}$ is a cut of the circuit $\widehat{S}$, which means that the path C contains an element of V which is different from u_i. Suppose the contrary. It follows from the definition of u_i that there is a subpath C'' in S that joins some input of the circuit with the gate u_i and contains no elements of V. Consider the subpath C' in S obtained by extending the subpath C'' with the help of the path C. It follows from the definition of the set V that $C' \cap V \neq \varnothing$. However, in this case we have $(C \setminus \{u_i\}) \cap V \neq \varnothing$, which contradicts our assumption. Hence, $V \cap \widehat{S}$ is a cut of the circuit $\widehat{S}$.

If the gate u_i is not followed by an element of V on the path C, then u_i is the direct predecessor of some gate u_j, which contradicts the condition that in the circuit $\widehat{S}$ all the elements of U are constants. Thus, all edges belonging to $U \cap \widehat{S}$ have their heads in V.

Let u_i and v_j be the first elements of the path C; denote the rest of the path by C'. Then $\Psi(C) = \Psi(C')$ and as the set $\Psi(v_j)$ is the disjunction of all possible $\Psi(C')$, $v_j \in C'$, we obtain the equality

$$\operatorname{mon} f = \bigvee_{\substack{i,C \\ u_i \in C}} \varphi(u_i) \times \Psi(C) = \bigvee_{\substack{i,C' \\ \{u_i\} \cup C' \text{ is a path}}} \varphi(u_i) \times \Psi(C') = \bigvee_{\substack{i,j \\ \beta_{i,j}=1}} \varphi(u_i) \times \Psi(v_j).$$

The proof of the lemma is complete.

Lemma 7. *The following relation holds*: $\sum_{i,j} \beta_{i,j} \geqslant h^{-1} |\operatorname{mon} f|$.

Proof. It follows from

$$|\varphi(v_j)| \geqslant l, \qquad \varphi(v_j) \times \Psi(v_j) \subset \operatorname{mon} f,$$

that $|\Psi(v_j)| < k$ for all j. Otherwise the set $\operatorname{mon} f$ would not be (k, l)-thin.

Now we will verify that any set $\varphi(u_i)$, where $u_i \in U$, can be represented in the form $B_1 \times \cdots \times B_p$, where $|B_j| < l$, $B_j \subset N^n$ for any j. According to the definition of U, there exists a path in which the gate (or constant) u_i is not preceded by the OR gates having weight higher than $l - 1$. Then the set $\varphi(u_i)$, which is computed by the subpath ending up at u_i, admits the required representation.

Using Lemma 1, from the facts established above we obtain the estimate $|\varphi(u_i) \times \Psi(v_j)| \leqslant h$, and now the inequality in the proof follows directly from Lemma 6. The proof of the lemma is complete.

We again consider the circuit $\widehat{S}$ and show that the number of OR gates in this circuit is not less than $\sum_{i,j} \beta_{i,j} - 1$.

We denote the number of gates which have exactly i incoming edges by r_i, $i = 1, 2$, and count up the total number of edges in this circuit in two ways. On the one hand, this number equals $r_1 + 2r_2$ (the total number of incoming edges), on the other hand, it is not less than $r_1 + r_2 + \sum_{i,j} \beta_{i,j} - 1$ (the total number of outgoing edges). Consequently, $r_2 \geqslant \sum_{i,j} \beta_{i,j} - 1$ (in fact, we are using known arguments, which can be found in [2], for example). Finally we obtain

$$\sum_{i,j} \beta_{i,j} - 1 \leqslant r_2 \leqslant L_\vee(\widehat{S}) \leqslant L_\vee(S),$$

which, with Lemmas 2 and 7 proves inequality (i) of the theorem.

To prove item (ii) of the theorem, on every path of the circuit S we distinguish the gate $v_i \in V$ which is closest to the circuit inputs. Also, distinguish the single-input gate that precedes v_i and is closest to it along this path (or the constant from which this path emanates, if v_i has no single-input predecessors) and the closest single-input gate that succeeds v_i (or the circuit output, if v_i has no single-input successors). Denote the set of all distinguished predecessors by $W = \{w_1, \ldots, w_{p'}\}$ and the set of distinguished successors by $Z = \{z_1, \ldots, z_{q'}\}$. If the output e' of the circuit S is contained in Z, then we set $\psi(e') = \{(0, \ldots, 0)\}$.

Let us change all elements of W to constants using the same arguments as we used when constructing the circuit $\widehat{S}$, and denote the resulting circuit by $\breve{S}$.

Lemma 8. *There exists a Boolean matrix $(\mu_{i,j})$ such that*

$$\operatorname{mon} f = \bigvee_{\substack{i,j \\ \mu_{i,j}=1}} \varphi(w_i) \times \psi(z_j) \times \Psi(z_j).$$

Moreover, $\mu_{i,j} = 0$ if $w_i \notin \breve{S}$ or $z_j \notin \breve{S}$.

Proof. The set $W \cap \breve{S}$ is a cut of the circuit $\breve{S}$ since it contains all the inputs. Therefore, by Lemma 3 we have

$$\operatorname{mon} f = \bigvee_{\substack{i,C \\ w_i \in C}} \varphi(w_i) \times \Psi(C),$$

where $\{C\}$ denotes the set of paths that connect constants w_i with the output of the circuit $\breve{S}$. The sets $V \cap \breve{S}$ and $Z \cap \breve{S}$ are also cuts of circuit $\breve{S}$ — this can be demonstrated in the same way as in Lemma 6.

We will show that $W \cap Z \cap \breve{S} = \varnothing$. Suppose the contrary, that is, assume that there exists an element $w_i = z_j \in \breve{S}$. Obviously, such an element cannot be a constant of the circuit S; nor can it be an OR gate. Then it is a single-input gate and in any path that connects the input and the output of circuit S, this gate is preceded by the same element e. Since there is a path in which z_j is preceded by an OR gate with weight at least l, we have $|\varphi(e)| \geqslant l$. Now if e is a product gate, then z_j cannot belong to Z, whereas if e is an OR gate, then w_i cannot belong to W, which contradicts our assumption.

The above arguments also imply that a product gate belonging to the set Z is necessarily preceded by an OR gate with weight at least l.

Consider an arbitrary path C starting at constant w_i. By the construction of circuit $\breve{S}$, the path C contains no elements of W other than w_i. Let z_j be the element of the set Z on the path C that is closest to the circuit input. We will show that the path segment C'' between w_i and z_j contains no other single-input gates.

First, this segment necessarily contains an OR gate with weight at least l. If the element z_j itself is not an OR gate (that is, the output of the circuit), then this follows from the above remark about the direct predecessor of a single-input element of Z. Let v be the OR gate which is closest to w_i. Then, in accordance with the definition of w_i, the element v is the closest to the input OR gate having weight at least l in some path of S that contains C'' as a subpath (that is, $v \in V$). Then the existence of a single-input gate in C'' that differs from w_i and z_j would immediately imply that the subpath C'' contains either an element of W other than w_i, or an element of Z other than z_j. This, in turn, disagrees with the definition of the circuit $\breve{S}$ or with the choice of the element z_j, respectively.

Thus, the only elements that can occur between w_i and z_j are OR gates.

Consider the subpath C' of C which connects the element z_j with the circuit output. According to the definition of Ψ, we have $\Psi(C) = \psi(z_j) \times \Psi(C')$. As a consequence, any path C' that joins the element z_j with the circuit output may be extended to some path C that joins the element w_i with the circuit output and satisfies the condition $\Psi(C) = \psi(z_j) \times \Psi(C')$. Therefore,

$$\psi(z_j) \times \Psi(z_j) = \bigvee_{C'} \psi(z_j) \times \Psi(C') = \bigvee_{\substack{C \\ w_i, z_j \in C}} \Psi(C),$$

where the first disjunction involves all subpaths $\{C'\}$ starting from z_j. This means that there exists a Boolean matrix $(\mu_{i,j})$ such that

$$\operatorname{mon} f = \bigvee_{\substack{i,C \\ w_i \in C}} \varphi(w_i) \times \Psi(C) = \bigvee_{\substack{i,j \\ \mu_{i,j}=1}} \varphi(w_i) \times \psi(z_j) \times \Psi(z_j).$$

Here, by construction, the last disjunction involves only pairs of elements w_i and z_j in $\breve{S}$. The proof of the lemma is complete.

Lemma 9. *The following relation holds*: $\sum_{i,j} \mu_{i,j} \geqslant h^{-1}|\operatorname{mon} f|$.

Proof. As in the proof of Lemma 7, it is sufficient to show that any set $\varphi(w_i) \times \psi(z_j) \times \Psi(z_j)$ can be represented as a product of sets each having weight less than l. Once we have established this the required inequality follows directly from Lemmas 1 and 8.

It is evident that $|\psi(z_j)| < l$. Moreover, since $|\varphi(z_j)| \geqslant l$ and $\varphi(z_j) \times \Psi(z_j) \subset \operatorname{mon} f$, we have $|\Psi(z_j)| < k \leqslant l$. Finally, the set $\varphi(w_i)$ is calculated by a certain path which contains no OR gates of weight higher than $l-1$. Hence, the set $\varphi(w_i)$ and, consequently, the set $\varphi(w_i) \times \psi(z_j) \times \Psi(z_j)$ has the required form. The proof of the lemma is complete.

Let $|W \cap \breve{S}| = p$ and $|Z \cap \breve{S}| = q$. Then, since all the elements of $W \cup Z$ apart from, perhaps, $n+2$ elements, are single-input elements, and since $W \cap Z \cap \breve{S} = \varnothing$ (this was proved in Lemma 8), we have

$$L_{\times}(\breve{S}) \geqslant p + q - n - 2.$$

Using the inequalities $p + q \geqslant 2\sqrt{pq}$ and $pq \geqslant \sum_{i,j} \mu_{i,j}$, we obtain

$$L_{\times}(S) \geqslant L_{\times}(\breve{S}) \geqslant p + q - n - 2 \geqslant 2\sqrt{\sum_{i,j} \mu_{i,j}} - n - 2.$$

With Lemmas 2 and 9 this estimate yields inequality (ii) of the theorem.

Now we will establish inequality (iii), which improves inequality (ii) in the asymptotic sense. For the sake of convenience we shall remove from the sets W and Z all the elements that correspond to zero rows and zero columns of the matrix $(\mu_{i,j})$. We will also remove all the zero rows and columns from $(\mu_{i,j})$ again denoting the resulting matrix by $(\mu_{i,j})$. The statement of Lemma 8 remains valid for the modified sets (with an appropriate rearrangement of the indices) and matrix.

Now we assume that $(\mu_{i,j})$ has the least size (the number of rows and the number of columns) among all matrices for which Lemma 8 holds true.

Then none of the sets $\varphi(w_i)$ can be represented as a disjunction of some other sets $\varphi(w_j)$, $j \neq i$, and the same is true of the sets $\psi(z_i) \times \Psi(z_i)$. Indeed if, for instance, the set $\varphi(w_i)$ were represented in the form $\bigvee_{j \in J} \varphi(w_j)$, $i \notin J$, then replacing all occurrences of $\varphi(w_i)$ in the statement of Lemma 8 with $\bigvee_{j \in J} \varphi(w_j)$, making the corresponding transformations, and removing w_i from the set W, we would obtain a similar formula with a new matrix $(\mu'_{i,j})$ having fewer rows.

