# Spectral Analysis of Boolean Functions under Non-uniformity of Arguments

Kanstantsin Miranovich
E-mail: Miranovich@yandex.ru

**Abstract**

For some classes of Boolean functions we study charecteristics

$$\Delta_F(f(),\epsilon) = \max_{|\epsilon_i|\le\epsilon, i=\overline{1,n}} |\frac{1}{2} - P\{y=1\}|,$$

where $y = F(x),\ \epsilon_i = \frac{1}{2} - P\{x_i = 1\},\ i = \overline{1,n},\ x = (x_1,\dots,x_n) \in B^n,\ B = \{0,1\}$, and $F()$ being equal to

$$F(x) = f(x),\ F(x) = f(x)\oplus(a,x),\ F(x) = f(x)\oplus f(x\oplus a),$$

where $a = (a_1,\dots,a_n) \in B^n,\ (a,x) = a_1x_1 \oplus \dots \oplus a_nx_n$.

## 1 Introduction

It is common that in work that concern design and analysis of Boolean functions, the probability properties of the functions – balance, probability of coinciding with an affine function, balance of a directional derivative (the propagation criteria) – are investigated under the assumption that function's arguments are independent binary random variables with the uniform probability distribution ([2], [3], [4], [7], [8], [9]). This paper brings attention to the case when the arguments' distributions differ from the uniform distribution.

The necessity of such an investigation can be explained by adducing the task of combining pseudorandom binary sequences. Let $x_{1t},\dots,x_{nt}$ be n binary pseudorandom sequences generated by one of the simple methods. In order to construct a pseudorandom sequence that is closer to the sequence of independent binary random variables with the uniform probability distribution, the parallel combining of the sequences is used:

$$y_t = f(x_{1t},\dots,x_{nt}),$$

where $f(x_1,\dots,x_n)$ is a Boolean function. When choosing a suitable function $f(x_1,\dots,x_n)$ the following reasons are taken into account. It is known ([5], Chapter 6.3) that if the sequences $x_{it}$ are generated by linear feedback shift registers (LFSR) the *linear complexity* of the output sequence $y_t$ (the length of the shortest LFSR that generates this sequence) is equal to

$$L(y_t) = f^*(L(x_{1t}), \dots, L(x_{nt})),$$

where $L(x_{it})$ is the linear complexity of the sequence $x_{it}$ and $f^*(x)$ is the algebraic normal form of the function $f(x)$ evaluated over the reals with respective replacement of the operations to the real multiplication and addition. The function $f(x_1, \dots, x_n)$ is chosen to maximize $L(y_t)$. The good probability properties of the function are of importance too: $f(x)$ should be balanced and correlation immune. Let us consider the balance of a Boolean function. It implies that if the function's arguments are independent and uniformly distributed binary random variables then the function's value is also uniformly distributed. But it seems reasonable to suppose that the probability distributions of the input sequences differ from the uniform distribution due to weakness of the modelling. Therefore it is desirable to know how much the distribution of the output sequence differ from the uniform distribution in its turn.

We will consider Boolean functions $f(x),\ x = (x_1, \dots, x_n) \in B^n,\ B = \{0, 1\}$, and will suppose that $x_1, \dots, x_n$ are independent binary random variables with probability distributions $P\{x_i = 1\} = \frac{1}{2} - \epsilon_i,\ i = \overline{1, n}$.

We assume that we know the value that is not exceeded by the deviations from the uniform distribution of the probability distributions of the function's arguments:

$$|\epsilon_i| \le \epsilon,\ i = \overline{1, n}.$$

Under these conditions we will investigate characteristics of a general form

$$\Delta_F(f(), \epsilon) = \max_{|\epsilon_i| \le \epsilon, i = \overline{1,n}} |\frac{1}{2} - P\{y = 1\}|, \tag{1}$$

where $y = F(x)$. We will study $\Delta_F(f(), \epsilon)$ with $F()$ equal to:

1. $F(x) = f(x)$,
2. $F(x) = f(x) \oplus (a, x)$,
3. $F(x) = f(x) \oplus f(x \oplus a)$,

where $a = (a_1, \dots, a_n) \in B^n,\ (a, x) = a_1 x_1 \oplus \dots \oplus a_n x_n$.

In the following we will denote by $\Delta_f(\epsilon)$, $\Delta_f^{(a)}(\epsilon)$, $D_f^{(a)}(\epsilon)$ the characteristics $\Delta_F(f(), \epsilon)$ for the choices 1, 2, 3 of $F()$ respectively.

At first we will study the characteristic $\Delta_f(\epsilon)$ – the maximum deviation from the uniform distribution of the probability distribution of the function's value, when the distributions of the function's arguments deviate from the uniform distribution for not more than $\epsilon$. Since $\Delta_f^{(a)}(\epsilon) = \Delta_g(\epsilon)$ and $D_f^{(a)}(\epsilon) = \Delta_{d_{f,a}}(\epsilon)$, where $g(x) = f(x) \oplus (a, x)$ and $d_{f,a}(x) = f(x) \oplus f(x \oplus a)$, their properties will be derived as an application of the properties of $\Delta_f(\epsilon)$.

In conclusion we will pay attention to the behaviour of $\Delta_f(\epsilon)$ when $\epsilon \to \frac{1}{2}$ and will show that it is determined by the minimum sensitivity of $f(x)$.

## 2 Preliminaries

We will define the algebraic normal form, the Walsh-Hadamard transform, the classes of balanced and correlation immune Boolean functions, bent functions, and adduce their well known properties (see e.g. [2], [4], [8], [9]).

The *algebraic normal form* of a Boolean function $f(x)$ is its representation as a polynomial modulo 2. The *(nonlinearity) order* of $f(x)$ is defined as the degree of this polynomial.

The *Walsh-Hadamard transform* of a real valued function $f(x)$ is a function

$$F(w) = \sum_{x \in B^n} f(x)(-1)^{(x,w)}, \; w \in B^n. \tag{2}$$

Often instead of a Boolean function $f(x)$, the function $\hat{f}(x) = (-1)^{f(x)} = 1 - 2f(x)$ is considered that takes values from $\{-1, 1\}$. The Walsh-Hadamard transforms of $f(x)$ and $\hat{f}(x)$ are related as follows:

$$\hat{F}(w) = -2F(w) + 2^n\delta(w), \; \delta(w) = \begin{cases} 1, & w = 0, \\ 0, & w \neq 0. \end{cases} \tag{3}$$

The values of the Walsh Hadamard transform satisfy the *inversion formula*:

$$\sum_{w \in B^n} (-1)^{(x,w)}\hat{F}(w) = \hat{f}(x)2^n,$$

particularly,

$$\sum_{w \in B^n} \hat{F}(w) = \hat{f}(0)2^n, \tag{4}$$

and *Parseval's equation*:

$$\sum_{w \in B^n} \hat{F}^2(w) = 2^{2n}. \tag{5}$$

$\hat{F}^2(w)$ values are called the *Walsh-Hadamard spectrum* of the function $f(x)$. From (5) it follows that $0 \leq \hat{F}^2(w) \leq 2^{2n}$.

Let us by $\hat{F}(w)$, $\hat{G}(w)$, $\hat{H}(w)$ denote the Walsh-Hadamard transforms of the functions $\hat{f}(x)$, $\hat{g}(x)$, $\hat{h}(x)$ respectively.

