On Resilient Boolean Functions with Maximal Possible Nonlinearity

Yuriy Tarannikov

Mech. & Math. Department
Moscow State University
119899 Moscow, Russia
emails: yutaran@nw.math.msu.su, taran@vertex.inria.msu.ru

Abstract

It is proved that the maximal possible nonlinearity of n-variable m-resilient Boolean function is $2^{n-1}-2^{m+1}$ for $\frac{2n-7}{3} \le m \le n-2$. This value can be achieved only for optimized functions (i. e. functions with an algebraic degree $n-m-1$). For $\frac{2n-7}{3} \le m \le n-\log_2\frac{n-2}{3}-2$ it is suggested a method to construct an n-variable m-resilient function with maximal possible nonlinearity $2^{n-1}-2^{m+1}$ such that each variable presents in ANF of this function in some term of maximal possible length $n-m-1$. For $n \equiv 2 \pmod 3$, $m=\frac{2n-7}{3}$, it is given a scheme of hardware implementation for such function that demands approximately $2n$ gates EXOR and $(2/3)n$ gates AND.

Keywords: *stream cipher, Boolean function, nonlinear combining function, correlation-immunity, resiliency, nonlinearity, algebraic degree, Siegenthaler's Inequality, hardware implementation, pseudorandom generator.*

1 Introduction

One of the most general types of stream cipher systems is several Linear Feedback Shift Registers (LFSRs) combined by nonlinear Boolean function. This function must satisfy certain criteria to resist different attacks (in particular, correlation attacks suggested by Siegenthaler [16] and different types of linear attacks). Besides this function must have sufficiently simple scheme implementation in hardware (it is widely known that the main advantages of stream ciphers over block ciphers are the cheapness and the speed). So, the following factors are considered as important properties of Boolean functions for using in stream cipher applications.

1. *Balancedness.* A Boolean function must output zeroes and ones with the same probabilities.

2. Good *correlation-immunity* (of order m). The output of Boolean function must be statistically independent of combination of any m its inputs. A balanced correlation-immune of order m Boolean function is called *m-resilient.*

3. Good *nonlinearity.* The Boolean function must be at the sufficiently big distance from any affine function.

4. High *algebraic degree.* The degree of Algebraic Normal Form (ANF) of Boolean function must be sufficiently large.

5. High *algebraic degree of each individual variable.* Each variable of Boolean function must appear in ANF of this function in some term of sufficiently large length.

6. Simple *implementation in hardware.* The Boolean function must have sufficiently simple scheme implementation.

There are a lot of papers where only one of these criteria is studied. It was found that the nonlinearity of a Boolean function does not exceed $2^{n-1} - 2^{\frac{n}{2}-1}$ [13]. The consideration of pairs of these criteria gave some trade-offs between them. So, the Boolean function with maximal possible nonlinearity can not be balanced. Another result is Siegenthaler's Inequality: [15] if the function f is a correlation-immune function of order m then $\deg(f) \leq n - m$, moreover, if f is an m-resilient, $m \leq n-2$, then $\deg(f) \leq n - m - 1$. Siegenthaler and other authors pointed out that if the Boolean function is *affine* or depends *linearly* on a big number of variables then this function has a simple implementation. But such function can not be considered as a good for cryptographic applications because of another criteria, in particular, algebraic degrees of linear variables are 1.

The variety of criteria and complicated trade-offs between them caused the next approach: to fix one or two parameters and try to optimize others. The most general model is when researchers fix the parameters n (number of variables) and m (order of correlation-immunity) and try to optimize some other criptographically important parameters. Here we can call the works [14], [2], [6], [4] [7], [8], [10].

The present paper continues the investigations in this direction and gives new results. In Section 2 we give preliminary concepts, notions and some simple lemmas. In Section 3 we establish a new trade-off between resiliency and nonlinearity, namely, we prove that the nonlinearity of n-variable m-resilient Boolean function does not exceed $2^{n-1} - 2^{m+1}$. Moreover, it is appears that this bound can be achieved only if Siegenthaler's Inequality is achieved too. In Section 4 we discuss a concept of a linear variable and introduce a new important concept of a pair of *quasilinear* variables which works in the following sections. We discuss the connection of linear and quasilinear dependence with resiliency and nonlinearity of the function and give a representation form for the function with a pair of quasilinear variables. In Section 5 we present our main construction method. This method allows to construct recursively the functions with good cryptographic properties using the functions with good cryptographic properties and smaller number of variables. By means of this method for $\frac{2n-7}{3} \leq m \leq n-2$ we construct an m-resilient Boolean function of n variables with nonlinearity $2^{n-1} - 2^{m+1}$, i. e. the function that achieves the upper bound for the nonlinearity proven in Section 3. The combination of this construction with upper bound gives the exact result: the maximal possible nonlinearity of n-variable m-resilient Boolean function is $2^{n-1} - 2^{m+1}$ for $\frac{2n-7}{3} \leq m \leq n-2$. This result was known only for $m = n-2$ (trivial), $m = n-3$ [10] and some small values of n. In Section 6 we strengthen the previous construction and show that for $\frac{2n-7}{3} \leq m \leq n - \log_2 \frac{n-2}{3} - 2$ it is possible to construct an n-variable m-resilient function with maximal possible nonlinearity $2^{n-1} - 2^{m+1}$ such that each variable presents in ANF of this function in some term of maximal possible length $n - m - 1$ (i. e. each individual variable achieves Siegenthaler's Inequality). In Section 7 we discuss how to implement in hardware the functions constructed in previous sections. We suggest a concrete hardware scheme for n-variable, m-resilient function, $n \equiv 2 \pmod 3$, $m = \frac{2n-7}{3}$, that achives a maximal possible nonlinearity and a maximal possible algebraic degree for each variable simultaneously. It is given a scheme of hardware implementation for such function. It is remarkably that this scheme has a circuit complexity **linear** on n. It contains $2n-4$ gates EXOR and $\frac{2n-1}{3}$ gates AND. This scheme has a strongly regular cascade structure and can be used efficiently in practical design. In Section 8 we establish a trade-off between nonlinearity and correlation-immunity of nonbalanced functions. We prove that the nonlinearity of nonbalanced n-variable correlation-immune of order m Boolean function does not exceed $2^{n-1}-2^m$ and give some examples where this bound is achieved.

Summarizing, in the case $\frac{2n-7}{3} \le m \le n - \log_2 \frac{n-2}{3} - 2$ the problem is closed: for given n and m provided these relations we construct a (balanced) m-resilient function of n variables with maximal possible (for such n and m) nonlinearity, maximal possible (for such n and m) algebraic degrees of this function in a whole as well as its individual variables. Moreover, we implement this function in hardware with a circuit complexity linear on n.

2 Preliminary concepts and notions

We consider V^n, the vector space of n tuples of elements from $GF(2)$. A *Boolean function* is a function from V^n to $GF(2)$. The *weight* $wt(f)$ of a function f on V^n is the number of vectors $\tilde{\sigma}$ on V^n such that $f(\tilde{\sigma})=1$. A function f is said to be *balanced* if $wt(f)=wt(f\oplus 1)$. Obviously, if a function f on V^n is balanced then $wt(f)=2^{n-1}$. A *subfunction* of the Boolean function f is a function f' obtained by substitution some constants for some variables in f. If we substitute in the function f the constants $\sigma_{i_1},\ldots,\sigma_{i_s}$ for the variables $x_{i_1},\ldots,x_{i_s}$ respectively then the obtained subfunction is denoted by $f_{x_{i_1},\ldots,x_{i_s}}^{\sigma_{i_1},\ldots,\sigma_{i_s}}$. If a variable x_i is not substituted by constant then x_i is called a *free* variable for f'.

It is well known that a function f on V^n can be uniquely represented by a polynomial on $GF(2)$ whose degree is at most n. Namely,

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

where g is also a function on V^n. The polynomial representation of f is called the *algebraic normal form* (briefly, ANF) of the function and each $x_1^{a_1}\ldots x_n^{a_n}$ is called a *term* in ANF of f. The *algebraic degree* of f, denoted by $\deg(f)$, is defined as the number of variables in the longest term of f. The *algebraic degree of variable* x_i in f, denoted by $\deg(f,x_i)$, is the number of variables in the longest term of f that contains x_i. If $\deg(f,x_i)=0$ then the variable x_i is called *fictitious* for the function f. If $\deg(f,x_i)=1$, we say that f depends on x_i *linearly.* If $\deg(f,x_i)\ge 2$, we say that f depends on x_i *nonlinearly.* The term of length 1 is called a *linear* term. If $\deg(f)\le 1$ then f is called an *affine* function.

The *Hamming distance* $d(\tilde{\sigma}_1,\tilde{\sigma}_2)$ between two vectors $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ is the number of components where vectors $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ differ. For two Boolean functions f_1 and f_2 on V^n, we define the distance between f_1 and f_2 by $d(f_1,f_2)=\#\{\tilde{\sigma}\in V^n | f_1(\tilde{\sigma})\neq f_2(\tilde{\sigma})\}$. The minimum distance between f and the set of all affine functions is called the *nonlinearity* of f and denoted by $nl(f)$.

