Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters

Yuriy Tarannikov [*]

Mech. & Math. Department
Lomonosov Moscow State University
119991 Moscow, Russia
email: taran@butovo.com

ABSTRACT. Nonlinearity and resiliency are well known as some of the most important cryptographic parameters of Boolean functions, it is actual the problem of the constructing of functions that have high nonlinearity and resiliency simultaneously. In 2000 three groups of authors obtained independently the upper bound $2^{n-1}-2^{m+1}$ for the nonlinearity of an m-resilient function of n variables. It was shown that if this bound is achieved then $(n-3)/2 \leq m \leq n-2$. Simultaneously in 2000 Tarannikov constructed functions that achieve this bound for $(2n-7)/3 \leq m \leq n-2$. In 2001 Tarannikov constructed such functions for $0.6n-1 \leq m$ introducing for this aim so called proper matrices; later in 2001 Fedorova and Tarannikov constructed by means of proper matrices the functions that achieve the bound $2^{n-1}-2^{m+1}$ for $m \geq cn(1+o(1))$ where $c = 1/\log_2(\sqrt{5}+1) = 0.5902...$ but proved simultaneously that by means of proper matrices it is impossible to improve this result. During the period since 2001 it was not any further progress in the problem on the achievability of the bound $2^{n-1}-2^{m+1}$ in spite of this problem was well known and actual except the constructing in 2006–2007 by three groups of authors by means of a computer search concrete functions for $n = 9$, $m = 3$. In this paper we find the new approach that uses the generalization of the concept of proper matrices. We formulate combinatorial problems solutions of which allow to construct generalized proper matrices with parameters impossible for old proper matrices. As a result we obtain the constructions of m-resilient functions of n variables with maximal nonlinearity for $m \geq cn(1+o(1))$ where $c = 0.5789...$, and also we demonstrate how further advance in combinatorial problems follows an additional decrease of the constant c.

Keywords: Boolean functions, symmetric-key cryptography, nonlinearity, resiliency, maximal possible nonlinearity, bounds, plateaued functions, constructions, implementation complexity.

[*] This work is supported by RFBR, grant 13-01-00183-a.

1 Introduction

Nonlinearity and correlation immunity (resiliency) belong to the number of the most important cryptographic characteristics of Boolean functions required for the resistance of cryptosystems (in particular, ciphers) with Boolean functions as building blocks against linear, correlation and other kinds of cryptographic attacks. Therefore it is very desirable that functions used in ciphers have high nonlinearity and resiliency simultaneously. However, in 2000 [11, 15, 20] it was proved the upper bound for the nonlinearity of m-resilient functions on $\mathbf{F}_2^n$:

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^{m+1}$$

for $m \leq n-2$, and it was shown that if an equality in this bound is achieved then $\frac{n-3}{2} \leq m \leq n-2$. Hence, it has become important the problem of the constructing of functions that achieve an equality in this bound (as said, the constructing of functions with maximal possible nonlinearity). After some steps of consecutive improvements in 2001 Fedorova and Tarannikov [3] obtained the best result before a long break: they constructed m-resilient functions on $\mathbf{F}_2^n$ with maximal possible nonlinearity for $0.5902...n(1+o(1)) \leq m \leq n-2$ but proved simultaneously that by means of used technique of proper matrices it is impossible to decrease the constant 0.5902... During the following period it was not any further progress in this problem except the constructing of concrete functions on small number of variables ($n = 9$, $m = 3$) by means of a computer search. At the same time in recent years it is studied intensively the problem on the constructing of functions with high nonlinearity for small (constant) values of m, we can mention the works [4, 5, 14, 17, 19]. The reason of such shift of interest was the difficulty of the problem on the constructing of functions with maximal possible nonlinearity and a research stagnation in this problem as well as an opinion that the nonlinearity is some more important cryptographic property whereas for the resiliency it is sufficient to have a constant order. However, from a practical point of view the nonlinearity is not important so much as the *relative nonlinearity,* i. e. the value $\frac{\mathrm{nl}(f)}{2^n}$. More exactly, the deviation of relative nonlinearity from 0.5 is important. From well-known upper bound for the nonlinearity of an arbitrary Boolean function $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ it follows that the deviation of relative nonlinearity of any Boolean function on $\mathbf{F}_2^n$ from 0.5 is at least $\frac{1}{2^{\frac{n}{2}+1}}$; at the same time, if to construct an m-resilient function on $\mathbf{F}_2^n$ with maximal possible nonlinearity $2^{n-1} - 2^{m+1}$ for m close to $0.5n$ then the deviation of its relative nonlinearity from 0.5 will be equal to $\frac{1}{2^{n-m-1}}$, i. e. close to the lower bound of the best possible deviation. Therefore a progress in the problem of the constructing of an m-resilient function on $\mathbf{F}_2^n$ with maximal possible nonlinearity $2^{n-1} - 2^{m+1}$ for m close to $0.5n$ is still important since it allows to combine the nonlinearity close to optimal with very high resiliency.

In this paper the new approach is found. This approach uses the generalization of the concept of proper matrices. New combinatorial problems are formulated. The solutions of these problems allow to construct the generalized proper matrices with parameters impossible for simply proper matrices. As a result we obtain constructions of m-resilient functions of n variables with maximal nonlinearity for $m \geq cn(1+o(1))$ where $c = 0.5789...$, and also we demonstrate how further advance in combinatorial problems follows an additional decrease of the constant c.

2 General information and the history of the problem

We consider $\mathbf{F}_2^n$, the space of vectors of the length n with components from $\mathbf{F}_2$. *A Boolean function* of n variables is a mapping from $\mathbf{F}_2^n$ to $\mathbf{F}_2$. We shall denote a function f of n variables also in the form $f(x) = f(x_1, x_2, \ldots, x_n)$ implying that variables x_1, x_2, $\ldots$, x_n correspond uniquely to components of $\mathbf{F}_2^n$. Below we denote the vector from $\mathbf{F}_2^n$ by a letter without a low index whereas a component of this vector by the same letter with the low index that points to the ordinal number of this component in the vector.

The weight $|x|$ of the vector x from $\mathbf{F}_2^n$ is the number of ones in x. *The weight* $\mathrm{wt}(f)$ of a function f on $\mathbf{F}_2^n$ is the number of vectors x from $\mathbf{F}_2^n$ such that $f(x) = 1$. A function f is called *balanced* if $\mathrm{wt}(f) = \mathrm{wt}(f \oplus 1) = 2^{n-1}$ (i. e. a function takes the values 0 and 1 at the same numbers of vectors. *A subfunction* of a Boolean function f is the function f' obtained by the substitution into f some constants 0 or 1 instead of some variables.

It is well known that a function f defined on $\mathbf{F}_2^n$ has the unique polynomial representation over $\mathbf{F}_2$ which degree on each variable does not exceed 1, namely

$$f(x_1, \ldots, x_n) = \bigoplus_{(a_1, \ldots, a_n) \in F_2^n} g(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}$$

where g is also some function on $\mathbf{F}_2^n$. Such polynomial representation of f is called the *algebraic normal form* (briefly, ANF) of the function f, and each monomial $x_1^{a_1} \ldots x_n^{a_n}$ is called *the term* in ANF of the function f.

The algebraic degree of a function f denoted by $\deg(f)$ is defined as the number of variables in the longest term in ANF of the function f. *The algebraic degree of a variable* x_i in function f denoted by $\deg(f, x_i)$ is the number of variables in the longest term in ANF of the function f that contains x_i. If $\deg(f, x_i) = 1$ then we say that f depends on x_i *linearly.* The term of the length 1 is called a *linear* term. If $\deg(f) \leq 1$ then f is called the *affine* function. If f is an affine function and $f(0) = 0$ then f is called the *linear* function.