- If $g(x) = f(x) \oplus 1$ then

$$\hat{G}(w) = -\hat{F}(w). \tag{6}$$

- If $g(x) = f(x) \oplus (a, x), \; a \in B^n$, then

$$\hat{G}(w) = \hat{F}(w \oplus a). \tag{7}$$

- If $g(x) = f(x \oplus a),\ a \in B^n$, then

$$\hat{G}(w) = (-1)^{(a,w)} \hat{F}(w). \tag{8}$$

- If $g(x) = f(xA)$, where $A$ is a nonsingular matrix, then

$$\hat{G}(w) = \hat{F}(w(A^{-1})^T) \tag{9}$$

  ($A^T$ denotes the transpose of $A$).

- If $h(x) = f(x) \oplus g(x)$ then

$$\hat{H}(w) = \frac{1}{2^n} \sum_{v \in B^n} \hat{F}(v)\hat{G}(v \oplus w). \tag{10}$$

If $f(x) = l_{a,a_0}(x) = (a,x) \oplus a_0,\ a \in B^n,\ a_0 \in B$, i.e. $f(x)$ is an *affine function*, then

$$\hat{F}(w) = \begin{cases} (-1)^{a_0} 2^n, & w = a, \\ 0, & \text{otherwise.} \end{cases} \tag{11}$$

By $W(x)$ we denote the *Hamming weight* of a Boolean vector $x$ (the number of ones in the vector), and let $W(f) = \sum\limits_{x \in B^n} f(x)$ for a real valued function $f(x)$. Take notice that it follows from (2) and (3) that

$$\hat{F}(0) = 2^n - 2W(f) = W(\hat{f}). \tag{12}$$

A Boolean function $f(x)$ is called *balanced* if

$$W(f) = 2^{n-1}\ (W(\hat{f}) = 0), \tag{13}$$

i.e. $f(x)$ takes the value 1 for the half of all $n$-tuples of its arguments. It follows from (12) and (13) that $f(x)$ is balanced if and only if

$$\hat{F}(0) = 0. \tag{14}$$

Balance of a Boolean function provides the uniform probability distribution of the function's value if the function's arguments are independent and uniformly distributed binary random variables.

A Boolean function $f(x)$ is called *$k$-th order correlation immune*, $1 \le k \le n-1$, if

$$\hat{F}(w) = 0,\ 1 \le W(w) \le k. \tag{15}$$

There are only two functions that are balanced and have the highest (equal to $n-1$) order of correlation immunity, namely:

$$f(x) = x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus a_0,\ a_0 \in B. \tag{16}$$

If a Boolean function is $k$-th order correlation immune then there is no statistical dependency between its value and any of its $m,\ 1 \leq m \leq k$, arguments.

A Boolean function $f(x)$ is called *bent* if

$$|\hat{F}(w)| = 2^{\frac{n}{2}},\ \forall w \in B^n. \tag{17}$$

The important property of bent-functions $f(x)$ is that their *nonlinearity* $N(f) = \min_{a \in B^n, a_0 \in B} d(f, l_{a,a_0})$, where $d(f,g) = W(f \oplus g)$ is the *Hamming distance* between $f(x)$ and $g(x)$, reaches the maximum value $(N(f) = 2^{n-1} - 2^{\frac{n}{2}-1})$.

We define by $d_{f,a}(x) = f(x) \oplus f(x \oplus a)$ the *directional derivative* of $f(x)$ in direction $a$.

All bent functions $f(x)$ satisfy the *propagation criterion* of the highest degree $n$, which means balance of $d_{f,a}(x)$ for all vectors $a \in B^n,\ a \neq 0$.

On the other hand, it is clear that bent functions are never balanced or correlation immune. Bent functions exist only for even $n$.

Also for a Boolean vector $w$ we will denote by $i(w),\ 1 \leq i \leq W(w)$, the index of the $i$-th non-zero component of $w$.

## 3 The basic results

Hereafter we will suppose that $x_1, \dots, x_n$ are independent binary random variables with probability distributions $P\{x_i = 1\} = \frac{1}{2} - \epsilon_i,\ P\{x_i = 0\} = \frac{1}{2} + \epsilon_i,\ i = \overline{1,n}$.

The results reported in the paper are based on the following theorem that relates the probability distribution of a Boolean function's value with the probability distributions of its arguments.

**Theorem 3.1.** *For an arbitrary Boolean function $f(x)$*

$$\frac{1}{2} - P\{y = 1\} = \frac{1}{2^{n+1}}\hat{F}(0) + \frac{1}{2^{n+1}} \sum_{s=1}^{n} 2^s \sum_{w \in B^n, W(w)=s} \hat{F}(w)\epsilon_{1(w)} \dots \epsilon_{s(w)}, \tag{18}$$

*where $y = f(x)$.*

*Proof.*

$$
\begin{aligned}
\frac{1}{2}-P\{y=1\} &= \frac{1}{2}-\sum_{\alpha\in B^n, f(\alpha)=1} P\{x_1=\alpha_1,\dots,x_n=\alpha_n\} = \\
&= \frac{1}{2}-\sum_{\alpha\in B^n, f(\alpha)=1} P\{x_1=\alpha_1\}\dots P\{x_n=\alpha_n\} = \\
&= \frac{1}{2}-\sum_{\alpha\in B^n, f(\alpha)=1} (\frac{1}{2}+(-1)^{\alpha_1}\epsilon_1)\dots(\frac{1}{2}+(-1)^{\alpha_n}\epsilon_n) = \\
&= \frac{1}{2}-\frac{1}{2^n}W(f)-\sum_{\alpha\in B^n, f(\alpha)=1}\sum_{s=1}^{n}\frac{1}{2^{n-s}}\sum_{w\in B^n, W(w)=s}(-1)^{(\alpha,w)}\epsilon_{1(w)}\dots\epsilon_{s(w)} = \\
&= \frac{1}{2}-\frac{1}{2^n}W(f)-\sum_{s=1}^{n}\frac{1}{2^{n-s}}\sum_{w\in B^n, W(w)=s}\;\sum_{\alpha\in B^n, f(\alpha)=1}(-1)^{(\alpha,w)}\epsilon_{1(w)}\dots\epsilon_{s(w)},
\end{aligned} \tag{19}
$$

where $\alpha=(\alpha_1,\dots,\alpha_n)$. Using (19), (2), (3), and (12) we get (18). □

**Corollary 3.1.**

$$
\Delta_f(\epsilon)=\frac{1}{2^{n+1}}\max_{u\in B^n}\left|\sum_{w\in B^n}(-1)^{(u,w)}\hat{F}(w)(2\epsilon)^{W(w)}\right|. \tag{20}
$$

*Proof.* From (18) it follows that $\frac{1}{2}-P\{y=1\}$ depends linearly on every $\epsilon_i,\ i=\overline{1,n}$. Hence the expression $|\frac{1}{2}-P\{y=1\}|$ reaches its maximum value on every $\epsilon_i$ at one of the ends of the interval $[-\epsilon,\epsilon]$, i.e.

$$
\Delta_f(\epsilon)=\max_{|\epsilon_i|=\epsilon, i=\overline{1,n}}\left|\frac{1}{2}-P\{y=1\}\right|,
$$

which implies that if we let $\epsilon_i=(-1)^{u_i}\epsilon,\ u_i\in B$, we can reduce maximization on $\epsilon_i,\ i=\overline{1,n}$, to maximization on a Boolean vector of signs $u\in B^n$. Further, $\epsilon_{1(w)}\dots\epsilon_{s(w)}=(-1)^{(u,w)}\epsilon^s$, and thus we have (20). □

The following technical lemma will be helpful in the further reasonings.