A Boolean matrix will be called (k,l)-thin if it contains no $(k \times l)$-submatrix whose entries are all 1.

Lemma 10. *Matrix* $(\mu_{i,j})$ *is* $(\alpha(k), \alpha(l))$*-thin and* $(\alpha(l), \alpha(k))$*-thin.*

Proof. Suppose, for example, that $(\mu_{i,j})$ is not $(\alpha(k), \alpha(l))$-thin. Then according to Lemma 8, there exist an $\alpha(k)$-element set I and an $\alpha(l)$-element set J which satisfy the inclusion

$$\left(\bigvee_{i \in I} \varphi(w_i)\right) \times \left(\bigvee_{j \in J} \psi(z_j) \times \psi(Z_j)\right) \subset \operatorname{mon} f.$$

Now if $|\bigvee_{i\in I}\varphi(w_i)| < k$, then in a certain $(k-1)$-element set there is a system of $\alpha(k)$ distinct nonempty subsets none of which can be represented as a disjunction of two other subsets (in fact, any assembly of other subsets). Adding the empty set to it, we obtain a system of $\alpha(k)+1$ subsets with the same property, which contradicts the definition of $\alpha(k)$. Therefore, $|\bigvee_{i\in I}\varphi(w_i)| \geqslant k$ and similarly $|\bigvee_{j\in J}\psi(z_j)\times\psi(Z_j)| \geqslant l$. However, this contradicts the (k,l)-thinness of the set $\operatorname{mon} f$.

The fact that $(\mu_{i,j})$ is $(\alpha(l),\alpha(k))$-thin is verified in the same way. The proof of the lemma is complete.

The following lemma is an immediate corollary of the estimate for the weight of a thin Boolean matrix in [53], where Nikiforov improved the corresponding estimate proposed in [54]. In what follows the number of 1s in a Boolean matrix is referred to as its *weight*.

Lemma 11. *Let $\alpha \leqslant \beta$. Then the weight of an (α,β)-thin and (β,α)-thin Boolean $(p\times q)$-matrix A does not exceed*

$$(\beta-\alpha+1)^{1/\alpha}\left(\frac{p+q}{2}\right)^{2-1/\alpha} + (\alpha-1)\left(\frac{p+q}{2}\right)^{2-2/\alpha} + (\alpha-2)\frac{p+q}{2}.$$

Proof. The upper estimate [53] for the weight of a (β,α)-thin $(p\times q)$-matrix A has the form

$$(\beta-\alpha+1)^{1/\alpha}p^{1-1/\alpha}q + (\alpha-1)p^{2-2/\alpha} + (\alpha-2)p.$$

We write down a similar estimate for the weight of its transpose (which is (β,α)-thin as well) and consider the arithmetic mean of both estimates. Using the known inequalities

$$pq \leqslant \left(\frac{p+q}{2}\right)^2, \qquad \frac{p^{1/\alpha}+q^{1/\alpha}}{2} \leqslant \left(\frac{p+q}{2}\right)^{1/\alpha},$$

which imply the relations

$$\begin{aligned}\frac{p^{1-1/\alpha}q + q^{1-1/\alpha}p}{2} &= \frac{pq}{2}\left(\frac{1}{p^{1/\alpha}}+\frac{1}{q^{1/\alpha}}\right) \leqslant \frac{pq}{2}\left(\frac{1}{p}+\frac{1}{q}\right)^{1/\alpha}\\ &= (pq)^{1-1/\alpha}\left(\frac{p+q}{2}\right)^{1/\alpha} \leqslant \left(\frac{p+q}{2}\right)^{2-1/\alpha},\end{aligned}$$

we finally establish the desired bound. The proof of the lemma is complete.

Together with Lemma 9 the last two lemmas yield the estimate

$$\begin{aligned}h^{-1}|\operatorname{mon} f| \leqslant{}& (\alpha(l)-\alpha(k)+1)^{1/\alpha(k)}\left(\frac{p+q}{2}\right)^{2-1/\alpha(k)}\\ &+ (\alpha(k)-1)\left(\frac{p+q}{2}\right)^{2-2/\alpha(k)} + (\alpha(k)-2)\frac{p+q}{2},\end{aligned}$$

which implies that

$$p+q \geqslant 2(D - aD^{(2\alpha(k)-2)/(2\alpha(k)-1)} - bD^{\alpha(k)/(2\alpha(k)-1)})^{\alpha(k)/(2\alpha(k)-1)}, \qquad (1)$$

where

$$D = \frac{|\operatorname{mon} f|}{h(\alpha(l)-\alpha(k)+1)^{1/\alpha(k)}},$$
$$a = \frac{\alpha(k)-1}{(\alpha(l)-\alpha(k)+1)^{1/\alpha(k)}}, \qquad b = \frac{\alpha(k)-2}{(\alpha(l)-\alpha(k)+1)^{1/\alpha(k)}},$$

if the expression in the parentheses in (1) is positive; this in turn is guaranteed by the condition in item (iii): it can be assumed that for a sufficiently large D we have $D > (a+b) \times D^{(2\alpha(k)-2)/(2\alpha(k)-1)}$. Now the inequality in item (iii) follows from the estimate $L_{\times}(f) \geqslant p+q-n-2$. The proof of the theorem is complete.

Remark 1. It also follows from the proof that $\alpha(k)$ in estimate (iii) can be replaced by the function $\alpha^*(k)$, which is defined in the same way as $\alpha(k)$ with the difference that now disjunctions not only of pairs but of any assemblies of other vectors are disallowed. However, this yields no essential improvement of the estimates, since it follows from Kleitman's result that $\alpha^*(k) \sim \alpha(k)$, and in addition, $\alpha^*(k) = \alpha(k)$ for $k \leqslant 4$.

Remark 2. In the particular case $k = 2$ the bound in item (iii) implies that $L_{\times}(f) = \Omega_l(|\operatorname{mon} f|^{2/3})$ and, if $k = 3$, that $L_{\times}(f) = \Omega_l(|\operatorname{mon} f|^{3/5})$. Below we show in Theorem 6 that none of these estimates can be improved in order.

§ 4. Additive complexity of the permanent

We set

$$\operatorname{per}_n = \sum_{\pi \in S_n} x_{1,\pi(1)} \cdots x_{n,\pi(n)},$$

where S_n is the set of all permutations of $\{1, \ldots, n\}$.

Lemma 12. *Let $f = \operatorname{per}_n$. Then for any $m = 0, \ldots, \lceil n/2 \rceil - 1$ the set $\operatorname{mon} f$ is $(m!+1, (n-m-1)!+1)$-thin.*

Proof. Suppose that $A \times B \subset \operatorname{mon} f$. Denote the set of indices of all nonzero rows in matrices in A by R_A, and the set of indices of nonzero columns by C_A. We shall denote the same sets of rows and columns in matrices in B by R_B and C_B.

It is clear that the entries of a matrix in $A \cup B$ can only be zeros and ones. It is also evident that any row or column of such a matrix has at most one entry that is one. Therefore, each matrix in A (in B) contains at most $\min\{|R_A|, |C_A|\}$ (at most $\min\{|R_B|, |C_B|\}$, respectively) ones.

We will verify that $R_A \cap R_B = \varnothing = C_A \cap C_B$. If, for instance, $R_A \cap R_B \neq \varnothing$, then the sets A and B contain matrices which have a one in the same rows and then the sum of such matrices contains either a two or more than one entry of 1 in the corresponding row; hence, the sum of these matrices does not belong to $\operatorname{mon} f$.

Now we observe that the total number of ones in any two matrices belonging to A and B equals n. Thus, we have $|R_A| + |R_B| = |C_A| + |C_B| = n$, where $|R_A| = |C_A| = k$ and $|R_B| = |C_B| = n-k$. Consequently, any matrix in A has exactly k ones, which are arranged one in each row of R_A and one in each column of C_A. Therefore, $|A| \leqslant k!$. Similarly, we have $|B| \leqslant (n-k)!$.

As a result, we see that there is no value of $m = 0, \dots, n$ for which the inequalities $|A| > m!$ and $|B| > (n-1-m)!$ can hold simultaneously. The proof of the lemma is complete.

Theorem 2. *The additive complexity of the permanent obeys the bound*

$$L_+(\operatorname{per}_n) \geqslant \frac{n!}{(\lfloor n/2 \rfloor !)^2} - 1.$$

Proof. We will show that the quantity h in the statement of Theorem 1 satisfies the inequality $h \leqslant (\lfloor n/2 \rfloor !)^2$.

By Lemma 12 in the definition of h it can be assumed that $l = \lfloor n/2 \rfloor ! + 1$. Let $A_1 \times \dots \times A_p \subset \operatorname{mon} f$, $|A_i| \leqslant \lfloor n/2 \rfloor !$ for all $i = 1, \dots, p$, and each set A_i consists of $n \times n$ Boolean matrices.

Repeating the arguments in the proof of Lemma 12, we find that each of the Boolean matrices in A_i has exactly k_i ones. These entries are arranged one in each row determined by the index set R_i and one in each column determined by the index set C_i. At the same time,

$$|R_i| = |C_i| = k_i, \qquad \sum_{i=1}^{p} k_i = n, \qquad \bigcup_{i=1}^{p} R_i = \bigcup_{i=1}^{p} C_i = \{1, \dots, n\}, \qquad |A_i| \leqslant k_i! \,.$$

Without loss of generality we can assume that $k_1 \geqslant k_i \geqslant 1$ for all i. For $p = 2$ the inequality $|A_1 \times \dots \times A_p| \leqslant (\lfloor n/2 \rfloor !)^2$ is obvious; thus, below we assume that $p \geqslant 3$.

If $k_1 \geqslant \lfloor n/2 \rfloor$, then

$$|A_1 \times \dots \times A_p| \leqslant |A_1| \cdot k_2! \cdots k_p! \leqslant \left\lfloor \frac{n}{2} \right\rfloor ! \, (n - k_1 - 1)! \leqslant \left(\left\lfloor \frac{n}{2} \right\rfloor ! \right)^2.$$

In deriving this estimate we have used the inequality $k! \, (n-k)! \leqslant (n-1)!$, which holds for $0 < k < n$ and, in turn, implies that $k_2! \cdots k_p! \leqslant (k_2 + \dots + k_p - 1)! = (n - k_1 - 1)!$.

If $k_1 < \lfloor n/2 \rfloor$, then we apply the inequality $x! \, y! \leqslant (x-1)! \, (y+1)!$, which is valid for $x \leqslant y$, and obtain

$$|A_1 \times \dots \times A_p| \leqslant k_1! \cdots k_p! \leqslant \left\lfloor \frac{n}{2} \right\rfloor ! \cdot k_2'! \cdots k_s'!,$$

where $1 \leqslant k_i' \leqslant \lfloor n/2 \rfloor$, $s \leqslant p$, $\sum_{i=1}^{s} k_i' = \lceil n/2 \rceil$. This also gives the required estimate. The proof of the theorem is complete.

