S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 18, №1, стр. 561–578 (2021) УДК 519.7
DOI 10.33048/semi.2021.18.041 MSC 06E30, 11T71, 14G50

CONNECTIONS BETWEEN QUATERNARY AND BOOLEAN BENT FUNCTIONS

N.N. TOKAREVA, A.S. SHAPORENKO, P. SOLÉ

Abstract. Boolean bent functions were introduced by Rothaus (1976) as combinatorial objects related to difference sets, and have since enjoyed a great popularity in symmetric cryptography and low correlation sequence design. In this paper connections between classical Boolean bent functions, generalized Boolean bent functions and quaternary bent functions are studied. We also study Gray images of bent functions and notions of generalized nonlinearity for functions that are relevant to generalized linear cryptanalysis.

Keywords: Boolean functions, generalized Boolean functions, quaternary functions, bent functions, semi bent functions, nonlinearity, linear cryptanalysis, Gray map, $\mathbb{Z}_4$-linear codes.

1. Introduction

Boolean bent functions were introduced by Rothaus [23] as combinatorial objects related to difference sets, and have since enjoyed a great popularity in symmetric cryptography and sequence design. They are, in particular, maps from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ with some special spectral properties. Their importance in symmetric cryptography stems from linear cryptanalysis of stream ciphers [15, 16, 17]. In that context bent functions are the ones which are the worst approximated by affine functions, or, equivalently have the best possible nonlinearity. More information concerning bent functions can be found in the monographs [19, 32]. Several researchers [3, 6, 20, 21]

Tokareva, N.N., Shaporenko, A.S., Solé, P., Connections between quaternary and Boolean bent functions.

The work of the first and the second authors was supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

Received October, 5, 2020, published May, 26, 2021.

have explored extensions of linear cryptanalysis to groups other than the usual elementary abelian 2-groups. In this paper we study a notion of nonlinearity that seems consistent with their notions. We discuss the connection between two notions of $\mathbb{Z}_4$-bentness introduced from a sequence design viewpoint (for applications in CDMA systems) and the classical notion of bent function.

The first approach is to consider functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, q is any integer, see the paper [10] of Kumar, Scholtz and Welch. We call them **q-ary functions**. Another, more recent approach, which is more natural from the viewpoint of cyclic codes over rings is to consider functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$. This is the approach of Schmidt in [24]. We call these latter functions **generalized Boolean functions**. In this paper we focus on the quaternary case ($q = 4$), and explore the interplay between the three types of definitions for bentness.

Let us note that there exist other ways to generalize the concept of bent function. See surveys of distinct generalizations in [31] and [32].

The material is organized as follows. Necessary definitions are given in section 2. In section 3 we prove that a generalized Boolean function $f(x, y) = a(x, y)+2b(x, y)$ is bent if and only if Boolean functions b and $a\oplus b$ are both bent. Section 4 shows that there is no direct link between notions of Boolean and quaternary bent functions but we obtain several facts related to bent Boolean and quaternary functions. There is no direct connection between notions of quaternary and generalized bent functions either, which is shown in section 5. Then in section 6 we show that quaternary generalized Boolean bent functions in n variables yield Boolean bent functions by Gray map, or semi bent functions, depending on the parity of n. Section 7 characterizes bent functions by their nonlinearity. Section 8.1 illustrates our results by a survey of the known constructions of generalized bent functions and their Gray images. In section 8.2 we introduce two simple constructions for quaternary bent functions.

Note that the first variant of this paper appeared at ePrint archive [27], see also [28]. After that several related results were obtained by different authors. Thus, Stănică et al. [29] extended the results of [27] related to generalized Boolean bent functions by considering functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_8$. Later the results were extended for functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{16}$ by Martinsen et al. [13]. Finally, Hodžić et al. [8] gave a complete characterization of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{2^k}$ for $k > 1$ in terms of both the necessary and sufficient conditions their component Boolean functions need to satisfy. Two open problems that were mentioned in the original paper [27] were solved. More specifically, in [29] the quaternary analogue of Dillon's construction was presented. Then Li et al. [11] characterized the functions in n variables of the form $f(x) = Tr(ax + 2bx^{1+2^k})$ for odd $n/\gcd(n, k)$. The results obtained in the original paper [27] were instrumental in the following works [4, 5, 11, 18, 22]. The original paper [27] was also mentioned in [14, 26, 30].

2. Definitions and Notation

In what follows by $\oplus$ we mean addition over $\mathbb{Z}_2$ (modulo 2). We will use $+$ for two types of addition: over $\mathbb{Z}_4$ and natural one. It always depends on the context. We will also use the following two types of inner product:

$$\langle x, y\rangle = x_1y_1 \oplus ... \oplus x_ny_n,$$

$$x.y = x_1y_1 + ... + x_ny_n.$$

Let n, q be integers, $q \geqslant 2$.

We consider the following mappings:

1) $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — **Boolean function** in n variables. Its *sign function* is $F := (-1)^f$. The *Walsh–Hadamard transform* (WHT) of f is

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_2^n} (-1)^{f(y) \oplus \langle x,y \rangle} = \sum_{y \in \mathbb{Z}_2^n} F(y)(-1)^{\langle x,y \rangle}. \tag{1}$$

A Boolean function f is said to be *bent*, iff $|\widehat{F}(x)| = 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$. It is *semi bent* iff $\widehat{F}(x) \in \{0, \pm 2^{(n+1)/2}\}$ (sometimes such functions are called *near bent*). This is a special case of *plateaued functions* [33]. Note that Boolean bent (resp. semi bent) functions exist only if the number of variables, n, is even (resp. odd).