The Hamming distance $d(x', x'')$ between two vectors x' and x'' is the number of components where vectors x' and x'' differ. For two Boolean functions f_1 and f_2 on $\mathbf{F}_2^n$ the distance between f_1 and f_2 is defined as $d(f_1, f_2) = |\{x \in \mathbf{F}_2^n | f_1(x) \neq f_2(x)\}|$. It is easy to see that $d(f_1, f_2) = \mathrm{wt}(f_1 \oplus f_2)$. For given function f from $\mathbf{F}_2^n$ the minimum of distances $d(f, l)$ where l is running through the set of all affine functions on $\mathbf{F}_2^n$ is called *the nonlinearity* of f and is denoted by $\mathrm{nl}(f)$.

Let $x = (x_1, \ldots, x_n)$ and $u = (u_1, \ldots, u_n)$ be vectors of the length n over $\mathbf{F}_2$. *The inner product* of x and u is defined as

$$< x, u >= \sum_{i=1}^{n} x_i u_i.$$

We assume that the sum $x + u$ of two vectors x and u from $\mathbf{F}_2^n$ is their component-wise addition over $\mathbf{F}_2$.

The Walsh Transform of a Boolean function f is the integer-valued function on $\mathbf{F}_2^n$ defined as follows:

$$W_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x) + <u,x>}.$$

For each $u \in F_2^n$ the value $W_f(u)$ is called the *Walsh coefficient* or the *spectral coefficient.* The collection of Walsh coefficients $W_f(u)$ of the function f for all vectors $u \in \mathbf{F}_2^n$ is called *the* *spectrum* of the function f. The collection of all vectors $u \in \mathbf{F}_2^n$ such that $W_f(u) \neq 0$ is called *the spectrum support* of the function f.

The set of all Walsh coefficients of a Boolean function f on $\mathbf{F}_2^n$ satisfies the *Parseval's Equality*:

$$\sum_{u \in \mathbf{F}_2^n} W_f^2(u) = 2^{2n}.$$

It is well known that the nonlinearity of a function f on $\mathbf{F}_2^n$ is expressed via its Walsh coefficients by formula

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbf{F}_2^n} |W_f(u)|. \tag{1}$$

A Boolean function f is called *plateaued* if there exists the positive integer c such that for any vector $u \in \mathbf{F}_2^n$ we have $W_f(u) \in \{0, \pm 2^c\}$.

A Boolean function f defined on $\mathbf{F}_2^n$ is called *correlation-immune of order* m, $1 \leq m \leq n$, if the output of f and any set of m its input variables are statistically independent. This concept was introduced by Siegenthaler [13]. In an equivalent non-probabilistic formulation a Boolean function f is called correlation-immune of order m if $\mathrm{wt}(f') = \mathrm{wt}(f)/2^m$ for any its subfunction f' of $n-m$ variables. The balanced correlation-immune function of order m is called *m-resilient.* In other words, a Boolean function f is called m-resilient if $\mathrm{wt}(f') = 2^{n-m-1}$ for any its subfunction f' of $n-m$ variables. From this point of view we can formally consider any balanced Boolean function as 0-resilient and an arbitrary Boolean function as (-1)-resilient (a function of n variables has not a subfunction of $n+1$ variables, therefore for any its subfunction of $n+1$ variables all statements hold). The concept of an m-resilient function was introduced in [2].

There is the characterization of a correlation-immune function via its Walsh coefficients. For the first time this characterization was obtained in [18].

Lemma 1 *[18] A function f on $\mathbf{F}_2^n$ is the correlation-immune function of order m if and only if $W_f(u) = 0$ for all vectors $u \in \mathbf{F}_2^n$ such that $1 \leq |u| \leq m$.*

It is easy to see that a function f is balanced if and only if $W_f(0) = 0$. Therefore the next corollary holds.

Corollary 1 *A function f on $\mathbf{F}_2^n$ is m-resilient if and only if $W_f(u) = 0$ for all vectors $u \in \mathbf{F}_2^n$ such that $|u| \leq m$.*

It holds also the next property of Walsh coefficients of correlation-immune functions [11].

Lemma 2 *[11] If f is a correlation-immune function of order m on $\mathbf{F}_2^n$, $m \leq n-1$, then for any $u \in \mathbf{F}_2^n$ the formula $W_f(u) \equiv 0 \pmod{2^{m+1}}$ holds. Moreover, if f is m-resilient, $m \leq n-2$, then $W_f(u) \equiv 0 \pmod{2^{m+2}}$.*

In [11, 15, 20] it was proved the upper bound for the nonlinearity of correlation-immune functions.

Lemma 3 *[11, 15, 20] Let f be a correlation-immune of order m Boolean function on $\mathbf{F}_2^n$, $m \leq n-1$. Then the inequality*

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^m \tag{2}$$

holds. Moreover, if f is an m-resilient Boolean function on $\mathbf{F}_2^n$, $m \leq n-2$, then the inequality

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^{m+1} \tag{3}$$

holds.

Corollary 2 *If in Lemma 3 in formulas (2) or (3) an exact equality is achieved then the function f must be plateaued.*

Proof. The corollary follows immediately from the representation (1), Lemma 2 and the definition of plateaued functions. □

Thus, if an equality in bounds (2) or (3) is achieved then the function f is plateaued, its Walsh coefficients take values only from the set $\{0, \pm 2^{m+1}\}$ for the bound (2) and $\{0, \pm 2^{m+2}\}$ for the bound (3). Conversely, if Walsh coefficients of a function f on $\mathbf{F}_2^n$ take values only from the set $\{0, \pm 2^{m+a}\}$ then $\mathrm{nl}(f) = 2^{n-1} - 2^{m+a-1}$.

Khalyavin proved [22] that if in (2) an exact equality is achieved then either $n = 2^{s+1}+1$, $m = 2^s$, or $n = 2^{s+1}+2$, $m = 2^s+1$ for some positive integer s. Examples of functions that achieve an equality in the bound (2) for $n = 5$, $m = 2$ and $n = 6$, $m = 3$ are given in [15] and for $n = 9$, $m = 4$ and $n = 10$, $m = 5$ were constructed by Khalyavin in [21, 23].

The remained part of this paper is devoted to the constructing of functions that achieve an equality in the bound (3).

Note that if in the bound (3) an exact equality is achieved then $\frac{n-3}{2} \leq m \leq n-2$ since in the case $\frac{n-3}{2} > m$ for m-resilient Boolean functions on $\mathbf{F}_2^n$ there is more strong bound

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$$

that was proved in [11].

Even before obtaining the bound (3) different researchers ([1, 12] etc.) proposed constructions of m-resilient functions on $\mathbf{F}_2^n$ that achieve an equality in (3) for $n - m = O(\log_2 n)$. Tarannikov in 2000 [15] constructed functions that achieve an equality in (3) for $\frac{2n-7}{3} \leq m \leq n-2$. In [9] Pasalic, Maitra, Johansson and Sarkar modifying constructions from [15] expanded the achievability range of the bound (3) till $\frac{2n-8}{3} \leq m \leq n-2$, $n \geq 7$. In [16] Tarannikov by means of proper matrices constructed functions that achieve an equality in (3) for $0.6n - 1 \leq m \leq n-2$. In 2001 Fedorova and Tarannikov [3] constructed functions that achieve an equality in (3) for $m \geq 0.5902...n(1+o(1))$ but proved simultaneously that by means of proper matrices it is impossible to decrease the constant $0.5902... = \frac{1}{\log_2(\sqrt{5}+1)}$. During the next more than 10 years it was not any progress in the problem on the constructing of functions achieving an equality in (3) except the constructing in 2006–2007 in works [6, 7, 10] by means of advanced algorithms of a computer search some examples of functions that achieve an equality in (3) for $n = 9$, $m = 3$. In the next sections we generalize the concept of a proper matrix, decrease the constant 0.5902... and show how it is possible to obtain further improvements by means of a progress in combinatorial problems formulated by us.