**Lemma 3.1.** *For any $s,\ 0\le s\le n$,*

$$
\sum_{w\in B^n, W(w)=s}(-1)^{(u,w)}\hat{F}(w)=0,\ \forall u\in B^n,
$$

*if and only if*

$$
\hat{F}(w)=0,\ \forall w:\ W(w)=s.
$$

*Proof.* For $s=0$ the statement of the lemma is trivial. Let $1 \leq s \leq n$. Since sufficiency is evident we have to prove only the necessity part of the statement. For $l$ such that $n-l+1 \geq s$ we define

$$S_{l,n}^{(s)}(\alpha_l,\ldots,\alpha_n) = \sum_{l\leq i_1<\ldots<i_s\leq n} (-1)^{\alpha_{i_1}\oplus\ldots\oplus\alpha_{i_s}} \hat{F}(e_{i_1,\ldots,i_s}),$$

where $\alpha_i \in B,\ i=\overline{1,n},\ e_{i_1,\ldots,i_s}$ is the vector whose components with indexes $i_1,\ldots,i_s$ are equal to 1, and the other are equal to 0.

Since by assumption,

$$S_{1,n}^{(s)}(u_1,\ldots,u_n)=0,\ \forall u_i \in B,\ i=\overline{1,n},$$

we have

$$S_{1,n}^{(s)}(0,u_2,\ldots,u_n)+S_{1,n}^{(s)}(1,u_2,\ldots,u_n)=0.$$

On the other hand,

$$S_{1,n}^{(s)}(0,u_2,\ldots,u_n)+S_{1,n}^{(s)}(1,u_2,\ldots,u_n)=S_{2,n}^{(s)}(u_2,\ldots,u_n),$$

and consequently we have

$$S_{2,n}^{(s)}(u_2,\ldots,u_n)=0.$$

Continuing this way, we achieve:

$$S_{n-s+1,n}^{(s)}(u_{n-s+1},\ldots,u_n)=(-1)^{u_{n-s+1}\oplus\ldots\oplus u_n}\hat{F}(e_{n-s+1,\ldots,n})=0,$$

i.e.

$$\hat{F}(e_{n-s+1,\ldots,n})=0.$$

For reasons of symmetry, we have

$$\hat{F}(w)=0, \forall w : W(w)=s.$$

□

The next important theorem states that the higher is the correlation order of a Boolean function the better is the function from the viewpoint of order of smallness of $\Delta_f(\epsilon)$.

**Theorem 3.2.** $\Delta_f(\epsilon)=o(\epsilon^k)$ *if and only if* $f(x)$ *is a balanced and* $k$*-th order correlation immune function.*

*Proof.* First, we will prove that

$$\Delta_f(\epsilon)=o(\epsilon^k) \Leftrightarrow \sum_{w\in B^n, W(w)=s} (-1)^{(u,w)}\hat{F}(w)=0,\ \forall u \in B^n,\ s=\overline{0,k}. \quad (21)$$

The sufficiency is evident and follows from (20). We will prove the necessity part of this statement. Let $s$ be such that $\hat{F}(w)=0,\ \forall w : W(w)<s$, and there

exists $w_0,\ W(w_0) = s$, such that $\hat{F}(w_0) \neq 0$. If $s > k$ then the right side of (21) holds true. Suppose that $s \leq k$ and for a certain $u_0 \in B^n$

$$\left| \sum_{w \in B^n, W(w)=s} (-1)^{(u_0,w)} \hat{F}(w) \right| = C > 0,$$

then by choosing small enough $\epsilon'$ we can write for all $\epsilon:\ 0 \leq \epsilon \leq \epsilon'$

$$\Delta_f(\epsilon) \geq \frac{1}{2^{n+1}} \left( C(2\epsilon)^s + A(u_0, \epsilon) \right),$$

where

$$|A(u_0, \epsilon)| < \frac{1}{2} C(2\epsilon)^s.$$

Hence

$$\Delta_f(\epsilon) \geq \frac{1}{2^{n+2}} C(2\epsilon)^s,$$

but this contadicts the assumption that $\Delta_f(\epsilon) = o(\epsilon^k),\ k \geq s$. The contradiction leads to:

$$\sum_{w \in B^n, W(w)=s} (-1)^{(u,w)} \hat{F}(w) = 0,\ \forall u \in B^n,\ \forall s : s \leq k.$$

And then we obtain from Lemma 3.1:

$$\hat{F}(w) = 0,\ \forall w:\ W(w) \leq k,$$

which means that $f(x)$ is balanced and $k$-th order correlation immune. □

Note that a particular case of Theorem 3.2 is the following statement:

$$\Delta_f(\epsilon) = o(1) \Leftrightarrow f(x) \text{ is balanced} \tag{22}$$

**Lemma 3.2.**

1. $0 \leq \Delta_f(\epsilon) \leq \frac{1}{2},\ \forall \epsilon : 0 \leq \epsilon \leq \frac{1}{2}$.

2. *f(x) is balanced* $\Leftrightarrow$ $\Delta_f(0) = 0$.

3. $\Delta_f(\frac{1}{2}) = \frac{1}{2}$.

4. *If* $\epsilon_1 < \epsilon_2$ *then* $\Delta_f(\epsilon_1) \leq \Delta_f(\epsilon_2)$.

5. *If* $\Delta_f(\epsilon) = 0$ *then* $\epsilon = 0$.

*Proof.* Statements 1 and 4 follow directly from the definition of $\Delta_f(\epsilon)$.

Statements 2 and 3 follow from (20) by substituting $\epsilon = 0$ and $\epsilon = \frac{1}{2}$ into (20) and by (14), (4) and (8).

Suppose that there exists $\epsilon_0$, $0 < \epsilon_0 <= \frac{1}{2}$, such that $\Delta_f(\epsilon_0) = 0$. Hence from property 4 we have: $\Delta_f(\epsilon) = 0$, $\forall \epsilon : \ 0 \leq \epsilon \leq \epsilon_0$. This means $\Delta_f(\epsilon) = o(\epsilon^k)$, $\forall k \geq 0$, and hence Theorem 3.1 demands $f(x)$ to be $n$-th order correlation immune, which is impossible. Thus we have: $\Delta_f(\epsilon) = 0$ implies $\epsilon = 0$. $\square$

Equality (20) allows us to calculate $\Delta_f(\epsilon)$ in practice by looking through all the $2^n$ values of the vector $u$. Let us consider some examples.