A Boolean function f on V^n is said to be *correlation-immune of order* m, with $1\le m\le n$, if the output of f and any m input variables are statistically independent. This concept was introduced by Siegenthaler [15]. In equivalent non-probabilistic formulation the Boolean function f is called correlation-immune of order m if $wt(f')=wt(f)/2^m$ for any its subfunction f' of $n-m$ variables. A balanced mth order correlation immune function is called an *m-resilient.* In other words the Boolean function f is called m-resilient if $wt(f')=2^{n-m-1}$ for any its subfunction f' of $n-m$ variables. From this point of view we can consider formally any balanced Boolean function as 0-resilient (this convention is accepted in [1], [8], [10]) and an arbitrary Boolean function as (-1)-resilient. The concept of an m-resilient function was introduced in [3].

Siegenthaler's Inequality [15] states that if the function f is a correlation-immune function of order m then $\deg(f) \leq n-m$. Moreover, if f is an m-resilient, $m \leq n-2$, then $\deg(f) \leq n-m-1$. An m-resilient Boolean function f is called *optimized* if $\deg(f) = n-m-1$ $(m \leq n-2)$.

The next two lemmas are well-known.

Lemma 2.1 *Let $f(x_1,\dots,x_n)$ be a Boolean function on V^n. Then $\deg(f) = n$ iff $wt(f)$ is odd.*

Proof. The function f can be represented in the form

$$f(x_1,\dots,x_n) = \bigoplus_{\substack{(\sigma_1,\dots,\sigma_n)\in V^n\\ f(\sigma_1,\dots,\sigma_n)=1}} (x_1 \oplus \sigma_1 \oplus 1)\dots(x_n \oplus \sigma_n \oplus 1).$$

The number of terms in this sum is the weight of f. Therefore after the removing of the parentheses and the reducing of similar terms the term of the length n will present in ANF of f iff the weight of f is odd. □

Lemma 2.2 *Let $f(x_1,\dots,x_n)$ be a Boolean function represented in the form*

$$f(x_1,\dots,x_n) = \bigoplus_{(\sigma_1,\dots,\sigma_l)} (x_1 \oplus \sigma_1)\dots(x_l \oplus \sigma_l) f(\sigma_1 \oplus 1,\dots,\sigma_l \oplus 1, x_{l+1},\dots,x_n).$$

Suppose that all 2^l subfunctions $f(\sigma_1 \oplus 1,\dots,\sigma_l \oplus 1, x_{l+1},\dots,x_n)$ are m-resilient. Then the function f is an m-resilient too.

The Lemma 2.2 was proved in a lot of papers including (for $l=1$) the pioneering paper of Siegenthaler (Theorem 2 in [15]). General case follows immediately from the case $l=1$.

3 Upper bound for the nonlinearity of resilient functions

Let m and m be integers, $-1 \leq m \leq n$. Denote my $nlmax(n,m)$ the maximal possible nonlinearity of m-resilient Boolean function on V^n. It is well-known that the nonlinearity of a Boolean function does not exceed $2^{n-1} - 2^{\frac{n}{2}-1}$ [13]. Thus,

$$nlmax(n,-1) \leq 2^{n-1} - 2^{\frac{n}{2}-1}, \tag{1}$$

This value can be achieved only for even n. The functions with such nonlinearity are called *bent functions.* Thus, for even n we have $nlmax(n,-1) = 2^{n-1} - 2^{\frac{n}{2}-1}$. It is known [11, 12, 6] that for odd n, $n \leq 7$, $nlmax(n,-1) = 2^{n-1} - 2^{(n-1)/2}$, and for odd n, $n \geq 15$, the inequality $nlmax(n,-1) > 2^{n-1} - 2^{(n-1)/2}$ holds. Bent functions are nonbalanced always, so, for balanced (0-resilient) n-variable function f we have $nl(f) < 2^{n-1} - 2^{\frac{n}{2}-1}$, and

$$nlmax(n,m) < 2^{n-1} - 2^{\frac{n}{2}-1} \text{ for } m \geq 0. \tag{2}$$

If f is n-variable m-resilient function, $m \geq n-2$, then by Siegenthaler's Inequality [15] $deg(f) \leq 1$, so $nlmax(n,m) = 0$. In [10] it is proved that $nlmax(n,n-3) = 2^{n-2}$ and it is conjectured that $nlmax(n,n-4) = 2^{n-1} - 2^{n-3}$. For some small values of parameters n and m exact values of maximal nonlinearity are known. So, $nlmax(4,0) = 4$, $nlmax(5,-1) =$

$nlmax(5,0) = nlmax(5,1) = 12$, $nlmax(6,0) = 26$ [5], $nlmax(6,1) = nlmax(6,2) = 24$ [10], $nlmax(7,-1) = 56$ [9], $nlmax(7,0) = nlmax(7,1) = 56$ [2]. All these values are the combining of the constructions of concrete functions with upper bounds (1), (2) or, maybe [5], [10], some exhaustive search techniques.

In this section we present new upper bound for the nonlinearity of resilient functions.

Theorem 3.1 *Let $f(x_1, \ldots, x_n)$ be an m-resilient Boolean function, $m \le n-2$. Then*

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

Proof. If $m = n-2$ then by Siegenthaler's Inequality $\deg(f) \le 1$, therefore f is an affine function and $nl(f) = 0$. If $m \le n-3$ then without loss of generality we can assume that f is an m-resilient but it is not an $(m+1)$-resilient (in opposite case we prove more strong inequality $nl(f) \le 2^{n-1} - 2^{m+2}$). Then f has a subfunction of $n-m-1$ variables $f_{x_{i_1},\ldots,x_{i_{m+1}}}^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}$ such that $wt\left(f_{x_{i_1},\ldots,x_{i_{m+1}}}^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}\right) = h \ne 2^{n-m-2}$. We can assume that $h < 2^{n-m-2}$ because of

$$wt(f) = \sum_{(\delta_{i_1},\ldots,\delta_{i_{m+1}})} wt\left(f_{x_{i_1},\ldots,x_{i_{m+1}}}^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}\right) = 2^{n-1},$$

where sum is taken over all binary vectors $\widetilde{\delta} = (\delta_{i_1}, \ldots, \delta_{i_{m+1}})$ of length $m+1$, and if this sum contains a term greater than 2^{n-m-2} then this sum contains also a term less than 2^{n-m-2}.

Consider the function $f_{x_{i_1},\ldots,x_{i_{m+1}}}^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}$, where the vectors $\widetilde{\sigma} = (\sigma_{i_1}, \ldots, \sigma_{i_{m+1}})$ and $\widetilde{\delta} = (\delta_{i_1}, \ldots, \delta_{i_{m+1}})$ differ only in one jth component. Then

$$wt\left(f_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}^{\sigma_{i_1},\ldots,\sigma_{i_{j-1}},\sigma_{i_j},\sigma_{i_{j+1}},\ldots,\sigma_{i_{m+1}}}\right) + wt\left(f_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}^{\delta_{i_1},\ldots,\delta_{i_{j-1}},\delta_{i_j},\delta_{i_{j+1}},\ldots,\delta_{i_{m+1}}}\right) = \\ wt\left(f_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_{j+1}},\ldots,x_{i_{m+1}}}^{\sigma_{i_1},\ldots,\sigma_{i_{j-1}},\sigma_{i_{j+1}},\ldots,\sigma_{i_{m+1}}}\right) = 2^{n-m-1},$$

because of the function f is an m-resilient. Therefore,

$$wt\left(f_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}^{\delta_{i_1},\ldots,\delta_{i_{j-1}},\delta_{i_j},\delta_{i_{j+1}},\ldots,\delta_{i_{m+1}}}\right) = 2^{n-m-1} - h.$$

Arguing by the same way we prove that

$$wt\left(f_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}^{\delta_{i_1},\ldots,\delta_{i_{j-1}},\delta_{i_j},\delta_{i_{j+1}},\ldots,\delta_{i_{m+1}}}\right) = \begin{cases} h, & \text{if } d(\widetilde{\sigma},\widetilde{\delta}) \text{ is even,} \\ 2^{n-m-1} - h, & \text{if } d(\widetilde{\sigma},\widetilde{\delta}) \text{ is odd.} \end{cases}$$

Consider the affine function l,

$$l = \bigoplus_{j=1}^{m+1} x_{i_j} \oplus \left(|\widetilde{\sigma}| \pmod 2\right).$$

Then

$$d(f,l) = \sum_{(\delta_{i_1},\ldots,\delta_{i_{m+1}})} d\left(f_{x_{i_1},\ldots,x_{i_{m+1}}}^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}, \bigoplus_{j=1}^{m+1} \delta_{i_j} \oplus \left(|\widetilde{\sigma}| \pmod 2\right)\right) =$$

$$\sum_{\substack{\widetilde{\delta}\\ d(\widetilde{\sigma},\widetilde{\delta}) \text{ is even}}} wt\left(f_{x_{i_1},\dots,x_{i_{m+1}}}^{\delta_{i_1},\dots,\delta_{i_{m+1}}}\right) +$$

$$\sum_{\substack{\widetilde{\delta}\\ d(\widetilde{\sigma},\widetilde{\delta}) \text{ is odd}}} \left(2^{n-m-1} - wt\left(f_{x_{i_1},\dots,x_{i_{m+1}}}^{\delta_{i_1},\dots,\delta_{i_{m+1}}}\right)\right) = h2^m + h2^m = h2^{m+1}.$$

Therefore,

$$nl(f) \le d(f,l) = h2^{m+1} \le (2^{n-m-2}-1)2^{m+1} = 2^{n-1} - 2^{m+1}.$$

□

Corollary 3.1 *$nlmax(n,m) \le 2^{n-1} - 2^{m+1}$ for $m \le n-2$.*

If $m \le \frac{n}{2} - 2$ the inequality (3) does not give us any new information because of well-known inequality (1). But in the following sections we show that the inequality (3) is achieved for wide spectrum of large m.

