Pavel V. Roldugin and Alexey V. Tarasov

Functions without short implicents. Part I: lower estimates of weights

DOI: 10.1515/dma-2016-0004
Received January 27, 2015

Abstract: The paper is concerned with n-place Boolean functions not admitting implicents of k variables, $1 \le k < n$. Estimates for the minimal possible weight $w(n,\ k)$ of such functions are obtained. It is shown that $w(n,\ 1) = 2, n = 2, 3, ...$, and $w(n,\ 2) \sim \log_2 n$ as $n \to \infty$, and moreover, for $k > 2$ there exists n_0 such that $w(n,\ k) > 2^{k-2} \cdot \log_2 n$ for all $n > n_0$.

Keywords: Boolean function, implicent, combinatorially complete matrix

Note: Originally published in *Diskretnaya Matematika* (2015) **27**, №2, 94–105 (in Russian).

Inroduction and an account of the results

We introduce some definitions and notation.

- V_n is the set of binary vectors of length n;
- E_f is the set of executive vectors of an n-place Boolean function $f(x_1, ..., x_n)$; that is, $E_f = \{(\alpha_1,\ ...,\ \alpha_n) \in V_n :\ f(\alpha_1,\ ...,\ \alpha_n) = 1\}$;
- $\|f\| = \left|E_f\right|$ is the weight of a function f;
- $\|\alpha\|$ is the weight of a vector $\alpha \in V_n$;
- $f \equiv g$ indicates the equality of Boolean functions f and g;
- $\bar{f} = f \oplus 1$ is the inversion of a function f;
- given a Boolean variable x and $\alpha \in \{0, 1\}$, we set

$$x^\alpha = \begin{cases} \bar{x}, & \alpha = 0; \\ x, & \alpha = 1. \end{cases}$$

An *implicent* of a Boolean function $f(x_1, ..., x_n)$ is a nonconstant Boolean function g such that $f \cdot g \equiv f$; this is equivalent to the inclusion $E_f \subseteq E_g$ (see [1]). A number of definitions similar to that of an implicent appear in the literature. For example, in [2]–[5] there is the definition of an annihilator of a Boolean function f: an *annihilator* of a function f is a function h such that $f \cdot h \equiv 0$. It is clear that h is an annihilator of a function f if and only if the function $\bar{h} = h \oplus 1$ is an implicent of a function f. Sometimes (see [7]) an implicent of a Boolean function f is called the upper analogue of a function f (see [4]). The well-known problem of minimizing a DNF (see [9]) involves the definition of an implicant of a Boolean function (a function g is called an *implicant* of a function f if $f \vee g = g$), which is dual to the concept of the implicent (see, for example, [3]). There is a straightforward relation between the concepts of the implicent and the implicant of a Boolean function f: g is an implicent of a function f if and only if $\bar{g}$ is an implicant of $\bar{f}$. Correspondingly, one may reformulate, with clear modifications, the main results of the paper in these terms.

The present paper is concerned with estimates of the minimal possible value of the weight of a Boolean function not admitting an implicent of at most k variables. Similar problems were addressed, for example, in

Pavel V. Roldugin: Moscow State Institute of Radio-Engineering, Electronics and Automation (Technical University), e-mail: PavRoldugin@rambler.ru
Alexey V. Tarasov: Moscow State Institute of Radio-Engineering, Electronics and Automation (Technical University) e-mail: alextar1@yandex.ru

the paper [5], which gives some conditions for the existence of annihilators with constraints on the number of essential variables. For example, Corollary 3 of the present paper may be derived easily from the results of [5]. On the other hand, in the study of annihilators of Boolean functions the main attention was paid to the study of the algebraic immunity of functions, which is defined as the smallest possible degree of an annihilator of a function f or $f \oplus 1$. A number of variables in the annihilator implies a constraint on its degree. However, the absence of annihilators of a function f depending on at most k variables does not in general impose any constraints on the value of the algebraic immunity of a function f.

By the *length* of a Boolean function we shall understand the number of its essential variables; the length of a constant function (0 or 1) will be assumed to be 0.

Let n and k, $n > k \geq 1$, be fixed natural numbers. We consider the class $G_n^{(k)}$ of n-place Boolean functions not admitting implicents of length not exceeding k. Note that for $n = k$ any n-place nonconstant function always has an implicent of length n (the function itself). Hence, this case is excluded from consideration. For $n > k \geq 1$ the class $G_n^{(k)}$ is nonempty—for example, it contains any function of n variables with weight $2^n - 1$. Indeed, if $E_f = V_n \setminus \{(\alpha_1, \ldots, \alpha_n)\}$ for a function f, then $f(x_1, \ldots, x_n) = x_1^{\alpha_1 \oplus 1} \vee \ldots \vee x_n^{\alpha_n \oplus 1}$. If g is an implicent of a function f, then by definition $E_f \subseteq E_g$ and $E_g \neq V_n$, and hence $E_f = E_g$; that is, $f \equiv g$. Clearly, all the variables of the function f are essential, and hence the length of the function g is n and is not k for $k < n$. Hence, the function f admits no implicents of length k. So, the class $G_n^{(k)}$ is nonempty for $k < n$.

Considering the above, we may correctly write $w(n, k)$ for the minimal weight of a function from the class $G_n^{(k)}$.

If a Boolean function of n variables has weight 0, then its implicents are all nonconstant Boolean functions of n variables. Hence, for any n and k, $n > k$, the identically zero function does not belong to the class $G_n^{(k)}$, and hence, $w(n, k) > 0$.

The purpose of the present paper is to find lower estimates of $w(n, k)$ for various n and k, $n > k$. For $k = 1$ the problem is very easily solved.