**Example 3.1.** *An affine function:*

$$f(x) = (a, x) \oplus a_0, \ \ a \in B^n, \ \ a_0 \in B.$$

*Using (11) we have*

$$\Delta_f(\epsilon) = \frac{1}{2^{n+1}} \max_{u \in B^n} \left| (-1)^{(u,a)} (-1)^{a_0} 2^n (2\epsilon)^{W(a)} \right| = \frac{1}{2} (2\epsilon)^{W(a)}. \tag{23}$$

**Example 3.2.** *The combining function of the Geffe generator ([5], Chapter 6.3):*

$$f(x_1, x_2, x_3) = x_1 x_2 \oplus x_1 x_3 \oplus x_3.$$

*Performing the fast Walsh-Hadamard transform (see e.g. [10]) we have*

$$\hat{F}(0,0,0) = \hat{F}(0,1,1) = \hat{F}(1,0,0) = \hat{F}(1,1,1) = 0;$$
$$\hat{F}(0,0,1) = \hat{F}(0,1,0) = \hat{F}(1,0,1) = 4; \hat{F}(1,1,0) = -4.$$

*Substituting these values of $\hat{F}(w)$, $w \in B^3$, into (20), we have:*

$$\Delta_f(\epsilon) =$$
$$= \frac{1}{16} \max_{u_1 \in B, u_2 \in B, u_3 \in B} |((-1)^{u_2} + (-1)^{u_3}) 8\epsilon + ((-1)^{u_1 \oplus u_3} - (-1)^{u_1 \oplus u_2}) 16 \epsilon^2| =$$
$$= \epsilon.$$

**Example 3.3.** *The majority function ([1]):*

$$f(x) = \begin{cases} 1, & W(x) > k, \\ 0, & W(x) \leq k, \end{cases}$$

*where $x \in B^{2k+1}$, $k \geq 0$. It is known ([1]) that for the majority function*

$$\hat{F}(w) = \begin{cases} 0, & W(w) = 2s, \\ (-1)^s 2 \frac{\binom{2s}{s}\binom{2k-2s}{k-s}}{\binom{k}{s}}, & W(w) = 2s+1, \end{cases}$$

*for* $s = \overline{0,k}$. *It leads to the relation*

$$\Delta_f(\epsilon) = \frac{\binom{2k}{k}(2k+1)}{2^{2k}}\epsilon + o(\epsilon^2),$$

*and hence*

$$\frac{\Delta_f(\epsilon)}{\epsilon} \to M(k) > 1, \ \epsilon \to 0,$$

*and* $M(k)$ *increases when* $k$ *increases.*

Let us investigate now the general properties of $\Delta_f(\epsilon)$.

**Corollary 3.2.**

$$\Delta_f(\epsilon) \le \frac{1}{2^{n+1}} \sum_{w \in B^n} |\hat{F}(w)|(2\epsilon)^{W(w)} = \frac{1}{2^{n+1}} \sum_{s=0}^{n} \sum_{w \in B^n, W(w)=s} |\hat{F}(w)|(2\epsilon)^s. \tag{24}$$

*Proof.* Follows directly from (20). □

Inequality (24) provides an upper estimate of $\Delta_f(\epsilon)$ for an arbitrary Boolean function $f(x)$. Hereafter we will derive upper estimates of $\Delta_f(\epsilon)$ for Boolean functions from certain classes of Boolean functions using (24) and known restrictions on $|\hat{F}(w)|$ for these classes of functions.

Consider the behaviour of $\Delta_f(\epsilon)$ under some simple transformations of $f(x)$.

**Lemma 3.3.** *If* $g(x) = f(x) \oplus 1$ *then* $\Delta_g(\epsilon) = \Delta_f(\epsilon)$.

*Proof.* Follows from (6). □

**Lemma 3.4.** *If* $g(x) = f(x \oplus a)$, $a \in B^n$, *then* $\Delta_g(\epsilon) = \Delta_f(\epsilon)$.

*Proof.* From (8) we have $\hat{G}(w) = (-1)^{(a,w)}\hat{F}(w)$. Substituting this into (20) we have:

$$\begin{aligned}\Delta_g(\epsilon) = \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)}(-1)^{(a,w)}\hat{F}(w)(2\epsilon)^{W(w)} \right| = \\ = \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u \oplus a,w)}\hat{F}(w)(2\epsilon)^{W(w)} \right| = \\ = \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)}\hat{F}(w)(2\epsilon)^{W(w)} \right| = \\ = \Delta_f(\epsilon).\end{aligned}$$

□

**Lemma 3.5.** *If* $\Delta_f(\epsilon) = o(\epsilon^k)$ *and* $g(x) = f(x) \oplus (a,x)$, $a \in B^n$, $W(a) = r \le k$, *then* $\Delta_g(\epsilon) = o(\epsilon^{k-r})$.

*Proof.* Theorem 3.2 implies that $f(x)$ is balanced and $k$-th order correlation immune. Hence $\hat{F}(w) = 0, \ \forall w : W(w) \leq k$. From (7) we have $\hat{G}(w) = \hat{F}(w \oplus a)$. Further, $W(w \oplus a) \leq W(w) + W(a) = W(w) + r$. Hence $\hat{G}(w) = 0$ if $W(w) \leq k - r$. This means that $g(x)$ is balanced and $(k-r)$-th order correlation immune, which implies that $\Delta_g(\epsilon) = o(\epsilon^{k-r})$. □

**Lemma 3.6.** *If $\Delta_f(\epsilon) = o(\epsilon^k)$ and $g(x) = f(xA)$ with $A$ being a non-singular $(n \times n)$-matrix, for which $W(a_i') \leq r \leq k, \ i = \overline{1,n}$, where $a_i'$ is the $i$-th column of the matrix $A^{-1}$, then $\Delta_g(\epsilon) = o(\epsilon^l), \ l = \left[\frac{k}{r}\right]$ ($[\alpha]$ denotes the integer part of $\alpha$).*

*Proof.* From (9) we have $\hat{G}(w) = \hat{F}(w(A^{-1})^T)$. We denote

$$v = w(A^{-1})^T = \bigoplus_{i=1}^{W(w)} (a'_{i(w)})^T.$$

If $W(a_i') \leq r, \ i = \overline{1,n}$, then $W(v) \leq W(w)r$. And for all $w : \ W(w) \leq l$, we have $W(v) \leq lr = \left[\frac{k}{r}\right] r \leq k$. Hence $\hat{G}(w) = \hat{F}(v) = 0, \ \forall w : W(w) \leq l$, which implies $\Delta_g(\epsilon) = o(\epsilon^l)$. □

**Lemma 3.7.** *If $\Delta_f(\epsilon) = o(\epsilon^k)$ and $g(x) = f(s(x))$, where $s() : x \in B^n \to y \in B^n$ such that $y_i = x_{\pi(i)}, \ i = \overline{1,n}$, and $\pi()$ being a permutation on $\{1, \ldots, n\}$, then $\Delta_g(\epsilon) = o(\epsilon^k)$.*

*Proof.* This lemma follows from Lemma 3.6 if we notice that for an arbitrary mapping $s(x)$ that permutes coordinates of $x$, $s(x) = xA$ with a non-singular matrix A such that $W(a_i) = 1, \ i = \overline{1,n}$, where $a_i$ denotes $i$-th column of $A$, and for the mapping that performs the invert permutation of coordinates $s^{-1}(x) = xA^{-1}$. Hence $W(a_i') = 1, \ i = \overline{1,n}$, i.e. under the conditions of Lemma 3.6 $r = 1$ and hence $l = k$. □

# 4 Balanced and correlation immune functions

We showed that $\Delta_f(\epsilon) = o(\epsilon^k)$ for balanced and $k$-th order correlation immune functions. Let us investigate $\Delta_f(\epsilon)$ if $\epsilon$ is fixed.