Theorem 3.2 *Let $f(x_1,\dots,x_n)$ be an m-resilient nonoptimized Boolean function, $m \le n-3$. Then*

$$nl(f) \le 2^{n-1} - 2^{m+2}.$$

Proof. As in the proof of the Theorem 3.1 let $f_{x_{i_1},\dots,x_{i_{m+1}}}^{\sigma_{i_1},\dots,\sigma_{i_{m+1}}}$ be a subfunction of f such that $wt\left(f_{x_{i_1},\dots,x_{i_{m+1}}}^{\sigma_{i_1},\dots,\sigma_{i_{m+1}}}\right) = h < 2^{n-m-2}$. The function f is not optimized. It follows that $\deg\left(f_{x_{i_1},\dots,x_{i_{m+1}}}^{\sigma_{i_1},\dots,\sigma_{i_{m+1}}}\right) \le \deg(f) \le n-m-2$. By Lemma 2.1 it follows that h is even. Therefore, $h \le 2^{n-m-2} - 2$ and $nl(f) \le h2^{m+1} \le (2^{n-m-2}-2)2^{m+1} = 2^{n-1} - 2^{m+2}$. □

Corollary 3.2 *The inequality (3) can be achieved only for optimized functions.*

Thus, the inequality (3) can be achieved only if Siegenthaler's Inequality is achieved too.

4 On linear and quasilinear variables

Recall that a variable x_i is called *a linear* for a function $f = f(x_1,\dots,x_{i-1},\, x_i,\, x_{i+1},\dots,x_n)$ if $\deg(f,x_i) = 1$. Also we say that a function f depends on a variable x_i *linearly.* If a variable x_i is linear for a function f we can represent f in the form

$$f(x_1,\dots,x_{i-1},x_i,x_{i+1},\dots,x_n) = g(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n) \oplus x_i.$$

Other equivalent definition of a linear variable is that a variable x_i is linear for a function f if $f(\widetilde{\delta}_1) \ne f(\widetilde{\delta}_2)$ for any two vectors $\widetilde{\delta}_1$ and $\widetilde{\delta}_2$ that differ only in ith component. By analogy with the last definition we give a new definition for a pair of quasilinear variables.

Definition 4.1 *We say that a Boolean function $f = f(x_1,\dots,x_n)$ depends on a pair of its variables (x_i,x_j)* quasilinearly *if $f(\widetilde{\delta}_1) \ne f(\widetilde{\delta}_2)$ for any two vectors $\widetilde{\delta}_1$ and $\widetilde{\delta}_2$ of length n that differ only in ith and jth components. A pair (x_i,x_j) in this case is called a* pair of quasilinear variables *in f.*

Lemma 4.1 *Let $f(x_1,\dots,x_n)$ be a Boolean function. Then (x_i,x_j), $i<j$, is a pair of quasilinear variables in f iff f can be represented in the form*

$$f(x_1,\dots,x_n) = g(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{j-1},x_{j+1},\dots,x_n,x_i \oplus x_j) \oplus x_i. \qquad (4)$$

Proof. If f is represented in the form (4) then, obviously, a pair (x_i, x_j) is quasilinear in f. Suppose that a pair (x_i, x_j) is quasilinear in f. Then

A) variables x_i and x_j do not present in ANF of f in the same term. Indeed, assume the converse. Consider the shortest term X in ANF of f that contains x_i and x_j simultaneously (if there are some shortest terms chose one of them arbitrary). Substitute a constant 0 for all variables that are not contained in X and a constant 1 for all variables that are contained in X (excluding x_i and x_j). Then the term X is the only term in ANF of f that produces $x_i x_j$ under such substitution. Thus, we obtain a nonlinear function of two variables, x_i and x_j. By Lemma 2.1 the weight of this function is odd. Therefore there exist two vectors $\widetilde{\delta}_1$ and $\widetilde{\delta}_2$ of length n that differ only in ith and jth components such that $f(\widetilde{\delta}_1) = f(\widetilde{\delta}_2)$. This contradiction proves the proposition A.

B) exactly one of two linear terms x_i and x_j presents in ANF of f. Indeed, suppose that the part of ANF that does not contain variables different from x_i and x_j has the form $c_0 \oplus c_i x_i \oplus c_j x_j$ (in the proposition A we have proved that the term $x_i x_j$ is not contained in ANF of f). Let $\widetilde{\delta}$ be a vector of length n where ith and jth components are ones and all another components are zeroes, let $\widetilde{0}$ be a zero vector of length n. Then $c_0 = f(\widetilde{0}) \neq f(\widetilde{\delta}) = c_0 \oplus c_i \oplus c_j$. It follows $c_i \oplus c_j = 1$. This equality proves the proposition B.

C) let X be some conjunction $x_{i_1} x_{i_2} \ldots x_{i_k}$ that does not contain neither x_i nor x_j. Then the term $x_i X$ presents in ANF of f iff the term $x_j X$ presents in ANF of f. Indeed, suppose that X is a shortest conjunction that does not satisfy to this proposition (if there are some shortest terms chose one of them arbitrary). Substitute a constant 0 for all variables that are not contained in X and a constant 1 for all variables that are contained in X (excluding x_i and x_j). Then taking into account the propositions A and B we obtain the function $x_i \oplus x_j \oplus c$ or the constant function c, $c \in \{0,1\}$. Therefore there exist two vectors $\widetilde{\delta}_1$ and $\widetilde{\delta}_2$ of length n that differ only in ith and jth components such that $f(\widetilde{\delta}_1) = f(\widetilde{\delta}_2)$. This contradiction proves the proposition C.

A collection of the propositions A, B and C proves the representation (4). □

Lemma 4.2 *Let $f(x_1, \ldots, x_n)$ be a Boolean function. If f depends on some variable x_i linearly then f is balanced.*

Proof. Combine all 2^n vectors of the function f into pairs so that any pair $(\widetilde{\sigma}_1, \widetilde{\sigma}_2)$ contains vectors $\widetilde{\sigma}_1$ and $\widetilde{\sigma}_2$ that differ in ith component and coincide in all other components. Then $f(\widetilde{\sigma}_1) \neq f(\widetilde{\sigma}_2)$. So, $wt(f) = 2^{n-1}$ and f is balanced. □

Corollary 4.1 *Let $f(x_1, \ldots, x_n)$ be a Boolean function. If f depends on some variables x_{i_1}, x_{i_2}, ..., x_{i_s} linearly then f is $(s-1)$-resilient.*

Note that the Corollary 4.1 agrees with our assumption that a balanced function is 0-resilient, and an arbitrary Boolean function is (-1)-resilient. (In the last case $s = 0$.)

Lemma 4.3 *Let $f(x_1, \ldots, x_n)$ be a Boolean function. If f depends on some pair of variables (x_i, x_j) quasilinearly then f is balanced.*

Proof. Combine all 2^n vectors of the function g into pairs so that any pair $(\widetilde{\sigma}_1, \widetilde{\sigma}_2)$ contains vectors $\widetilde{\sigma}_1$ and $\widetilde{\sigma}_2$ that differ in ith and jth components and coincide in all other components. Then $f(\widetilde{\sigma}_1) \neq f(\widetilde{\sigma}_2)$. So, the function f is balanced. □

Lemma 4.4 *Let $f(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus c x_{n+1}$ where $c \in \{0,1\}$. Then $nl(f) = 2nl(g)$.*

Proof. The nonlinearity of the function $f(x_1, \ldots, x_n, x_{n+1})$ is the minimum of the weights of functions

$$f_{\widetilde{\alpha}} = \bigoplus_{i=1}^{n} \alpha_i x_i \oplus \alpha_{n+1} x_{n+1} \oplus g(x_1, \ldots, x_n) \oplus \delta$$

over all binary vectors $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \delta)$ of length $n+2$. If $\alpha_{n+1} = 1$ then the function $f_{\widetilde{\alpha}}$ is balanced by Lemma 4.2. So, in this case $wt(f_{\widetilde{\alpha}}) = 2^n$. If $\alpha_{n+1} = 0$ then we have $wt(f_{\widetilde{\alpha}}) = 2wt\left(g(x_1, \ldots, x_n) \bigoplus\limits_{i=1}^{n} \alpha_i x_i \oplus \delta\right) \geq 2nl(f)$. The last inequality achieves for some vector $\widetilde{\alpha}$. Thus, $nl(f) = \min\{2^n, 2nl(g)\} = 2nl(g)$. □

Lemma 4.5 *Let $f(x_1, \ldots, x_n)$ be a Boolean function on V^n and f depends on some pair of variables (x_i, x_j) quasilinearly. Then $nl(f) = 2nl(g)$ where g is a function used in the representation of f in the form (4) in Lemma 4.1.*