2) $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ — **generalized Boolean function** in n variables. Its *sign function* is $F := \omega^f$, with ω a primitive complex root of unity of order q, i. e. $\omega = e^{2\pi i/q}$. When $q = 4$, we write $\omega = i$. Its WHT is given as

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_2^n} \omega^{f(y)} (-1)^{\langle x,y \rangle} = \sum_{y \in \mathbb{Z}_2^n} F(y)(-1)^{\langle x,y \rangle}. \tag{2}$$

As above, a generalized Boolean function f is *bent*, iff $|\widehat{F}(x)| = 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$. In comparison to the previous case it does not follow that n should be even if f is bent. Such functions for $q = 4$ were studied by K.-U. Schmidt (2006) in [24]. Here we consider only this partial case $q = 4$.

3) $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ — **q-ary function** in n variables. Its *sign function* is given by $F := \omega^f$ as in the previous case. Its WHT is defined by

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_q^n} \omega^{f(y)+x.y} = \sum_{y \in \mathbb{Z}_q^n} F(y)\omega^{x.y}. \tag{3}$$

Here $+$ and $x.y$ are addition and inner product over $\mathbb{Z}_q$. Note that the matrix of this transform is no longer a Sylvester type Hadamard matrix as in the previous case, but a generalized (complex) Hadamard matrix. A q-ary function f is called *bent*, iff $|\widehat{F}(x)| = q^{n/2}$ for all $x \in \mathbb{Z}_q^n$. Notice that again it does not follow from the definition that q-ary bent functions do not exist if n is odd. P. V. Kumar, R. A. Scholtz and L. R. Welch [10] studied q-ary bent functions in 1985. They proved that such functions exist for any even n and $q \neq 2 (\mathrm{mod}\, 4)$. Later S. V. Agievich [1] proposed an approach to describe regular q-ary bent functions in terms of bent rectangles. If $q = 4$ we call f a **quaternary function**. Here we study such functions only. Note that in 1994 A. S. Ambrosimov [2] studied another type of q-ary bent functions defined over the finite field.

A bent function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called **regular** if each of its Walsh–Hadamard coefficients can be expressed as $\widehat{F}(z) = q^{n/2}\omega^{h(z)}$ for every $z \in \mathbb{Z}_q^n$ and some q-ary function h. From [10] it is known that for quaternary ($q = 4$) case all bent functions are regular.

3. Connections between Boolean and generalized Boolean bent functions

Let $f : \mathbb{Z}_2^{2n} \to \mathbb{Z}_4$ be a generalized Boolean function. Represent it as $f(x, y) = a(x, y) + 2b(x, y)$, for any $x, y \in \mathbb{Z}_2^n$ where $a, b : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2$ are Boolean functions.

In this section we study connection between properties of bentness of generalized Boolean and Boolean functions.

Here and further by $\widehat{A \cdot B}$ we mean WHT of $a \oplus b$. It is natural, since $A \cdot B = (-1)^{a \oplus b}$. In this section and in what follows, by $x.y$ we mean the inner product over $\mathbb{Z}_4$: $x.y = x_1 y_1 + ... + x_n y_n \bmod 4$.

Lemma 1. *Between Walsh–Hadamard transforms of f, $a \oplus b$, b, there is the relation*

$$|\widehat{F}(x,y)|^2 = \frac{1}{2}\left(\widehat{B}^2(x,y) + \widehat{A \cdot B}^2(x,y)\right).$$

Proof. Let us study the Walsh–Hadamard transform of f. According to (2) we have

$$\widehat{F}(x,y) = \sum_{x',y'} (-1)^{\langle x,x'\rangle \oplus \langle y,y'\rangle \oplus b(x',y')}\, i^{\,a(x',y')}.$$

Applying the formula $i^s = \frac{1+(-1)^s}{2} + \frac{1-(-1)^s}{2} i$ for $s = a(x',y')$ we get

$$\widehat{F}(x,y) = \frac{1}{2}\left(\widehat{B}(x,y) + \widehat{A \cdot B}(x,y)\right) + \frac{i}{2}\left(\widehat{B}(x,y) - \widehat{A \cdot B}(x,y)\right).$$

From this we directly get what we need. □

Note that Lemma 1 holds for any (not only even) number of variables of the function f.

Theorem 1. *The following statements are equivalent*:
(i) *the generalized Boolean function f is bent in $2n$ variables*;
(ii) *the Boolean functions in $2n$ variables b and $a \oplus b$ are both bent.*

Proof. By Lemma 1 we have $|\widehat{F}(x,y)|^2 = \frac{1}{2}\left(\widehat{B}^2(x,y) + \widehat{A \cdot B}^2(x,y)\right)$. If $a \oplus b$ and b are bent functions then $|\widehat{F}(x,y)|^2 = \frac{1}{2}(2^{2n} + 2^{2n}) = 2^{2n}$ and f is a bent function. Conversely, if f is bent, then it holds $\widehat{B}^2(x,y) + \widehat{A \cdot B}^2(x,y) = 2^{2n+1}$. Since WHT coefficients of a Boolean function are integer, this equality has the unique solution $\widehat{B}^2(x,y) = \widehat{A \cdot B}^2(x,y) = 2^{2n}$ (see [9] for details). So, functions $a \oplus b$ and b are bent. □

Note that there are some intersections between Lemma 1, the part (i)→(ii) of Theorem 1 and results of the last version of [24].

4. Connections between Boolean and quaternary bent functions

Define a quaternary function $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ as $g(x + 2y) = a(x,y) + 2b(x,y)$, for any $x, y \in \mathbb{Z}_2^n$ where $a, b : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2$ are Boolean functions. In this section we study connection between properties of bentness of quaternary and Boolean functions.

4.1. Preliminaries and necessary statements.

In this section we present several facts that will be instrumental in what follows.

Lemma 2. *Let $x, y \in \mathbb{Z}_2^n$. If $x.y \neq \langle x,y\rangle$ then $x.y = \langle x,y\rangle + 2$.*

Proof. There are four possible values for $x.y$: $0, 1, 2$ and 3. For $x.y = 0$ or 1, it is obvious that $x.y = \langle x, y\rangle$. For two remaning cases, we have

$$x.y = 2 \to \langle x, y\rangle = 0 \to x.y = \langle x, y\rangle + 2,$$

$$x.y = 3 \to \langle x, y\rangle = 1 \to x.y = \langle x, y\rangle + 2.$$

□

The following fact is well known for Boolean functions.