The next lemma provides a common for all balanced and $k$-th order correlation immune functions of $n$ arguments upper estimate of $\Delta_f(\epsilon)$.

**Lemma 4.1.** *If $f(x)$ is balanced and $k$-th order correlation immune then*

$$\Delta_f(\epsilon) \leq \frac{1}{2} \sum_{s=k+1}^{n} \binom{n}{s} (2\epsilon)^s. \tag{25}$$

*Proof.* Follows from (24), (14), and (15). □

**Lemma 4.2.** *If $f(x)$ is balanced and $k$-th order correlation immune then*

$$0 \le \epsilon \le \bar{\epsilon}_f \Rightarrow \Delta_f(\epsilon) \le \epsilon, \tag{26}$$

*where*

$$\bar{\epsilon}_f = \frac{1}{2}\left(\sum_{s=k+1}^{n} \binom{n}{s}\right)^{-\frac{1}{k}}. \tag{27}$$

*Proof.* It follows from (25) that

$$\Delta_f(\epsilon) \le \frac{1}{2}\sum_{s=k+1}^{n} \binom{n}{s}(2\epsilon)^{k+1}. \tag{28}$$

Solving the inequality

$$\frac{1}{2}\sum_{s=k+1}^{n} \binom{n}{s}(2\epsilon)^{k+1} \le \epsilon,$$

we have

$$\epsilon \le \bar{\epsilon}_f.$$

□

**Corollary 4.1.** *If $f(x)$ is balanced and $(n-1)$-th order correlation immune (i.e. a function of the form (16)), then*

$$0 \le \epsilon \le \frac{1}{2} \Rightarrow \Delta_f(\epsilon) \le \epsilon,$$

*Proof.* Follows from (26) and (27), since $\bar{\epsilon}_f = \frac{1}{2}$ if $k = n-1$. □

From (27) we have that when $k$ – the order of correlation immunity – increases ($n$ is fixed), the value of $\bar{\epsilon}_f$ also increases. That means expansion of the set of such $\epsilon$ for which it is assured that the property $\Delta_f(\epsilon) \le \epsilon$ is valid. When $k = n-1$ this set coincides with the set of all $\epsilon \le \frac{1}{2}$ (this follows from Corollary 4.1).

Let us consider now the behaviour of $\Delta_f(\epsilon)$ in the case when we step from a function with a less number of arguments to a function with a greater number of arguments preserving certain their properties.

**Lemma 4.3.** *Let $f^{(n_0)}(x), f^{(n_0+1)}(x), f^{(n_0+2)}(x), \ldots$ be a sequence of balanced and $(n-r)$-th order correlation immune functions of $n = n_0, n_0+1, n_0+2, \ldots$ arguments respectivly. Then for any fixed $r$, $r \le n_0 - 1$, and $\epsilon < \frac{1}{2}$,*

$$\Delta_{f^{(n)}}(\epsilon) \to 0, \ n \to \infty.$$

*Proof.* From (28) we have

$$\Delta_{f^{(n)}}(\epsilon) \le \frac{1}{2}\sum_{l=0}^{r-1}\binom{n}{n-l}(2\epsilon)^{n-r+1}.$$

Since $\binom{n}{n-l} = \frac{1}{l!}n(n-1)\ldots(n-l+1)$ is a polynomial on $n$ of degree $l$, then $Q_{r-1}(n) = \frac{1}{2}\sum\limits_{l=0}^{r-1}\binom{n}{n-l}$ is a polynomial on $n$ of degree $r-1$. Thus we have

$$\Delta_{f^{(n)}}(\epsilon) \le Q_{r-1}(n)(2\epsilon)^{n-r+1} \to 0,\ n \to \infty.$$

□

# 5 Bent functions

The following lemma provides a common for all bent functions of $n$ arguments upper estimate of $\Delta_f(\epsilon)$.

**Lemma 5.1.** *If $f(x)$ is a bent function then*

$$\Delta_f(\epsilon) \le \frac{1}{2}\left(\frac{1+2\epsilon}{\sqrt{2}}\right)^n - \frac{1}{2^{\frac{n}{2}}}\sum_{s=\frac{n}{2}+1}^{n}\binom{n}{s}(2\epsilon)^s. \tag{29}$$

*Proof.* Substituting (17) into (24) we have

$$\Delta_f(\epsilon) \le \frac{2^{\frac{n}{2}}}{2^{(n+1)}}\left|\sum_{w\in B^n,\hat{F}(w)>0}(2\epsilon)^{W(w)} - \sum_{w\in B^n,\hat{F}(w)<0}(2\epsilon)^{W(w)}\right|.$$

Let $a = |w : \hat{F}(w) > 0|$, $b = |w : \hat{F}(w) < 0|$, then $a + b = 2^n$ and $2^{\frac{n}{2}}(a-b) = \pm 2^n$, and hence $a = 2^{n-1} \pm 2^{\frac{n}{2}-1}$, $b = 2^n - a$. Let us consider the case when $a = 2^{n-1} + 2^{\frac{n}{2}-1}$.

Since $\sum\limits_{s=0}^{\frac{n}{2}-1}\binom{n}{s} = \sum\limits_{s=\frac{n}{2}+1}^{n}\binom{n}{s}$ and $\sum\limits_{s=0}^{n}\binom{n}{s} = 2^n$, we have

$$\sum_{s=0}^{\frac{n}{2}}\binom{n}{s} = 2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}.$$

Using the inequality $\binom{n}{\frac{n}{2}} \ge 2^{\frac{n}{2}}$ we have

$$\sum_{s=0}^{\frac{n}{2}}\binom{n}{s} \ge 2^{n-1} + 2^{\frac{n}{2}-1},$$

which implies

$$|w : W(w) \le \frac{n}{2}| \ge |w : \hat{F}(w) > 0|,$$

therefore

$$\left| \sum_{w\in B^n, \hat{F}(w)>0} (2\epsilon)^{W(w)} - \sum_{w\in B^n, \hat{F}(w)<0} (2\epsilon)^{W(w)} \right| \leq$$

$$\leq \sum_{w\in B^n, W(w)\leq \frac{n}{2}} (2\epsilon)^{W(w)} - \sum_{w\in B^n, W(w)>\frac{n}{2}} (2\epsilon)^{W(w)} =$$

$$= \sum_{w\in B^n} (2\epsilon)^{W(w)} - 2 \sum_{w\in B^n, W(w)>\frac{n}{2}} (2\epsilon)^{W(w)} =$$

$$= (1+2\epsilon)^n - 2 \sum_{s=\frac{n}{2}+1}^{n} \binom{n}{s} (2\epsilon)^s.$$

The case when $a = 2^{n-1} - 2^{\frac{n}{2}-1}$ is treated in a similar way. □

Here we will formulate an analogue to Lemma 4.3 for bent functions.