Proof. The nonlinearity of the function f is the minimum of the weights of functions

$$f_{\widetilde{\alpha}} = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n, x_i \oplus x_j) \oplus \bigoplus_{i=1}^{n} \alpha_i x_i \oplus \delta$$

over all binary vectors $\widetilde{\alpha} = (\alpha_1, \alpha_n, \delta)$ of length $n+1$. If $\alpha_i \neq \alpha_j$ then by Lemma 4.2 the function $f_{\widetilde{\alpha}}$ is balanced. But for the function on V^n the nonlinearity is always less than 2^{n-1}. Therefore we can exclude the case $\alpha_1 \neq \alpha_2$ from our consideration. So, we suppose that $\alpha_1 = \alpha_2 = \alpha$. In this case $f_{\widetilde{\alpha}} = g'(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n, x_i \oplus x_j)$ for some function g' on V^{n-1}, $nl(g') = nl(g)$. It is easy to see that $wt(f_{\widetilde{\alpha}}) = 2wt(g') \geq 2nl(g)$, so, $N(g) \geq 2N(f)$. On the other hand, for some vector $\widetilde{\alpha}$ the weight of the correspondence function g' takes a minimum of nonlinearity for g. Thus, $nl(f) = 2nl(g)$. □

5 A method of constructing

Theorem 3.1 shows that the nonlinearity of m-resilient Boolean function on V^n can not exceed $2^{n-1} - 2^{m+1}$. Earlier in papers [14], [2], [7], [8] the authors developed methods for the constructing of m-resilient Boolean functions of n variables with high nonlinearity, and, in particular, the nonlinearity $2^{n-1} - 2^{m+1}$ in these four papers can be achieved for $m+3 \geq 2^{n-m-2}$. The methods suggested in these papers are quite different but in the part of spectrum given by the inequality $m+3 \geq 2^{n-m-2}$ these methods give really the same construction. Combination of these results with our upper bound (3) from Theorem 3.1 proves that $nlmax(n,m) = 2^{n-1} - 2^{m+1}$ for $m+3 \geq 2^{n-m-2}$. In this section we prove more strong result, namely, we prove that $nlmax(n,m) = 2^{n-1} - 2^{m+1}$ for $\frac{2n-7}{3} \leq m \leq n-2$.

Lemma 5.1 *Let n be a positive integer. Let $f_1(x_1, \ldots, x_n)$ and $f_2(y_1, \ldots, y_n)$ be m-resilient Boolean functions on V^n such that $nl(f_1) \geq N_0$, $nl(f_2) \geq N_0$. Moreover, there exist two variables x_i and x_j such that f_1 depends on the variables x_i and x_j linearly, and f_2 depends on a pair of the variables (x_i, x_j) quasilinearly. Then the function*

$$f'_1(x_1, \ldots, x_n, x_{n+1}) = (x_{n+1} \oplus 1) f_1(x_1, \ldots, x_n) \oplus x_{n+1} f_2(x_1, \ldots, x_n) \tag{5}$$

is an m-resilient Boolean function on V^{n+1} with nonlinearity $nl(f'_1) \geq 2^{n-1} + N_0$, and the function

$$\begin{aligned} f'_2(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = (x_{n+1} \oplus x_{n+2} \oplus 1) f_1(x_1, \ldots, x_n) \oplus \\ (x_{n+1} \oplus x_{n+2}) f_2(x_1, \ldots, x_n) \oplus x_{n+1} \end{aligned} \tag{6}$$

is an $(m+1)$-resilient Boolean function on V^{n+2} with nonlinearity $nl(f_2') \geq 2^n + 2N_0$. Moreover, f_2' depends on a pair of the variables (x_{n+1}, x_{n+2}) quasilinearly.

Proof. At first, consider the equation (5). Both subfunctions $(f_1')^0_{x_{n+1}} = f_1(x_1, \ldots, x_n)$ and $(f_1')^1_{x_{n+1}} = f_2(x_1, \ldots, x_n)$ are m-resilient, hence by Lemma 2.2 f_1' is m-resilient too. Let $l = \bigoplus_{i=1}^{n+1} c_i x_i \oplus c_0$ be an arbitrary affine function on V^{n+1}. Then $d(f_1', l) = d(f_1, l^0_{x_{n+1}}) + d(f_2, l^1_{x_{n+1}}) = wt(f_1 \oplus l^0_{x_{n+1}}) + wt(f_2 \oplus l^1_{x_{n+1}})$. We state that at least one of two functions $f_1 \oplus l^0_{x_{n+1}}$ and $f_2 \oplus l^1_{x_{n+1}}$ is balanced. Indeed, if $c_i = 0$ or $c_j = 0$ then the function $f_1 \oplus l^0_{x_{n+1}}$ depends on x_i or x_j linearly, hence, by Lemma 4.2 the function $f_1 \oplus l^0_{x_{n+1}}$ is balanced. In the remained case $c_i = 1$ and $c_j = 1$ it is easy to see from the representation (4) that the function $f_2 \oplus l^1_{x_{n+1}}$ depends on a pair of the variables (x_i, x_j) quasilinearly, therefore by Lemma 4.3 the function $f_2 \oplus l^1_{x_{n+1}}$ is balanced. Thus, $d(f_1', l) \geq 2^{n-1} + N_0$. An affine function l was chosen arbitrary, therefore, $nl(f_1') \geq 2^{n-1} + N_0$.

Next, consider the equation (6). By conctruction (6) and representation (4) we see that f_2' depends on a pair of the variables (x_{n+1}, x_{n+2}) quasilinearly. Now we want to prove that the function f_2' is $(m+1)$-resilient. Substitute arbitrary $m+1$ variables by constants generating the subfunction $\hat{f}$. If both variables x_{n+1} and x_{n+2} are free in $\hat{f}$ then $\hat{f}$ depends on a pair (x_{n+1}, x_{n+2}) quasilinearly, therefore by Lemma 4.3 the function $\hat{f}$ is balanced. If at least one of two variables x_{n+1} and x_{n+2} was substituted by constant then we substituted by constants at most m of first n variables $x_1, \ldots, x_n$. But the functions $\hat{f}^{0\ \ 0}_{x_{n+1}, x_{n+2}} = f_1$, $\hat{f}^{0\ \ 1}_{x_{n+1}, x_{n+2}} = f_2$, $\hat{f}^{1\ \ 0}_{x_{n+1}, x_{n+2}} = f_2 \oplus 1$, $\hat{f}^{1\ \ 1}_{x_{n+1}, x_{n+2}} = f_1 \oplus 1$ are m-resilient, thus, by Lemma 2.2 the function $\hat{f}$ is balanced. A subfunction $\hat{f}$ was chosen arbitrary. So, the function f_2' is $(m+1)$-resilient.

Finally, we need to prove the lower bound for the nonlinearity of f_2'. Let $l = \bigoplus_{i=1}^{n+2} c_i x_i \oplus c_0$ be an arbitrary affine function on V^{n+2}. Then $d(f_2', l) = d(f_1, l^{0\ \ 0}_{x_{n+1}, x_{n+2}}) + d(f_2, l^{0\ \ 1}_{x_{n+1}, x_{n+2}}) + d(f_2 \oplus 1, l^{1\ \ 0}_{x_{n+1}, x_{n+2}}) + d(f_1 \oplus 1, l^{1\ \ 1}_{x_{n+1}, x_{n+2}}) = wt(f_1 \oplus l^{0\ \ 0}_{x_{n+1}, x_{n+2}}) + wt(f_2 \oplus l^{0\ \ 1}_{x_{n+1}, x_{n+2}}) + wt(f_2 \oplus l^{1\ \ 0}_{x_{n+1}, x_{n+2}} \oplus 1) + wt(f_1 \oplus l^{1\ \ 1}_{x_{n+1}, x_{n+2}} \oplus 1)$. By the same reason as it was given above at least one of two functions $f_1 \oplus l^{0\ \ 0}_{x_{n+1}, x_{n+2}}$ and $f_2 \oplus l^{0\ \ 1}_{x_{n+1}, x_{n+2}}$ is balanced, and at least one of two functions $f_2 \oplus l^{1\ \ 0}_{x_{n+1}, x_{n+2}} \oplus 1$ and $f_1 \oplus l^{1\ \ 1}_{x_{n+1}, x_{n+2}} \oplus 1$ is balanced. Thus, $d(f_2', l) \geq 2^n + 2N_0$. An affine function l was chosen arbitrary, therefore, $nl(f_2') \geq 2^n + 2N_0$. □

Lemma 5.2 *Suppose that there exist an m-resilient Boolean function $f_{n,1}$ on V^n, $nl(f_{n,1}) \geq N_0$, and $(m+1)$-resilient Boolean function $f_{n+1,2}$ on V^{n+1}, $nl(f_{n+1,2}) \geq 2N_0$, besides the function $f_{n+1,2}$ depends on some pair of its variables (x_i, x_j) quasilinearly. Then there exist an $(m+2)$-resilient Boolean function $f_{n+3,1}$ on V^{n+3}, $nl(f_{n+3,1}) \geq 2^{n+1} + 4N_0$, and $(m+3)$-resilient Boolean function $f_{n+4,2}$ on V^{n+4}, $nl(f_{n+4,2}) \geq 2^{n+2} + 8N_0$, besides the function $f_{n+4,2}$ depends on some pair of its variables quasilinearly.*

Proof. We can assume that $i < j$. Denote

$$f_1(x_1, \ldots, x_{n+2}) = f_{n,1}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n+2}) \oplus x_i \oplus x_j,$$

$$f_2(x_1, \ldots, x_{n+2}) = f_{n+1,2}(x_1, \ldots, x_{n+1}) \oplus x_{n+2}.$$

By Lemmas 4.2 and 4.4 the functions f_1 and f_2 are $(m+2)$-resilient functions on V^{n+2}, $nl(f_1) \geq 4N_0$, $nl(f_2) \geq 4N_0$. Moreover, f_1 depends on the variables x_i and x_j linearly, and f_2 depends on a pair of the variables (x_i, x_j) quasilinearly. Substituting f_1 and f_2 to (5) and (6) (we shift