Lemma 3. *Let f be a linear Boolean function in n variables. Then there are two possible values of WHT coefficients of f: 0 and 2^n.*

Proof. Any linear Boolean function f in n variables can be represented for some $a \in \mathbb{Z}_2^n$ as $f(x) = \langle a, x\rangle$. Therefore, by (1)

$$\widehat{F}(x) = \sum_{y\in\mathbb{Z}_2^n} (-1)^{\langle a,y\rangle \oplus \langle x,y\rangle} = \sum_{y\in\mathbb{Z}_2^n} (-1)^{\langle a\oplus x,y\rangle}.$$

Using the well-known fact that

$$\sum_{b\in\mathbb{Z}_2^n} (-1)^{\langle b,c\rangle} = \begin{cases} 2^n, & if\ c = 0, \\ 0, & otherwise. \end{cases}$$

the result follows. □

Proposition 1. *(see, for instance, [32]) All quadratic Boolean functions in two variables, i.e. $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$ such that $f(x, y) = xy \oplus c$, where $x, y, c \in \mathbb{Z}_2$, are bent.*

Proposition 2. *(Rothaus, [23]) The degree of Boolean bent function f in $n \geq 4$ variables is not more than $n/2$.*

Proposition 3. *(Rothaus, [23]) Let $x \in \mathbb{Z}_2^r$ and $y \in \mathbb{Z}_2^k$, where $r, k \geqslant 2$ and even. A Boolean function $f(x, y) = f_1(x) \oplus f_2(y)$ is a bent function in $r + k$ variables if and only if the functions f_1 and f_2 are bent functions in r and k variables respectively.*

Proposition 4. *(Singh et al., [25]) Let $x \in \mathbb{Z}_4^r$ and $y \in \mathbb{Z}_4^k$ for $r, k \geqslant 1$. A quaternary function $g(x, y) = g_1(x) \oplus g_2(y)$ is a bent function in $r + k$ variables if and only if functions g_1 and g_2 are quaternary bent functions in r and k variables respectively.*

Note that results of Propositions 3 and 4 can be easily extended to sums with more than two functions.

4.2. **Quaternary bent functions in small number of variables.** Here we present results on connections between notions of quaternary bent functions in one and two variables and Boolean bent functions. Using computer search we obtain the following facts.

Statement 1. *For every quaternary function $g(x + 2y) = a(x, y) + 2b(x, y)$ in one variable with $x, y \in \mathbb{Z}_2$, it is true that g is a quaternary bent function if and only if b is bent and a does not depend on y, i.e. $a(x, y)$ is equal to 0, 1, x or $x \oplus 1$. Moreover, if g is bent then b and $a \oplus b$ are bent functions too.*

		Number of quaternary bent functions	
Cases for b and $a \oplus b$	Types of a in the case	For each type of a	Total in the case
b and $a \oplus b$ are nonlinear (not bent)	a is bent	49152	147456
	a is linear (not constant)	3072	
	a is nonliear (not bent)	95232	
b and $a \oplus b$ are bent	a is bent	16384	53248
	a is linear (not constant)	2304	
	a is constant	768	
	a is nonlinear (not bent)	33792	

Table 1. Classification of functions b and $a \oplus b$ for quaternary bent functions in 2 variables.

Computer search shows that the number of quaternary bent functions in one variable is equal to 32.

There are 200704 quaternary bent functions in 2 variables. Among them there are 98304 fuctions such that none of Boolean functions a, b and $a \oplus b$ is bent but for 3072 of them a is a linear Boolean function. There are 36864 quaternary bent functions such that b and $a \oplus b$ are bent functions, while for 33792 of them a is a nonlinear function, and for 2304 and 768 functions a is a linear function or constant respectively. The number of quaternary bent functions in 2 variables with each of a, b and $a \oplus b$ being bent is equal to 16384. For the remaining 49152 quaternary functions, a is bent and b and $a \oplus b$ are nonlinear Boolean functions. We summarize the data described above in Table 1.

For functions in three and more variables an exhaustive search is unfeasible (there are 2^{128} quaternary functions in three variables).

4.3. **Possibilities for bentness.** From Statement 1, we know that for $n = 1$ if g is quaternary bent then b and $a \oplus b$ are bent functions too. In the previous section we showed that it does not hold for quaternary functions in 2 variables. Let us prove that it does not hold for arbitrary $n \geqslant 2$.

Proposition 5. *For every $n \geqslant 2$ there exists a quaternary bent function $g(x+2y) = a(x,y) + 2b(x,y)$ in n variables, with b and $a \oplus b$ being not bent in $2n$ variables.*

Proof. In what follows, '+' denotes the addition over $\mathbb{Z}_4$ excepting summation of indices. Any quaternary function g in n variables can be uniquely represented as follows: $g(x_1+2x_{n+1}, ..., x_n+2x_{2n}) = a(x_1, ..., x_{2n})+2b(x_1, ..., x_{2n})$. Let $b(x_1, .., x_{2n}) = \bigoplus_{i=3}^{n} x_i x_{i+n} \oplus x_1 x_{n+2} \oplus x_2 x_{n+1} \oplus x_1 x_2 x_{n+1}$,$a(x_1, .., x_{2n}) = x_1 x_{n+1}$. One can see that b can be divided into sum of $n-2$ Boolean functions in two variables and one Boolean function in four variables like this:

$$b(x_1, ..., x_{2n}) = b_1(x_1, x_2, x_{n+1}, x_{n+2}) \oplus b_2(x_3, x_{n+3}) \oplus ... \oplus b_{n-1}(x_n, x_{2n}),$$

$$b_1(x_1, x_2, x_{n+1}, x_{n+2}) = x_1 x_{n+2} \oplus x_2 x_{n+1} \oplus x_1 x_2 x_{n+1},$$

$$b_i(x_{i+1}, x_{n+i+1}) = x_{i+1} x_{n+i+1}, \quad i = 2, ..., n-1.$$

From Proposition 3, we know that b is bent if and only if all b_i are bent. According to Proposition 2, we get that function b_1 in four variables is not bent since its degree is equal to three. Therefore, b is not bent.