Assertion 1. *Let $n \geq 2$ be a natural number. Then $w(n, 1) = 2$.*

Proof. There are no functions of weight 1 without implicents of length 1, because if a function f assumes the value 1 on a unique tuple $(\alpha_1, \ldots, \alpha_n) \in V_n$, then $f(x_1, \ldots, x_n) = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, and hence the function $g = x_i^{\alpha_i}$ is an implicent of f. As a result, $w(n, 1) \geq 1$. Besides, one may directly indicate an n-place function of weight 2 not admitting implicents of length 1: this is the function $f(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n \vee \bar{x}_1 \cdot \ldots \cdot \bar{x}_n$. Indeed, $x_i^{\alpha} \cdot f = x_1^{\alpha} \cdot \ldots \cdot x_n^{\alpha} \neq x_1 \cdot \ldots \cdot x_n \vee \bar{x}_1 \cdot \ldots \cdot \bar{x}_n = f$ for any $i \in \overline{1, n}$ and $\alpha \in \{0, 1\}$. Hence, $w(n, 1) = 2$. □

In addition to the case $k = 1$ already considered, we succeeded in finding the exact value of $w(n, k)$ only for $k = 2$: below it will be shown that $w(n, k) \sim \log_2 n$ as $n \to \infty$. For $k \geq 3$, we shall prove that there exists n_0 such that $w(n, k) > 2^{k-2} \cdot \log_2 n$ for all $n \geq n_0$. Moreover, it will be shown that $\min\limits_{n>k} w(n, k) = 2^k$, and besides, if $w(n, k) = 2^k$, then $n = k + 1$.

1 Relation between functions without short implicents and combinatorially complete matrices

An implicent is called *elementary* if it may be written as an elementary disjunction. The following straightforward assertion allows one to reduce the study of functions without short implicents to the study of functions not admitting short elementary implicents.

Assertion 2. *A nonconstant Boolean function f has an implicent of length k if and only if it has an elementary implicent of length k.*

Proof. Let $g\left(x_{i_1},\ \ldots,\ x_{i_k}\right)$ be an implicent of a function $f\left(x_1,\ \ldots,\ x_n\right)$. We represent the function g as the principal conjunctive normal form (CNF):

$$g = \prod_{\left(a_1,\ \ldots,\ a_k\right)\in V_n\setminus E_g} \left(x_{i_1}^{a_1\oplus 1} \vee \ldots \vee x_{i_k}^{a_k\oplus 1}\right).$$

Consider any elementary disjunction $K = x_{i_1}^{a_1\oplus 1} \vee \ldots \vee x_{i_k}^{a_k\oplus 1}$, $\left(a_1,\ \ldots,\ a_k\right) \in V_n\setminus E_g$, of this principal CNF. It has k essential variables. Next, we have

$$f \cdot K \equiv \left(f \cdot g\right) \cdot K \equiv f \cdot \left(g \cdot K\right) \equiv f \cdot g \equiv f,$$

that is, K is an implicent of the function f.

The converse is obvious. □

The absence of elementary implicents in a Boolean function has an obvious combinatorial meaning. We need the following definition.

Definition 1. Let $k,\ 1 \le k < n$, be a natural number. A $(0,\ 1)$-matrix A of size $m \times n$ will be called *combinatorially complete of order k* if in any submatrix of A of size $m \times k$, for any Boolean vector $\overrightarrow{v}$ of length k, there exists a row coinciding with $\overrightarrow{v}$.

In other words, the submatrix formed by any k columns of the matrix A must contain each of the 2^k possible rows (not necessarily only once).

We indicate several straightforward properties of combinatorially complete matrices. It is clear that $m \ge 2^k \ge 2$ and that any matrix which is combinatorially complete of order k, $k \ge 2$, is combinatorially complete of order s for all $s < k$. It is also easy to show that the inversion of any column of a combinatorially complete matrix (that is, the inversion of all its entries) also gives a combinatorially complete matrix of the same order. In particular, the inversion of the matrix also produces a combinatorially complete matrix and augmenting a combinatorially complete matrix with any number of arbitrary rows also gives a combinatorially complete matrix of the same order.

We give an example. Let n and k be fixed, $n \ge k$. Consider the matrix A, whose rows are all possible vectors of length n and of weight k. The matrix A has $\binom{n}{k}$ rows. We choose arbitrary k columns of A. In each row of the matrix A, in the coordinates corresponding to the $n - k$ columns that were not chosen, one may place at most $(n - k)$ units; the remaining 1's will be in the chosen k columns. Hence, the so-obtained submatrix will contain all possible rows of length k and of weight at least $t = \max\{0, 2k - n\}$. Hence, for $n \ge 2k$, this submatrix will contain all rows of length k, which implies that the matrix A itself is combinatorially complete of order k.

In this example, the number m of rows in the matrix A with small fixed k and increasing n behaves as $O\left(n^k\right)$. However, it is possible to construct combinatorially complete matrices with substantially smaller number of rows. As a matter of fact, the present paper is concerned with finding the smallest number of rows of a combinatorially complete matrix. The underlying consideration here is that there is a straightforward relation between the combinatorially complete matrices and the Boolean functions not admitting elementary implicents. We denote by $\tilde{E}_f$ the matrix, whose rows are executive vectors of a Boolean function f of n variables; that is,

$$\tilde{E}_f = \begin{pmatrix} \left(\alpha_1^{(1)},\ \ldots,\ \alpha_n^{(1)}\right) \\ \ldots \\ \left(\alpha_1^{(\|f\|)},\ \ldots,\ \alpha_n^{(\|f\|)}\right) \end{pmatrix},$$

where $\left(\alpha_1^{(i)},\ \ldots,\ \alpha_n^{(i)}\right) \in E_f, i = \overline{1,\ \|f\|}$.