$n \to n+2$) we have

$$f_1'(x_1,\dots,x_n,x_{n+3}) = (x_{n+3}\oplus 1)f_1(x_1,\dots,x_{n+2}) \oplus x_{n+3}f_2(x_1,\dots,x_{n+2})$$

and

$$f_2'(x_1,\dots,x_n,x_{n+4}) = (x_{n+3}\oplus x_{n+4}\oplus 1)f_1(x_1,\dots,x_{n+2})\oplus$$
$$(x_{n+3}\oplus x_{n+4})f_2(x_1,\dots,x_{n+2})\oplus x_{n+3}.$$

By Lemma 5.1 we have constructed an $(m+2)$-resilient Boolean function $f_{n+3,1} = f_1'$ on V^{n+3}, $nl(f_{n+3,1}) \geq 2^{n+1} + 4N_0$, and an $(m+3)$-resilient Boolean function $f_{n+4,2} = f_2'$ on V^{n+4}, $nl(f_{n+4,2}) \geq 2^{n+2} + 8N_0$, besides the function $f_{n+4,2}$ depends on a pair of its variables (x_{n+3}, x_{n+4}) quasilinearly. □

Corollary 5.1 *Suppose that for $m \leq n-2$ there exist an m-resilient Boolean function $f_{n,1}$ on V^n, $nl(f_{n,1}) = 2^{n-1}-2^{m+1}$, and $(m+1)$-resilient Boolean function $f_{n+1,2}$ on V^{n+1}, $nl(f_{n+1,2}) = 2^n - 2^{m+2}$, besides the function $f_{n+1,2}$ depends on some pair of its variables (x_i, x_j) quasilinearly. Then there exist an $(m+2)$-resilient Boolean function $f_{n+3,1}$ on V^{n+3}, $nl(f_{n+3,1}) = 2^{n+2}-2^{m+3}$, and $(m+3)$-resilient Boolean function $f_{n+4,2}$ on V^{n+4}, $nl(f_{n+4,2}) = 2^{n+3} - 2^{m+4}$, besides the function $f_{n+4,2}$ depends on some pair of its variables quasilinearly.*

Proof. The hypothesis of Corollary 5.1 is the hypothesis of Lemma 5.2 for $N_0 = 2^{n-1}-2^{m+1}$. By Lemma 5.2 we can construct the functions $f_{n+3,1}$ and f_{n+4} with required properties and nonlinearities $nl(f_{n+3,1}) \geq 2^{n+1} + 4N_0 = 2^{n+2} - 2^{m+3}$, $nl(f_{n+4,2}) \geq 2^{n+2} + 8N_0 = 2^{n+3} - 2^{m+4}$. By Theorem 3.1 the right parts of the last inequalities are also upper bounds. So, we have equalities $nl(f_{n+3,1}) = 2^{n+2} - 2^{m+3}$, $nl(f_{n+4,2}) = 2^{n+3} - 2^{m+4}$. □

Theorem 5.1 *$nlmax(n,m) = 2^{n-1} - 2^{m+1}$ for $\frac{2n-7}{3} \leq m \leq n-2$.*

Proof. If $m = n-2$ then by Siegenthaler's Inequality any $(m-2)$-resilient function on V^n is affine. So, $nlmax(n, n-2) = 0$. Next, take $f_{2,1} = x_1x_2$, $f_{3,2} = x_1(x_2\oplus x_3)\oplus x_2$. These functions satisfy to the hypothesis of Corollary 5.1 with $n=2$, $m=-1$. By Corollary 5.1 we construct the functions $f_{5,1}$ and $f_{6,2}$ such that the function $f_{5,1}$ is an 1-resilient Boolean function on V^5, $nl(f_{5,1}) = 2^4 - 2^2$, the function $f_{6,2}$ is a 2-resilient Boolean function on V^6, $nl(f_{6,2}) = 2^5 - 2^3$, besides $f_{6,2}$ depends on a pair of the variables (x_5, x_6) quasilinearly. Substitute the functions $f_{5,1}$ and $f_{6,2}$ to the hypothesis of Corollary 5.1, and so on. By this way, for each integer k, $k \geq 3$, we construst an m-resilient Boolean function $f_{n,1}$ on V^n with nonlinearity $2^{n-1} - 2^{m+1}$ where $n = 3k-7$, $m = 2k-7$. Let $\frac{2n-7}{3} \leq m \leq n-3$. Put

$$f(x_1,\dots,x_n) = f_{3(n-m)-7,1}(x_1,\dots,x_{3(n-m)-7}) \bigoplus_{i=3(n-m)-6}^{n} x_i.$$

By the hypothesis of Theorem 5.1 we have $3(n-m)-7 \leq n$. The resiliency of the function f is $(2(n-m)-7) + (n-(3(n-m)-7)) = m$, the nonlinearity of the function f is $2^{n-(3(n-m)-7)}\left(2^{(3(n-m)-7)-1} - 2^{(2(n-m)-7)+1}\right) = 2^{n-1} - 2^{m+1}$. Thus, for $\frac{2n-7}{3} \leq m \leq n-2$ we have constructed an m-resilient Boolean function on V^n with nonlinearity $2^{n-1} - 2^{m+1}$. Taking into account the upper bound (3) from Theorem 3.1 we complete the proof. □

Note that a recent conjecture $nlmax(n, n-4) = 2^{n-1} - 2^{n-3}$ (for $n \geq 5$) in [10] is a special case of our Theorem 5.1.

Examples. It was noted that we take $f_{2,1} = x_1x_2$, $f_{3,2} = x_1(x_2\oplus x_3)\oplus x_2 = x_1x_2\oplus x_1x_3\oplus x_2$. Next, $f_{5,1} = (x_5\oplus 1)(x_1x_4\oplus x_2\oplus x_3)\oplus x_5(x_1x_2\oplus x_1x_3\oplus x_2\oplus x_4) = x_1x_2x_5\oplus x_1x_3x_5\oplus x_1x_4x_5\oplus x_1x_4\oplus x_3x_5\oplus x_4x_5\oplus x_2\oplus x_3$, $f_{6,2} = (x_5\oplus x_6\oplus 1)(x_1x_4\oplus x_2\oplus x_3)\oplus(x_5\oplus x_6)(x_1x_2\oplus x_1x_3\oplus x_2\oplus x_4)\oplus x_5 =$

$x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_2 \oplus x_3 \oplus x_5$.

At the next step we have $f_{8,1} = (x_8 \oplus 1)(x_1x_2x_7 \oplus x_1x_3x_7 \oplus x_1x_4x_7 \oplus x_1x_4 \oplus x_3x_7 \oplus x_4x_7 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6) \oplus x_8(x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_7) = x_1x_2x_5x_8 \oplus x_1x_2x_6x_8 \oplus x_1x_2x_7x_8 \oplus x_1x_3x_5x_8 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_7x_8 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_6x_8 \oplus x_1x_4x_7x_8 \oplus x_1x_2x_7 \oplus x_1x_3x_7 \oplus x_1x_4x_7 \oplus x_3x_5x_8 \oplus x_3x_6x_8 \oplus x_3x_7x_8 \oplus x_4x_5x_8 \oplus x_4x_6x_8 \oplus x_4x_7x_8 \oplus x_1x_4 \oplus x_3x_7 \oplus x_4x_7 \oplus x_6x_8 \oplus x_7x_8 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6$.

The function $f_{8,1}$ is a 3-resilient function of 8 variables with nonlinearity 112. Note that until now the maximal known value for the nonlinearity of a 3-resilient function on V^8 was 96 [2],[8],[10]. Note that now it is unknown even 1-resilient function on V^8 with better nonlinearity than 112.

The constructing of 29-resilient Boolean functions on V^{50} is quite popular in the literature. Note that the method in [2] allows to construct a 29-resilient Boolean function on V^{50} with nonlinearity $2^{49} - 2^{34}$ with an algebraic degree 16. In [7] and [8] the optimized functions are studied, i. e. the functions that achieve Siegenthaler's Inequality. In [7] it is constructed a 29-resilient Boolean function on V^{50} with an algebraic degree 20 and nonlinearity $2^{49} - 2^{39} - 2^{30}$, and in [7] it is constructed such function with the nonlinearity $2^{49} - 2^{37} - 2^{30}$. Note that by means of the method developed in this section it is possible to construct the function $f_{50,1}$. This function is 31-resilient function on V^{50} with an algebraic degree 18 and the nonlinearity $2^{49} - 2^{32}$ (we proved that this nonlinearity is maximal possible). Of course, this function can be considered as a 29-resilient too (in any case the function $f_{50,1} \oplus x_1 \oplus x_2$ is a 29-resilient because of spectral properties of correlation-immune functions, see [17]). If we are interested in optimized functions then we can take the function $f_{47,1}$. This function is a 29-resilient function on V^{47} with an algebraic degree 17 and the nonlinearity $2^{46} - 2^{30}$. Put $f(x_1, \ldots, x_{50}) = \bigoplus_{(\sigma_{48},\sigma_{49},\sigma_{50})} (x_{48} \oplus \sigma_{48})(x_{49} \oplus \sigma_{49})(x_{50} \oplus \sigma_{50}) f_{47,1}^{\sigma_{48},\sigma_{49},\sigma_{50}}(x_1, \ldots, x_{47})$, where $f_{47,1}^{\sigma_{48},\sigma_{49},\sigma_{50}}(x_1, \ldots, x_{47})$ are the functions obtained from $f_{47,1}(x_1, \ldots, x_{47})$ by some permutations of the variables. It is easy to provide an algebraic degree of f equal to 20 (for example, if some term of the length 17 will be contained in ANF of only one of eight functions $f_{47,1}^{\sigma_{48},\sigma_{49},\sigma_{50}}(x_1, \ldots, x_{47})$). Thus, the constructed function f is a 29-resilient optimized Boolean function on V^{50} with the nonlinearity at least $8(2^{46} - 2^{30}) = 2^{49} - 2^{33}$. Thus, our method allows to construct the functions with better parameters than in [2],[8],[10].