It is easy to check that

$$2b(x_1, .., x_{2n}) = (2x_3 x_{n+3} + ... + 2x_n x_{2n}) + 2x_1 x_{n+2} + 2x_2 x_{n+1} + 2x_1 x_2 x_{n+1}.$$

Moreover, g can be divided into sum of $n-2$ quaternary functions in one variable and one quaternary function in two variables

$$g(x_1+2x_{n+1},...,x_n+2x_{2n}) = g_1(x_1+2x_{n+1},x_2+2x_{n+2})+$$
$$+g_2(x_3+2x_{n+3})+...+g_{n-1}(x_n+2x_{2n}),$$

where

$$g_1(x_1+2x_{n+1},x_2+2x_{n+2}) = x_1x_{n+1}+2x_1x_{n+2}+2x_2x_{n+1}+2x_1x_2x_{n+1},$$
$$g_i(x_{i+1}+2x_{n+i+1}) = 2x_{i+1}x_{n+i+1},\ \ i=2,...,n-1.$$

From Proposition 1, we know that all $x_{i+1}x_{n+i+1}$ are bent, $i=2,...,n$. Therefore, according to Statement 1 functions g_i are quaternary bent functions, $i=2,...,n-1$. It was checked that the quaternary function g_1 is also bent according to the definition: its WHT coefficients are the following:

$x\in\mathbb{Z}_4^2$	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
$\widehat{G_1(x)}$	4	$4i$	4	4	4	$4i$	-4	4	4	$-4i$	4	-4	4	$-4i$	-4	-4

From Proposition 4, g is a quaternary bent function if and only if all g_i are quaternary bent functions, $i=1,...,n-1$. This completes the proof. □

The next result shows that bentness of a quaternary function does not follow from bentness of Boolean functions in general.

Proposition 6. *For every $n\geqslant 1$, there exists a quaternary function $g(x+2y)=a(x,y)+2b(x,y)$ in n variables that is not bent, while b and $a\oplus b$ are Boolean bent functions in $2n$ variables.*

Proof. Any quaternary function g in n variables can be uniquely represented as $g(x_1+2x_{n+1},...,x_n+2x_{2n}) = a(x_1,...,x_{2n})+2b(x_1,...,x_{2n})$.

Let $b(x_1,..,x_{2n}) = \bigoplus_{i=1}^{n} x_ix_{i+n}$,$a(x_1,..,x_{2n}) = x_{n+1}$. It is easy to check that $2b(x_1,..,x_{2n}) = 2x_1x_{n+1}+...+2x_nx_{2n}$. Note that g can be divided into sum of n quaternary functions in one variable:

$$g(x_1+2x_{n+1},...,x_n+2x_{2n}) = g_1(x_1+2x_{n+1})+...+g_n(x_n+2x_{2n}),$$

where

$$g_i(x_i+2x_{n+i}) = a_i(x_i,x_{n+i})+2b_i(x_i,x_{n+i}),\ i=1,..,n,$$
$$b_i(x_i,x_{n+i}) = x_ix_{n+i},\ i=1,..,n,$$
$$a_1(x_1,x_{n+1}) = x_{n+1},$$
$$a_i(x_i,x_{n+i}) = 0,\ i=2,..,n.$$

From Proposition 4, we know that g is a quaternary bent function if and only if all g_i are quaternary bent functions, $i=1,...,n$. From Statement 1 and by the choice of a and b, we get that g_1 is not quaternary bent. This completes the proof. □

From Propositions 5 and 6, we conclude that there is no direct link between notions of Boolean and quaternary bent functions. Additionally, Proposition 5 shows that if b and $a\oplus b$ are not bent, it does not imply that g is not bent. According to Proposition 6, it is also true that if g is not bent, it does not imply that b and $a\oplus b$ are not bent.

From the previous section, we can see that for quaternary bent functions in one and two variables, a Boolean function b is bent if and only if $a \oplus b$ is also bent. Whether this statement is true for arbitrary n remains an open problem.

4.4. **Nonlinearity of component Boolean functions.** Let $g(x+2y) = a(x,y) + 2b(x,y)$ be a quaternary function in n variabes, where $x, y \in \mathbb{Z}_2^n$ and a, b are Boolean functions in $2n$ variables.

Let us represent WHT coefficients of quaternary functions in terms of the coefficients of Boolean functions b and $a \oplus b$ as we did for generalized functions in section 4. Here by $\widehat{A \cdot B}$ we mean the WHT of $a \oplus b$.

Lemma 4. *Between the WHT coefficients of g, $a \oplus b$, b there is the relation*

$$\widehat{G}(x+2y) = \frac{1}{2}\left(\widehat{B}(x \oplus y, x) + \widehat{A \cdot B}(y,x) - 2c_{\,b}(x \oplus y, x) - 2c_{\,a\oplus b}(y,x)\right) +$$
$$+\frac{i}{2}\left(\widehat{B}(y,x) - \widehat{A \cdot B}(x \oplus y, x) - 2c_{\,b}(y,x) + 2c_{\,a\oplus b}(x \oplus y, x)\right),$$

with

$$c_{\,f}(u,x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle},$$

where f is a Boolean function in $2n$ variables, $V_x = \{\, x' \in \mathbb{Z}_2^n \,|\, \langle x, x' \rangle \neq x.x' \,\}$, and $u \in \mathbb{Z}_2^n$.