Thus, for odd n we have $L_+(\operatorname{per}_n) \geqslant n C_{n-1}^{(n-1)/2} - 1 \asymp \sqrt{n} 2^n$. Since the complexity of the permanent of order n is clearly no less than that of the permanent of order $n-1$, for even n we have an estimate of the same order. As is known (see, for instance, [14], exercises to Section 4.6.4), $L_+(\operatorname{per}_n) = O(n 2^n)$. Hence, the estimate obtained is almost sharp.

At the same time, the estimate for $L_\times(\operatorname{per}_n)$ obtained by the method suggested in Theorem 1 is much lower than the actual value of $L_\times(\operatorname{per}_n) \sim n 2^{n-1}$, which was established in [30].

As a corollary, we obtain the estimate $L_+(HC_n) = \Omega(2^n/\sqrt{n})$ for the additive complexity of the Hamiltonian HC_n, since $\operatorname{mon} HC_n \subset \operatorname{mon} \operatorname{per}_n$ and $|\operatorname{mon} HC_n| = (n-1)!$.

§ 5. Examples of thin sets

To show how Theorem 1 can be applied to derive high lower estimates for the monotone complexity of individual polynomials, we shall need effective examples of thin sets of sufficiently large cardinality. Set $E_n = \{0, \dots, n-1\}$.

We noted earlier that in an Abelian group the notion of a 2-thin subset coincides with that of a Sidon set.

A survey of the known approaches to constructing Sidon sets and of the bounds for their cardinality is given in [52] and the works cited there. For our purposes the following facts are important: the cardinality of a Sidon set in E_n and in the group $\mathbb{Z}_n$ is asymptotically no greater than $\sqrt{n}$. This bound is sharp in the first case for all (sufficiently large) n; in the second case — for some values of n. We give some well-known examples.

a) Singer's set of cardinality $q+1$ in $\mathbb{Z}_{q^2+q+1}$, where q is a prime power, is defined as

$$\{0\} \cup \{s_i \mid \theta^{s_i}/(\theta + \alpha_i) \in GF(q),\ GF(q) = \{\alpha_1, \dots, \alpha_q\}\},$$

where the notation $GF(q)$ is used for the Galois field of order q, θ is a primitive element of the field $GF(q^3)$. See [55] for details.

b) Bose's set of cardinality q in $\mathbb{Z}_{q^2-1}$, where q is a prime power, is defined as $\{s_i \mid \theta^{s_i} = \theta + \alpha_i,\ GF(q) = \{\alpha_1, \dots, \alpha_q\}\}$, where θ is a primitive element of the field $GF(q^2)$.

c) Alekseev's set [56] of cardinality $p-1$ in $\mathbb{Z}_{p(p-1)}$, where p is prime, is defined as $\{s_i \mid s_i \equiv i \mod (p-1),\ s_i \equiv \zeta^i \mod p\}$, where ζ is a generator of the multiplicative group of the field $GF(p)$.

Any of the sets in the above examples can be transformed into a Sidon set of cardinality $(1-o(1))\sqrt{n}$ in E_n. This is due, first, to the fact that a thin subset in $\mathbb{Z}_Q$ must also be thin in E_Q (in the sense of the natural one-to-one homomorphism from E_Q to $\mathbb{Z}_Q$). Second, if $Q_R(m)$ denotes the largest number not greater than m of the form $R(p)$, where R is a given polynomial and p is prime, then it is known that $Q_R(m) \sim m$ as $m \to \infty$ (this follows from the results on the density of the distribution of prime numbers, see, for instance, [57]).

Some more examples of thin subsets are given by the following theorem.

Let ψ_n denotes the following (quite natural) mapping from $GF(2^n)$ to N^n. We will represent $GF(2^n)$ as a vector space of dimension n over $GF(2)$. Then ψ_n maps vectors over $GF(2)$ to vectors over N so that zeros go to zeros and ones to ones.

Theorem 3. (i.a) *In the group* $(GF(q)^2, +)$, *where* q *is odd, the parabola*

$$\{(x, x^2) \mid x \in GF(q)\}$$

is a 2*-thin subset of cardinality* q.

(i.b) *In the semigroup* $(N^{2n}, +)$ *the 'cubic parabola'*

$$\{(\psi_n(x), \psi_n(x^3)) \mid x \in GF(2^n)\}$$

is a 2*-thin subset of cardinality* 2^n.

(ii.a) *In the group* $(GF(q)^3, +)$, *where* q *is odd, the sphere*

$$\{(x, y, z) \mid x^2 + y^2 + z^2 = \gamma\},$$

where $-\gamma$ *is a quadratic nonresidue in* $GF(q)$, *is a* 3*-thin subset of cardinality* $q^2 - q$.

(ii.b) *In the group* $(GF(q)^3, +)$, *where* $q = 2^{2k+1}$, *the surface*

$$\{(x, y, z) \mid x^3 + y^7 + z^{15} = 1\}$$

is a $(47, 315)$*-thin subset of cardinality* q^2.

(iii) *In the group* $(GF(q^t), +)$ *the set* $\{x \mid x^{(q^t-1)/(q-1)} = 1\}$ *of elements with unit norm is a* $(t, t! + 1)$*-thin subset of cardinality* $(q^t - 1)/(q - 1)$.

Proof. First we prove item (i.a). We need to verify that the nonzero differences of two-dimensional vectors over $GF(q)$ being equal:

$$(x, x^2) - (y, y^2) = (z, z^2) - (u, u^2) \neq (0, 0)$$

implies that $x = z$ and $y = u$. Indeed, the system of equations

$$\begin{cases} x - y = a, \\ x^2 - y^2 = b \end{cases}$$

over this field for $a \neq 0$ is equivalent to the system

$$\begin{cases} x - y = a, \\ x + y = \dfrac{b}{a}, \end{cases}$$

which has a unique solution.

Thus, the parabola under consideration is a semi-difference and, hence, a 2-thin subset in $GF(q)^2$.

The example considered in item (i.b) was suggested in [39], [40] (overall the proof is similar to that of item (i.a)).

The statement of item (ii.a) was actually proved by Brown [58] for the case of a prime number q. To be precise, he showed that the intersection of any three distinct spheres $S(a, b, c) = \{(x, y, z) \mid (x - a)^2 + (y - b)^2 + (z - c)^2 = \gamma\}$ consists of at most two points. However, his reasoning applies to the general case as well.

So, assume that the sphere $S(0, 0, 0)$ is not a 3-thin subset, that is, $A + B \subset S(0, 0, 0)$, where $|A| = |B| = 3$. Then, as any sphere $S(a, b, c)$ can be represented in the form $\{(a, b, c)\} + S(0, 0, 0)$, we can deduce that the set B of cardinality 3 is contained in each of the spheres $S(a, b, c)$, where $(-a, -b, -c) \in A$, which contradicts Brown's result.

The fact that the cardinality of $S(0, 0, 0)$ is equal to $q^2 - q$ follows, for instance, from the statement of problem 14 in [59], Algebraic Supplement, § 3.

The example considered in item (ii.b) was presented in [43]. We omit its proof because it is complicated.

The statement of item (iii) follows directly from results in [50], where it is shown that any t distinct sets

$$N(a) = \{x \mid (x-a)^{(q^t-1)/(q-1)} = 1\}$$

intersect in at most $t!$ points and conversely, any $t!+1$ such sets have at most $t-1$ common points. Now the fact that the set $N(0)$ is $(t, t!+1)$-thin is established by the same arguments as in item (ii). The proof of the theorem is complete.

Theorem 3 provides examples of thin sets of large cardinality in multidimensional vector spaces. We will now give a method for transforming such sets into ('one-dimensional') thin sets of numbers. We shall need

Lemma 13. *Set* $N_{q,t} = \{\sum_{i=0}^{t-1} a_i(2q-1)^i \mid a_i \in E_q t\}$ *and let* $A, B \subset N$ *and* $A \times B \subset N_{q,t}$. *Then there exist one-to-one mappings* $\xi_A \colon A \to N_{q,t}$ *and* $\xi_B \colon B \to N_{q,t}$ *such that relation* $a + b = \xi_A(a) + \xi_B(b)$ *holds for any* $a \in A$, $b \in B$.

In essence, this lemma claims that if the elements of the Minkowski sum $A \times B$ of two sets of numbers A and B written in the number system of the base $2q-1$ only use 'digits' from 0 to $q-1$, then the elements of the sets may be transformed in such a way that writing them in the indicated number system will also only involve the digits from 0 to $q-1$, while the pairwise sums remain unchanged.

Proof. We shall use induction on t. If $t = 1$, then inevitably $A, B \subset E_q$; thus, we can take ξ_A and ξ_B to be the identity mappings. Before we perform the inductive step we shall conduct an auxiliary discussion.

In the residue ring $\mathbb{Z}_m = \{\overline{0}, \ldots, \overline{m-1}\}$ we introduce the concept of a *segment* $[\overline{a}, \overline{b}]$ defined for $a \leqslant b$ as $\{\overline{a}, \overline{a+1}, \ldots, \overline{b}\}$, and for $a > b$ as $\{\overline{a}, \ldots, \overline{m-1}, \overline{0}, \ldots, \overline{b}\}$. The *length* of the segment is defined as $|[\overline{a}, \overline{b}]| - 1$, that is, in the first case it is $b-a$ and in the second case it is $b+m-a$. For any subset $M \subset \mathbb{Z}_m$ there exists a segment of shortest length (perhaps, not unique) that contains M. Obviously, both ends of this segment must belong to M. The length of the shortest segment containing M will be called the *diameter* of M, denoted by $d(M)$. We note that if $d(M) \leqslant (m-1)/2$, then the shortest segment for M is uniquely defined and is contained in any other segment containing M and having length at most $(m-1)/2$. It is easy to show that

$$\max\{d(M_1), d(M_2)\} \leqslant d(M_1 \times M_2) \leqslant \min\{d(M_1) + d(M_2),\, m-1\}.$$

We will prove the following fact. If $d(M_1 \times M_2) \leqslant (m-1)/2$, then $d(M_1 \times M_2) = d(M_1) + d(M_2)$. Moreover, if $[\overline{a}, \overline{b}]$ and $[\overline{c}, \overline{d}]$ are the shortest segments for the sets M_1 and M_2, respectively, then the shortest segment for the set $M_1 \times M_2$ is

$$\rho = \left[\, \overline{(a+c) \bmod m},\ \overline{(b+d) \bmod m} \,\right]$$

(we recall that under the conditions we have imposed all shortest segments are uniquely defined).