6 Optimization of Siegenthaler's Inequality for each individual variable

Some lack of the construction given in the proof of Theorem 5.1 is that for $\frac{2n-7}{3} < m$ the constructed function depends on some variables linearly. Note that the functions with the nonlinearity $2^{n-1} - 2^{m+1}$ constructed in [14], [2], [7], [8] (for $m+3 \geq 2^{n-m-2}$) depends nonlinearly on all its variables only in some cases when $m + 3 = 2^{n-m-2}$ or $m + 2 = 2^{n-m-2}$. In general, those functions depends nonlinearly on $2^{n-m-2} + n - m - 4$ or $2^{n-m-2} + n - m - 3$ variables. In this section for $\frac{2n-7}{3} \leq m \leq n - \log_2 \frac{n-2}{3} - 2$ we suggest a method to construct an m-resilient Boolean function on V^n that achieves Siegenthaler's Inequality for each its individual variable (i. e. $\deg(f, x_i) = n - m - 1$ for all variables x_i). Simultaneously we give a more general way of constructing than it was done in previous section.

We say that a variable x_i is a *covering* for a function f if each other variable of f is contained together with x_i in some term of maximal length in ANF of f. We say that a quasilinear pair of variables (x_i, x_j) is a *covering* for a function f if each other variable of f is contained together with x_i in some term of maximal length in ANF of f (and consequently together with x_j in some term of maximal length in ANF of f).

Lemma 6.1 *For integers k and n provided $k \geq 3$, $3k-7 \leq n < 3 \cdot 2^{k-2} - 2$, there exists a Boolean function $f^k_{n,1}$ on V^n satisfied to the next properties:*

(1 i) $f^k_{n,1}$ is an $(n-k)$-resilient;

(1 ii) $nl(f^k_{n,1}) = 2^{n-1} - 2^{n-k+1}$;

(1 iii) $\deg(f^k_{n,1}, x_i) = k-1$ for each variable x_i;

(1 iv) $f^k_{n,1}$ has a covering variable.

For integers k and n provided $k \geq 3$, $3k-7 < n \leq 3 \cdot 2^{k-2} - 2$, there exists a Boolean function $f^k_{n,2}$ on V^n satisfied to the next properties:

(2 i) $f^k_{n,2}$ is an $(n-k)$-resilient;

(2 ii) $nl(f^k_{n,2}) = 2^{n-1} - 2^{n-k+1}$;

(2 iii) $\deg(f^k_{n,2}, x_i) = k-1$ for each variable x_i;

(2 iv) $f^k_{n,2}$ has a quasilinear pair of covering variables.

Proof. The proof is by induction on k. For $k=3$ we can take $f^3_{2,1} = x_1x_2$, $f^3_{3,1} = f^3_{3,2} = x_1(x_2 \oplus x_3) \oplus x_2$, $f^3_{4,2} = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$. It is easy to check that these functions satisfy to all required conditions.

Suppose that the statement is valid for k. We want to prove it for $k+1$. We search the functions $f^{k+1}_{n,1}$ and $f^{k+1}_{n,2}$ in the form

$$\begin{gathered} f^{k+1}_{n,1} = (x_n \oplus 1)\left(f^k_{n_1}(x_1, \ldots, x_{n_1}) \bigoplus_{i=n_1+1}^{n-1} x_i\right) \\ \oplus x_n \left(\bigoplus_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2}, \ldots, x_{n-1})\right), \\ n_1 + n_2 \geq n-1, \quad n_1 \leq n-3, \quad n_2 \leq n-2, \end{gathered} \tag{7}$$

and

$$\begin{gathered} f^{k+1}_{n,2} = (x_{n-1} \oplus x_n \oplus 1)\left(f^k_{n_1}(x_1, \ldots, x_{n_1}) \bigoplus_{i=n_1+1}^{n-2} x_i\right) \\ \oplus (x_{n-1} \oplus x_n) \left(\bigoplus_{i=1}^{n-2-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2-1}, \ldots, x_{n-2})\right) \oplus x_{n-1}, \\ n_1 + n_2 \geq n-2, \quad n_1 \leq n-4, \quad n_2 \leq n-3, \end{gathered} \tag{8}$$

where $f^k_{n_1}(x_1, \ldots, x_{n_1})$ is $f^k_{n_1,1}(x_1, \ldots, x_{n_1})$ or $f^k_{n_1,2}(x_1, \ldots, x_{n_1})$ (if $f^k_{n_1} = f^k_{n_1,2}$ then $n_2 \neq n-2$ in (7) and $n_2 \neq n-3$ in (8)). Besides we suppose that a covering variable in $f^k_{n_1}$ is x_1 (or a quasilinear pair of covering variables in $f^k_{n_1,2}$ is (x_1, x_2)), and we suppose that a quasilinear pair of covering variables in $f^k_{n_2,2}$ is (x_{n-2}, x_{n-1}) in (7) or (x_{n-3}, x_{n-2}) in (8).

The functions $f^{k+1}_{n,1}$ and $f^{k+1}_{n,2}$ satisfy to all required properties. Indeed:

(1 i) The resiliency of the function $f^k_{n_1}(x_1, \ldots, x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ is $(n_1 - k) + (n-1-n_1) = n-k-1$, the resiliency of the function $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2}, \ldots, x_{n-1})$ is $n-1-n_2+(n_2-k) = n-k-1$. So, by Lemma 5.1 the resiliency of the function $f^{k+1}_{n,1}$ is $n-(k+1)$.

(2 i) The resiliency of the function $f^k_{n_1}(x_1,\ldots,x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-2} x_i$ is $(n_1-k)+(n-2-n_1) = n-k-2$, the resiliency of the function $\bigoplus\limits_{i=1}^{n-2-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2-1},\ldots,x_{n-2})$ is $n-2-n_2+(n_2-k) = n-k-2$. So, by Lemma 5.1 the resiliency of the function $f^{k+1}_{n,1}$ is $n-(k+1)$.

(1 ii) The nonlinearity of the function $f^k_{n_1}(x_1,\ldots,x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ is $(2^{n_1-1}-2^{n_1-k+1})2^{n-1-n_1} = 2^{n-2}-2^{n-k}$, the nonlinearity of the function $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\ldots,x_{n-1})$ is $2^{n-1-n_2}(2^{n_2-1}-2^{n_2-k+1}) = 2^{n-2}-2^{n-k}$. The function $f^k_{n_1}(x_1,\ldots,x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ depends on variables x_{n-2} and x_{n-1} linearly whereas the function $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\ldots,x_{n-1})$ depends on a pair of variables (x_{n-2},x_{n-1}) quasilinearly. So, by Lemma 5.1 the nonlinearity of the function $f^{k+1}_{n,1}$ is $2^{n-2}+(2^{n-2}-2^{n-k}) = 2^{n-1}-2^{n-(k+1)+1}$.

(2 ii) The nonlinearity of the function $f^k_{n_1}(x_1,\ldots,x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-2} x_i$ is $(2^{n_1-1}-2^{n_1-k+1})2^{n-2-n_1} = 2^{n-3}-2^{n-k-1}$, the nonlinearity of the function $\bigoplus\limits_{i=1}^{n-2-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2-1},\ldots,x_{n-2})$ is equal to $2^{n-2-n_2}(2^{n_2-1}-2^{n_2-k+1}) = 2^{n-3}-2^{n-k-1}$. The function $f^k_{n_1}(x_1,\ldots,x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-2} x_i$ depends on variables x_{n-3} and x_{n-2} linearly whereas the function $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\ldots,x_{n-1})$ depends on a pair of variables (x_{n-3},x_{n-2}) quasilinearly. So, by Lemma 5.1 the nonlinearity of the function $f^{k+1}_{n,2}$ is $2^{n-2}+2(2^{n-3}-2^{n-k-1}) = 2^{n-1}-2^{n-(k+1)+1}$.