3 Lemmas on spectra

Lemma 4 *Let $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_k)$ be vectors of variables, $\sigma = (\sigma_1, \ldots, \sigma_k)$, $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_k)$. Suppose that the representation*

$$g(X,Y) = \bigoplus_{\sigma \in \mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus \sigma_i) \right) f_\sigma(X)$$

takes place. Then

$$W_g(uv) = \sum_{\sigma \in \mathbf{F}_2^k} (-1)^{<\sigma,v>} W_{f_{\sigma+(1,\ldots,1)}}(u).$$

Proof. We have

$$W_g(uv) = \sum_{X\sigma \in \mathbf{F}_2^{n+k}} (-1)^{g(X\sigma)+<X\sigma,uv>} =$$

$$\sum_{\sigma \in \mathbf{F}_2^k} (-1)^{<\sigma,v>} \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X\sigma)+<X,u>} = \sum_{\sigma \in \mathbf{F}_2^k} (-1)^{<\sigma,v>} W_{f_{\sigma+(1,\ldots,1)}}(u).$$

□

Lemma 5 *Let $f(x_1, \ldots, x_n)$ be a Boolean function on $\mathbf{F}_2^n$, and let $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}$, $u = (u_1, \ldots, u_n)$. Then*
a) $W_g(u0) = 0$, $W_g(u1) = 2W_f(u)$;
b) if f is m-resilient then g is $(m+1)$-resilient.

Proof. a) Denote $X = (x_1, \ldots, x_n)$. We have

$$W_g(uu_{n+1}) = \sum_{Xx_{n+1} \in \mathbf{F}_2^{n+1}} (-1)^{g(Xx_{n+1})+<Xx_{n+1},uu_{n+1}>} =$$

$$\sum_{X \in \mathbf{F}_2^n} (-1)^{g(X0)+<X,u>} + (-1)^{u_{n+1}} \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X1)+<X,u>} = W_f(u) - (-1)^{u_{n+1}} W_f(u).$$

It follows the statement of a).
b) Each vector from the spectrum support of the function f has by Corollary 1 the weight greater than m and, as we see from the proof of the item a), each vector from the spectrum support of the function g has one in the $(n+1)$th component. From here by Corollary 1 the function g is $(m+1)$-resilient. □

Corollary 3 *If a function $(x_1, \ldots, x_n)$ achieves an equality in the bound (3) then the function $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}$ also achieves an equality in the bound (3).*

Corollary 4 *All vectors from the spectrum support of the function $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}$ have 1 in the $(n+1)$th component.*

In [15] in was introduced the concept of *a pair of quasilinear variables.* We say that a function g depends on a pair of variables (x_i, x_j) *quasilinearly* if at any two vectors that differ in the ith and the jth components and identical in all remained components the function g takes different values. It is easy to see that if a function g on $\mathbf{F}_2^{n+1}$ depends on the pair of variables

(x_n, x_{n+1}) quasilinearly then it is possible to represent g in the form $g(x_1, \ldots, x_{n-1}, x_n, x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_{n+1}$ where $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, 0)$.

Note that if some function f has at least one pair of quasilinear variables then this function is balanced since it is possible to combine all vectors of $\mathbf{F}_2^n$ into pairs (vectors in a pair differ only in two components corresponding to these variables) such that the function f takes the value 1 at exactly one vector from a pair of vectors.

Lemma 6 *Let $f(x_1, \ldots, x_n)$ be a Boolean function on $\mathbf{F}_2^n$, and let $g(x_1, \ldots, x_{n-1}, x_n,\ x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_{n+1}$, $u = (u_1, \ldots, u_{n-1})$. Then*
$W_g(uu_nu_{n+1}) = 0$ if $u_n = u_{n+1}$, and $W_g(uu_nu_{n+1}) = 2W_f(uu_n)$ if $u_n \neq u_{n+1}$.

Proof. Denote $X = (x_1, \ldots, x_n)$. We have

$$W_g(uu_nu_{n+1}) = \sum_{Xx_{n+1} \in \mathbf{F}_2^{n+1}} (-1)^{g(Xx_{n+1}) + <Xx_{n+1}, uu_nu_{n+1}>} = \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X0) + <X, uu_n>} +$$

$$(-1)^{u_{n+1}} \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X1) + <X, uu_n>} = W_f(uu_n) - (-1)^{u_n \oplus u_{n+1}} W_f(uu_n).$$

It proves the lemma. □

Corollary 5 *All vectors from the spectrum support of the function $g(x_1, \ldots, x_{n-1}, x_n,\ x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_n) \oplus x_{n+1}$ have in the pair of components $(n, n+1)$ either the combination* 01 *or the combination* 10.

Corollary 6 *If a function $f(x_1, \ldots, x_n)$ achieves an equality in the bound (3) and f is m-resilient whereas the function $g(x_1, \ldots, x_n,\ x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_{n+1}$ is $(m+1)$-resilient then the function g also achieves an equality in the bound (3).*

Note that the transformation of some variable into a pair of quasilinear variables, in general, does not guarantee the growth of the resiliency of a function. Nevertheless, below we show that in Construction 2 the transformation of some just added variable into a pair of quasilinear variables leads to the growth of the resiliency.

4 Recursive construction and proper matrices

Construction 1. Let $X = (x_1, \ldots, x_{n+t})$, $Y = (y_1, \ldots, y_k)$ be vectors of Boolean variables. Let $\{f_\sigma(X)\}_{\sigma \in \mathbf{F}_2^k}$ be the set of 2^k functions possessing the next properties:
1) each $f_\sigma(X)$ is an $(m+t)$-resilient Boolean function on $\mathbf{F}_2^{n+t}$;
2) each $f_\sigma(X)$ achieves the bound (3);
3) for any two functions $f_{\sigma'}(X)$ and $f_{\sigma''}(X)$, $\sigma' \neq \sigma''$, the spectrum supports of the functions $f_{\sigma'}(X)$ and $f_{\sigma''}(X)$ are disjoint.

Lemma 7 *In definitions of Construction 1 the function*

$$g(X, Y) = \bigoplus_{\sigma \in \mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus \sigma_i) \right) f_\sigma(X)$$

is an $(m+t)$-resilient Boolean function on $\mathbf{F}_2^{n+t+k}$ that achieves the bound (3).

Proof. By Corollary 2 any of functions $f_\sigma(X)$ is plateaued and all nonzero Walsh coefficients of each of these functions have the absolute value 2^{m+t+2}. From the property of the spectrum supports of functions $f_\sigma(X)$ to be mutually disjoint by Lemma 4 it follows that all nonzero Walsh coefficients of the function g also have the absolute value 2^{m+t+2}. The fact that all $f_\sigma(X)$ are $(m+t)$-resilient follows that g is also $(m+t)$-resilient. Therefore g really achieves the bound (3). □

Construction 2. Let $X = (x_1, \ldots, x_{n+t})$, $Y = (y_1, \ldots, y_k)$, $Z = (z_1, \ldots, z_k)$ be vectors of Boolean variables. Let $c = (c_1, \ldots, c_k) \in \mathbf{F}_2^k$ be a fixed binary vector, $|c| = s$. Let $\{f_\sigma(X)\}_{\sigma \in \mathbf{F}_2^k}$ be the set of 2^k functions possessing the same properties as in Construction 1:
1) each $f_\sigma(X)$ is an $(m+t)$-resilient Boolean function on $\mathbf{F}_2^{n+t}$;
2) each $f_\sigma(X)$ achieves the bound (3);
3) for any two functions $f_{\sigma'}(X)$ and $f_{\sigma''}(X)$, $\sigma' \neq \sigma''$, the spectrum supports of the functions $f_{\sigma'}(X)$ and $f_{\sigma''}(X)$ are disjoint.