The following assertion is a natural generalization of the analogous fact for $k = 2$, which was proved in [8]. This fact is easily shown to be equivalent to Theorem 1.1 of [5].

Assertion 3. *A nonconstant function f has an elementary implicent of length k if and only if the matrix $\tilde{E}_f$ is not combinatorially complete of order k.*

Proof. Consider an elementary disjunction of length k : $g = x_{i_1}^{a_1} \vee ... \vee x_{i_k}^{a_k}$. This disjunction is an implicent of the function f if and only if $f \cdot g \equiv f \cdot \left(x_{i_1}^{a_1} \vee ... \vee x_{i_k}^{a_k}\right) \equiv f$. The last equality is equivalent to saying that the equality $f\left(x_1, \ ..., \ x_n\right) = 0$ should be satisfied on all vectors $\left(\alpha_1, \ ..., \ \alpha_n\right)$ such that $\alpha_{i_j} = a_j \oplus 1$, $j = \overline{1,k}$. In other words, among the executive vectors of the function f there are no such ones for which the values $a_1 \oplus 1, \ ..., \ a_k \oplus 1$ are, respectively, on the places $i_1, ..., i_k$. By definition, this happens if and only if the columns $i_1, ..., i_k$ of the matrix $\tilde{E}_f$ does not contain rows of the form $\left(a_1 \oplus 1, \ ..., \ a_k \oplus 1\right)$; that is, the matrix $\tilde{E}_f$ is not combinatorially complete of order k. □

Let $m_{\min}^{(k)}(n)$ be the smallest number of rows in a combinatorially complete matrix of order k with n columns, $n > k$.

Corollary 1. *Let n, k be natural numbers, $n > k \geq 1$. Then*

$$w(n, \ k) = m_{\min}^{(k)}(n).$$

Proof. From Assertion 3 it follows that if a Boolean function f of n variables has no implicents of length k and if its weight is $w(n, \ k)$, then the matrix $\tilde{E}_f$ with $w(n, \ k)$ rows and n columns is combinatorially complete of order k. Hence, $w(n, \ k) \geq m_{\min}^{(k)}(n)$. On the other hand, we consider a combinatorially complete matrix A of order k with $m_{\min}^{(k)}(n)$ rows and n columns. In this matrix there are no equal rows—otherwise, when deleting the repeated rows, we get a combinatorially complete matrix of order k with n columns and with smaller than $m_{\min}^{(k)}(n)$ rows, but this is impossible by the definition of $m_{\min}^{(k)}(n)$. In particular, the absence of equal rows means that $m_{\min}^{(k)}(n) \leq 2^n$. But in this case the matrix A may be looked upon as the matrix $\tilde{E}_f$ for the function f defined as follows: $E_f = \left\{\vec{A}_1, \ \vec{A}_2, \ ..., \ \vec{A}_{m_{\min}^{(k)}(n)}\right\}$, where $\vec{A}_i$ are the rows of the matrix A. The n-place function f of weight $m_{\min}^{(k)}(n)$ has no implicents by Assertion 3, and so we get the reverse inequality $w(n, \ k) \leq m_{\min}^{(k)}(n)$, which proves the corollary. □

Since the number of rows in a combinatorially complete matrices of order k is not smaller than 2^k, we get the first estimate for $w(n, \ k)$.

Corollary 2. *Let n, k be natural numbers, $n > k \geq 1$. Then*

$$w(n, \ k) \geq 2^k.$$

The dual problem to the problem of evaluating $m_{\min}^{(k)}(n)$ is the problem of finding, given a fixed number of rows m, the maximum possible value $n_{\max}^{(k)}(m)$ of the number of columns for which there a exists combinatorially complete matrix of order k and size $m \times n_{\max}^{(k)}(m)$. In the language of Boolean functions, this problem is reduced to searching, for fixed m and k, a function of weight m depending on the largest possible number of variables, but which has no implicents of length k.

We note that $m_{\min}^{(k)}(n)$ is defined for all $k \geq 1$; on the other hand, $n_{\max}^{(k)}(m)$ is defined only for $k > 1$, because for $k = 1$ one may take as a combinatorially complete matrix of order 1 the matrix $\begin{pmatrix} 0 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 \end{pmatrix}$, which has only two rows and arbitrary number of columns. Hence, we shall be concerned only with $k > 1$.

Given a fixed $k > 1$, $n_{\max}^{(k)}(m)$ is defined for all $m \geq 2^k$. The function $n_{\max}^{(k)}(m)$ is nondecreasing; that is, $n_{\max}^{(k)}(m) \leq n_{\max}^{(k)}(m+1)$, because according to the above a combinatorially complete matrix may be augmented with any number of rows. However, it is not yet proved that for any fixed k the function $n_{\max}^{(k)}(m)$ is strictly increasing (this fact was proved only for $k = 2$; see [8]). Similarly, since from a combinatorially complete matrix of order k with at most k columns one may delete any column to keep the matrix combinatorially complete, the function $m_{\min}^{(k)}(n)$, $n > k > 1$, is nondecreasing.

In some cases it is more easy to write explicitly the function $n_{\max}^{(k)}(m)$ than the function $m_{\min}^{(k)}(n)$ (the case $k = 2$ treated in [8] may serve as an example). The following question arises: how one may pass from the function $n_{\max}^{(k)}(m)$ to the function $m_{\min}^{(k)}(n)$ and employ Corollary 1 to Assertion 3 to evaluate $w(n, \ k)$?

The following result gives a relation between $m_{\min}^{(k)}(n)$ and $n_{\max}^{(k)}(m)$.