**Lemma 5.2.** *Let $f^{(n_0)}(x), f^{(n_0+2)}(x), f^{(n_0+4)}(x), \ldots$ be a sequence of bent functions of $n = n_0, n_0+2, n_0+4, \ldots$ arguments respectively ($n_0$ is even). Then, provided that $\epsilon < \frac{\sqrt{2}-1}{2}$, we have*

$$\Delta_{f^{(n)}}(\epsilon) \to 0, \;\; n \to \infty.$$

*Proof.* Follows from (29). □

# 6 Second order functions

It is known that any Boolean function of the second order, i.e. a function of the form

$$f(x) = \bigoplus_{1\leq i<j\leq n} b_{ij} x_i x_j \oplus \bigoplus_{i=1}^{n} b_i x_i \oplus b_0, \tag{30}$$

where $b_{ij} \in B,\ 1 \leq i < j \leq n,\ b_i \in B,\ i = \overline{0,n}$, can be reduced by an invertible affine transformation of coordinates to the form

$$f(x) = s(x) \oplus (c,x) \oplus c_0, \tag{31}$$

where

$$s(x) = \bigoplus_{i=1}^{h} x_{2i-1}x_{2i},\ \ 1 \leq h \leq \left[\frac{n}{2}\right], \tag{32}$$

$$c = (c_1, \ldots, c_n),\ \ c_i = 0,\ \ i = \overline{1,2h}.$$

It is shown in [8] that

$$\hat{S}(w) = \begin{cases} 2^{n-h}, & w_i = 0,\ i = \overline{2h+1, n}, \\ 0, & \text{otherwise}, \end{cases}$$

where $\hat{S}(w)$ is the Walsh-Hadamard transform of $\hat{s}(x)$. Hence by (6) and (7) we obtain for the Walsh-Hadamard transform of $\hat{f}(x)$ if $f(x)$ is of the form (31):

$$\hat{F}(w) = \begin{cases} (-1)^{c_0} 2^{n-h}, & w_i = c_i,\ i = \overline{2h+1, n}, \\ 0, & \text{otherwise}. \end{cases} \tag{33}$$

That allows us to estimate $\Delta_f(\epsilon)$.

**Lemma 6.1.** *If $f(x)$ is of the form (31) then*

$$\Delta_f(\epsilon) \le \frac{1}{2} \left( \frac{1+2\epsilon}{\sqrt{2}} \right)^{2h} (2\epsilon)^r, \tag{34}$$

*where $r = W(c)$.*

*Proof.* We substitute (33) into (24) and get

$$\Delta_f(\epsilon) \le \frac{1}{2^{n+1}} \sum_{s=0}^{2h} (2\epsilon)^{s+r} \binom{2h}{s} 2^{n-h},$$

and hence (34) follows. □

Since an invertible affine transformation of coordinates keeps constant the set of the Walsh-Hadamard spectrum values (see (9)), for second order functions we have

$$|\hat{F}(w)| = 2^{n-h}, \text{ if } |\hat{F}(w)| \ne 0, \tag{35}$$

which allows us to estimate $\Delta_f(\epsilon)$ for an arbitrary second order Boolean function.

**Lemma 6.2.** *If $f(x)$ is a second order function then*

$$\Delta_f(\epsilon) \le \frac{1}{2^{h+1}} (1+2\epsilon)^n - \frac{1}{2^h} \sum_{s=n-h+1}^{n} (2\epsilon)^s.$$

*Proof.* The lemma can be proved in the way that is similar to the proof of Lemma 5.1, taking into account (35) and the fact: $|w : |\hat{F}(w)| = 2^{n-h}| = 2^{2h}$. □

Let us obtain for second order functions an analogue of Lemmas 4.3 and 5.2.

**Lemma 6.3.** *Let $f^{(n_0)}(x), f^{(n_0+1)}(x), f^{(n_0+2)}(x), \ldots$ be a sequence of second order functions of $n = n_0, n_0+1, n_0+2, \ldots$ arguments respectively. Let $h_n$ be the value of $h$ evaluated for $f^{(n)}(x)$. If $\epsilon < \frac{\sqrt{2}-1}{2}$ and $\exists H : \frac{n}{2} - h_n \le H$, then*

$$\Delta_{f^{(n)}}(\epsilon) \to 0, \ n \to \infty.$$

*Proof.*

$$\Delta_{f^{(n)}}(\epsilon) \le \frac{1}{2^{h_n+1}}(1+2\epsilon)^n - \frac{1}{2^{h_n}} \sum_{s=n-h_n+1}^{n} (2\epsilon)^s \le 2^{H-1}\left(\frac{1+2\epsilon}{\sqrt{2}}\right)^n \to 0,$$

if $\epsilon < \frac{\sqrt{2}-1}{2}$. □

# 7 Characteristics $\Delta_f^{(a)}(\epsilon)$ and $D_f^{(a)}(\epsilon)$

## 7.1 $\Delta_f^{(a)}(\epsilon)$

As we defined earlier,

$$\Delta_f^{(a)}(\epsilon) = \frac{1}{2^{n+1}} \max_{|\epsilon_i| \le \epsilon, i=\overline{1,n}} |\frac{1}{2} - P\{f(x) \oplus (a,x) = 1\}|.$$

Note that from (22) and (7) we have

$$\Delta_f^{(a)}(0) = 0 \Leftrightarrow g(x) \text{ is balanced } \Leftrightarrow \hat{F}(x \oplus a) = 0,$$

where $g(x) = f(x) \oplus (a,x), \ a \in B^n$. Moreover,

$$\Delta_{f \oplus a_0}^{(a)}(0) = \left| \frac{1}{2} - \frac{1}{2^n} d(f, l_{a,a_0}) \right|,$$

where $a_0 \in B$. Since (by Lemma 3.3) $\Delta_f^{(a)}(\epsilon) = \Delta_{f\oplus a_0}^{(a)}(\epsilon)$ and $d(f, l_{a,a_0}) = 2^{n-1} + s$ implies $d(f, l_{a,a_0\oplus 1}) = 2^{n-1} - s$, we have

$$\begin{aligned}
\max_{a \in B^n} \Delta_f^{(a)}(0) &= \max_{a \in B^n, a_0 \in B} \left| \frac{1}{2} - \frac{1}{2^n} d(f, l_{a,a_0}) \right| = \\
&= \max_{a \in B^n, a_0 \in B} \left( \frac{1}{2} - \frac{1}{2^n} d(f, l_{a,a_0}) \right) = \frac{1}{2} - \frac{1}{2^n} \min_{a \in B^n, a_0 \in B} d(f, l_{a,a_0}) = \\
&= \frac{1}{2} - \frac{1}{2^n} N(f),
\end{aligned}$$

or conversely:

$$N(f) = 2^{n-1} - 2^n \max_{a \in B^n} \Delta_f^{(a)}(0).$$

**Lemma 7.1.**

$$\Delta_f^{(a)}(\epsilon) = \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)} \hat{F}(w \oplus a)(2\epsilon)^{W(w)} \right|.$$

*Proof.* Follows from (7) and (20). □

By Lemma 3.5 we have showed already that if $f(x)$ is a **balanced and $k$-th order correlation immune function** and $W(a) = r \leq k,\ a \in B^n$, then

$$\Delta_f^{(a)}(\epsilon) = o(\epsilon^{k-r}),$$

i.e. $g(x)$ is balanced and $(k-r)$-th order correlation immune, and hence

$$\Delta_f^{(a)}(\epsilon) \leq \sum_{s=k-r+1}^{n} \binom{n}{s} (2\epsilon)^s.$$

For **bent functions**, since $|F(x \oplus a)| = |F(x)| = 2^{\frac{n}{2}}$, we have for $\Delta_f^{(a)}(\epsilon)$ the same upper estimate as for $\Delta_f(\epsilon)$:

$$\Delta_f^{(a)}(\epsilon) \leq \frac{1}{2}\left(\frac{1+2\epsilon}{\sqrt{2}}\right)^n - \frac{1}{2^{\frac{n}{2}}} \sum_{s=\frac{n}{2}+1}^{n} \binom{n}{s} (2\epsilon)^s.$$

Also we have

$$\Delta_f^{(a)}(\epsilon) \leq \frac{1}{2}\left(\frac{1+2\epsilon}{\sqrt{2}}\right)^{2h} (2\epsilon)^r$$

for **functions of the form (31)**, where $r = \sum_{i=2h+1}^{n} (a_i \oplus c_i)$, and

$$\Delta_f^{(a)}(\epsilon) \leq \frac{1}{2^{h+1}}(1+2\epsilon)^n - \frac{1}{2^h} \sum_{s=n-h+1}^{n} (2\epsilon)^s$$

for **second order functions**.