Lemma 8 *In notation of Construction 2 the function*

$$g_c(X, Y, Z_c) = \bigoplus_{\sigma \in \mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus c_i z_i \oplus \sigma_i) \right) f_\sigma(X) \bigoplus_{i=1}^{k} c_i z_i$$

is an $(m+t+s)$-resilient Boolean function on $\mathbf{F}_2^{n+t+k+s}$ that achieves the bound (3) and has s nonintersecting pairs of quasilinear variables. We assume that if $c_i = 0$ then the variable z_i does not belong to the set Z_c of variables of the function g_c.

Proof. If $s = 0$ then the statement of lemma was already proved in Lemma 7 for the function g_0 which is plateaued by Corollary 2. If $s > 0$ then we shall successive replace in g_0 for all i such that $c_i = 1$ variables y_i to pairs of quasilinear variables (y_i, z_i). At every step of such replacement by Lemma 6 the absolute value of all nonzero Walsh coefficients of a new function will be 2 times greater than in a previous function. Therefore at every step we will obtain a plateaued function again. After all s steps we shall find that all Walsh coefficients of the function g_c belong to the set $\{0, \pm 2^{m+t+s+2}\}$. Show that the function g_c is $(m+t+s)$-resilient. Consider an arbitrary vector α from the spectrum support of the function g_c. In left $(n+t)$ components the vector α by Lemma 4 has more than $m+t$ ones since each of functions $f_\sigma(X)$ is $(m+t)$-resilient. In each pair of components corresponding to the pairs of variables (y_i, z_i) for $c_i = 1$ the vector α has one 1 by Corollary 5. Therefore the weight of the vector α is greater than $m+t+s$. It follows that the function g_c is $(m+t+s)$-resilient and according to arguments given above it achieves the bound (3). The lemma is proved. □

Having an m-resilient function f on $\mathbf{F}_2^n$ that achieves the bound (3) we can obtain from f an $(m+t)$-resilient function on $\mathbf{F}_2^{n+t}$ that achieves the bound (3) adding to f new t' linear variables and transforming s variables, $t'+s = t$, into pairs of quasilinear variables. The required nonlinearity is guaranteed by Lemmas 5 and 6 whereas the required growth of the resiliency can be achieved according to Lemma 8 if we replace just added variables y_i by pairs of quasilinear variables.

However, for the application of Construction 2 it is necessary to guarantee that the spectrum supports of any two different functions f_σ are disjoint. In [16] for this aim it were introduced (k_0, k, p, t)-proper matrices. We shall not repeat now the definition of these matrices but give its generalization and after this explain the differences between old and new definitions.

5 Disjointed rows and generalization of proper matrices

Consider the set V of rows of the length p which components are symbols $1/2$, 1 or $*$, moreover, all symbols $1/2$ are joined in pairs inside of each row (thus, the total number of symbols $1/2$ in each row is even). We associate every row α from V with the states of last p variables $v_1, \ldots, v_k$ of some Boolean function $f_\alpha(u_1, \ldots, u_{n-p}, v_1, \ldots, v_p)$, namely, if $\alpha_i = 1$ then the corresponding variable v_i of the function f_α is linear; if $\alpha_i = \alpha_j = 1/2$ and the components i and j in the row α are joined in a pair then the variables (v_i, v_j) form the pair of quasilinear variables of the function f_α.

Two rows α and β from the set V are called *disjointed* if the spectrum supports of any correspondingly associated functions f_α and f_β are guaranteed to be disjoint.

Example 1. Let $\alpha_i = \alpha_j = 1$, $\beta_i = \beta_j = 1/2$ and the components i and j in the row β are joined in a pair. Then the spectrum supports of any associated functions f_α and f_β are guaranteed to be disjoint. Indeed, each vector from the spectrum support of f_α by Corollary 4 has ones in components corresponding to the variables v_i and v_j whereas every vector from the spectrum support of f_β by Corollary 5 has one in some of components corresponding to the variables v_i and v_j and zero in another component. In fact, at this property it was based the using of Construction 2 in [16] (at other language — without the Walsh coefficients) but it was restricted by this example. Below we show that disjointed rows can have more general form.

Lemma 9 *Let α and β be two rows from V of the length p. Let I be a set of indexes, $I \subseteq \{1, \ldots, p\}$. Suppose that the rows α and β do not contain symbols $*$ in components from I, inside of the row α each symbol $1/2$ in a component from I is joined in a pair with some symbol $1/2$ also in a component from I, the same is true for the row β. Besides, suppose that the rows α and β contain different number of pairs of symbols $1/2$ in components from I. Then the rows α and β are disjointed.*

Proof. Suppose that the row α contains exactly a pairs of symbols $1/2$ in components from I and consequently exactly $|I| - 2a$ ones in components from I. Then by Corollaries 4 and 5 any vector from the spectrum support of the function f_α in components from I contains exactly $|I| - a$ ones. If in the row β there are exactly b pairs of symbols $1/2$ in components from I, $a \neq b$, then $|I| - a \neq |I| - b$, so the spectrum supports of the functions f_α and f_β are disjoint that proves the lemma. □

Corollary 7 *Let α and β be two rows of the length p from V, moreover, there exist the components $i_1, \ldots, i_{2d}$ such that $\alpha_{i_1} = \alpha_{i_{2d}} = 1$, $\alpha_{i_j} = 1/2$, $j = 2, \ldots, 2d-1$; $\beta_{i_j} = 1/2$, $j = 1, \ldots, 2d$. Besides, join in pairs components (i_{2j}, i_{2j+1}), $j = 1, \ldots, d-1$, in the row α and components (i_{2j-1}, i_{2j}), $j = 1, \ldots, d$, in the row β. Then the rows α and β are disjointed.*

Lemma 10 *Let α and β be two rows from V of the length $p = n + k$. Let I be a set of indexes, $I \subseteq \{1, \ldots, p\}$, $|I| = n$. Denote by α_I and β_I the restrictions of α and β on I, correspondingly. Suppose that inside of the row α each symbol $1/2$ in a component from I is joined in a pair with some symbol $1/2$ also in a component from I, the same is true for the row β. Besides, suppose that the subrows α_I and β_I are disjointed. Then the rows α and β are disjointed too.*

Proof. By definition of disjointed rows for given $u \in \mathbf{F}_2^n$ we have either $W_{f_{\alpha(I)}}(u) = 0$ for any function $f_{\alpha(I)}$ associated with $\alpha(I)$ or $W_{f_{\beta(I)}}(u) = 0$ for any function $f_{\beta(I)}$ associated with

$\beta(I)$. By Lemma 4 it follows either $W_{f_\alpha}(uv) = 0$ for any $v \in \mathbf{F}_2^k$ and any function f_α on $\mathbf{F}_2^{n+k}$ associated with α or $W_{f_\beta}(uv) = 0$ for any $v \in \mathbf{F}_2^k$ and any function f_β on $\mathbf{F}_2^{n+k}$ associated with β. □

The concept of disjointed rows is helpful for the constructing of sets of functions with nonintersecting spectrum supports required in Construction 2. Introduce the concept of a generalized proper matrix.

A matrix A of size $2^k \times p$ is called *the generalized (k_0, k, p, t)-proper matrix* if in each of its cells the symbol from the set $\{1/2, 1, *\}$ is recorded, moreover, inside of each row all symbols $1/2$ are joined in nonintersecting pairs, and also the next conditions hold:
1) each row of the matrix A contains at most k_0 pairs of symbols $1/2$;
2) the sum of all number symbols in each row is equal to t (stars are not counted);
3) any two different rows of the matrix A are disjointed.

The difference of generalized proper matrices from simply proper matrices introduced in [16] is as follows. At first, in [16] all columns were inflexibly joined in pairs and two columns of every pair were identical (in notation of [16] they were joined in one column with doubled values of symbols) whereas symbols $1/2$ were automatically joined in pairs inside of pairs of columns. At second, in [16] de facto only such pairs of rows are considered as disjointed for which the configuration of Example 1 took place. At third, in [16] the condition 2) was relaxed — it was required that corresponding sums did not exceed t; but this unimportant relaxation led to additional awkwardness in further text.