The case where one of the sets has zero diameter is trivial. Therefore, without loss of generality we can assume that $0 < d(M_1) \leqslant d(M_2)$. Since $d(M_2) \leqslant (m-1)/2$, the segment ρ has length $d(M_1) + d(M_2)$ and contains the set $M_1 \times M_2$. Assume that this is not the shortest segment for $M_1 \times M_2$. Since all the residues

$$\overline{(a+c) \bmod m}, \quad \overline{(b+c) \bmod m}, \quad \overline{(a+d) \bmod m}, \quad \overline{(b+d) \bmod m}$$

belong to the set $M_1 \times M_2$, if $d(M_2) > d(M_1)$ any segment containing this set contains one of the segments

$$\rho = \bigl[\,\overline{(a+c) \bmod m}, \overline{(b+d) \bmod m}\,\bigr], \quad \bigl[\,\overline{(b+c) \bmod m}, \overline{(a+c) \bmod m}\,\bigr],$$
$$\bigl[\,\overline{(a+d) \bmod m}, \overline{(b+c) \bmod m}\,\bigr], \quad \bigl[\,\overline{(b+d) \bmod m}, \overline{(a+d) \bmod m}\,\bigr],$$

and for $d(M_1) = d(M_2)$ it contains one of these segments other than the third one.

The second and fourth segments have length $m - d(M_1) > (m-1)/2$, and for $d(M_2) > d(M_1)$ the third segment has length $m - (d(M_2) - d(M_1)) > (m-1)/2$. Consequently, the shortest segment for $M_1 \times M_2$ must include the segment ρ, which contradicts the assumption made above.

Now we shall proceed with the proof of the inductive step of the lemma. Let $t \geqslant 2$ and assume that the statement of the lemma holds for $t-1$ instead of t. Define the set of 'least significant digits' $A_0 = \{\overline{a \bmod (2q-1)} \mid a \in A\}$ and, accordingly, the set B_0. By hypothesis, in the residue ring $\mathbb{Z}_{2q-1}$ we have the inclusion $A_0 \times B_0 \subset [\,\overline{0}, \overline{q-1}\,]$. Let $\rho_A = [\,\overline{l_A}, \overline{r_A}\,]$ and $\rho_B = [\,\overline{l_B}, \overline{r_B}\,]$ be the shortest segments for A_0 and B_0, respectively. Then, by what we proved above,

$$\rho = \bigl[\,\overline{(l_A + l_B) \bmod (2q-1)}, \overline{(r_A + r_B) \bmod (2q-1)}\,\bigr]$$

is the shortest segment for $A_0 \times B_0$. It is clear that $\rho \subset [\,\overline{0}, \overline{q-1}\,]$ (since any segment that contains some subset of $\mathbb{Z}_m$ and has length at most $(m-1)/2$ also includes the shortest segment for this subset).

Now we observe that if $l_A = 0$ or $l_B = 0$, then $r_A, r_B \leqslant q-1$. Indeed, suppose that, for instance, $l_A = 0$. Then $l_B \leqslant q-1$ and $r_A \leqslant q-1$. If we assume that $r_B \geqslant q$, then in the case $l_B \leqslant r_A$ we have

$$d(A_0 \times B_0) = (r_A - l_A) + (r_B - l_B) \geqslant r_B \geqslant q$$

(which contradicts the condition $d(A_0 \times B_0) \leqslant q-1$), and in the case $l_B \geqslant r_A$ we have

$$q \leqslant r_A + r_B = (l_A + l_B) + d(A_0 \times B_0) \leqslant l_B + q - 1 \leqslant 2q - 2$$

(which contradicts the condition $\rho \subset [\,\overline{0}, \overline{q-1}\,]$). Therefore, $r_B \leqslant q-1$.

Further, we note that if $\overline{0} \in (\rho_A \cap \rho_B)$, then $\overline{0} \in \rho$, and consequently $l_A = l_B = 0$. Therefore, if $l_A \neq 0$ and $l_B \neq 0$, then $\overline{0} \notin (\rho_A \cap \rho_B)$; in other words, either $0 < l_A \leqslant r_A$ or $0 < l_B \leqslant r_B$.

Consequently, we either have $l_A \leqslant r_A$ or $l_B \leqslant r_B$. Without loss of generality we will assume that the first inequality is valid — it means that for any $a \in A$ we have $a \geqslant l_A$. We define the mappings ξ'_A and ξ'_B as follows: $\xi'_A(a) = a - l_A$, $\xi'_B(b) = b + l_A$.

It is clear that $\xi'_A(a) + \xi'_B(b) = a + b$. Because $l_{\xi'_A(A)} = 0$ we also have

$$0 \leqslant l_{\xi'_B(B)}, r_{\xi'_A(A)}, r_{\xi'_B(B)} \leqslant q - 1$$

(where $l_{\xi'_A(A)}$ and $r_{\xi'_A(A)}$ are defined in the same way as l_A and r_A). As a consequence, we have $\xi'_A(A), \xi'_B(B) \subset (2q-1)N \times E_q$, which means that an element a of either of the sets $\xi'_A(A), \xi'_B(B)$ can be written as $a = (2q-1)a' + a''$, where $a'' \in E_q$, $a' \in N$. Define the new sets

$$A' = \{a' \mid a = (2q-1)a' + a'' \in \xi'_A(A),\ a'' \in E_q\},$$
$$B' = \{b' \mid b = (2q-1)b' + b'' \in \xi'_B(B),\ b'' \in E_q\}.$$

For any $a' \in A'$ and $b' \in B'$ we have $a' + b' = \lfloor (a+b)/(2q-1) \rfloor$ for some $a \in \xi'_A(A)$ and $b \in \xi'_B(B)$ because $0 \leqslant a'' + b'' \leqslant 2q-2$, where $a'' = a \bmod (2q-1)$ and $b'' = b \bmod (2q-1)$, and there are no carries from least significant digits (in the number system of the base $2q-1$). Therefore, $A' \times B' \subset N_{q,t-1}$. Consequently, by the inductive hypothesis, there exist one-to-one mappings $\xi''_A\colon A' \to N_{q,t-1}$ and $\xi''_B\colon B' \to N_{q,t-1}$ which keep the pairwise sums unchanged.

Finally, we set $\xi_A(a) = (2q-1)\xi''_A(a') + a''$, where $\xi'_A(a) = (2q-1)a' + a''$, $a'' \in E_q$, and define $\xi_B(b)$ similarly. By construction, the mapping ξ_A (ξ_B) consists in adding (subtracting, respectively) some integer constant and is therefore bijective. The proof of the lemma is complete.

Remark 3. The statement of the lemma holds true if the sum of the powers of $2q-1$ in the definition of the set $N_{q,t}$ is replaced with the sum of the powers of an arbitrary number $Q \geqslant 2q-1$.

Consider the mapping $\psi_{q,s,t}$ from E_q^{st} to $E^s_{(2q-1)^t}$ which maps the vector $(a_0, \ldots, a_{st-1})$ to the vector

$$\left(\sum_{i=0}^{t-1} a_i (2q-1)^i,\ \sum_{i=0}^{t-1} a_{t+i} (2q-1)^i, \ldots, \sum_{i=0}^{t-1} a_{(s-1)t+i} (2q-1)^i \right). \tag{2}$$

Theorem 4. *If a subset $M \subset E_q^{st}$ of the semigroup $(N^{st}, +)$ is (k,l)-thin, then the subset $\psi_{q,s,t}(M)$ of the semigroup $(N^s, +)$ is (k,l)-thin as well.*

Proof. We shall denote the set of ith components of the set $A \subset N^s$ by $\mathrm{pr}_i(A)$; namely, $\mathrm{pr}_i(A) = \{a_i \mid (a_0, \ldots, a_{s-1}) \in A\}$. The operator pr_i possesses the obvious property $\mathrm{pr}_i(A \times B) = \mathrm{pr}_i(A) \times \mathrm{pr}_i(B)$.

We will verify that the mapping $\psi_{q,s,t}$ preserves the thinness of a set. Now, by Lemma 13 if some sets $A, B \subset N^s$ are such that the set $A \times B$ is contained in $\psi_{q,s,t}(M)$, then for any $i = 1, \ldots, s$ there is a pair of one-to-one mappings $\xi_{i,A}\colon \mathrm{pr}_i(A) \to N_{q,t}$ and $\xi_{i,B}\colon \mathrm{pr}_i(B) \to N_{q,t}$ such that $\xi_{i,A}(a) + \xi_{i,B}(b) = a + b$ (where $N_{q,t}$ is defined in Lemma 13). Consequently, the vector-valued mappings $\xi_A = (\xi_{0,A}, \ldots, \xi_{s-1,A})$ and $\xi_B = (\xi_{0,B}, \ldots, \xi_{s-1,B})$ establish one-to-one correspondences between the sets A and B and $N^s_{q,t} = \psi_{q,s,t}(E_q^{st})$ and they also have the property $\xi_A(a) + \xi_B(b) = a + b$.

Now, as the mapping $\psi_{q,s,t}^{-1}$ establishes a one-to-one correspondence and keeps the sums unchanged, we conclude that $\psi_{q,s,t}^{-1}(\xi_A(A)) \times \psi_{q,s,t}^{-1}(\xi_B(B)) \subset M$ and futhermore

$$|\psi_{q,s,t}^{-1}(\xi_A(A))| = |\xi_A(A)| = |A|, \qquad |\psi_{q,t}^{-1}(\xi_B(B))| = |\xi_B(B)| = |B|.$$

The proof of the theorem is complete.

We give one more method for constructing thin subsets in Lemma 14 below.

§ 6. Constructing polynomials of high monotone complexity

If we take mon f_1 to be a Sidon set in E_m of cardinality asymptotically equal to $\sqrt{m}$ and apply Theorem 1, (i) and (iii), we shall obtain an example of a monotone univariate polynomial f_1, $\deg f_1 < m$, such that $L_+(f_1) \gtrsim \sqrt{m}$ and $L_\times(f_1) \gtrsim 2\sqrt[3]{m}$.

For $m = d^n$, using the Kronecker substitution $x_i = x^{d^i}$ we transform the above polynomial to a polynomial $\widehat{f_1}$ in n variables of degree at most $d-1$ in each of the variables which clearly satisfies the complexity estimates $L_+(\widehat{f_1}) \gtrsim d^{n/2}$, $L_\times(\widehat{f_1}) \gtrsim 2d^{n/3}$ as $d^n \to \infty$.

Similar bounds for complexity may be derived using the sets defined in item (i) of Theorem 3. Higher bounds may be obtained with the help of item (ii).

Item (ii.a) of Theorem 3 says we can find a 3-thin set mon f_2 in $E_m^3 \subset N^3$ of cardinality asymptotically equal to m^2. Then, for the corresponding polynomial f_2 in three variables of degree at most $m-1$ in each of the variables, Theorem 1, (i) and (iii) provide the complexity estimates $L_+(f_2) \gtrsim (1/8)m^2$, $L_\times(f_2) \gtrsim 2^{-4/5}m^{6/5}$. As a consequence, we can find a polynomial $\widehat{f_2}$ in $3n$ variables of degree at most $d-1$ in each of the variables which obeys the bounds $L_+(\widehat{f_2}) \gtrsim (1/8)d^{2n}$ and $L_\times(\widehat{f_2}) \gtrsim 2^{-4/5}d^{6n/5}$ as $d^n \to \infty$.

These results were obtained in [43], up to multiplicative constants in some of the estimates and the method of derivation. Combining item (iii) of Theorem 3 with Theorem 4 gives a stronger result.