(1 iii), (1 iv) Each variable from the set $\{x_2,x_3,\ldots,x_{n_1}\}$ is contained together with x_1 in some term of length $k-1$ in ANF of the function $f^k_{n_1,1}(x_1,\ldots,x_{n_1})$ if $f^k_{n_1} = f^k_{n_1,1}$ or each variable from the set $\{x_3,x_4,\ldots,x_{n_1}\}$ is contained together with x_1 in some term of length $k-1$ (and also together with x_2 in some term of this length) in ANF of the function $f^k_{n_1,2}(x_1,\ldots,x_{n_1})$ if $f^k_{n_1} = f^k_{n_1,2}$. The function $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\ldots,x_{n-1})$ depends on the variable x_1 linearly (and also on the variable x_2 if $f^k_{n_1} = f^k_{n_1,2}$). So, after the removing of the parentheses and the reducing of similar terms each variable from the set $\{x_1,x_2,x_3,\ldots,x_{n_1}\}$ will be contained together with x_n in some term of length k in ANF of the function $f^{k+1}_{n,1}$. Analogously, each variable from the set $\{x_{n-n_2},\ldots,x_{n-3}\}$ is contained together with x_{n-2} in some term of length $k-1$ (and also together with x_{n-1} in some term of such length) in ANF of the function $f^k_{n_2,2}(x_{n-n_2},\ldots,x_{n-1})$. The function $f^k_{n_1}(x_1,\ldots,x_{n_1}) \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ depends on the variables x_{n-2} and x_{n-1} linearly. So, after the removing of the parentheses and the reducing of similar terms each variable from the set $\{x_{n-n_2},\ldots,x_{n-1}\}$ will be contained together with x_n in some term of length k in ANF of the function $f^{k+1}_{n,1}$. Bu condition $n_1+n_2 \le n-1$, therefore the union of the sets $\{x_1,x_2,x_3,\ldots,x_{n_1}\}$ and $\{x_{n-n_2},\ldots,x_{n-1}\}$ is the set $\{x_1,\ldots,x_{n-1}\}$. Thus, x_n is a covering variable in $f^k_{n,1}$.

The proof of properties (2 iii) and (2 iv) is analogous.

Finally, we note that according to (7) we can construct the function $f^k_{n,1}$ if $n \ge n_1+3 \ge (3k-7)+3 = 3(k+1)-7$ and if $n \le n_1+n_2+1 \le 2(3\cdot 2^{k-2}-2)+1 \le 3\cdot 2^{(k+1)-2}-3$, and according to (8) we can construct the function $f^k_{n,2}$ if $n \geq n_1 + 4 \geq (3k-7)+4 = 3(k+1)-4$ and if $n \leq n_1 + n_2 + 2 \leq 2(3 \cdot 2^{k-2} - 2) + 2 \leq 3 \cdot 2^{(k+1)-2} - 2$. So, the step of induction is completely proven. □

Theorem 6.1 *For integers m and n provided $\frac{2n-7}{3} \leq m \leq n - \log_2 \frac{n-2}{3} - 2$, there exists an m-resilient Boolean function on V^n with nonlinearity $2^{n-1} - 2^{m+1}$ that achieves Siegenthaler's Inequality for each individual variable.*

Proof. Straightforword corollary from Lemma 6.1. □

Examples. Let $n = 7$, $m = 3$. We chose $n_1 = 3$, $n_2 = 4$, and construct according to (7):

$$\begin{gathered} f^4_{7,1} = (x_7 \oplus 1)\left(f^3_{3,1}(x_1,x_2,x_3) \bigoplus_{i=4}^{6} x_i\right) \oplus x_7 \left(\bigoplus_{i=1}^{2} x_i \oplus f^3_{4,2}(x_3,x_4,x_5,x_6)\right) = \\ (x_7 \oplus 1)(x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6) \oplus \\ x_7(x_1 \oplus x_2 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_3 \oplus x_5) = \\ x_1x_2x_7 \oplus x_1x_3x_7 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus \\ x_1x_2 \oplus x_1x_3 \oplus x_1x_7 \oplus x_3x_7 \oplus x_4x_7 \oplus x_6x_7 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6. \end{gathered}$$

The function $f^4_{7,1}$ is a 3-resilient Boolean function on V^7 with nonlinearity $2^6 - 2^4 = 48$ and an algebraic degree of each variable in $f^4_{7,1}$ is 3.

Let $n = 10$, $m = 6$. We chose $n_1 = 4$, $n_2 = 4$, and construct according to (8):

$$\begin{gathered} f^4_{10,2} = (x_9 \oplus x_{10} \oplus 1)\left(f^3_{4,2}(x_1,x_2,x_3,x_4) \bigoplus_{i=5}^{8} x_i\right) \oplus \\ (x_9 \oplus x_{10})\left(\bigoplus_{i=1}^{4} x_i \oplus f^3_{4,2}(x_5,x_6,x_7,x_8)\right) \oplus x_9 = \\ (x_9 \oplus x_{10} \oplus 1)(x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8) \oplus \\ (x_9 \oplus x_{10})(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5x_7 \oplus x_5x_8 \oplus x_6x_7 \oplus x_6x_8 \oplus x_5 \oplus x_7) \oplus x_9 = \\ x_1x_3x_9 \oplus x_1x_3x_{10} \oplus x_1x_4x_9 \oplus x_1x_4x_{10} \oplus x_2x_3x_9 \oplus x_2x_3x_{10} \oplus x_2x_4x_9 \oplus \\ x_2x_4x_{10} \oplus x_5x_7x_9 \oplus x_5x_7x_{10} \oplus x_5x_8x_9 \oplus x_5x_8x_{10} \oplus x_6x_7x_9 \oplus x_6x_7x_{10} \oplus \\ x_6x_8x_9 \oplus x_6x_8x_{10} \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_9 \oplus x_2x_{10} \oplus x_4x_9 \oplus \\ x_4x_{10} \oplus x_6x_9 \oplus x_6x_{10} \oplus x_8x_9 \oplus x_8x_{10} \oplus x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9. \end{gathered}$$

The function $f^4_{10,2}$ is a 6-resilient Boolean function on V^{10} with nonlinearity $2^9 - 2^7 = 384$ and an algebraic degree of each variable in $f^4_{10,2}$ is 3.

7 Implementation

The problem of the implementation of Boolean functions in hardware is very important. Even if some function has a complex of best cryptographic properties but tries too many gates for its impementation the practical using of such function can be too expensive. Note that the circuit complexity of straightforword implementation of the functions constructed by usual methods, in general, is exponential on n. In [8] the authors discuss the circuit complexity of the implementation of functions constructed by their methods and give an exponential estimation. It is remarkably that the functions constructed by the methods developed in this paper have a circuit complexity of its implementation in hardware **linear** on n.

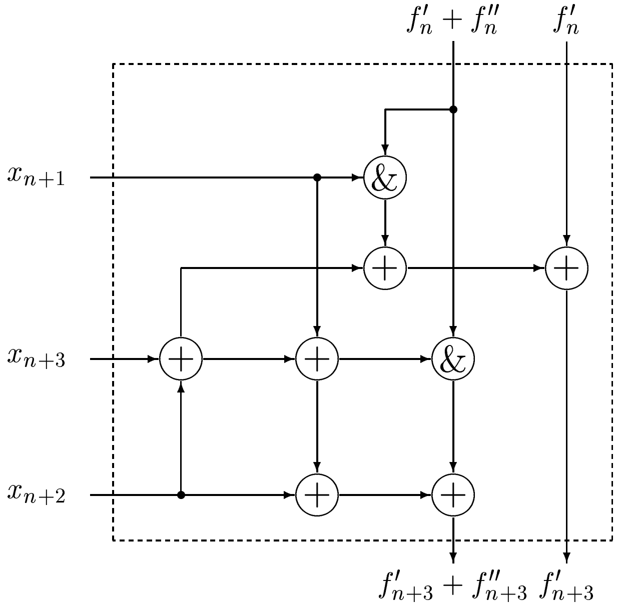

Fig 1. Scheme of block B

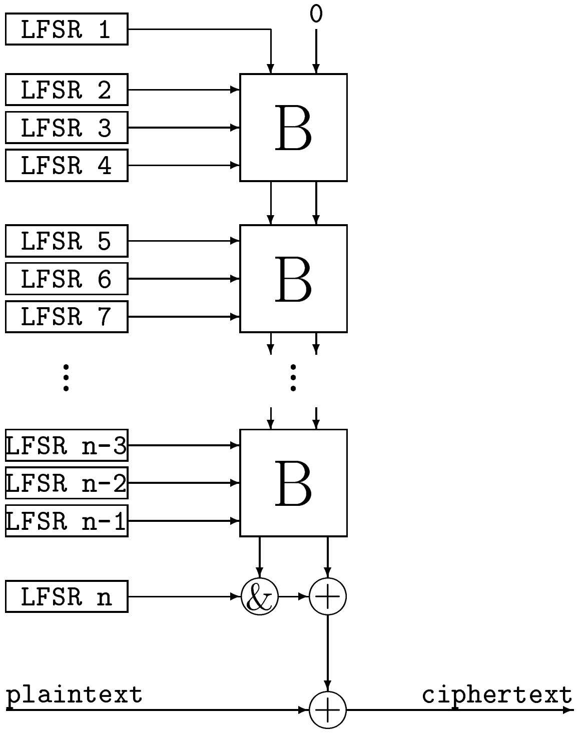

Fig 2. Stream cipher based on the function f_n

Now we give concrete details of such implementation. Put

$$\begin{array}{l} f'_{n+3} = (x_{n+1} \oplus 1) f'_n \oplus x_{n+1} f''_n \oplus x_{n+2} \oplus x_{n+3}, \\ f''_{n+3} = (x_{n+2} \oplus x_{n+3} \oplus 1) f'_n \oplus (x_{n+2} \oplus x_{n+3}) f''_n \oplus x_{n+1} \oplus x_{n+2} \end{array} \qquad (9)$$

By Lemma 5.1 if f'_n and f''_n are m-resilient Boolean functions on V^n with maximal possible nonlinearity $(2^{n-1} - 2^{m+1})$, f'_n depends on its last two variables linearly and f''_n depends on a pair of its last variables quasilinearly then f''_{n+3} and f''_{n+3} are $(m+2)$-resilient Boolean functions on V^{n+3} with maximal possible nonlinearity $(2^{n+2}-2^{m+3})$, f'_n depends on its last two variables linearly and f''_n depends on a pair of its last variables quasilinearly.