Assertion 4. *Let n_0, k be natural numbers, $n_0 > k > 1$. Then one of the following two cases is possible:*
1) for some natural number $m_0 \geq 2^k + 1$ the inequalities

$$n_{\max}^{(k)}(m_0 - 1) < n_0 \leq n_{\max}^{(k)}(m_0)$$

hold, hence, $m_{\min}^{(k)}(n_0) = m_0$, $w(n_0,\ k) = m_0$;
2) the inequality

$$n_0 \leq n_{\max}^{(k)}\left(2^k\right)$$

hold and therefore $m_{\min}^{(k)}(n_0) = 2^k$, $w(n_0,\ k) = 2^k$.

Proof. According to the above, the range of the function $n_{\max}^{(k)}(m)$, $m \geq 4$, $k > 1$, is bounded from below by $n_{\max}^{(k)}\left(2^k\right)$ and is unbounded from above, and hence for n_0 only one of the cases from the statement of the assertion is possible. Consider the first case: assume that there exists $m_0 \geq 2^k + 1$ such that $n_{\max}^{(k)}(m_0 - 1) < n_0 \leq n_{\max}^{(k)}(m_0)$. The inequality $n_0 \leq n_{\max}^{(k)}(m_0)$ means that there exists a combinatorially complete matrix of order k and of size $m_0 \times n_0$. It follows that $m_{\min}^{(k)}(n_0) \leq m_0$. We claim that $m_{\min}^{(k)}(n_0) = m_0$. We argue by *reductio ad absurdum*: suppose that $m_{\min}^{(k)}(n_0) = m_0'$ and $m_0' < m_0$. Then there exists a combinatorially complete matrix of size $m_0' \times n_0$. Augmenting this matrix with $m_0 - m_0' - 1$ arbitrary rows, we obtain a combinatorially complete matrix of order k and of size $(m_0 - 1) \times n_0$. In other words, $n_0 \leq n_{\max}^{(k)}(m_0 - 1)$, which contradicts the hypothesis. The second case is straightforward. □

The following assertion, enabling one to consider upper estimates of $n_{\max}^{(k)}(m)$ as lower estimates of $m_{\min}^{(k)}(n)$, and vice versa, has a simpler form.

Assertion 5. *Let n_0, m_0, k be natural numbers, $n_0 > k > 1$, $m_0 \geq 2^k$. Then $n_{\max}^{(k)}(m_0) < n_0$ if and only if $m_{\min}^{(k)}(n_0) > m_0$.*

Proof. Both inequalities are clearly equivalent to the fact that there does not exist a combinatorially complete matrix of order k and size $m_0 \times n_0$. □

In what follows we give lower estimates for $w(n,\ k)$: we estimate $n_{\max}^{(k)}(m)$ from above, and next, using Assertions 4 or 5, we obtain lower estimates of $m_{\min}^{(k)}(n)$, which in view of Corollary 1 to Assertion 3 are lower estimates for $w(n, k)$.

2 Upper estimates of $n_{\max}^{(k)}(m)$

We start with the consideration of combinatorially complete matrices of order k with smallest number of rows $m = 2^k$.

Assertion 6. *Let $k > 1$. Then $n_{\max}^{(k)}\left(2^k\right) = k + 1$.*

Proof. Consider a matrix A of size $2^k \times (k+1)$ which is combinatorially complete of order k. Its first k columns contain 2^k distinct rows. Hence, the set of all rows of the matrix A is the set of all bit strings of length $k+1$ of the form $\left\{\left(\alpha_1,\ \ldots,\ \alpha_k,\ \beta_{(\alpha_1,\ \ldots,\ \alpha_k)}\right) :\ (\alpha_1,\ \ldots,\ \alpha_k) \in V_k\right\}$.

We claim that the matrix A is combinatorially complete of order k if and only if, for any $i \in \overline{1,\ k}$,

$$\beta_{(\alpha_1,\ \ldots,\ \alpha_{i-1},\ 0,\ \alpha_{i+1},\ \ldots,\ \alpha_k)} \oplus \beta_{(\alpha_1,\ \ldots,\ \alpha_{i-1},\ 1,\ \alpha_{i+1},\ \ldots,\ \alpha_k)} = 1. \tag{1}$$

Indeed, the first k columns of A contain all possible 2^k rows. We take any other k columns of the matrix A; this is equivalent to choosing $i \in \overline{1,\ k}$ and considering the columns with numbers $1,\ 2,\ \ldots,\ i-1,\ i+1,\ \ldots,\ k,\ k+1$. In the so-chosen submatrix A_i we consider the first $k-1$ columns. We denote this submatrix (of size $2^k \times (k-1)$) by A_i'. The matrix A_i' contains as rows all possible vectors of length $k-1$, each vectors appears exactly two times. Correspondingly, in order to the matrix A_i contains as rows all vectors of length k,

it is necessary and sufficient that equal rows of the matrix A_i' are continued in the matrix A_i by distinct elements, but this means that (1) is satisfied.

We now consider the graph of the Boolean cube G_k, whose vertex set is the set V_k of binary vectors of length k, two vertices of the cube are adjacent if the corresponding vectors are neighbouring, that is, if they differ by exactly one component. It is known that the graph G_k is connected and bipartite: one colour class of G_k is formed by the vertices $(\alpha_1, \ldots, \alpha_k)$ of even weights, and the other colour class by the vertices of odd weight.