Theorem 5. *Let $m \geqslant 2$ and $n \geqslant 1$. Then a monotone polynomial f in n variables of degree at most $m-1$ in each of the variables can be effectively specified such that*

$$L_+(f) = \Omega(m^{n(1-o(1))}), \qquad L_\times(f) = \Omega(m^{n(1/2-o(1))})$$

as $m^n \to \infty$.

Proof. Let $n = 1$. Choose the parameters q and t according to the conditions that q is a prime number, $(2q-1)^t \leqslant m$ and $q^{t-1}/(t!)^2 = m^{1-o(1)}$, and define the set mon f as the image of the corresponding thin set appearing in item (iii) of Theorem 3 under the mapping $\psi_{q,1,t}$, see (2). By Theorem 4 the set constructed in this way is $(t, t!+1)$-thin. The bounds for the complexity of f follow from items (i), (iii) of Theorem 1.

An example of a polynomial in $n > 1$ variables $x_0, \ldots, x_{n-1}$ is obtained by applying the Kronecker substitution $x_i = x^{m^i}$ to the univariate polynomial of degree $m^n - 1$ constructed above.

The nonzero coefficients of these polynomials may take arbitrary positive values: the lower bounds derived from Theorem 1 depend only on the set mon f. We shall restrict our attention to polynomials with coefficients 0 and 1 and show their effectiveness. Namely, we shall establish that the Boolean functions which express the coefficients of the polynomial in terms of the degree of the corresponding monomial have polynomial complexity.

The implementation of the Boolean function $c_f(d_{n-1},\dots,d_0)$ in question may be reduced to the following steps (by d_i we denote the binary representation of the degree of the variable x_i in the monomial).

1) Computing the binary representation of d by its representation $[d_{n-1},\dots,d_0]_m$ in the base-m number system (that is, reducing to a univariate polynomial, see above).

2) Representing d in the number system of the base $2q-1$, which will be denoted by $[a_{t-1},\dots,a_0]_{2q-1}$.

3) Checking the inequalities $0 \leqslant a_i < q$ hold. If any of these inequalities is violated, then the value of function c_f is set equal to 0.

4) If all the inequalities in item 3) are satisfied, then the vector $(a_{t-1},\dots,a_0)$ is interpreted as an element X of the field $GF(q)^t$. The element $X^{(q^t-1)/(q-1)}$ is computed and the function c_f is set equal to 1 if the result is $1 \in GF(q)^t$, and 0 otherwise.

The above steps can be implemented by a circuit of complexity $b\log^{O(1)} b$ with respect to the size $b = \Theta(\log m^n)$ of the input of function c_f, provided that the conversion between the number systems is performed using the fast Schönhage algorithm (see, for instance, [14]), and raising to the power of special form in a finite field is carried out using the method of additive chains (see, for instance, [60]).

The proof of the theorem is complete.

Since the additive monotone complexity of any polynomial in n variables of degree at most $m-1$ in each of the variables is not higher than m^n, and the multiplicative monotone complexity is of order at most $m^{n/2}$, the bounds established in the theorem are close to the best possible estimates.

In the particular cases $m = 2$ and $n = 1$ the above theorem provides examples of a multilinear polynomial and a univariate polynomial of high monotone complexity.

Remark 4. The results in [22] imply the lower bound $\Omega(2^{n/2}/n)$ for the additive complexity (in the complete basis) of the class of all multilinear polynomials in n variables with coefficients $0, 1$. In turn, it follows from Theorem 5 that in the case of a monotone basis one can effectively construct a multilinear polynomial in n variables with coefficients $0, 1$ having the additive complexity $\Omega(2^{(1-o(1))n})$.

§ 7. Some upper bounds

In this section we consider the problem of how sharp the estimates given by Theorem 1 are. It is evident that if l does not grow with increasing n, then the estimate of item (i) for $L_+(f)$ cannot be improved in order, because for any polynomial f we have $L_+(f) \leqslant |\operatorname{mon} f| - 1$, and in the case $k = l = 2$ the estimate (i) is sharp.

Now we will show that, in general, the estimates of items (ii) and (iii) cannot be essentially improved either.

Theorem 6. *For any n if $k=2$, and any $n>1$ if $k>2$, there exists a k-thin set $\operatorname{mon} f \subset E_m^n$ such that $|\operatorname{mon} f| \geqslant m^{c_k n^{\log_2 3-1}}$ and*

$$L_\times(\operatorname{mon} f) \lesssim \begin{cases} \Theta(|\operatorname{mon} f|^{(k+1)/(2k)}), & k>3, \\ 3|\operatorname{mon} f|^{3/5}, & k=3, \\ 3|\operatorname{mon} f|^{2/3}, & k=2. \end{cases}$$

Proof. If A is a finite set, then we shall denote the set of one-element subsets in A by A^*.

Lemma 14. (i) *Let $A_1=\{a_1,\dots,a_p\}\subset E_m^{n_1}$ and $A_2=\{b_1,\dots,b_q\}\subset E_m^{n_2}$ be k-thin subsets and let $(\mu_{i,j})$ be an l-thin Boolean $(p\times q)$-matrix, $n=n_1+n_2$, $k\leqslant l$. Then the set $A=\{(a_i,b_j)\mid \mu_{i,j}=1\}\subset E_m^n$ is $((k-1)(l-1)+1)$-thin. Moreover,*

$$L_\times(A)\leqslant L_\times(A_1^*)+L_\times(A_2^*)+|A_1|, \qquad L_\times(A^*)\leqslant L_\times(A_1^*)+L_\times(A_2^*)+|A|.$$

(ii) *Let $A_1=\{a_1,\dots,a_p\}\subset E_m^n$ and $A_2=\{b_1,\dots,b_q\}\subset E_m^n$ be k-thin subsets and let $(\mu_{i,j})$ be an l-thin Boolean $(p\times q)$-matrix. Then the set $A=\{a_i+(2m-1)b_j\mid \mu_{i,j}=1\}\subset E_{2m^2}^n$ is $((k-1)(l-1)+1)$-thin. Moreover,*

$$L_\times(A)\leqslant L_\times(A_1^*)+L_\times(A_2^*)+|A_1|+2n\log_2 m,$$
$$L_\times(A^*)\leqslant L_\times(A_1^*)+L_\times(A_2^*)+|A|+2n\log_2 m.$$

Proof. We set $r=(k-1)(l-1)+1$ and verify that the set A defined in item (i) is r-thin. Suppose the contrary. Then there exist distinct vectors $c_1,\dots,c_r$, $c_i=(c_{i,1},c_{i,2})$, $c_{i,j}\in E_m^{n_j}$, and distinct vectors $d_1,\dots,d_r$, $d_i=(d_{i,1},d_{i,2})$, $d_{i,j}\in E_m^{n_j}$, such that

$$\{c_1,\dots,c_r\}\times\{d_1,\dots,d_r\}\subset A.$$

Denote

$$C_j=\{c_{1,j},\dots,c_{r,j}\},\quad D_j=\{d_{1,j},\dots,d_{r,j}\},\qquad j=1,2.$$

Then for each $j=1,2$ we have the inclusion $C_j\times D_j\subset A_j$.

Since A_1 is a k-thin subset, it may be assumed without loss of generality that $|D_1|<k$. Then (by the pigeonhole principle) one can find at least l equal vectors $d_{i,1}$. Without loss of generality we shall assume that $d_{1,1}=\dots=d_{l,1}$. However, then all the vectors $d_{1,2},\dots,d_{l,2}$ must be distinct (as all the vectors d_i are distinct) and, consequently, $|D_2|\geqslant l\geqslant k$. Therefore, the k-thinness of the set A_2 implies that $|C_2|<k$, that is, for similar reasons it may be assumed that $c_{1,2}=\dots=c_{l,2}$ and, as a consequence, all the vectors $c_{1,1},\dots,c_{l,1}$ are distinct. The above arguments show that

$$\{c_1,\dots,c_r\}\times\{d_1,\dots,d_r\}\supset\{(c_{i,1}+d_{1,1},\,c_{1,2}+d_{j,2})\mid i,j=1,\dots,l\},$$

whence it follows that the matrix $(\mu_{i,j})$ contains an $(l\times l)$-submatrix of ones, which contradicts our assumption.

Now we will establish the complexity relations. Implementing all vectors $(a_i,\vec{0})$ and $(\vec{0},b_j)$ with the multiplicative complexity $L_\times(A_1^*)$ and $L_\times(A_2^*)$, respectively,

and using the identity $\{(a_i, b_j)\} = \{(a_i, \vec{0})\} \times \{(\vec{0}, b_j)\}$, we obtain the required estimate for $L_\times(A^*)$. To derive the first bound, we make use of the formula

$$A = \bigvee_{i=1}^{p} \{(a_i, \vec{0})\} \times \left(\bigvee_{\mu_{i,j}=1} \{(\vec{0}, b_j)\} \right). \tag{3}$$

Next we prove item (ii). According to what was established in item (i), the set $A' = \{(a_i, b_j) \mid \mu_{i,j} = 1\} \subset E_m^{2n}$ is r-thin. Then, by Theorem 4 the set $A = \psi_{m,n,2}(A')$ is r-thin as well.

We will derive bounds for the complexity. Implementation of the set $\{2m-1\}$ requires at most $2\log_2 m$ multiplications provided that a binary additive chain for the number $2m-1$ is constructed (see, for instance, [14]). Therefore, the n-tuple of vectors $\{(2m-1)e_0, \dots, (2m-1)e_{n-1}\}$, where $e_0, \dots, e_{n-1}$ are unit (basis) vectors in N^n, can be implemented using $2n\log_2 m$ multiplications. After that all one-element sets $\{a_i\}$ and $\{(2m-1)b_j\}$ are implemented with complexity $L_\times(A_1^*) + L_\times(A_2^*)$. Now the required relations follow from the formulae

$$\{a_i + (2m-1)b_j\} = \{a_i\} \times \{(2m-1)b_j\},$$
$$A = \bigvee_{i=1}^{p} \{a_i\} \times \left(\bigvee_{\mu_{i,j}=1} \{(2m-1)b_j\} \right). \tag{4}$$

The proof of the lemma is complete.

Now we go back to proving Theorem 6. The lemma proved above allows us to construct thin sets of sufficiently large cardinality and at the same time complexity which is not too big. Pippenger's result [61] on the additive complexity of an assembly of numerical vectors for an arbitrary set $A \subset E_m^n$ yields the estimate

$$L_\times(A) \leqslant L_\times(A^*) \leqslant n\log_2 m + (1+o(1))\frac{|A|n\log_2 m}{\log_2(|A|n\log_2 m)} + O(|A|). \tag{5}$$

Therefore, if in Lemma 14, (ii) we also require that $|A| = \Omega(\max\{|A_1|, |A_2|\}n\log_2 m)$, then implementing A_1^* and A_2^* by Pippenger's method we obtain the relation $L_\times(A^*) \lesssim |A|$.