It is a little more convenient to rewrite the relations (9) in the form

$$\begin{array}{l} f'_{n+3} = x_{n+1}(f'_n \oplus f''_n) \oplus f'_n \oplus x_{n+2} \oplus x_{n+3}, \\ f'_{n+3} \oplus f''_{n+3} = (x_{n+1} \oplus x_{n+2} \oplus x_{n+3})(f'_n \oplus f''_n) \oplus x_{n+1} \oplus x_{n+3}. \end{array} \tag{10}$$

The relations (10) allow to realize f'_{n+3} and $f'_{n+3} \oplus f''_{n+3}$ as two functions of five values f'_n, $f'_n \oplus f''_n$, x_{n+1}, x_{n+2}, x_{n+3} by means of the block B (see Figure 1). The block B contains 8 two-input gates. Initial functions can be chosen as

$$\begin{array}{l} f'_4 = x_1x_2 \oplus x_3 \oplus x_4, \\ f''_4 = x_2 \oplus x_1(x_3 \oplus x_4) \oplus x_3, \\ f'_4 \oplus f''_4 = x_1(x_2 \oplus x_3 \oplus x_4) \oplus x_2 \oplus x_4. \end{array}$$

Comparison with (10) shows that we can take $f'_1 = 0$, $f''_1 = x_1$. Finally, we put

$$f_n = x_n(f'_{n-1} \oplus f''_{n-1}) \oplus f'_{n-1}, \quad n \equiv 2 \pmod 3.$$

In fact, the function f_n is the function $f_{n,1}$ in Section 5 (up to some permutation of the variables). By Section 5 the function f_n is $\frac{2n-7}{3}$-resilient function on V^n, $n \equiv 2 \pmod 3$, with the nonlinearity $2^{n-1} - 2^{\frac{2n-4}{3}}$ and an algebraic degree of each variable in f_n is $\frac{n+4}{3}$. A complete scheme of pseudorandom generator for stream cipher based on the function f_n is shown in Figure 2 (one gate in the first block B that receives 0 can be omitted). The scheme of the function f_n contains $2n-4$ gates EXOR and $\frac{2n-1}{3}$ gates AND. Note that this scheme has a strongly regular cascade structure. For practical using it is sufficiently to stamp the block B, and varying the number of these blocks in the scheme we obtain the functions of different number of variables depending on our requirements.

If $\frac{2n-7}{3} < m$ we can add to previous construction some variables linearly as it was done in the proof of Theorem 5.1. If $\frac{2n-7}{3} < m \le n - \log_2 \frac{n-2}{3} - 2$ and we need to implement the function with maximal possible nonlinearity that achieves Siegenthaler's Inequality for each individual variable then we are able also to construct a scheme for this function with a circuit complexity linear on n following the technique developed in Section 6 but the lack of space forces us to omit the details of this construction.

8 Some words on the maximal nonlinearity for nonbalanced correlation-immune functions

In this section we consider the problem of maximal nonlinearity for nonbalanced correlation-immune function.

Theorem 8.1 *Let $f(x_1,\ldots,x_n)$ be a nonbalanced correlation-immune of order m Boolean function, $m < n$. Then*

$$nl(f) \le 2^{n-1} - 2^m. \tag{11}$$

Proof. Obviously, $nl(f) = nl(f \oplus 1)$. So, without loss of generality we can assume that $wt(f) < 2^{n-1}$. The weight of f can be calculated as

$$wt(f) = \sum_{(\delta_1,\ldots,\delta_m)} wt\left(f^{\delta_1,\ldots,\delta_m}_{x_1,\ldots,x_m}\right).$$

But the weights of all functions $f^{\delta_1,\dots,\delta_m}_{x_1,\dots,x_m}$ are the same. Therefore,

$$nl(f) \le wt(f) = 2^m wt\left(f^{0,\dots,0}_{x_1,\dots,x_m}\right) \le 2^m(2^{n-m-1}-1) = 2^{n-1} - 2^m.$$

□

The upper bound (11) in the Theorem 8.1 is weaker than the correspondent upper bound (3) in the Theorem 3.1. Nevertheless this bound is achieved for some functions.

Examples. If $m = n-1$ then by Siegenthaler's Inequality $\deg(f) \le 1$, therefore $nl(f) = 0$ and the bound (11) is achieved. But if $\deg(f) = 1$ then f is balanced. The only remained case $f \equiv$ const can be considered as degenerated.

$n = 2$, $m = 0$. Take $g_2(x_1, x_2) = x_1x_2$. Note that we considered g_2 as (-1)-resilient function but also g_2 can be considered as a nonbalanced correlation-immune function of order 0. $nl(g_2) = 1$, so, g_2 achieves the bound (11).

$n = 3$, $m = 1$. Take $g_3(x_1, x_2, x_3) = \bigoplus\limits_{1\le i<j\le 3} x_ix_j \oplus \bigoplus\limits_{1\le i\le 3} x_i \oplus 1$. The function g_3 is a nonbalanced correlation-immune of order 1, $nl(g_3) = 2^2 - 2^1 = 2$, so, g_3 achieves the bound (11). Note that $g_2 = (g_3)^1_{x_3}$.

$n = 6$, $m = 3$. Take $g_6(x_1, x_2, x_3, x_4, x_5, x_6) = \bigoplus\limits_{1\le i<j<k\le 6} x_ix_jx_k \oplus x_1x_2 \oplus x_2x_3 \oplus x_3x_4 \oplus x_4x_5 \oplus x_1x_5 \oplus \bigoplus\limits_{i=1}^{5} x_i \oplus 1$. The function g_6 is a nonbalanced correlation-immune of order 3, $nl(g_6) = 2^5 - 2^3 = 24$, thus, g_6 achieves the bound (11).

$n = 5$, $m = 2$. Take $g_5(x_1, x_2, x_3, x_4, x_5, x_5) = (g_6)^\sigma_{x_i}$ for arbitrary $i \in \{1, \dots, 6\}$, $\sigma \in \{0, 1\}$. It is obviously, that the function g_5 is a nonbalanced correlation-immune of order 2, it is possible to calculate straightforwordly that $nl(g_5) = 2^4 - 2^2 = 12$, thus, g_5 achieves the bound (11).

The examples given above are the only known functions that achieve the inequality (11) (up to permutations of variables and linear transformations). The existence of the functions that achieve the bound (11) with $n \ge 7$ is the open problem.

References

[1] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science, V. 576, 1991, pp. 86–100.

[2] Seongtaek Chee, Sangjin Lee, Daiki Lee and Soo Hak 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.

[3] 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.

[4] T. W. Cusick, On constructing balanced correlation immune functions, in Sequences and Their Applications, Proceedings of SETA '98, Springer Discrete Mathematics and Theoretical Computer Science, 1999, pp. 184-190.

[5] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, In B. Preneel, editor, Fast Software Encryption, Lecture Notes in Computer Sciences, Vol. 1008, 1994, pp. 61–74.

[6] E. Filiol, C. Fontaine, Highly Nonlinear Balanced Boolean Functions with a Good Correlation Immunity, Advanced in Cryptology, Eurocrypt '98, Helsinki, Finland, Lecture Notes in Computer Sciences, Vol. 1403, 1998, pp. 475–488.

[7] S. Maitra, P. Sarkar, Highly nonlinear resilient functions optimizing Siegenthaler's Inequality, Crypto '99, Lecture Notes in Computer Science, Vol. 1666, 1999, pp. 198–215.

[8] S. Maitra, P. Sarkar, Construction of nonlinear resilient Boolean functions, Indian Statistical Institute, Technical Report No. ASD/99/30, 19 pp.

[9] J. Mykkkeltveit, The covering radius of the $[128, 8]$ Reed–Muller code is 56, IEEE Transactions on Information Theory, V. 26, No 3, pp. 358–362, May 1980.

[10] E. Pasalic, T. Johansson, Further results on the relation between nonlinearity and resiliency for Boolean functions, IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science, Vol. 1746, 1999, pp. 35–44.

[11] N. J. Patterson, D. H. Wiedemann, The covering radius of the $[2^{15}, 16]$ Reed–Muller code is at least 16276, IEEE Transactions on Information Theory, V. 29, No. 3, pp. 354–356, May 1983.

[12] N. J. Patterson, D. H. Wiedemann, Correction to [11], IEEE Transactions on Information Theory, V. 36, No. 2, p. 443, March 1990.

[13] O. S. Rothaus, On bent functions, Journal of Combinatorial Theory, Series A20, pp. 300–305.

[14] J. Seberry, X. Zhang, Y. Zheng, On Constructions and Nonlinearity of Correlation Immune Functions, Advances in Cryptology, Eurocrypt '93, Proceedings, Lecture Notes in Computer Science, V. 765, 1993, pp. 181–199.

[15] 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.

[16] T. Siegenthaler, Decrypting a Class of Stream Ciphers Using Ciphertext Only, IEEE Transactions on Computer, V. C-34, No 1, Jan. 1985, pp. 81–85.

[17] Xiao Guo-Zhen, J. Massey, A Spectral Characterization of Correlation-Immune Combining Functions, IEEE Transactions on Information Theory, V. 34, No 3, May 1988, pp. 569–571.