We note that the presence of the last column in the matrix A may be interpreted as labeling each vertex $(\alpha_1, \ldots, \alpha_k)$ of the graph G_k by a mark $\beta_{(\alpha_1, \ldots, \alpha_k)}$, which is 0 or 1. Equality (1) means that adjacent vertices of the graph are labeled differently, in other words, (1) is equivalent to saying that for each vertex $(\alpha_1, \ldots, \alpha_k)$ with the even number of 1's (in the first colour class of the graph G_k) the label $\beta_{(\alpha_1, \ldots, \alpha_k)}$ is equal to some $\nu \in \{0, 1\}$, while for each vertex $(\alpha_1, \ldots, \alpha_k)$ with odd number of 1's (in the second colour class of G_k) the label $\beta_{(\alpha_1, \ldots, \alpha_k)}$ is $\bar{\nu}$. We write this as follows: for any vector $(\alpha_1, \ldots, \alpha_k) \in V_k$

$$\alpha_1 \oplus \ldots \oplus \alpha_k \oplus \nu = \beta_{(\alpha_1, \ldots, \alpha_k)}. \tag{2}$$

In other words, the entire last column of the matrix A is determined by the value of ν. Hence, there are only two possible values of this column, one of these values being the inversion of the other one.

We next assume that there exists a combinatorially complete matrix B of order k of size $2^k \times (k+2)$. Considering submatrices $\left(B_1^{\downarrow}, \ldots, B_k^{\downarrow}, B_{k+1}^{\downarrow}\right)$ and $\left(B_1^{\downarrow}, \ldots, B_k^{\downarrow}, B_{k+2}^{\downarrow}\right)$, we obtain two matrices of size $2^k \times (k+1)$ which are combinatorially complete of order k. Next, by the above the columns $B_{k+1}^{\downarrow}$ and $B_{k+2}^{\downarrow}$ either coincide or one column is the negation of the other one. In both cases we arrive at a contradiction, because the consideration of the last two columns shows that the matrix B is not combinatorially complete of order 2.

Hence, the largest number of columns in a combinatorially complete matrix of order k is $k+1$, which shows that $n_{\max}\left(2^k\right) = k+1$. □

Let us now examine the case $m > 2^k$. In [8] the exact value $n_{\max}^{(2)}(m)$ for $k = 2$ was found:

$$n_{\max}^{(2)}(m) = \begin{cases} \frac{1}{2} \cdot \binom{2r}{r}, & m = 2r, \\ \binom{2r}{r-1}, & m = 2r+1, \end{cases} \qquad m \geq 4.$$

We next consider the case $k \geq 3$.

Assertion 7. *Let $k \geq 3$ and $m \geq 2^k$. Then*

$$n_{\max}^{(k)}(m) \leq n_{\max}^{(k-1)}\left(\left[\frac{m}{2}\right]\right) + 1.$$

Proof. Let A be a combinatorially complete matrix of order k and size $m \times n$, $n = n_{\max}^{(k)}(m)$. The property of being combinatorially complete is invariant under rearrangement of rows and columns of a matrix, and hence we may assume that in the first column the first t entries are 0, and the last $m - t$ ones are 1, where $2^{k-1} \leq t \leq m - 2^{k-1}$.

Let A_0 and A_1 be the submatrices formed, respectively, by the first t and the last $m-t$ rows and the $n-1$ last columns of the matrix A (Fig. 1).

$$A = \begin{array}{c} \overbrace{}^{n-1} \\ \left.\begin{matrix} t \\ m-t \end{matrix}\right\{ \end{array} \left(\begin{array}{c|c} \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & A_0 \\ \hline \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} & A_1 \end{array}\right).$$

Fig. 1

Since A is a combinatorially complete matrix of order k, it follows in particular that for any set of k columns of the form $A_1^{\downarrow},\ A_{i_1}^{\downarrow},\ ...,\ A_{i_{k-1}}^{\downarrow}$, $1 < i_1 < i_2 < ... < i_{k-1} \le n$, these columns contain any combination $(a_1,\ ...,\ a_k) \in V_k$. Besides, the combinations of the form $(0,\ a_2,\ ...,\ a_k)$ are contained in the one of the first t rows, while the combinations of the form $(1,\ a_2,\ ...,\ a_k)$ are contained in one of the rows with numbers $t+1, \ldots, m$.

This means that, for any set of $k-1$ columns of the form $A_{i_1}^{\downarrow},\ ...,\ A_{i_{k-1}}^{\downarrow}, 1 < i_1 < i_2 < ... < i_{k-1} \le n$, in these columns any combination $(a_2,\ ...,\ a_k) \in V_{k-1}$ occurs at least two times: in one of the first t rows and in one of the last $m-t$ rows. Hence, both the matrices A_0 and A_1 are combinatorially complete of order $k-1$.

Each of these matrices has $n-1$ columns, and hence, $n-1 \le n_{\max}^{(k-1)}(t)$ and $n-1 \le n_{\max}^{(k-1)}(m-t)$; that is,

$$n \le \min\left\{n_{\max}^{(k-1)}(t),\ n_{\max}^{(k-1)}(m-t)\right\} + 1.$$

It was noted above that the function $n_{\max}^{(k)}(m)$ is nondecreasing and since either $t \le \left[\frac{m}{2}\right]$ or $m-t \le \left[\frac{m}{2}\right]$, it follows that $\min\left\{n_{\max}^{(k-1)}(t),\ n_{\max}^{(k-1)}(m-t)\right\} \le n_{\max}^{(k-1)}\left(\left[\frac{m}{2}\right]\right)$. We thus arrive at the required inequality:

$$n_{\max}^{(k)}(m) \le n_{\max}^{(k-1)}\left(\left[\frac{m}{2}\right]\right) + 1.$$

□

As a corollary of this inequality we have the following estimate involving the function $n_{\max}^{(2)}(m)$.