## 7.2 $D_f^{(a)}(\epsilon)$

By definition,

$$D_f^{(a)}(\epsilon) = \max_{|\epsilon_i| \leq \epsilon,\ i=\overline{1,n}} |\frac{1}{2} - P\{d_{f,a}(x) = 1\}|.$$

**Lemma 7.2.**

$$D_f^{(a)}(\epsilon) = \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)} \hat{H}(w)(2\epsilon)^{W(w)} \right|,$$

*where*

$$\hat{H}(w) = \frac{1}{2^n} \sum_{v \in B^n} (-1)^{(a,v)} \hat{F}(v) \hat{F}(v \oplus w) \tag{36}$$

*is the Walsh-Hadamard transform of* $\hat{d}_{f,a}(x)$.

*Proof.* Follows from (20), (8) and (10). □

The *auto-correlation function* of a Boolean function $f(x)$ is defined ([7]) as

$$\hat{r}_f(a) = W(\hat{d}_{f,a}).$$

From (36) and (12) it follows that

$$\hat{r}_f(a) = \frac{1}{2^n} \sum_{v \in B^n} (-1)^{(a,v)} \hat{F}^2(v),$$

which is known as the Wiener-Khintchin theorem. Hence

$$D_f^{(a)}(0) = \frac{1}{2^{n+1}} |\hat{r}_f(a)|.$$

In [7] the extended propagation criterion was defined. A Boolean function is said to satisfy the *extended propagation criterion of degree* $m$ *and order* $k$ (EPC($m$,$k$)) if knowledge of $k$ bits of $x$ gives no information on $d_{f,a}(x)$, $\forall a:\ 1 \leq W(a) \leq m$.

The propagation criterion of degree $m$ is a particular case of the above definition, namely, it is equal to EPC($m$,0).

It was shown also in [7] that $f(x)$ satisfies EPC($m$,$k$) if and only if the direction derivative $d_{f,a}(x)$ is balanced and $k$-th order correlation immune for all $a : 1 \leq W(a) \leq m$. This result leads to the following property of $D_f^{(a)}(\epsilon)$.

**Lemma 7.3.** $D_f^{(a)}(\epsilon) = o(\epsilon^k)$, $\forall a:\ 1 \leq W(a) \leq m$, *if and only if* $f(x)$ *satisfies EPC(*$m$,$k$*).*

In addition, for a function that satisfies EPC($m$,$k$) we have

$$D_f^{(a)}(\epsilon) \leq \frac{1}{2} \sum_{s=k+1}^{n} \binom{n}{s} (2\epsilon)^s,$$

for all $a:\ 1 \leq W(a) \leq m$.

Since **bent functions** satisfy EPC($m$,0) for all $m = \overline{1,n}$, then

$$D_f^{(a)}(\epsilon) = o(1),\ \forall a \neq 0,$$

for a bent function $f(x)$.

Let us consider a **second order function** (30), which can be written in the form $f(x) = xCx^T \oplus (b, x) \oplus b_0$, where $C = \{c_{ij}\}$, $c_{ij} \in B$, is an $(n \times n)$-matrix, $b = (b_1, \dots, b_n) \in B^n$, $b_0 \in B$. Since

$$f(x \oplus a) = (x \oplus a)C(x \oplus a)^T \oplus (b, x \oplus a) \oplus b_0 = f(x) \oplus (c, x) \oplus c_0,$$

where $c = a(C \oplus C^T)$, $c_0 \in B$, by (23) we have:

$$D_f^{(a)}(x) = \frac{1}{2}(2\epsilon)^{W(c)}.$$

# 8 The behaviour of $\Delta_f(\epsilon)$ when $\epsilon \to \frac{1}{2}$

Earlier, by Theorem 3.2, we have showed what functions are better from the viewpoint of order of smallness of $\Delta_f(\epsilon)$. Now we concern the case when $\epsilon \to \frac{1}{2}$. This means the situation when the probability distributions of the function's arguments can vary almost arbitrarily. We know (Lemma 3.2) that $\Delta_f(\frac{1}{2}) = \frac{1}{2}$, but for different functions the speed with which $\Delta_f(\epsilon)$ tends to $\frac{1}{2}$ can vary. We will show what it depends on.

We define the *sensitivity* of a Boolean function ([1]) on a Boolean vector $x \in B^n$ as

$$S_f(x) = \sum_{i=1}^{n} d_{f,e_i}(x).$$

Also we define the *minimum sensitivity* of a Boolean function as

$$S_{min}(f) = \min_{x \in B^n} S_f(x).$$

Note that

$$0 \leq S_{min}(f) \leq n.$$

**Theorem 8.1.**

$$\frac{1}{2} - \Delta_f(\frac{1}{2} - \alpha) = S_{min}(f)\alpha + o(\alpha). \tag{37}$$

*Proof.*

$$\begin{aligned}
&\frac{1}{2} - \Delta_f(\frac{1}{2} - \alpha) = \\
&\quad = \frac{1}{2} - \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)} \hat{F}(w)(1 - 2\alpha)^{W(w)} \right| = \\
&\quad = \frac{1}{2} - \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)} \hat{F}(w) \left(1 - 2W(w)\alpha + o(\alpha)\right) \right| = \\
&\quad = \frac{1}{2} - \frac{1}{2^{n+1}} \max_{u \in B^n} \left| \hat{f}(u)2^n - 2\alpha \sum_{w \in B^n} (-1)^{(u,w)} W(w)\hat{F}(w) + o(\alpha) \right| = \\
&\quad = \frac{1}{2^n} \min_{u \in B^n} \left| \sum_{w \in B^n} (-1)^{(u,w)} W(w)\hat{F}(w) \right| \alpha + o(\alpha).
\end{aligned}$$

Since it is shown in [1] that

$$S_f(u) = \frac{1}{2^n} \left| \sum_{w \in B^n} (-1)^{(u,w)} W(w) \hat{F}(w) \right|$$

we obtain (37). $\square$

Theorem 8.1 implies that if the minimum sensitivity of $f(x)$ is equal to 0 then $\Delta_f(\epsilon)$ tends to $\frac{1}{2}$ very fast while $\epsilon$ tends to $\frac{1}{2}$.