Below we shall use the following well-known facts: the set E_m contains a 2-thin subset whose cardinality is asymptotically equal to $\sqrt{m}$; there exists a k-thin $(n \times n)$-matrix with weight $\Omega_k(n^{(2k)/(k+1)})$ (see [62]), if $k = 3$, there is a matrix with weight $(1+o(1))n^{5/3}$ (see [54]), and if $k = 2$, there is a matrix with weight $(1+o(1))n^{3/2}$ (see [62]).

Now, applying Lemma 14, (i) recursively, with parameters $k = l = 2$, $n_1 = \lfloor n/2 \rfloor$, and $n_2 = \lceil n/2 \rceil$, for any $n \geqslant 2$ we can construct a 2-thin subset A in E_m^n with cardinality $\Theta(m^{1/2(3/2)^{\lfloor \log_2 n \rfloor}})$ and complexity $L_\times(A^*) \lesssim |A|$ (as $m \to \infty$).

If $n = 1$, we use item (ii) of Lemma 14 (substituting $\lfloor \sqrt{m/2} \rfloor$ for m) and construct a 2-thin subset A in E_m of cardinality $\Theta(m^{3/8})$ and complexity $L_\times(A^*) \lesssim |A|$.

Finally, for $n > 1$ with $n_1 = \lfloor n/2 \rfloor$ and $n_2 = \lceil n/2 \rceil$, we use the first construction in Lemma 14 and for $n = 1$ and $k = 2$ with parameter $\lfloor \sqrt{m/2} \rfloor$, the second with

the sets A_i taken equal to the 2-thin sets (or their subsets) constructed above, so that $|A_1| = |A_2|$. The matrices $(\mu_{i,j})$ are chosen equal to the aforementioned k-thin matrices of large weight. In both cases we obtain a k-thin set A satisfying the complexity estimate $L_\times(A) \lesssim 3|A_1|$. Here, by construction, if $n > 1$ and $k > 3$ we have $|A| \asymp |A_1|^{(2k)/(k+1)}$, if $n > 1$ and $k = 3$ we have $|A| \sim |A_1|^{5/3}$, and if $k = 2$ we have $|A| \sim |A_1|^{3/2}$. The proof of the theorem is complete.

As a consequence we see that when $k = 2$ or $k = 3$ the estimates of Theorem 1 cannot be improved in order (since a k-thin subset is (k, l)-thin).

Remark 5. The constant 3 in the estimate established in Theorem 6 for $k = 3$ can be reduced to $5\sqrt[5]{2/27} \approx 2,971\ldots$. To verify this, apply item (i) of Lemma 14 to the sets A_i such that $4|A_1| \sim 3|A_2|$ and take $(\mu_{i,j})$ equal to a 3-thin submatrix of Brown's matrix (which has weight $(1 + o(1))|A_1|\,|A_2|^{2/3}$).

Remark 6. If the hypothesis in [62] about k-thin matrices is true, then for $k > 3$ the exponent $(k + 1)/(2k)$ in the upper estimate for $L_\times(\operatorname{mon} f)$ in Theorem 6 can be reduced to $k/(2k - 1)$. However, even the last estimate is higher in order than the corresponding lower estimate established in Theorem 1.

§ 8. Thin subsets and thin matrices

It is obvious that with a (k, l)-thin set $M \subset \mathbb{Z}_m^n$ we can associate a symmetric Boolean matrix $(\mu_{\alpha,\beta})$ of size $m^n \times m^n$ that is simultaneously (k, l)-thin and (l, k)-thin (its rows and columns are indexed by the elements of $\mathbb{Z}_m^n$) defined by the condition

$$\mu_{\alpha,\beta} = 1 \quad \Longleftrightarrow \quad \alpha + \beta \in M.$$

This matrix proves to be cyclic, in a certain sense; for $n = 1$ it is a circulant matrix (consisting of unit cyclic diagonals).

The property of being cyclic is manifested in that the matrix $(\mu_{\alpha,\beta})$ can be treated as the matrix of multiplication by a certain element in the ring

$$K_{m,n} = \mathbb{R}[x_1, \ldots, x_n]/(x_1^m - 1, \ldots, x_n^m - 1).$$

In particular, a circulant matrix is the matrix of cyclic convolution with some constant vector. We will prove this.

For brevity, for any $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_m^n$ we introduce the notation $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Define the element $a = \sum_{\alpha \in \mathbb{Z}_m^n} a_\alpha X^\alpha$ of the ring $K_{m,n}$ by the following condition on its coefficients: $a_\alpha = 1$ if $\alpha \in M$, and $a_\alpha = 0$ otherwise. Thus, $\mu_{\alpha,\beta} = a_{\alpha+\beta}$ for any $\alpha, \beta \in \mathbb{Z}_m^n$.

We multiply the αth row of the matrix $(\mu_{\alpha,\beta})$ by the vector of coefficients of an arbitrary element $b = \sum_{\beta \in \mathbb{Z}_m^n} b_\beta X^\beta$ in the ring $K_{m,n}$ whose βth component is equal to $b_{-\beta}$ (the components of this vector are indexed in the same way as the columns of matrix $(\mu_{\alpha,\beta})$). We have

$$\sum_\beta \mu_{\alpha,\beta} b_{-\beta} = \sum_\beta a_{\alpha+\beta} b_{-\beta} = \sum_{\gamma+\delta=\alpha} a_\gamma b_\delta,$$

which equals the coefficient of X^α in the product $ab \in K_{m,n}$.

The existence of a thin subset of large cardinality means that there exists a thin matrix of large weight. The interest in constructing such matrices comes from the Zarankiewicz problem (see [63], [62], [58], [54] and [50]). Thin matrices are employed in the methodology in [12] and [9]. The role played by thin matrices in another problem in the theory of complexity of Boolean circuits is described in [64].

Examples of thin sets in Theorem 3, (ii.a) and (iii) in the sense above correspond to the examples of thin matrices constructed in [58] and [50]. However, for a thin matrix to be suitable for constructing a thin set (by the method presented above), the matrix has to satisfy some additional constraints, which means that constructing a thin set is, in general, more difficult than constructing a thin matrix.

Thin subsets have even more to offer. By the method of Theorem 4 (see also the proof of Theorem 5) they may be used to effectively construct k-thin subsets of cardinality $n^{1-o(1)}$ in the cyclic group $\mathbb{Z}_n$ for a slowly increasing k and, as a consequence, k-thin circulant matrices of weight $n^{2-o(1)}$. More precisely, item (iii) of Theorem 3 (with q taken to be prime) and Theorem 4 yield the following result.

Corollary 1. *For any n one can effectively*[16] *specify a (k,l)-thin circulant matrix of order n and weight αn^2, where*

$$k = O\left(\sqrt{\frac{\log n}{\log\log n}}\right), \qquad l, \alpha^{-1} \in 2^{O(\sqrt{\log n \log\log n})}.$$

Without effective specification the existence of circulant thin matrices of large weight was proved by Grinchuk [65], see also [66]. In view of Theorem 1, his result can be used to establish the existence of polynomials of degree n with coefficients $0, 1$ having additive monotone complexity $n^{1-o(1)}$ and multiplicative monotone complexity $n^{0,5-o(1)}$. Moreover, these estimates will be stronger (in the term $o(1)$) than those which follow from the proof of Theorem 5, (iii).

We shall mention one more corollary of item (i) of Theorem 1. For a Boolean matrix $A = (a_{i,j})$ we introduce the notation

$$L_+(A) = \min\bigl\{L_+(BX) \mid B = (b_{i,j}),\ b_{i,j} > 0 \implies a_{i,j} = 1\bigr\},$$

where BX is the linear operator with matrix B. If A_n is a (k,l)-thin and (l,k)-thin Boolean $(n \times n)$-matrix, then

$$L_+(A_n) \geqslant \frac{\sum_{i,j} a_{i,j}}{h} - n,$$

where $h = \max\{(k-1)^3, (l-1)^2\}$. To show this, it suffices to consider the polynomial $f_B = \sum b_{i,j} x_i y_j$ and apply Theorem 1 (the set $\operatorname{mon} f_B$ is (k,l)-thin).

It should be noted, however, that the inequality

$$L_+(A_n) \geqslant \frac{\sum_{i,j} a_{i,j}}{(k-1)(l-1)} - \frac{n}{l-1}$$

can easily be derived from the results of [67].

[16] A matrix is considered effective if its entries are determined by a Boolean function of (the binary representation of) their coordinates implemented by a circuit of polynomial complexity.

These inequalities are applicable in deriving effective high lower estimates for $L_+(A_nX)$, where A_n is a Boolean matrix. It suffices to set A_n equal to the matrix mentioned in Corollary 1. Then $L_+(A_n) = n^{2-o(1)}$. Moreover, such a matrix satisfies the upper estimate $L(A_n) = O(n^{1+o(n)})$ for the complexity in the complete linear basis $\{x+y\}\cup\{cx : c \in \mathbb{R}\}$ (see, for instance, [64]). Therefore, the matrix A_n satisfies the inequality $L_+(A_n)/L(A_n) \geqslant n^{1-o(1)}$. This fact is, in a sense, analogous to one result of [64]. The result in [23] (which, however, can also be established by Lupanov's method) yields the upper estimate $L_+(A_n)/L(A_n) \leqslant O(n/\log n)$ for an arbitrary Boolean matrix.

In [16] Heintz and Sieveking effectively construct examples of matrices of complexity $\Theta(n^2)$ not in the monotone, but in the complete basis. However, it is essential that the entries of these matrices are algebraic numbers. In deriving the lower bounds for matrices the authors of [16] follow the same line as in proving lower bounds for the complexity of univariate polynomials in the same work. In [68] it is shown that lower bounds for the complexity of matrices are easily derived from lower bounds for the complexity of univariate polynomials.

§ 9. Monotone and nonmonotone complexity

In this section we improve the result in [31] on the feasibility of reducing the complexity of a polynomial by means of adding negative constants to the monotone basis.

Consider the following construction. Let $A_1, A_2 \subset E_m^n$ be k-thin subsets of cardinality r. Denote by $(\mu_{i,j})$ the circulant matrix of order r from Corollary 1 and let the set A be constructed from the sets A_1, A_2 using the matrix $(\mu_{i,j})$ with the help of one of the methods presented in Lemma 14 ($A \subset E_m^{2n}$ if item (i) of Lemma 14 is used, and $A \subset E_{2m^2}^n$ if item (ii) is employed). The following assertion holds.

Lemma 15. *Let f be a polynomial with coefficients 0 and 1 such that* $\operatorname{mon} f = A$. *Let $k = r^{o(1)}$ and either $n\log m = r^{o(1)}$, or $\deg f = r^{o(1)}$. Then the monotone complexity of f satisfies $L_+(f) = \Omega(r^{2-o(1)})$, and the complexity $L(f)$ of computing f in the complete basis $\{x+y,\, xy\}\cup\mathbb{R}$ is no higher than $r^{1+o(1)}$.*

Proof. The lower bound $L_+(f) = \Omega(r^{2-o(1)})$ follows for $k = r^{o(1)}$ from item (i) of Theorem 1. Let us establish the upper estimate for the complexity of the implementation in the complete basis.