The next lemma is a reformulation for generalized proper matrices of the statement from [16].

Lemma 11 *Let A be a generalized (k_0, k, p, t)-proper matrix. Let n and m be positive integers, $p \le n + t$. Suppose that for any integer i such that*
(a) $0 \le i \le k_0$;
(b) the matrix A contains some row α with exactly i pairs of symbols $1/2$
the next condition holds: there exists the $(m + i)$-resilient function on $\mathbf{F}_2^{n+i}$ that has i nonintersecting pairs of quasilinear variables and achieves the bound (3). Then for each integer s, $0 \le s \le k$, it is possible to construct an $(m + t + s)$-resilient function on $\mathbf{F}_2^{n+t+k+s}$ that has s nonintersecting pairs of quasilinear variables and achieves the bound (3).

Proof. Suppose that the row α of the matrix A contains exactly i pairs of symbols $1/2$. Take the corresponding to this row the function f the existence of which is guaranteed by the condition of this lemma. Add to f new $t - i$ linear variables. Permute variables in the resulting the $(m+t)$-resilient function on $\mathbf{F}_2^{n+t}$ by the such way that the last p variables arrive in correspondence with the form of the row α: to components where 1 is in α we shift linear variables whereas to components corresponding to a pair of symbols $1/2$ we shift a pair of quasilinear variables. It is easy to see that after a permutation of variables the nonlinearity and the resiliency of a function are not changed. Make it for each row of the matrix A. As a result we obtain a family of functions satisfied to the condition of Construction 2 that by Lemma 8 guarantees the constructing of required new functions. The lemma is proved. □

Example 2. Suppose that p is even, $\binom{p/2}{2} \ge 2^k$. Then there exists the generalized $(2, k, p, p - 2)$-proper matrix. Indeed, join inflexibly in pairs the components $(2i-1, 2i)$, $i = 1, \ldots, p/2$. We shall record only rows with exactly two pairs of symbols $1/2$ (inside of inflexibly joined pairs) and ones in all remained components. There exist $\binom{p/2}{2}$ rows of such form. It is easy to see that any two different rows of such form are disjointed. By assumption we have $\binom{p/2}{2} \geq 2^k$, so we can record 2^k different rows of a desired form that is sufficient for the constructing of the generalized $(2, k, p, p-2)$-proper matrix.

The function $f(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_2 \oplus x_4$ has two nonintersecting pairs of quasilinear variables and f is 1-resilient achieving an equality in the bound (3). The condition $p \leq n+t = 4+(p-2)$ holds too. Therefore using in Lemma 11 for the function f just constructed generalized $(2, k, p, p-2)$-proper matrix for any fixed k for some p provided $\binom{p/2}{2} \geq 2^k$ we obtain $(m_0 + s)$-resilient functions on $\mathbf{F}_2^{n_0+s}$ that achieve the bound (3) for any number s of nonintersecting pairs of quasilinear variables from 0 till k for some n_0 and m_0.

Theorem 1 *If there exists the generalized (k, k, p, t)-proper matrix then it is possible to construct the sequence of m-resilient functions on $\mathbf{F}_2^n$ that achieve the bound (3) for $n \to \infty$, $\frac{m}{n} \to \frac{t}{t+k}$.*

Proof. In Example 2 it were constructed $(m_0 + s)$-resilient functions on $\mathbf{F}_2^{n_0+s}$ that achieve the bound (3) with any number s of nonintersecting pairs of quasilinear variables from 0 till k for some n_0 and m_0. Applying now r times Construction 2 we obtain an $(m_0 + s + rt)$-resilient function on $\mathbf{F}_2^{n_0+s+r(t+k)}$ that achieves the bound (3). Obviously, for $r \to \infty$ we have $\frac{m}{n} \to \frac{t}{t+k}$ that was required. □

Note that the construction of Example 2 is not effective and it was given here only to provide a simplicity of the proof of Theorem 1. From a practical points of view it is more profitable to make not one big transfer from k_0 to k but many small ones. Examples of such sequences of transfers are given in [3]. Note also that in Example 2 de facto it were used proper matrices in their old definition since columns were inflexibly joined in pairs and the property of any two rows to be disjointed was guaranteed by only two columns of some inflexible pair. The appropriateness of introducing of the definition of generalized proper matrices will be shown in the next section.

6 New constructions

We say that a matrix M is *disjoint* if in each of its cells the symbol from the set $\{1/2, 1, *\}$ is recorded, moreover, inside of each row all symbols 1/2 are joined in pairs, and also any two rows of M are disjointed. Thus, disjoint matrices differ from generalized proper matrices by the fact that for disjoint matrices there are no inflexible restrictions on the number of rows and on the values of sums of number symbols in rows. If the sum of number values in each row of a disjoint matrix is exactly t then such matrix is called *t-disjoint.*

Construction 3. Suppose that a disjoint matrix M has h rows and the sum of number symbols in the ith row of M is equal to t_i, $i = 1, \ldots, h$. Denote $t_{\max} = \max\limits_{1 \leq i \leq h} t_i$. We shall construct the sequence of t-disjoint matrices $A(t)$, $t = 0, 1, \ldots$ Denote by $s(t)$ the number of rows in the matrix $A(t)$. Define initial t-disjoint matrices $A(t)$, $t = 0, 1, \ldots, t_{\max-1}$, arbitrary (for example, certainly it is possible to take the row of t ones as an initial matrix $A(t)$ although from the practical reasons it is desirable that the matrix $A(t)$ contains as many rows as possible). Define for $t \geq t_{\max}$ the matrix $A(t)$ recursively by the next way. For the row α of the matrix M with the index i, $i = 1, \ldots, h$, record into $A(t)$ rows that are a result of the concatenation of α with each of rows of the matrix $A(t - t_i)$. Since, in general, the rows of the resulting matrix $A(t)$

can be of different length, for the alignment record stars to absents components on the right side of rows. From this construction and Lemma 10 it is easy to see that $A(t)$ is a t-disjoint matrix and there is the recurrence equation

$$s(t) = \sum_{i=1}^{h} s(t - t_i)$$

with the corresponding characteristic polynomial

$$x^{t_{\max}} - \sum_{i=1}^{h} x^{t_{\max} - t_i}. \qquad (4)$$

The largest root of the characteristic polynomial (4) is real and positive except some degenerate cases. The classification of degenerate and non-degenerate cases is connected closely with conditions of the Perron–Frobenius theorem for nonnegative matrices [8]. In non-degenerate cases if $X_{\max}$ is the largest root of the characteristic polynomial (4) then the asymptotics of the value $s(t)$ has the form $s(t) = CX^t_{\max}(1 + o(1))$ where the constant C is defined by initial conditions. If in the matrix $A(t)$ to remove rows up to the nearest power of two leaving 2^k rows where $k = \lfloor \log_2 s(t) \rfloor = t \log_2 X_{\max}(1 + o(1))$ then it is easy to see that the resulting matrix will be the generalized (t, k, p, t)-proper matrix where p is the number of columns in the matrix $A(t)$. However, if we are interested in the generalized (k_0, k, p, t)-proper matrix for $k = t \log_2 X_{\max}(1 + o(1))$ then we must remove in the matrix $A(t)$ all rows with the number of pairs of symbols 1/2 greater than k_0 and to prove that the number of such rows is asymptotically small in comparison with $s(t)$.

Note that in [3] in the capacity of a matrix M in fact it was used the matrix

$$\begin{pmatrix} 1 & 1 \\ (1/2)_2 & (1/2)_1 \end{pmatrix}$$

that gave the recurrence equation $s(t) = s(t - 2) + s(t - 1)$ and the characteristic polynomial $x^2 - x - 1$ with the largest root $X_{\max} = \frac{\sqrt{5}+1}{2} = 1.6180...$ This gave the possibility to construct a (k_0, k, p, t)-proper matrix for $k_0 < k$, $k = \log_2 X_{\max}(1 + o(1))$, and, thus, to achieve the ratio $\frac{t}{t+k} = \frac{1}{1+\log_2 X_{\max}}(1 + o(1)) = 0.5902...(1 + o(1))$.