Proof. Let us study the Walsh–Hadamard transform of g. By (3) we know that

$$\widehat{G}(x+2y) = \sum_{x',y'} i^{\,(x+2y).(x'+2y') + a(x',y') + 2b(x',y')}.$$

From the fact that for any $x'', x''' \in \mathbb{Z}_2^n$ it holds $2\langle x'', x''' \rangle \bmod 4 = 2x''.x'''$ and Lemma 2, we have

$$(x+2y).(x'+2y') = \begin{cases} \langle x,x' \rangle + 2\langle x,y' \rangle + 2\langle y,x' \rangle, & if \quad x.x' = \langle x,x' \rangle, \\ \langle x,x' \rangle + 2\langle x,y' \rangle + 2\langle y,x' \rangle + 2, & if \quad x.x' \neq \langle x,x' \rangle. \end{cases}$$

Let $U_x = \{\, x' \in \mathbb{Z}_2^n \,|\, x.x' = \langle x,x' \rangle \,\}$ and $V_x = \{\, x' \in \mathbb{Z}_2^n \,|\, x.x' \neq \langle x,x' \rangle \,\}$. Therefore, we get $U_x \cap V_x = \varnothing$ and $U_x \cup V_x = \mathbb{Z}_2^n$. Note that $|U_x| \neq |V_x|$ in general. Then

$$\widehat{G}(x+2y) = \sum_{x \in U_x, y'} (-1)^{\langle x,y' \rangle \oplus \langle y,x' \rangle \oplus b(x',y')} i^{\,\langle x,x' \rangle + a(x',y')} -$$
$$- \sum_{x' \in V_x, y'} (-1)^{\langle x,y' \rangle \oplus \langle y,x' \rangle \oplus b(x',y')} i^{\,\langle x,x' \rangle + a(x',y')}.$$

Here we use the standard maps $\beta, \gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ defined as

$$\beta : 0,1 \to 0 \text{ and } \beta : 2,3 \to 1;$$
$$\gamma : 0,2 \to 0 \text{ and } \gamma : 1,3 \to 1.$$

For any $t \in \mathbb{Z}_4$ it holds

$$i^t = (-1)^{\beta(t)} \left(\frac{1 + (-1)^{\gamma(t)}}{2} + \frac{1 - (-1)^{\gamma(t)}}{2} i \right).$$

Using this formula for $t = x.x' + a(x',y')$ and the fact that $\gamma(\langle x,x' \rangle + a(x',y')) = \langle x,x' \rangle \oplus a(x',y')$ we get

$$\widehat{G}(x+2y) = \frac{1}{2}\left(S_1 + S_2 - S_3 - S_4\right) + \frac{i}{2}\left(S_1 - S_2 - S_3 + S_4\right),$$

where

$$\begin{aligned}
S_1 &= \sum_{x'\in U_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))},\\
S_2 &= \sum_{x'\in U_x,y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))},\\
S_3 &= \sum_{x'\in V_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))},\\
S_4 &= \sum_{x'\in V_x,y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))}.
\end{aligned}$$

Let $M_{\delta,x} = \{\ x' \in \mathbb{Z}_2^n \mid \langle x,x'\rangle = \delta\ \}$ for $\delta \in \mathbb{Z}_2$. Note that $M_{0,x} \cup M_{1,x} = \mathbb{Z}_2^n$ and $|M_{0,x}| = |M_{1,x}| = 2^{n-1}$. Let us divide every sum S_1, S_2, S_3 and S_4 into two sums $\sum_{x'\in M_{0,x},y'}$ and $\sum_{x'\in M_{1,x},y'}$. Note that $\beta(a(x',y')+\langle x,x'\rangle)$ is equal to 0 or $a(x',y')$ for $x' \in M_{0,x}$ and $x' \in M_{1,x}$ respectively. Thus, we have

$$\begin{aligned}
S_1 &= \sum_{x'\in U_x\cap M_{0,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle} +\\
&+ \sum_{x'\in U_x\cap M_{1,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus a(x',y')},\\
S_2 &= \sum_{x'\in U_x\cap M_{0,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} +\\
&+ \sum_{x'\in U_x\cap M_{1,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus a(x',y')},\\
S_3 &= \sum_{x'\in V_x\cap M_{0,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle} +\\
&+ \sum_{x'\in V_x\cap M_{1,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus a(x',y')},\\
S_4 &= \sum_{x'\in V_x\cap M_{0,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} +\\
&+ \sum_{x'\in V_x\cap M_{1,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle a(x',y')}.
\end{aligned}$$

After grouping terms we obtain

$$\begin{aligned}
&S_1 + S_2 - S_3 - S_4 =\\
&= \sum_{x'\in U_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} +\\
&+ \sum_{x'\in U_x,y'} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle} -\\
&- \sum_{x'\in V_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} -\\
&- \sum_{x'\in V_x,y'} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle}.
\end{aligned}$$

Then

$$\begin{aligned} S_1 - S_2 - S_3 + S_4 = \\ = \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle} - \\ - \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle} - \\ - \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle} + \\ + \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle}. \end{aligned}$$

Since

$$c_f(u,x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle},$$

where f is a Boolean function in $2n$ variables and $u \in \mathbb{Z}_2^n$, then one can see that

$$S_1 + S_2 - S_3 - S_4 =$$

$$= (\widehat{B}(x \oplus y, x) - c_b(x \oplus y, x)) + (\widehat{A \cdot B}(y,x) - c_{a \oplus b}(y,x)) - c_b(x \oplus y, x) - c_{a \oplus b}(y,x)$$

and

$$S_1 - S_2 - S_3 + S_4 =$$

$$= (\widehat{B}(y,x) - c_b(y,x)) - (\widehat{A \cdot B}(x \oplus y, x) - c_{a \oplus b}(x \oplus y, x)) - c_b(y,x) + c_{a \oplus b}(x \oplus y, x).$$

After rearranging, the result follows. □

We can see that WHT coefficients of a quaternary function g do not directly depend on WHT coefficients of Boolean functions b and $a \oplus b$. This result will be used in proof of the next theorem and also in section 8.2.