Assertion 8. *Let $k \ge 3$ and $m \ge 2^k$. Then*

$$n_{\max}^{(k)}(m) \le n_{\max}^{(2)}\left(\left[\frac{m}{2^{k-2}}\right]\right) + k - 2.$$

Proof. We have $\left[\frac{[m/2]}{2}\right] = \left[\frac{m}{4}\right]$, and hence Assertion 7 implies that

$$n_{\max}^{(k)}(m) \le n_{\max}^{(k-2)}\left(\left[\frac{m}{4}\right]\right) + 2.$$

We iteratively find that, for any $r = 1,\ 2,\ ...,\ k-2$,

$$n_{\max}^{(k)}(m) \le n_{\max}^{(k-r)}\left(\left[\frac{m}{2^r}\right]\right) + r.$$

As a result, for $r = k-2$ we have

$$n_{\max}^{(k)}(m) \le n_{\max}^{(2)}\left(\left[\frac{m}{2^{k-2}}\right]\right) + k - 2.$$

□

In order to obtain an asymptotic estimate of the function $n_{\max}^{(k)}(m)$ we use the asymptotic formula for $n_{\max}^{(2)}(m)$.

Assertion 9. *Let $k \ge 3$ be a fixed number. Then, as $m \to \infty$,*

$$n_{\max}^{(k)}(m) \le 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}} \cdot (1 + o(1)).$$

Proof. From Corollary 4 to Theorem 1 of [8] if follows that as $m \to \infty$

$$n_{\max}^{(2)}(m) = \frac{2^m}{\sqrt{2\pi m}}\left(1 + \phi(m)\right), \quad \lim_{m\to\infty} \phi(m) = 0. \tag{3}$$

Substituting this relation in the estimate from Assertion 8, we find that

$$n_{\max}^{(k)}(m) \le \frac{2^{\left[\frac{m}{2^{k-2}}\right]}}{\sqrt{2\pi\left[\frac{m}{2^{k-2}}\right]}} \cdot \left(1 + \phi(m)\right) + k - 2.$$

Taking into account that $\frac{m}{2^{k-2}} - 1 \le \left[\frac{m}{2^{k-2}}\right] \le \frac{m}{2^{k-2}}$ for $k > 0$, we obtain

$$n_{\max}^{(k)}(m) \le \frac{2^{\frac{m}{2^{k-2}}}}{\sqrt{2\pi\left(\frac{m}{2^{k-2}} - 1\right)}} \cdot \left(1 + \phi(m)\right) + k - 2 \le$$

$$\le \sqrt{\frac{2^{k-3}}{\pi}} \cdot \frac{2^{\frac{m}{2^{k-2}}}}{\sqrt{m}} \cdot \left(\left(1 - \frac{2^{k-2}}{m}\right)^{-1/2} \cdot \left(1 + \phi(m)\right) + (k-2) \cdot \sqrt{\frac{\pi}{2^{k-3}}} \cdot \frac{\sqrt{m}}{2^{\frac{m}{2^{k-2}}}}\right). \tag{4}$$

Since $k \ge 3$, we have $\sqrt[2^{k-2}]{2} > 1$, and hence, $\frac{\sqrt{m}}{\left(\sqrt[2^{k-2}]{2}\right)^m} \underset{m\to\infty}{\to} 0$. Besides, $\frac{2^{k-2}}{m} \underset{m\to\infty}{\to} 0$. Consequently, the right-hand side of inequality (4) is $2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}}\left(1 + \phi(m)\right) = 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}}\left(1 + o(1)\right)$ as $m \to \infty$. □

3 Lower estimates of $m_{\min}^{(k)}(n)$

In this section we give lower estimates of $m_{\min}^{(k)}(n)$, which follow from the upper estimates of $n_{\max}^{(k)}(m)$ obtained in the previous section.

We start with the equality $n_{\max}^{(k)}\left(2^k\right) = k + 1, k > 1$ (see Assertion 6). This result can be formulated as the following refinement of Corollary 2 to Assertion 3: if $w(n,\ k) = 2^k$, then $n = k + 1$. In other words, among all Boolean functions not admitting implicents of length not exceeding k, the functions with the smallest weight (which is 2^k) depend on at most $k+1$ variables, this estimate being attainable. This estimate is attained at the functions f, for which, by (2), the equality $\alpha_1 \oplus \ldots \oplus \alpha_k \oplus \nu = \alpha_{k+1}$ with some fixed $\nu \in \{0,\ 1\}$ holds for any vector $(\alpha_1,\ \ldots,\ \alpha_{k+1}) \in E_f$. It is clear that there are only two such functions: $f(x_1,\ \ldots,\ x_{k+1}) = x_1 \oplus \ldots \oplus x_{k+1}$ and $f(x_1,\ \ldots,\ x_{k+1}) = x_1 \oplus \ldots \oplus x_{k+1} \oplus 1$. Hence, we have the following result.

Assertion 10. *The smallest weight of a Boolean functions without implicents of $k > 1$ variables is 2^k, this estimate is attained at the following two functions: $f(x_1,\ \ldots,\ x_{k+1}) = x_1 \oplus \ldots \oplus x_{k+1}$, $f(x_1,\ \ldots,\ x_{k+1}) = x_1 \oplus \ldots \oplus x_{k+1} \oplus 1$.*

An important particular case of Assertion 10 is the case $k = n-1$. We claim that if a function has an implicent of k variables, then it also has an implicent of k' variables for all k', $n > k' > k$. Indeed if g is an implicent of length k of a function $f(x_1,\ \ldots,\ x_n)$ and if x_i is a dummy variable of g, then the function $x_i \vee g$ is also an implicent of f of length $k+1$:

$$f \cdot (x_i \vee g) = \begin{cases} f, & x_i = 1, \\ f \cdot g = f, & x_i = 0. \end{cases}$$

As a result, the expression 'an n-place function does not have an implicent of $n-1$ variables' is equivalent to the expression 'an n-place function has no implicents of smaller number of variables'. Hence, using Assertion 10 with $k = n-1$ we reach the following result.