It is possible to develop this construction by the next way. We shall use our new terminology but for now actually not going beyond old proper matrices.

Construction 4. Suppose n is even. Join in pairs the columns $(2i - 1, 2i)$, $i = 1, \dots, n/2$, and record into the matrix M_n one copy of all such rows $a = (a_1, \dots, a_n)$ of symbols 1/2 and 1 that $a_{2i-1} = a_{2i}$, $i = 1, \dots, n/2$. As a result we obtain the matrix with $2^{n/2}$ rows. For example, for $n = 4$ we have

$$M_n = \begin{pmatrix} 1 & 1 & 1 & 1 \\ (1/2)_2 & (1/2)_1 & 1 & 1 \\ 1 & 1 & (1/2)_4 & (1/2)_3 \\ (1/2)_2 & (1/2)_1 & (1/2)_4 & (1/2)_3 \end{pmatrix}.$$

It is easy to see that the matrix M_n constructed by this way contains exactly $\binom{n/2}{j}$ rows with j pairs of symbols 1/2, the sum of number values equal to $n - j$, and M_n is disjoint. Therefore the recursive construction for $A(t)$ that uses the matrix M_n corresponds to the characteristic polynomial

$$x^n - \sum_{j=0}^{n/2} \binom{n/2}{j} x^{\frac{n}{2}-j} = \left(x^2\right)^{n/2} - (x+1)^{n/2} = (x^2-x-1)\left(\sum_{j=0}^{\frac{n}{2}-1} x^{2(\frac{n}{2}-1-j)}(x+1)^j\right). \quad (5)$$

The largest root of the characteristic polynomial (5) is real and positive, it can be shown easily from the Perron–Frobenius theorem. All real roots of the polynomial in the right-most bracket in (5) are negative, therefore the largest root of the characteristic polynomial (5) is the same as of $x^2 - x - 1$. However, we can try to improve the construction of the matrix M_n.

Construction 5. From Lemma 9 it is possible to see that if at least for one pair n and k where n is even and $0 \leq k \leq n/2$ we construct a set V of mutually disjointed rows of the length n with symbols from the set $\{1, 1/2\}$ (without stars) in any of which all symbols $1/2$ are joined in pairs, the number of such pairs is exactly k and the number of rows in V is greater than $\binom{n/2}{k}$ then replacing in M_n all rows that contain exactly k pairs of symbols $1/2$ by all rows from V we obtain the matrix M for which in the characteristic polynomial (5) the absolute value of the coefficient of $x^{\frac{n}{2}-k}$ will increase whereas other coefficients will not be changed. It is obvious that such transformation can not convert a non degenerate case into a degenerate one (in respect to conditions of the Perron–Frobenius theorem). Therefore the largest (real and positive) root $X_{\max}$ will increase, so the asymptotic order of magnitude of $s(t)$ will increase too.

The search of the set of mutually disjointed rows it is possible to realize at the language of the graph theory. To each of $\binom{n}{2k}(2k-1)!!$ possible rows we corresponds the vertex of a graph, two vertices of a graph are connected by an edge if and only if corresponding rows are disjointed. The problem of the search of maximal (large) set of mutually disjointed rows it is possible to solve by the way of the search of maximal (large) clique in a corresponding graph. It is not hard to prove that for $k = 0, 1, 2, \frac{n}{2}-1, \frac{n}{2}$ it is impossible to construct more than $\binom{n/2}{k}$ mutually disjointed rows. For $n = 10$, $k = 3$ it was made a computer search by the hill-climbing method with a random choice of some first rows. At a gradient step of the algorithm it was chosen the vertex of a graph (the row) connected with the greatest number of vertices that were still in consideration (i. e. not yet chosen nor rejected), all non-connected with it vertices in consideration were rejected after this. As a result of the work of this algorithm it was found the set of 15 rows given below:

$$V = \begin{pmatrix}
(1/2)_2 & (1/2)_1 & (1/2)_4 & (1/2)_3 & (1/2)_6 & (1/2)_5 & 1 & 1 & 1 & 1 \\
(1/2)_2 & (1/2)_1 & 1 & (1/2)_6 & 1 & (1/2)_4 & 1 & (1/2)_9 & (1/2)_8 & 1 \\
(1/2)_2 & (1/2)_1 & 1 & 1 & 1 & 1 & (1/2)_9 & (1/2)_{10} & (1/2)_7 & (1/2)_8 \\
(1/2)_3 & (1/2)_5 & (1/2)_1 & 1 & (1/2)_2 & 1 & (1/2)_8 & (1/2)_7 & 1 & 1 \\
(1/2)_4 & 1 & 1 & (1/2)_1 & (1/2)_7 & (1/2)_9 & (1/2)_5 & 1 & (1/2)_6 & 1 \\
(1/2)_5 & (1/2)_3 & (1/2)_2 & 1 & (1/2)_1 & 1 & 1 & 1 & (1/2)_{10} & (1/2)_9 \\
(1/2)_6 & 1 & (1/2)_{10} & (1/2)_8 & 1 & (1/2)_1 & 1 & (1/2)_4 & 1 & (1/2)_3 \\
(1/2)_7 & (1/2)_{10} & 1 & 1 & (1/2)_6 & (1/2)_5 & (1/2)_1 & 1 & 1 & (1/2)_2 \\
(1/2)_{10} & (1/2)_7 & (1/2)_4 & (1/2)_3 & 1 & 1 & (1/2)_2 & 1 & 1 & (1/2)_1 \\
1 & (1/2)_8 & (1/2)_7 & (1/2)_9 & 1 & 1 & (1/2)_3 & (1/2)_2 & (1/2)_4 & 1 \\
1 & (1/2)_9 & 1 & 1 & (1/2)_{10} & (1/2)_8 & 1 & (1/2)_6 & (1/2)_2 & (1/2)_5 \\
1 & 1 & (1/2)_5 & (1/2)_9 & (1/2)_3 & 1 & (1/2)_{10} & 1 & (1/2)_4 & (1/2)_7 \\
1 & 1 & (1/2)_5 & 1 & (1/2)_3 & (1/2)_8 & (1/2)_{10} & (1/2)_6 & 1 & (1/2)_7 \\
1 & 1 & (1/2)_8 & (1/2)_6 & (1/2)_9 & (1/2)_4 & 1 & (1/2)_3 & (1/2)_5 & 1 \\
1 & 1 & 1 & (1/2)_7 & 1 & (1/2)_{10} & (1/2)_4 & (1/2)_9 & (1/2)_8 & (1/2)_6
\end{pmatrix}.$$

At the next table in the intersection of the ith row and the jth column it is indicated the indexes of components that provide the property of the ith and the jth rows of V to be disjointed.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	X	8 9	3 4	7 8	2 1 4 3	9 10	2 1 6 5	3 4	5 6	5 6	3 4	1 2	1 2	1 2	1 2
2		X	4 6	4 6	5 7	4 6	3 10	8 9	8 9	3 7	4 6	1 2	1 2	1 2	1 2
3			X	3 1 2 5	8 10	5 1 2 3	7 9	5 6	3 4	3 7 9 4	1 2 9 7	1 2	1 2	1 2	1 2
4				X	6 9	7 8	2 5	3 1 7 8	5 2 7 8	4 9	1 3	4 9	1 3 5 2	4 6	1 3
5					X	2 3	5 7	2 10	6 9	2 8	1 4	1 4 9 6	1 4	3 8	1 4 7 5
6						X	4 8	7 1 5 6	7 2 3 4	1 5	6 8	1 5 3 2	6 8	4 6	1 5
7							X	4 8	4 8	1 6	2 9	1 6	1 6 8 4	5 9	7 4 8 9
8								X	5 6	5 6	1 7	4 9	3 5 6 8	1 7	8 9
9									X	1 10	3 4	5 3 4 9	6 8	1 10	8 9
10										X	3 7	2 8	4 9	2 8 3 7	6 10
11											X	6 8	2 9	3 8 6 4	4 7
12												X	4 9	7 10	3 5
13													X	7 10	3 5
14														X	3 8 9 5
15															X