Theorem 2. *Let $g(x + 2y) = a(x,y) + 2b(x,y)$ be a quaternary bent function with $x, y \in \mathbb{Z}_2^n$ and a, b be Boolean functions in $2n$ variables. Then b and $a \oplus b$ are nonaffine functions for any $n \geqslant 1$.*

Proof. According to Lemma 3 there are two possible values of WHT coefficients of a linear Boolean function in $2n$ variables: 0 and 2^{2n}.

From Lemma 4, we get

$$\widehat{G}(2y) = \frac{1}{2}(\widehat{B}(y,0) + \widehat{A \cdot B}(y,0)) + \frac{i}{2}(\widehat{B}(y,0) - \widehat{A \cdot B}(y,0)), \text{ where } y \in \mathbb{Z}_2^n.$$

Note that V_x is empty for $x = \mathbf{0}$, hence $c_b(x \oplus y, x), c_b(y,x), c_{a \oplus b}(x \oplus y, x)$ and $c_{a \oplus b}(y,x)$ are zero too.

As it was mentioned in section 2 all quaternary bent functions are regular. It means that there is only real or imaginary part of $\widehat{G}(2y)$. Thus, we get that there are two possible cases

$$\begin{cases} (\widehat{B}(y,0) + \widehat{A \cdot B}(y,0))^2 = 0, \\ (\widehat{B}(y,0) - \widehat{A \cdot B}(y,0))^2 = 4 \cdot 4^n. \end{cases}$$

or

$$\begin{cases} (\widehat{B}(y,0) + \widehat{A \cdot B}(y,0))^2 = 4 \cdot 4^n, \\ (\widehat{B}(y,0) - \widehat{A \cdot B}(y,0))^2 = 0. \end{cases}$$

From the first system we get

$$\begin{cases} \widehat{B}(y,0) = -\widehat{A \cdot B}(y,0), \\ (2 \cdot \widehat{B}(y,0))^2 = 4 \cdot \widehat{B}(y,0)^2 = 4 \cdot 4^n. \end{cases}$$

Hence,

$$\widehat{B}(y,0) = -\widehat{A \cdot B}(y,0) = \pm 2^n.$$

By solving the second system one can get

$$\widehat{B}(y,0) = \widehat{A \cdot B}(y,0) = \pm 2^n.$$

Therefore, b and $a \oplus b$ are nonaffine functions. □

5. Connections between quaternary and generalized Boolean bent functions

Let $g(x+2y) = f(x,y)$, where $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$, $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$ and $x, y \in \mathbb{Z}_2^n$.

In this section, we show that the approach of Kumar et al. and that of Schmidt are not equivalent.

Proposition 7. *For every $n \geqslant 1$, there exists a generalized bent function $f(x,y)$ in $2n$ variables such that a quaternary function $g(x+2y)$ in n variables defined as $g(x+2y) = f(x,y)$ for all $x, y \in \mathbb{Z}_2^n$ is not bent.*

Proof. From Proposition 6, there exists a quaternary function $g(x+2y) = a(x,y) + 2b(x,y)$ which is not bent, while b and $a \oplus b$ are both bent. Now from Theorem 1 we know that if b and $a \oplus b$ are both bent then $f(x,y)$ is a generalized bent function. □

Proposition 8. *For every $n \geqslant 2$, there exists a quaternary bent function $g(x+2y)$ in n variables such that a generalized function $f(x,y)$ in $2n$ variables defined as $f(x,y) = g(x+2y)$ for all $x, y \in \mathbb{Z}_2^n$ is not bent.*

Proof. From Proposition 5 there exists a quaternary bent function $g(x+2y) = a(x,y) + 2b(x,y)$ in $n \geqslant 1$ variables such that both b and $a \oplus b$ are not bent. From Theorem 1 we know that a generalized function $f(x,y)$ is bent iff b and $a \oplus b$ are both bent. Hence, $f(x,y)$ is not bent. □

6. Gray images of bent functions

Let f be a generalized Boolean function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4$. Write $f = a + 2b$ with a, b Boolean functions in n variables. Its *Gray map* $\phi(f)$ is the Boolean function in variables (x,z) with $x \in \mathbb{Z}_2^n$ and $z \in \mathbb{Z}_2$ defined as $a(x)z + b(x)$. The proof of the next result is implicit in the proof of [24, Th. 3.5] and is omitted.

Proposition 9. *For the WHTs of functions f and $\phi(f)$ it holds*

$$\widehat{\Phi(f)}(u,v) = 2\Re(i^{-v}\widehat{F}(u)) = \widehat{B}(u) + (-1)^v \widehat{A \cdot B}(u), \text{ where } u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2. \quad (4)$$

Here $\Re$ denotes real part of a complex number. As far as the left side of equation (4) is a WHT coefficient of a Boolean function, we easily get

Corollary 1. *For any generalized Boolean function f in n variables it holds*

$$\max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\Re(i^{-v}\widehat{F}(u))| \geqslant 2^{(n-1)/2}.$$

Corollary 2. *If f is generalized bent in n variables then $\phi(f)$ is either bent (n odd) or semi bent (n even).*

Proof. Write $\widehat{F}(u) = X + iY$ with X, Y integers. We know that $2^n = X^2 + Y^2$. We know that the solution to that diophantine equation in $X > 0$ and $X \geqslant Y \geqslant 0$ is unique, see e.g. [9]. The obvious solutions for n odd are $\{|X| = |Y| = 2^{(n-1)/2}\}$, $\{Y = 0,\ X = \pm 2^{n/2}\}$ and $\{Y = \pm 2^{n/2},\ X = 0\}$ for n even.