To implement the polynomial we shall use the more suitable of formulae (3) and (4). First, we show that all monomials corresponding to the elements of A_1, that is, in the above notation the assembly of polynomials $\operatorname{mon}^{-1}(A_1^*)$, can be computed by a circuit of complexity $r^{1+o(1)}$ (and the same result holds for A_2).

Now, if $\deg f = r^{o(1)}$, the degree of each monomial in $\operatorname{mon}^{-1}(A_1^*)$ is no higher than $r^{o(1)}$, and all r monomials may be implemented independently. If $n\log m = r^{o(1)}$, then the complexity estimate $r^{1+o(1)}$ follows from (5).

In calculations using (4) we need to recompute the $(2m-1)$st powers of all variables (since it is these powers that are supplied at the inputs of the circuit which implements monomials with exponents from A_2). The complexity of this step is at most $2n\log_2 m = r^{o(1)}$.

The next step consists in computing linear combinations of monomials corresponding to the set A_2 whose coefficients are determined by the rows of the matrix $(\mu_{i,j})$. A circulant matrix is a matrix of multiplication by a constant polynomial (see the previous section). Therefore, a linear transformation with such a matrix is performed using the Fast Fourier Transform algorithm (see, for example, [69]) with complexity $O(r \log r)$.

It remains to multiply the monomials which correspond to the elements of the set A_1 by the linear combinations obtained at the previous step and to add up the results. This can be done with complexity $2r$. The proof of the lemma is complete.

Theorem 7. *Let $m \geqslant 2$ and $n \geqslant 1$. Then a monotone polynomial f in n variables of degree at most $m-1$ in each of the variables can be effectively specified for which the ratio between the complexity of the implementation in the monotone basis $\{x+y,\, xy\} \cup \mathbb{R}_+$ to that of the implementation in the complete basis $\{x+y,\, xy\} \cup \mathbb{R}$ is at least $m^{(0{,}5-o(1))n}$ as $m^n \to \infty$.*

Proof. We will make use of the construction suggested in Lemma 15. We take A_1 and A_2 to be $r^{o(1)}$-thin subsets of maximum cardinality $r = m^{(0.5-o(1))n}$ in $E_{m'}^{n'}$, where $n' = \lfloor n/2 \rfloor$, $m' = m$ as $n \to \infty$ and $n' = n$, $m' = \lfloor \sqrt{m/2} \rfloor$ otherwise. For odd n, in the first case the set $A \subset E_m^{2n'}$ constructed above is immersed in E_m^n via the natural mapping $A \to (A, 0)$. Since the condition $n \log m = r^{o(1)}$ is fulfilled, by Lemma 15 the polynomial f, $\operatorname{mon} f = A$, satisfies the estimates $L_+(f) = \Omega(m^{n-o(n)})$ and $L(f) = O(m^{n/2+o(n)})$.

Effectiveness is established in the same way as in Theorem 5 with the difference that an additional step is introduced: checking that some element belongs to the set A obtained using the sets A_1 and A_2 by the method of Lemma 14 is reduced to checking that two easily determined elements belong to the sets A_1 and A_2. Then proof of the theorem is complete.

Remark 7. It can be shown in a standard way that the non-monotone complexity estimate given in Theorem 7 is even attained by a circuit that contains only one non-monotone gate (multiplication by a negative constant). To do this, we have to represent (an arbitrary) polynomial as the difference of two monotone polynomials. In such a representation, any operation in the complete arithmetic basis reduces to several monotone operations over monotone polynomials. The non-monotone operation is performed at the very end of the computations to pass back to the usual representation.

Lemma 15 also enables us to answer the 'open problem' 9 formulated in the survey [70]: establish the disagreement between monotone and non-monotone complexity for polynomials of constant degree (the example given in paper [31] involved polynomials of increasing degree).

First of all, we note that the problem had in fact already been solved by Schnorr in [29].[17] The appropriate examples here are the polynomials SC_n and SM_n, which are used to derive lower bounds for the complexity of matrix multiplication and convolution. But we shall give two more examples. The following assertion holds.

[17] We remark that no mention of the fundamental work [29] was made in [70].

Corollary 2. *A multilinear polynomial f can be effectively specified*

(i) *of degree $k(k-1)$ in $n(n-1)$ variables whose complexity satisfies the bounds $L_+(f) = \Omega(n^{2k-o(1)})$ and $L(f) = O(n^{k+o(1)})$ as $n \to \infty$;*

(ii) *of degree 2^k in $2^k n$ variables whose complexity satisfies the bounds $L_+(f) = \Omega(n^{2^k-o(1)})$ and $L(f) = O(n^{2^{k-1}+o(1)})$ as $n \to \infty$.*

Proof. We will prove (i). Take A_1 and A_2 to be the 2-thin subsets in $E_2^{C_n^2}$ which correspond to the characteristic polynomial of the k-clique [29]

$$CL_{n,k} = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} \prod_{1 \leqslant s < t \leqslant k} x_{i_s, i_t}.$$

Using the technique in Lemma 15 we use these sets to construct a new set $A \subset E_2^{n(n-1)}$ and take $f = f_A$. The complexity of f obeys the estimates of Lemma 15 since $\deg f = O(1)$. Item (i) is established.

The proof of (ii) for $k = 1$ mentions the polynomial f_B introduced in the previous section, which corresponds to a suitable thin matrix from Corollary 1. This polynomial is an example of a bilinear form in $2n$ variables having monotone complexity $n^{2-o(1)}$ and complexity $n^{1+o(1)}$ in the complete basis. Note that the ratio between the monotone and non-monotone complexity of f_B is almost the maximum possible for polynomials of degree 2, since it obviously cannot exceed $O(n)$.

Set $f_{B,1} = f_B$. For an arbitrary k the required polynomial $f = f_{B,k}$ may be constructed by following Lemma 15 using the sets $A_1 = A_2 = \operatorname{mon} f_{B,k-1}$ as in item (i).

The effectiveness of the polynomials constructed above follows from the effectiveness of the polynomials $CL_{n,k}$ and f_B. The proof of the corollary is complete.

In [29] exact estimates for the additive monotone complexity of systems of bilinear form were obtained which correspond to the problems of polynomial multiplication (that is, convolution) and matrix multiplication. Below we formulate a more general proposition in terms of thin sets.

Lemma 16. *Let $\{g_i(x_0, y_0, \dots, x_{n-1}, y_{n-1}) \mid i = 1, \dots, k\}$ be a system of bilinear forms such that $\operatorname{mon} g_i$ is a $(1,2)$-thin set, $\operatorname{mon} g_i \cap \operatorname{mon} g_j = \varnothing$ for any $i \neq j$. Then*

$$L_+(g_1, \dots, g_k) = \sum_{i=1}^{k} |\operatorname{mon} g_i| - k, \qquad L_\times(g_1, \dots, g_k) = \sum_{i=1}^{k} |\operatorname{mon} g_i|.$$

Proof. The upper estimates are obvious. To establish the lower bound for the multiplicative complexity it suffices to observe that all the forms g_i cannot be computed without computing all the monomials separately, which requires $|\operatorname{mon} g_i|$ product gates (this follows from the $(1,2)$-thinness), and to take into account that different forms have different monomials. This also gives the required estimate for the additive complexity, which can otherwise be derived by the method of proof of Theorem 1. The proof of the lemma is complete.

As a consequence, we see that the convolution

$$c_k(x_0, y_0, \dots, x_{n-1}, y_{n-1}) = \sum_{i+j=k} x_i y_j,$$

where $k = 0, \dots, 2n-2$, has additive monotone complexity $n^2 - 2n - 1$ and multiplicative monotone complexity n^2. For comparison, we notice that in the complete arithmetic basis these quantities are estimated as $O(n \log n)$ and $\Theta(n)$, respectively.

By Lemma 16, multiplication of $(n \times n)$-matrices has additive monotone complexity $n^3 - n^2$ and multiplicative monotone complexity n^3. In the complete basis both quantities are estimated above as $O(n^\omega)$, where $\omega < 2.4$.

These problems have Boolean analogues, in which disjunction and conjunction are used for the operations of addition and multiplication, respectively. While for the Boolean analogue of the problem of monotone computation of matrix multiplication the same sharp bounds have been established (see [71]) in the case of monotone computation of the Boolean convolution a lower bound $\Omega(n^2/\log^{O(1)} n)$ for the number of disjunctions was determined in [66] and an estimate $\Omega(n^{3/2})$ for the number of conjunctions was announced by Blum in [72]. The Boolean analogue of Lemma 16 established in [71], Theorem 7.1, allows nontrivial lower estimates to be derived, however these are not exact in the general case.

Bibliography

[1] M. R. Garey and D. S. Johnson, *Computers and intractability*, W. H. Freeman & Co., San Francisco, CA 1979.

[2] R. G. Nigmatullin, *The complexity of Boolean functions*, Nauka, Moscow 1991. (Russian)

[3] O. B. Lupanov, *Asymptotic estimates for the complexity of control systems*, Moscow State University Publishing House, Moscow 1984. (Russian)

[4] O. B. Lupanov, "Methods for obtaining estimates of the complexity of defining and computing individual functions", *Diskret. Analiz* **25** (1974), 3–18. (Russian)

[5] V. M. Khrapchenko, "Lower bounds for the complexity of circuits of functional elements (a survey)", Kibern. Sb., Nov. Ser., vol. 21, Mir, Moscow 1984, pp. 3–54. (Russian)

[6] R. G. Nigmatullin, *Lower bounds for complexity and the complexity of universal circuits*, Kazan University Publishing House, Kazan 1990. (Russian)

[7] A. A. Razborov, "Lower bounds for the monotone complexity of some Boolean functions", *Dokl. Akad. Nauk SSSR* **281**:4 (1985), 798–801; English transl. in *Soviet Math. Dokl.* **31**:2 (1985), 354–357.

[8] A. A. Razborov, "Lower bounds on monotone complexity of the logical permanent", *Mat. Zametki* **37**:6 (1985), 887–900; English transl. in *Math. Notes* **37**:6 (1985), 485–493.

[9] A. E. Andreev, "A method for obtaining efficient lower bounds for monotone complexity", *Algebra i Logika* **26**:1 (1987), 3–26; English transl. in *Algebra and Logic* **26**:1 (1987), 1–18.

[10] N. Alon and R. B. Boppana, "The monotone circuit complexity of boolean functions", *Combinatorica* **7**:1 (1987), 1–22.

[11] A. E. Andreev, *A method for deriving lower bounds for the complexity of individual monotone functions*, Preprint no. 248 of the Institute for Problems in Mechanics of the Moscow State University and the USSR Academy of Sciences, Moscow 1985. (Russian)

[12] A. E. Andreev, "On a method for obtaining lower bounds for the complexity of individual monotone functions", *Dokl. Akad. Nauk SSSR* **282**:5 (1985), 1033–1037; English transl. in *Soviet Math. Dokl.* **31**:3 (1985), 530–534.

[13] D. Harnik and R. Raz, "Higher lower bounds on monotone size", *Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computing*, ACM, New York 2000, pp. 378–387.