Construction 6. Replacing in M_{10} the submatrix consisted of 10 rows that contain exactly 3 pairs of symbols $1/2$ by the set of rows of V we obtain the matrix M'. Using M' in Construction

3 for the number of rows $s(t)$ of the matrix $A(t)$ we obtain the recurrence equation

$$s(t) = s(t-5) + 5s(t-6) + 15s(t-7) + 10s(t-8) + 5s(t-9) + s(t-10)$$

with the characteristic polynomial

$$x^{10} - x^5 - 5x^4 - 15x^3 - 10x^2 - 5x - 1$$

the largest root of which is equal to $X_{\max} = 1.6556...$ Then the ratio $\frac{t}{t+k}$ for the generalized proper matrices constructed by means of $A(t)$ tends to $\frac{1}{1+\log_2 X_{\max}} = 0.5789...$

It is remained to prove that the number of rows with the number of pairs of symbols 1/2 asymptotically greater than $t \log_2 X_{\max} = 0.7274...$ is small in comparison with $s(t)$. In [3] in the corresponding proof for the recurrence equation $s(t) = s(t-1) + s(t-2)$ it was used a simplicity of this equation, as a result its solution was written in almost explicit form that for the characteristic polynomial of 10th degree seems to be problematic. We shall not develop now any general theory and for the simplicity of a presentation we give the proof only for Construction 6 with the using of the matrix M'.

The recursive construction that uses the matrix M' works beginning with $t = 10$. In the capacity of initial matrices $A(t)$, $t = 0, 1, \ldots, 9$, it is possible to take arbitrary t-disjoint matrices; it is essentially that initial matrices must not be empty; the choice of these matrices affects the asymptotics but not the order of the growth of magnitude of $s(t)$ since the asymptotic of the value $s(t)$ is equal to $CX_{\max}^t$, and initial matrices affects only constant C. Of course, from a practical point of view it is better to take matrices $A(t)$, $t = 0, 1, \ldots, 9$, with maximal possible number of rows.

By construction, the set of rows of the matrix $A(t)$ is the collection of all possible concatenations of admissible parts of the length 10 corresponding to the steps of the recursive construction that are completed by a suffix which is a row of some initial matrix. Having a row of the matrix $A(t)$ it is possible to find its suffix uniquely, namely, separating step by step from the left side of a row parts of the length 10 we check the sum of number symbols in current prefix, and then this sum becomes no smaller than $t - 9$ we declare that all remained right part of the row is its suffix.

From the form of M' it follows that the set of all admissible parts of the length 10 consists of 1 part with 0 pairs of symbols 1/2 and the sum of symbols equal to 10; 5 parts with 1 pair of symbols 1/2 and the sum of symbols equal to 9; 10 parts with 2 pairs of symbols 1/2 and the sum of symbols equal to 8; 15 parts with 3 pairs of symbols 1/2 and the sum of symbols equal to 7; 5 parts with 4 pairs of symbols 1/2 and the sum of symbols equal to 6; 1 part with 5 pairs of symbols 1/2 and the sum of symbols equal to 5.

Denote by $l_j(t)$ the number of rows of the matrix $A(t)$ that contain exactly j pairs of symbols 1/2.

Lemma 12 *Let $\varepsilon > 0$. For the matrix $A(t)$ from Construction 3 constructed by means of the matrix M' from Construction 6 for $j \geq (2/3 + \varepsilon)t(1 + o(1))$ beginning with some t the inequality*

$$\frac{l_{j-2}(t+2)}{l_j(t)} > 15$$

holds.

Proof. For an arbitrary row α of the matrix $A(t)$ denote by $n_i(\alpha)$, $i = 0, 1, 2, 3, 4, 5$, the number of parts of the length 10 in the row α (not counting its suffix) that contain exactly i pairs of symbols 1/2. Let $j_0(\alpha)$ be the number of pairs of symbols 1/2 in the suffix of α and let $t_0(\alpha)$ be the sum of number symbols in the suffix of α. For the ratio of the number $j(\alpha)$ of pairs of symbols 1/2 to the sum $t(\alpha)$ of number symbols in the row α we have

$$\frac{j(\alpha)}{t(\alpha)} = \frac{5n_5(\alpha) + 4n_4(\alpha) + 3n_3(\alpha) + 2n_2(\alpha) + n_1(\alpha) + j_0(\alpha)}{5n_5(\alpha) + 6n_4(\alpha) + 7n_3(\alpha) + 8n_2(\alpha) + 9n_1(\alpha) + 10n_0(\alpha) + t_0(\alpha)}. \tag{6}$$

We are interested by only such rows α from the set $A^*(t)$ "bad" rows of $A(t)$ for which beginning with some t the inequality $\frac{j(\alpha)}{t(\alpha)} > \frac{2}{3} + \varepsilon'$, $0 < \varepsilon' < \varepsilon$, holds. Therefore by (6) we can assume that $\min\limits_{\alpha \in A^*(t)} n_5(\alpha) \to \infty$ for $t \to \infty$ and beginning with some t for each row α of $A^*(t)$ the inequality $n_5(\alpha) > n_3(\alpha) + 1$ holds.

Denote by $S(t, j, n_5)$ the set of rows of the matrix $A(t)$ that contain exactly j pair of symbols 1/2 and exactly n_5 parts of the length 10 that consists of 5 pairs of symbols 1/2. For given j and sufficiently large t for all values of n_5 for which the set $S(t, j, n_5)$ is not empty, replace in each row α from $S(t, j, n_5)$ one of parts of the length 10 with 5 pairs of symbols 1/2 by admissible part of the length 10 with 3 pairs of symbols 1/2. It is possible to do it by $15n_5$ ways. We obtain a row of the matrix $A(t+2)$ that contains exactly $j-2$ pairs of symbols 1/2 and could be obtained by such way from $n_3(\alpha) + 1 < n_5$ rows of $S(t, j, n_5)$. Thus, the set $S(t, j, n_5)$ is associated with the set of rows $S(t+2, j-2, n_5-1)$ the cardinality of which exceed the first one in more than 15 times. Running through all values of n_5 we prove the statement of the lemma. □

Lemma 13 *In the matrix $A(t)$ from Construction 3 constructed by means of the matrix M' from Construction 6 the number of rows with the number of pairs of symbols 1/2 no less than $k_0 = \lfloor 0.70t \rfloor$ is asymptotically small in comparison with the number of all rows in $A(t)$.*

Proof. Estimate the ratio of the number of rows indicated in the statement of this lemma to the number of all rows in $A(t)$. Choose d so that $d \to \infty$ for $t \to \infty$ but $\frac{\lfloor 0.70t \rfloor - 2d}{t+2d} > 2/3 + \varepsilon$. Using Lemma 12 beginning with some t we have

$$\frac{\sum\limits_{j=k_0}^{t} l_j(t)}{s(t)} < \frac{\sum\limits_{j=k_0-2d}^{t-2d} l_j(t+2d)}{15^d s(t)} < \frac{s(t+2d)}{15^d s(t)} \leq \left(\frac{X_{\max}^2}{15}\right)^d (1 + o(1)) \to 0.$$

The lemma is proved. □

Thus, we showed that the number of rows with the number of pairs of symbols 1/2 asymptotically greater than $t \log_2 X_{\max} = 0.7274...$ is really small in comparison with $s(t)$. Thus, Lemma 13 and Theorem 1 prove the next theorem.