Thus, if n is odd it holds $\widehat{\Phi(f)}(u, v) = \pm 2^{(n+1)/2}$ for all u, v, and hence $\phi(f)$ is bent in $n + 1$ variables. If n is even we see that $\widehat{\Phi(f)}(u, v)$ equals 0 or $\pm 2^{(n+2)/2}$, so $\phi(f)$ is semi bent in $n + 1$ variables. □

There is a partial converse to Corollary 2. The proof is immediate.

Proposition 10. *Let n be odd. If $\phi(f)$ is a Boolean bent function in $n+1$ variables then f is a generalized Boolean bent function in n variables.*

Proof. Let $\widehat{F}(u) = X + iY$ with X, Y integers. We know that for all u, v it holds $\widehat{\Phi(f)}(u, v) = \pm 2^{(n+1)/2}$. Therefore, from Proposition 9

$$\widehat{\Phi(f)}(u, 0) = 2\Re(\widehat{F}(u)) = 2X = \pm 2^{(n+1)/2},$$

and

$$\widehat{\Phi(f)}(u, 1) = 2\Re(i^{-1}\widehat{F}(u)) = 2Y = \pm 2^{(n+1)/2}.$$

Hence, $|\widehat{F}(u)|^2 = X^2 + Y^2 = 2^n$. □

This fact has also been obtained in the last variant of [24].

7. Notions of nonlinearity

It is well-known that Boolean bent functions are characterized by their maximal distance to the first order Reed–Muller code. This fact is generalized in this section to their quaternary analogues.

7.1. **Generalized Boolean functions.** Let $RM(r, k)$ be the Reed–Muller code of length 2^k and of order r, see [12]. Define, for $0 \leqslant r \leqslant m$ the quaternary code $ZRM(r, m) = \phi^{-1}(RM(r, m + 1))$. This code is spanned by vectors of values for functions of degree at most $r - 1$ together with twice functions of degree at most r, see [7] for details. We introduce the **nonlinearity** $N(f)$ of a generalized bent Boolean function f in n variables as

$$N(f) := 2^n - \frac{1}{2} \max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\widehat{\Phi(f)}(u, v)|. \tag{5}$$

The Lee weights of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$, respectively, and the Lee weight $wt_L(a)$ of $a \in \mathbb{Z}_4^N$ is the rational sum of the Lee weights of its components. This weight function defines a distance $d_L(f, g) = wt(f - g)$ between two generalized functions on $\mathbb{Z}_4^N$ called the Lee distance. Analogously, let $d_H(\cdot, \cdot)$ be the Hamming distance on $\mathbb{Z}_2^{2N}$. According to Corollary 1 we have

Proposition 11. *For any generalized Boolean function f in n variables, it is true $N(f) \leqslant 2^n - 2^{(n-1)/2}$.*

Proposition 12. *With the above notation, for any generalized Boolean function in n variables f we have*

$$N(f) = d_L(f, ZRM(1, n)) = d_H(\Phi(f), RM(1, n + 1)).$$

Proof. Let x, y be arbitrary vectors of $\mathbb{Z}_4^N$. Denote by i^x the vector $(i^{x_1}, \ldots, i^{x_N})$. Recall first the well-known identities

$$d_E^2(i^x, i^y) = 2d_L(x, y) = 2(N - \Re(\sum_{j=1}^{N} i^{x_j - y_j})),$$

where d_E stands for the Euclidean distance. Observe that $ZRM(1, n)$ is spanned by the all-one vector, along with twice the binary linear functions, and that $\widehat{F}(u) = \sum_{y \in \mathbb{Z}_2^n} i^{f(y)+2u.y}$. The second equality holds by the isometry property of the Gray map [7]. □

Hence, using Propositions 11 and 12 we can reformulate one partial case from Corollary 2 and Proposition 10 as follows.

Corollary 3. *Let n be odd. A generalized function f is bent if and only if $N(f)$ attains the maximal possible value $2^n - 2^{(n-1)/2}$.*

The case of even n is more complicated. We have

Corollary 4. *Let n be even. If a function f is bent then $N(f) = 2^n - 2^{n/2}$.*

Proof. By Corollary 2 the Boolean function $\phi(f)$ is semi bent in $n+1$ variables. Hence the maximum value of $|\widehat{\Phi(f)}(u, v)|$ is equal to $2^{(n+2)/2}$. Then by Proposition 9 and definition (5) we get $N(f) = 2^n - 2^{n/2}$. □

The converse statement is not right in general as far as from the equality

$$\max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\widehat{\Phi(f)}(u, v)| = 2^{(n+2)/2}$$

it does not follow that $|\widehat{F}(u)| = 2^{n/2}$ for any $u \in \mathbb{Z}_2^n$. Actually, it is not clear what is the maximum possible value of $N(f)$ if n is even. To know it one should find the value of covering radius of the code $RM(1, n+1)$ when $n+1$ is odd. But it is a hard old problem without analogy to the easy case of even $n+1$.

7.2. **Quaternary functions.** Let g be a quaternary function in n variables. In this case, an immediate reduction to the preceding subsection (namely, passing from g to f in the notations of section 5) yields the definition

$$N(g) := 2^{2n} - \frac{1}{2} \max_{u, v \in \mathbb{Z}_2^n, w \in \mathbb{Z}_2} |\widehat{\Phi(g)}(u, v, w)|.$$

The following analogue of Proposition 12 is immediate.

Proposition 13. *For any quaternary function g in n variables we have*

$$N(g) = d_L(g, ZRM(1, 2n)) = d_H(\phi(g), RM(1, 2n+1)).$$

In particular if g is bent then $N(g) = 2^{2n} - 2^n$. As it was mentioned above the maximal possible value of $N(g)$ is not known yet.