[14] D. E. Knuth, *The art of computer programming*, vol. 2: *Seminumerical algorithms*, 3rd ed., Bonn, Reading, MA 1998.

[15] J. von zur Gathen and V. Strassen, "Some polynomials that are hard to compute", *Theoret. Comput. Sci.* **11**:3 (1980), 331–335.

[16] J. Heintz and M. Sieveking, "Lower bounds for polynomials with algebraic coefficients", *Theoret. Comput. Sci.* **11**:3 (1980), 321–330.

[17] H.-J. Stoss, "Lower bounds for the complexity of polynomials", *Theoret. Comput. Sci.* **64**:1 (1989), 15–23.

[18] W. Baur and K. Halupczok, "On lower bounds for the complexity of polynomials and their multiples", *Comput. Complexity* **8**:4 (1999), 309–315.

[19] M. S. Paterson and L. J. Stockmeyer, "On the number of nonscalar multiplications necessary to evaluate polynomials", *SIAM J. Comput.* **2** (1973), 60–66.

[20] D. Yu. Grigor'ev, "Lower bounds in algebraic computational complexity", *Theory of computational complexity. I*, Zap. Nauchn. Semin. Leningr. Otd. Mat. Inst. Steklova, vol. 118, Nauka, Leningrad Branch, Leningrad 1982, pp. 25–82; English transl. in *J. Sov. Math.* **29** (1985), 1388-1425.

[21] P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer-Verlag, Berlin–Heidelberg 1997.

[22] C. P. Schnorr and J. P. van de Wiele, "On the additive complexity of polynomials", *Theoret. Comput. Sci.* **10**:1 (1980), 1–18.

[23] J. E. Savage, "An algorithm for the computation of linear forms", *SIAM J. Comput.* **3** (1974), 150–158.

[24] V. Strassen, "Berechnungen in partiellen Algebren endlichen Typs", *Computing* **11**:3 (1973), 181–196.

[25] S. B. Gashkov, "On the complexity of the computation of certain classes of polynomials of several variables", *Vestn. Moskov. Univ. Ser.* 1 *Mat. Mekh.*, 1988, no. 1, 89–91; English transl. in *Moscow Univ. Math. Bull.* **43**:2 (1988), 65–67.

[26] S. B. Gashkov, "On parallel evaluation of certain classes of polynomials with an increasing number of variables", *Vestn. Moskov. Univ. Ser.* 1 *Mat. Mekh.*, 1990, no. 2, 88–92; English transl. in *Moscow Univ. Math. Bull.* **45**:2 (1990), 64–67.

[27] S. B. Gashkov, "The complexity of realization of Boolean functions by systems of functional elements and formulae in bases, whose elements realize continuous functions", *Probl. Kibernet.*, vol. 37, Nauka, Moscow 1980, pp. 57–118. (Russian)

[28] I. I. Zhegalkin, "Arithmetizing symbolic logic", *Mat. Sb.* **35**:3–4 (1928), 311–377. (Russian)

[29] C. P. Schnorr, "A lower bound on the number of additions in monotone computations", *Theoret. Comput. Sci.* **2**:3 (1976), 305–315.

[30] R. Jerrum and M. Snir, "Some exact complexity results for straight-line computations over semirings", *J. Assoc. Comput. Mach.* **29**:3 (1982), 874–897.

[31] L. G. Valiant, "Negation can be exponentially powerful", *Theoret. Comput. Sci.* **12**:3 (1980), 303–314.

[32] L. G. Valiant, "The complexity of computing the permanent", *Theoret. Comput. Sci.* **8**:2 (1979), 189–201.

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

[34] G. Malod, "The complexity of polynomials and their coefficient functions", *Proc. IEEE Conf. Comput. Complexity* **13** (2007), 193–204.

[35] L. Blum, F. Cucker, M. Shub and S. Smale, *Complexity and real computation*, Springer-Verlag, New York 1998.

[36] R. Sengupta and H. Venkaterswaran, "A lower bound for monotone arithmetic circuits computing 0–1 permanent", *Theoret. Comput. Sci.* **209**:1–2 (1998), 389–398.

[37] M. Agraval, "Determinant versus permanent", *Proc. International Congress of Mathematicians*, vol. 3, Eur. Math. Soc., Zürich 2006, pp. 985–997.

[38] R. Raz, "Multi-linear formulas for permanent and determinant are of super-polynomial size", *Proc. of the 36th annual ACM symposium on the theory of computing* (Chicago, IL, USA 2004), ACM Press, New York 2004, pp. 633–641.

[39] O. M. Kasim-Zade, "Arithmetic complexity of monotone polynomials", *Theoretical Problems in Cybernetics. Abstracts of lectures*, Saratov State University Publishing House, Saratov 1986, pp. 68–69. (Russian)

[40] O. M. Kasim-Zade, "The complexity of monotone polynomials", *Proceedings of the All-Union seminar on discrete mathematics and applications*, Moscow State University Publishing House, Moscow 1986, pp. 136–138. (Russian)

[41] S. E. Kuznetsov, "Monotone computations of polynomials and circuits without zero chains", VII *All-Union Conference on Problems in Theoretical Cybernetics*, Abstracts of talks. Pt. 1, Irkutsk 1985, pp. 108–109. (Russian)

[42] S. E. Kuznetsov, "Circuits of functional elements without zero chains in the basis $\{\&, v\}$", *Iz. Vysh. Uchebn. Zaved. Mat.*, 1981, no. 5, 56–63; English transl. in *Soviet Math.* (*Iz. VUZ*) **25**:5 (1981), 62–73.

[43] S. B. Gashkov, "The complexity of monotone computations of polynomials", *Vestn. Moskov. Univ. Ser.* 1 *Mat. Mekh.*, 1987, no. 5, 7–13; English transl. in *Mosc. Univ. Math. Bull.* **42**:5 (1987), 1–8.

[44] R. Raz and A. Yehudayoff, "Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors", *J. Comput. System Sci.* **77**:1 (2011), 167–190.

[45] N. Nisan and A. Wigderson, "Lower bounds on arithmetic circuits via partial derivatives", *Comput. Complexity* **6**:3 (1996), 217–234.

[46] S. B. Gashkov, "The complexity of the realization of Boolean functions by schemes and formulas in bases consisting of continuous functions", *Dokl. Akad. Nauk SSSR* **250**:4 (1980), 782–787; English transl. in *Soviet Math. Dokl.* **21**:5 (1980), 186–190.

[47] G. Turán and F. Vatan, "On the computation of boolean functions by analog circuits of bounded fan-in", *J. Comput. System Sci.* **54**:1 (1997), 199–212.

[48] A. Haken and S. A. Cook, "An exponential lower bound for the size of monotone real circuits", *J. Comput. System Sci.* **58**:2 (1999), 326–335.

[49] P. Pudlák, "Lower bounds for resolution and cutting plane proofs and monotone computations", *J. Symbolic Logic* **62**:3 (1997), 981–998.

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

[51] D. J. Kleitman, "Extremal properties of collections of subsets containing no two sets and their union", *J. Combinatorial Theory Ser. A* **20**:3 (1976), 390–392.

[52] K. O'Bryant, "A complete annotated bibliography of work related to Sidon sequences", *Electron. J. Combin.*, DS11, Dynamic Surveys, 2004.

[53] V. Nikiforov, "A contribution to the Zarankiewicz problem", *Linear Algebra Appl.* **432**:6 (2010), 1405–1411.

[54] Z. Füredi, "An upper bound on Zarankiewicz' problem", *Combin. Probab. Comput.* **5**:1 (1996), 29–33.

[55] M. Hall, *Combinatorial theory*, Blaisdell Publ., Waltham, MA–Toronto–London 1967.

[56] V. E. Alekseev, "Two constructions of difference sets", *Probl. Kibernet.*, vol. 38, Nauka, Moscow 1981, pp. 259–262. (Russian)

[57] J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers", *Illinois J. Math.* **6** (1962), 64–94.

[58] W. G. Brown, "On graphs that do not contain a Thomsen graph", *Canad. Math. Bull.* **9** (1966), 281–285.

[59] A. I. Borevich and I. R. Shafarevich, *Number theory*, 3rd ed., Nauka, Moscow 1985; English transl. of 1st ed., Academic Press, New York–London 1966.

[60] S. B. Gashkov and I. S. Sergeev, "An application of the method of additive chains to inversion in finite fields", *Diskret. Mat.* **18**:4 (2006), 56–72; English transl. in *Discrete Math. Appl.* **16**:6 (2006), 601–618.

[61] N. Pippenger, "On the evaluation of powers and monomials", *SIAM J. Comput.* **9**:2 (1980), 230–250.

[62] P. Erdős and J. Spencer, *Probabilistic methods in combinatorics*, Wiley-Intersci. Ser. Discrete Math. Optim., Academic Press, New York–London 1974.

[63] A. E. Andreev, "On a family of Boolean matrices", *Vestnik Moskov. Univ. Ser.* 1 *Mat. Mekh.*, 1986, no. 2, 97–100; English transl. in *Moscow Univ. Math. Bull.* **41**:2 (1986), 79–82.

[64] S. B. Gashkov and I. S. Sergeev, "On the complexity of linear Boolean operators with thin matrices", *Diskret. Anal. Issled. Oper.* **17**:3 (2010), 3–18; English transl. in *J. Appl. Ind. Math.* **5**:2 (2011), 202–211.

[65] M. I. Grinchuk, "Complexity of implementing cyclic Boolean matrices by means of gate circuits", *Izv. Vyssh. Uchebn. Zaved. Mat.*, 1988, no. 7, 39–44; English transl. in *Soviet Math.* (*Iz. VUZ*) **32**:7 (1988), 65–72.

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

[67] K. Mehlhorn, "Some remarks on Boolean sums", *Acta Inf.* **12**:4 (1979), 371–375.

[68] S. B. Gashkov and I. B. Gashkov, "On the complexity of calculation of differentials and gradients", *Diskret. Mat.* **17**:3 (2005), 45–67; English transl. in *Discrete Math. Appl.* **15**:4 (2005), 327–350.

[69] A. V. Aho, J. E. Hopcroft and J. D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, Reading, MA 1974.

[70] A. Shpilka and A. Yehudayoff, "Arithmetic circuits: a survey of recent results and open questions", *Found. Trends Theor. Comput. Sci.* **5**:3–4 (2010), 207–388.

[71] I. Wegener, *The complexity of Boolean functions*, Wiley-Teubner Ser. Comput. Sci., Wiley, Stuttgart 1987.

[72] N. Blum, "On negations in Boolean networks", *Efficient algorithms*, Lecture Notes in Comput. Sci., vol. 5760, Springer-Verlag, Berlin–Heidelberg 2009, pp. 18–29.

S. B. Gashkov
Faculty of Mechanics and Mathematics,
Moscow State University
E-mail: sbgashkov@gmail.com

I. S. Sergeev
Faculty of Mechanics and Mathematics,
Moscow State University
E-mail: isserg@gmail.com

Received 29/JUN/11 and 11/APR/12
Translated by A. PANKRAT'EV