Theorem 2 *Construction 6 with the using of the matrix M' allows to construct the sequence of m-resilient functions on $\mathbf{F}_2^n$ that achieve the bound (3) for which*

$$m = \frac{1}{1 + \log_2 X_{\max}} n(1 + o(1)) = 0.5789...n(1 + o(1))$$

where $X_{\max} = 1.6556...$ is the largest root of the characteristic polynomial $x^{10} - x^5 - 5x^4 - 15x^3 - 10x^2 - 5x - 1$.

Corollary 8 *Let α be a real constant, $0.5789... \leq \alpha \leq 1$. Then there exists the sequence of m-resilient functions on $\mathbf{F}_2^n$ that achieve the bound (3) for which $\frac{m}{n} \to \alpha$.*

The Corollary 8 is arised easily from the fact that taking the functions of the sequence from the formulation of Theorem 2 and adding t new linear variables to them we increase the order of resiliency and the number of variables at t whereas an equality in the bound (3) will be remain valid. Such functions with linear variables have cryptographic weaknesses, therefore from practical considerations it is more reasonable to apply a bit more complicated constructions using the results and methods of this or cited papers.

7 Issues on implementation complexity

In this section we discuss briefly the implementation complexity of functions from constructions proposed by us above. There exists the prejudice that an application in ciphers functions of large number of variables is unprofitable in practice due to high computational complexity. However, in some cases including our ones functions of large number of variables could have small computational complexity.

Show how to calculate effectively the value of our function by a branching program. Look at the functions $g(X, Y)$ and $g(X, Y, Z)$ in Constructions 1 and 2. At every step of a cipher performance it is necessary to calculate the values of the function at some concrete vector (X, Y) or (X, Y, Z). Knowing subvectors Y and Z we reduce the calculation of the value of the function $g(X, Y)$ (or $g(X, Y, Z)$) to the calculation of only one its subfunction $f_\sigma(X)$ where the index σ can be found immediately and uniquely from Y and Z. For the calculation of the value $f_\sigma(X)$ we look, at first, how variables in the vector X were rearranged for the producing $f_\sigma(X)$ from the function constructed at the previous step of the recursion. In the proof of Lemma 11 we described the process of a permutation of variables in accordance to the form of a corresponding row in a generalized proper matrix but not specified this process since for the proof of lemma it was not important. In the aims of effective implementation this process should be strictly defined. It is possible to permute variables only to attribute the required state (linearity or quasilinearity) to last p variables of the function although it could be appeared that in the aims of the resistance of a cipher (obfuscation) it could be helpful more global permutation. In any case, after the inverse permutation of variables we obtain the function $f'(X)$ constructed at the previous step of the recursion and apply to it the procedures already described above. It is easy to see that if to fix a generalized (k, k, p, t)-proper matrix and to apply it successively in Construction 2 a growing number of times restricting permutations of variables at each step by at most last $2p$ variables then the computation complexity for the value of the constructed function by a branching program will be linear.

The author is grateful to Prof. Oleg A. Logachev and Mikhail S. Lobanov for helpful discussions and the anonymous referee for valuable remarks.

References

[1] S. Chee, S. Lee, D. Lee, S.–H. Sung, On the correlation immune functions and their nonlinearity, Advances in Cryptology — Asiacrypt'96, Lecture Notes in Computer Science, V. 1163, 1996, pp. 232–243.

[2] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, R. Smolensky, The bit extraction problem or t-resilient functions, IEEE Symposium on Foundations of Computer Science, V. 26, 1985, pp. 396–407.

[3] M. Fedorova, Y. Tarannikov, On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Lecture Notes in Computer Science, V. 2247, pp. 254–266, Springer-Verlag, 2001, full version M. Fedorova, Y. Tarannikov, On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2001/083, October 2001, 16 pp.

[4] S. Fu, B. Sun, C. Li, L. Qu, Construction of odd-variable resilient Boolean functions with optimal degree, Journal of information science and engineering 27, pp. 1931–1942 (2011).

[5] S. Gao, W. Ma, Y. Zhao, Z. Zhuo, Walsh Spectrum of Cryptographically Concatenating Functions and Its Applications in Constructing Resilient Boolean Functions, Journal of Computational Information Systems 7:4 (2011) 1074–1081.

[6] S. Kavut, M. Yusel, S. Maitra, Construction of resilient functions by the concatenation of Boolean functions having nonintersecting Walsh spectra, In Third International Workshop of Boolean functions, BFCA 07, May 2–3, 2007, Paris, France.

[7] A. Khalyavin, Constructing Boolean functions with extremal properties, Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Zvenigorod, 8-18 September 2007, Edited by B. Preenel and O. A. Logachev, NATO science for peace and security series D: Information and communication security, Vol. 18, 2008, pp. 289-295, see also A. Khalyavin, The constructing of 3-resilient Boolean functions of 9 variables with nonlinearity 240, Cryptology ePrint Archive (http://eprint.iacr.org/), Report 2007/212, 2007, 7 pp.

[8] H. Minc, Nonnegative matrices, New York: John Wiley and Sons, 1988.

[9] E. Pasalic, S. Maitra, T. Johansson, P. Sarkar, New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity, WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001, Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

[10] Z. Saber, M. Faisal Uddin, A. Youssef, On the existence of $(9, 3, 5, 240)$ resilient functions, IEEE Transactions on Information Theory, 52(5):2269–2270, May, 2006.

[11] P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, In Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science, V. 1880, 2000, pp. 515–532.

[12] J. Seberry, X.–M. Zhang, Y. Zheng, On constructions and nonlinearity of correlation immune functions, Advances in Cryptology — Eurocrypt'93, Lecture Notes in Computer Science, V. 765, 1994, pp. 181–199.

[13] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information theory, V. IT-30, No 5, 1984, p. 776–780.

[14] D. Singh, Construction of highly nonlinear plateaued resilient functions with disjoint spectra, Mathematical Modelling and Scientific Computation. Communications in Computer and Information Science, Volume 283, 2012, pp. 522–529.

[15] Y. Tarannikov, On resilient Boolean functions with maximal possible nonlinearity, Proceedings of Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, pp. 19–30, Springer-Verlag, 2000.

[16] Y. Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity, in Fast Software Encryption. 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001. Revised Papers, Lecture Notes in Computer Science, V. 2355, 2002, pp. 66-77.

[17] T. Wang, M. Liu, D. Lin, Construction of resilient and nonlinear Boolean functions with almost perfect immunity to algebraic and fast algebraic attacks, Information Security and Cryptology, Lecture Notes in Computer Science, Volume 7763, 2013, pp. 276–293

[18] G.-Z. Xiao, J. Massey, A spectral characterization of correlation-immune combining functions, IEEE Transactions on Information Theory, V. 34, No 3, May 1988, pp. 569–571.

[19] F. Zhang, C. Carlet, Y. Hu, W. Zhang, Secondary constructions of bent functions and highly nonlinear resilient functions, Eprint arXiv:1211.4191, November 20, 2012.

[20] Y. Zheng, X.-M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science, V. 2012, pp. 264–274, Springer-Verlag, 2001.

[21] A. Khalyavin, On constructions and estimations of characteristics of correlation-immune Boolean functions and related combinatorial objects, Ph. D. Thesis, Moscow, 2011 (in Russian).

[22] A. Khalyavin, The bound for the nonlinearity of correlation-immune Boolean functions, Applied discrete mathematics, No 1 (11), 2011, pp. 34–69 (in Russian). (http://www.lib.tsu.ru/mminfo/000349342/11/image/11-034.pdf)

[23] A. Khalyavin, Constructing of 4-correlation-immune Boolean functions of 9 variables with nonlinearity 240, Proceeding of X International seminar "Discrete mathematics and its applications", Moscow, MSU, February 1–6, 2010. Moscow, Publishing house of. Mech.& Math. Department of MSU, 2010, pp. 534–537 (in Russian).