Corollary 3. *Any n-place equiprobable Boolean function distinct from the functions $f(x_1,\ \ldots,\ x_n) = x_1 \oplus \ldots \oplus x_n$ and $f(x_1,\ \ldots,\ x_n) = x_1 \oplus \ldots \oplus x_n \oplus 1$ has an implicent of smaller number of variables.*

We note that this result may also be easily obtained from the results of [5].

Our next aim is to obtain an asymptotically exact formula for $m_{\min}^{(2)}(n)$.

Assertion 11. *The asymptotic equality holds as $n \to \infty$:*

$$m_{\min}^{(2)}(n) \sim \log_2 n.$$

Proof. We first show that $m_{\min}^{(2)}(n) \to \infty$ as $n \to \infty$. Given any $m_0 \ge 2^k > 4$, we set $n_0 = n_{\max}^{(2)}(m_0)$. Hence, $n_{\max}^{(2)}(m_0) < n$ for any $n > n_0$. In view of Assertion 5 the last inequality is equivalent to the inequality

$m^{(2)}_{\min}(n) > m_0$. In other words, for any $m_0 > 4$ there exists n_0 such that $m^{(2)}_{\min}(n) > m_0$ for all $n > n_0$. But this means that $m^{(2)}_{\min}(n) \to \infty$ as $n \to \infty$.

The function $n^{(2)}_{\max}(m)$ is nondecreasing, and hence Assertion 6 implies that the minimal value of $n^{(2)}_{\max}(m)$ is 3. Inserting this value in Assertion 4, we have the following result: for any $n \geq 4$ there exists $m \geq 5$ such that $m^{(2)}_{\min}(n)$ satisfies the inequalities

$$n^{(2)}_{\max}\left(m^{(2)}_{\min}(n) - 1\right) < n \leq n^{(2)}_{\max}\left(m^{(2)}_{\min}(n)\right). \tag{5}$$

We have $m^{(2)}_{\min}(n) \to \infty$ as $n \to \infty$, and hence it follows from the formula (3) in the proof of Assertion 9 and inequalities (5) that

$$\frac{2^{m^{(2)}_{\min}(n)-1}}{\sqrt{2\pi \cdot \left(m^{(2)}_{\min}(n) - 1\right)}}\left(1 + \phi\left(m^{(2)}_{\min}(n) - 1\right)\right) \quad < \quad n \quad \leq \quad \frac{2^{m^{(2)}_{\min}(n)}}{\sqrt{2\pi \cdot m^{(2)}_{\min}(n)}}\left(1 + \phi\left(m^{(2)}_{\min}(n)\right)\right).$$

Setting $\delta(m) = \log_2\left(1 + \phi(m)\right)$ and taking $\log_2$ of both sides, we get

$$m^{(2)}_{\min}(n) - 1 - \frac{1}{2}\log_2 2\pi - \frac{1}{2}\log_2\left(m^{(2)}_{\min}(n) - 1\right) + \delta\left(m^{(2)}_{\min}(n) - 1\right) < \log_2 n \leq$$

$$\leq m^{(2)}_{\min}(n) - \frac{1}{2}\log_2 2\pi - \frac{1}{2}\log_2 m^{(2)}_{\min}(n) + \delta\left(m^{(2)}_{\min}(n)\right),$$

and so,

$$m^{(2)}_{\min}(n) - 1 - \tfrac{1}{2}\log_2\left(m^{(2)}_{\min}(n) - 1\right) + \delta\left(m^{(2)}_{\min}(n) - 1\right) < \log_2 n \leq$$

$$\leq m^{(2)}_{\min}(n) - \tfrac{1}{2}\log_2 m^{(2)}_{\min}(n) + \delta\left(m^{(2)}_{\min}(n)\right).$$

Hence,

$$\begin{aligned} &1 - \frac{1}{m^{(2)}_{\min}(n)} - \frac{\log_2\left(m^{(2)}_{\min}(n)-1\right)}{2\cdot m^{(2)}_{\min}(n)} + \frac{\delta\left(m^{(2)}_{\min}(n)-1\right)}{m^{(2)}_{\min}(n)} < \frac{\log_2 n}{m^{(2)}_{\min}(n)} \leq \\ &\leq 1 - \frac{\log_2 m^{(2)}_{\min}(n)}{2\cdot m^{(2)}_{\min}(n)} + \frac{\delta\left(m^{(2)}_{\min}(n)\right)}{m^{(2)}_{\min}(n)}. \end{aligned} \tag{6}$$

Further, we have $\lim\limits_{m\to\infty}\phi(m) = 0$, and so $\lim\limits_{m\to\infty}\log_2\left(1 + \phi(m)\right) = 0$. Next, we recall that $m^{(2)}_{\min}(n) \to \infty$ as $n \to \infty$. Hence, making $n \to \infty$,

$$\delta\left(m^{(2)}_{\min}(n)\right) \to 0,\ \delta\left(m^{(2)}_{\min}(n) - 1\right) \to 0,\ \frac{\log_2\left(m^{(2)}_{\min}(n) - 1\right)}{2 \cdot m^{(2)}_{\min}(n)} \to 0 \text{ and } \frac{\log_2 m^{(2)}_{\min}(n)}{2 \cdot m^{(2)}_{\min}(n)} \to 0.$$

As a result, using (6) we get $\frac{\log_2 n}{m^{(2)}_{\min}(n)} = 1 + o(1)$, the result required. □

Let us now estimate $m^{(k)}_{\min}(n)$ from below for $k \geq 3$.