**Lemma 8.1.** *If $f(x) = l_{a,a_0}(x)$, $a \in B^n$, $a_0 \in B$, then $S_{min}(f) = W(a)$.*

*Proof.* Since $d_{l_{a,a_0},e_i}(x) = a_i$,

$$S_{min}(f) = \min_{x \in B^n} \sum_{i=1}^{n} a_i = W(a).$$

$\square$

**Lemma 8.2.** *$S_{min}(f) = n$ if and only if f(x) is of the form (16).*

*Proof.* If $f(x)$ is of the form (16) then by Lemma 8.1 we have $S_{min}(f) = n$.
If $S_{min}(f) = n$ then

$$S_f(x) = n, \ \forall x \in B^n,$$

hence

$$\sum_{i=1}^{n} d_{f,e_i}(x) = n, \ \forall x \in B^n,$$

and consequently

$$d_{f,e_i}(x) = 1, \ \forall x \in B^n, \ i = \overline{1,n},$$

which leads to

$$f(x_1, \ldots, x_n) = g_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus x_i, \ i = \overline{1,n},$$

which implies

$$f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n \oplus a_0, \ a_0 \in B.$$

$\square$

It is worth noting that the best functions from the viewpoint of maximum of $S_{min}(f)$ are the best functions from the viewpoint of order of smallness of $\Delta_f(\epsilon)$.

**Lemma 8.3.** *If there is no terms of the first order in the algebraic normal form of $f(x)$ then $S_{min}(f) = 0$.*

*Proof.* Under these conditions the algebraic normal form of $d_{f,e_i}(x)$ has no constant term. Hence $d_{f,e_i}(0) = 0,\ i = \overline{1,n}$, and

$$S_{min}(f) = S_f(0) = \sum_{i=1}^{n} d_{f,e_i}(0) = 0.$$

$\square$

**Lemma 8.4.** *If $f(x) = g(x) \oplus l_{a,a_0}(x),\ a \in B^n,\ a_0 \in B$, with $g(x)$ such that it has no terms of the first order in its algebraic normal form, then $S_{min}(f) > 0$ if and only if the system*

$$d_{g,e_i}(x) = a_i,\ \ i = \overline{1,n},$$

*has no solutions.*

*Proof.* Note that $d_{f,e_i}(x) = d_{g,e_i}(x) \oplus a_i$. Then we have the following reasonings.
$S_{min}(f) = 0$ if and only if
there exists $x_0 \in B^n$ such that $S_f(x_0) = 0$ if and only if
$d_{f,e_i}(x_0) = 0,\ i = \overline{1,n}$, if and only if
$d_{g,e_i}(x_0) \oplus a_i = 0,\ i = \overline{1,n}$,
which implies the statement of the lemma. $\square$

Let us continue with the examples of $f(x)$ considered above.

**Example 8.1.** *The combining function of the Geffe generator.*

$$\begin{aligned}
&S_{min}(f) = \\
&= \frac{1}{8} \min_{u_1 \in B, u_2 \in B, u_3 \in B} \left| ((-1)^{u_2} + (-1)^{u_3})4 + ((-1)^{u_1 \oplus u_2} + (-1)^{u_1 \oplus u_3})8 \right| = \\
&\qquad = 1.
\end{aligned}$$

**Example 8.2.** *The majority function. Let $u_0 = (1, 1, \ldots, 1)$, then*

$$\begin{aligned}
&S_f(u_0) = \\
&= \frac{1}{2^n} \left| \sum_{s=0}^{k} \sum_{w \in B^n, W(w) = 2s+1} (-1)^{\bigoplus_{i=1}^{n} w_i} 2(-1)^s \frac{\binom{2s}{s}\binom{2k-2s}{k-s}}{\binom{k}{s}} (2s+1) \right| = \\
&\qquad = \frac{1}{2^{n-1}} \left| \sum_{s=0}^{k} (-1)^s \frac{\binom{2s}{s}\binom{2k-2s}{k-s}}{\binom{k}{s}} (2s+1) \binom{2k+1}{2s+1} \right| = \\
&\qquad\qquad = \frac{1}{2^{n-1}} \binom{2k}{k} (2k+1) \left| \sum_{s=0}^{k} (-1)^s \binom{k}{s} \right| = 0.
\end{aligned}$$

*Hence $S_{min}(f) = 0$.*

## 9 Conclusion

In this paper we supposed that the probability distributions of a Boolean function's arguments deviate from the uniform distribution and these deviations do not exceed $\epsilon$. Under these conditions we presented new characteristics $\Delta_F(f(), \epsilon)$ of the probability properties of Boolean functions.

The relation between the probability distribution of a Boolean function's value and the probability distributions of its arguments was established, and by use of this the explicit formula for evaluating of $\Delta_F(f(), \epsilon)$ was obtained.

We presented two approaches to determine what functions are better than others – for small $\epsilon$, and for large $\epsilon$. We paid special attention to the classes of balanced and correlation immune functions, bent functions, and second order functions, for which upper estimates of $\Delta_F(f(), \epsilon)$ were found and statements on behaviour of sequences $f^{(n)}(x)$ of functions of $n$ arguments with $n \to \infty$ were made.

The main results of this paper were reported in [6].

## Acknowledgements

The author wishes to express his thanks to Sergey Agievich for his fruitful suggestions.

## References

[1] A.Bernasconi, B.Codenotti, J.Simon, On the Fourier Analysis of Boolean Functions, Preprint, 1996

[2] R.Forre, The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition, Advances in Cryptology - Crypto'88, Proceedings, pp.450-468, Springer-Verlag, 1990

[3] K.Kurosawa, T.Satoh, Design of SAC/PC($l$) of Order $k$ Boolean Functions, and Three Other Cryptographic Criteria, Advances in Cryptology - Eurocrypt'97, Proceedings, pp.434-449, Springer-Verlag, 1997

[4] W.Meier, O.Staffelbach, Nonlinearity Criteria for Cryptographic Functions, Advances in Cryptology - Eurocrypt'89, Proceedings, pp.549-562, Springer-Verlag, 1990

[5] A.J.Menezes, P.C. van Oorschot, S.A.Vanstone, Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida, 1997

[6] K.Miranovich, On Probability Properties of Certain Classes of Boolean Functions, in Russian, Proceedings of VIII All-Russian School-Colloquium for Stochastic Methods, Joshkar-Ola, 2001

[7] B.Preneel, Van Leekwijck, Van Linden, R.Govaerts, J.Vandewalle, Propagation characteristics of Boolean functions, Advances in Cryptology - Eurocrypt'90, Proceedings, pp.161-173, Springer-Verlag, 1991

[8] B.Preneel, R.Govaerts, J.Vandewalle, Boolean Functions Satisfying Higher Order Propagations Criteria, Advances in Cryptology - Eurocrypt'91, Proceedings, pp.141-152, Springer-Verlag, 1991

[9] J.Seberry, X.Zhang, Y.Zheng, Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics, Advances in Cryptology - Eurocrypt'93, Proceedings, pp.49-60, Springer-Verlag, 1994

[10] M.A.Thornton, D.M.Miller, R.Drechsler, Transformations Amongst the Walsh, Haar, Arithmetic and Reed-Muller Spectral Domains, International Workshop on Applications of the Reed-Muller Expansion in Circuit Design, pp. 215-225, 2001