Assertion 12. *Let $k \geq 3$ be a fixed number. Then there exists n_0 such that, for all $n \geq n_0$,*

$$m^{(k)}_{\min}(n) > 2^{k-2} \cdot \log_2 n.$$

Proof. From Assertion 9 it follows that, for any constant $C > 1$, there exists m_0 such that, for all $m > m_0$,

$$n^{(k)}_{\max}(m) < C \cdot 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}}. \tag{7}$$

We extend the function $n^{(k)}_{\max}(m)$ to all $x \geq 2^k$ as follows: $n^{(k)}_{\max}(x) = n^{(k)}_{\max}([x])$. It is clear that the function $n^{(k)}_{\max}(x)$ is also nondecreasing. Besides, for any real $x \geq 2^k$ and any natural $n_0 > k$ the inequality

$n^{(k)}_{\max}(x) < n_0$ holds if and only if $n^{(k)}_{\max}([x]) < n_0$. By Assertion 5 the last inequality is equivalent to the inequality $m^{(k)}_{\min}(n_0) > [x]$. The function $m^{(k)}_{\min}(n)$ assumes only natural values, and consequently, $m^{(k)}_{\min}(n_0) \geq [x] + 1 > x$. Hence, if $n^{(k)}_{\max}(x) < n_0$, then $m^{(k)}_{\min}(n_0) > x$.

Next, let $\theta_m = C \cdot 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}}$. Then

$$2^{k-2} \cdot \log_2 \theta_m = m + 2^{k-2} \cdot \left(\log_2 C + \frac{k-3}{2} - \frac{1}{2}\log_2 \pi - \frac{1}{2}\log_2 m \right).$$

For sufficiently large m we have

$$\log_2 C + \frac{k-3}{2} - \frac{1}{2}\log_2 \pi - \frac{1}{2}\log_2 m < 0,$$

and hence, $2^{k-2} \cdot \log_2 \theta_m < m$.

The function $n^{(k)}_{\max}(m)$ is nondecreasing, and now (7) implies that

$$n^{(k)}_{\max}\left(2^{k-2} \cdot \log_2 \theta_m\right) \leq n^{(k)}_{\max}(m) < \theta_m.$$

Hence, by the above, $m^{(k)}_{\min}(\theta_m) > 2^{k-2} \cdot \log_2 \theta_m$.

Setting $n_0(n) = 2^{k-2} \cdot \log_2 n$, we have $\theta_{n_0(n)} = n \cdot \frac{C}{\sqrt{2\pi \cdot \log_2 n}} < n$ for all sufficiently large n. The function $m^{(k)}_{\min}(n)$, $n > k > 1$, is nondecreasing and hence,

$$m^{(k)}_{\min}(n) \geq m^{(k)}_{\min}\left(\theta_{n_0(n)}\right) > 2^{k-2} \cdot \log_2 \theta_{n_0(n)} =$$

$$= n_0(n) + 2^{k-2} \cdot \left(\log_2 C + \frac{1}{2}\log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2}\log_2 n_0(n) \right) =$$

$$= 2^{k-2} \cdot \log_2 n + 2^{k-2} \cdot \left(\log_2 C + \frac{1}{2}\log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2}(k-2) - \frac{1}{2}\log_2 \log_2 n \right) =$$

$$= 2^{k-2} \cdot \log_2 n \left(1 + \frac{1}{\log_2 n} \cdot \left(\log_2 C + \frac{1}{2}\log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2}(k-2) - \frac{1}{2}\log_2 \log_2 n \right) \right).$$

It remains to observe that $\frac{1}{\log_2 n} \cdot \left(\log_2 C + \frac{1}{2}\log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2}(k-2) - \frac{1}{2}\log_2 \log_2 n \right) < 0$ for all $n \geq n_0$ starting with some n_0. □

References

[1] Glushkov V. M., *Synthesis of digital authomata*, M.: GIFML, 1962 (in Russian).

[2] Courtois N., Meier W., "Algebraic attacks on stream ciphers with linear feedback", EUROCRYPT, Lect. Notes Comput. Sci., **2656**, Springer-Verlag, 2003, 346-359.

[3] Logachev O.A., Sal'nikov A.A., Smyshlyaev S.V., Yashchenko V.V., *Boolean function in coding theory and cryptology*, M.: MCCME, 2012, 583 pp.

[4] Dalai D., Maitra S., Sarkar S., "Basic theory in construction of Boolean functions with maximum possible annihilator immunity", *Designs, Codes and Cryptography*, **40**:1 (2006), 41-58.

[5] Jiao L., Wang M., Li Y., Liu M., "On annihilators in fewer variables: basic theory and applications", *Chinese Journal of Electronics*, **22**:3 (2013), 489-494.

[6] Glukhov M.M., Shishkov A.B., *Mathematical logic. Discrete function. Theory of algorithms*, SPb.: Lan, 2012 (in Russian).

[7] Gorshkov S.P., "Application of the theory of NP-complete task for the estimate of the complexity of solving of Boolean equation systems", *Obozr. prikl. and prom. matem.*, **2**:3 (1995), 325–399 (in Russian).

[8] Roldugin P.V., Tarasov A.V., "On Boolean functions without upper bijunctive counterparts", *Matematiceskie voprosy kriptografii*, **4**:1 (2013), 123–140 (in Russian).

[9] *Vocabulary of cryptographic terms*, eds. B.A. Pogorelova and V.N. Sachkova, M.: MCCME, 2006 (in Russian).