8. Examples of Constructions

Define algebraic normal form (ANF) of generalized Boolean function f in n variables as follows:

$$f(x_1, ..., x_n) = \sum_{k=1}^{n} \sum_{i_1,...,i_k} a_{i_1,...,i_k} x_{i_1} \cdots x_{i_k} + a_0,$$

where for each k indices $i_1, ..., i_k$ are pairwise distinct and sets $\{i_1, ..., i_k\}$ are exactly all different nonempty subsets of the set $\{1, ..., n\}$; coefficients $a_{i_1,...,i_k}, a_0$ take values from $\mathbb{Z}_4$. The number of variables in the longest item of its ANF is called the degree of a generalized function and is denoted by $\deg(f)$. For computing degrees we require the following lemma.

Lemma 5. *For a generalized Boolean function f the degree of $\phi(f)$ is at most the degree of f.*

Proof. Follows by definition of the $ZRM(r, m)$ code by its generators [7]. □

8.1. **Generalized Boolean bent functions.** In [24, Th. 4.3] figures a natural generalization of the classical Maiorana–McFarland construction.

Proposition 14. *(Schmidt,* [24]*) The generalized Boolean function f in $2n$ variables defined for x, y in $\mathbb{Z}_2^n$ by $f(x, y) = 2x.\pi(y) + \tau(y)$, with τ an arbitrary generalized Boolean function in n variables and π an arbitrary permutation of $\mathbb{Z}_2^n$ is bent.*

By Corollary 2 the Gray map of this function is a binary Boolean semi bent function in $2n + 1$ variables. By Lemma 5 its degree is $\max(2, \deg(\tau))$.

It is well-known that the binary Kerdock code contains bent functions. We assume the reader has some familiarity with Galois rings as can be gained in, e.g. [7].

For completeness, the next result from [24] we present with the proof.

Proposition 15. *(Schmidt,* [24]*) Let $n \geqslant 3$ denote an integer. Let R_n denote the Galois ring of characteristic 4 and size 4^n. Let R_n^x denote $R_n \setminus 2R_n$. Let T_n denote the Teichmuller set of R_n, and Tr the trace function of R_n. The generalized Boolean function in n variables defined for $x \in T_n$ by*

$$f(x) = \epsilon + Tr(sx)$$

for constants ϵ, s ranging in $\mathbb{Z}_4, R_n^x$ is bent. Its Gray image is either bent (n odd) or semi bent (n even).

Proof. The first assertion follows by [24, Construction 5.2] upon observing that $ZRM(1, n)$ is described by functions $f(x) = \epsilon + 2Tr(sx)$. The second assertion follows by Corollary 2. □

A monomial construction of a bent generalized Boolean function is presented in [24, Th. 5.3]. Intuitively it detects the generalized bent functions in the dual of the Goethals code.

Proposition 16. *(Schmidt,* [24]*) Keep the notation of Proposition 15. Let μ denote the "reduction mod 2"map from R_n to $\mathbb{F}_{2^n}$. The generalized Boolean function in n variables defined for $x \in T_n$ by $f(x) = \epsilon + Tr(sx + 2tx^3)$ for constants ϵ, s, t ranging*

in $\mathbb{Z}_4, R_n, T_n \setminus \{0\}$ *is bent if* $\mu(s) = 0$ *and the equation* $\mu(t)z^3 + 1 = 0$ *has no solutions in* $\mathbb{F}_{2^n}$, *or if* $\mu(s) \neq 0$ *and the equation*

$$z^3 + z + \frac{\mu(t)^2}{\mu(t)^6} = 0$$

has no solutions in $\mathbb{F}_{2^n}$.

By Corollary 2 the Gray map of this function is a binary Boolean function in $n+1$ variables which is semi bent if n is even or bent if n is odd. It is quadratic by Lemma 5.

In the original paper [27] it was mentioned that it would be interesting, for instance, to replace the exponent 3 in Proposition 16 by a Gold exponent $2^k + 1$. Then Li et al. [11] characterized the functions in n variables of the form $f(x) = Tr(ax + 2bx^{1+2^k})$ for odd $n/gcd(n/k)$.

8.2. **Quaternary bent functions.**

Proposition 17. *For every* n *a quaternary function*

$$g(x_1 + 2x_{n+1}, ..., x_n + 2x_{2n}) = c_1x_1 + ... + c_nx_n + 2(x_1x_{n+1} + ... + x_nx_{2n})$$

is a quaternary bent function with $c_i \in \mathbb{Z}_2$ *and* '$+$' *is addition over* $\mathbb{Z}_4$.

Proof. One can see that g can be divided into sum of n quaternary functions in one variable $g(x_1 + 2x_{n+1}, ..., x_n + 2x_{2n}) = g_1(x_1 + 2x_{1+n}) + ... + g_n(x_n + 2x_{2n})$,

$$g_i(x_i + 2x_{i+n}) = c_ix_i + 2x_ix_{i+n}.$$

From Proposition 1, we know that all x_ix_{i+n} are bent, $i = 1, ..., n$. From Statement 1 each of g_i is a quaternary bent function in one variable, therefore, from Proposition 4 g is also a quaternary bent function. □

Proposition 18. *Let* $g(x + 2y) = a(x, y) + 2b(x, y)$ *and* $g'(x + 2y) = a(x, y) + 2(a(x, y) \oplus b(x, y))$ *be quaternary functions with* $x, y \in \mathbb{Z}_2^n$ *and* a, b *be Boolean functions in* $2n$ *variables. Then* g *is bent if and only if* g' *is bent.*

Proof. Study the Walsh–Hadamard transform of g and g'. From Lemma 4, we have

$$\widehat{G}(x + 2y) = \frac{1}{2}\left(\widehat{B}(x \oplus y, x) + \widehat{A \cdot B}(y, x) - 2c_b(x \oplus y, x) - 2c_{a\oplus b}(y, x)\right) +$$

$$+\frac{i}{2}\left(\widehat{B}(y, x) - \widehat{A \cdot B}(x \oplus y, x) - 2c_b(y, x) + 2c_{a\oplus b}(x \oplus y, x)\right)$$

and

$$\widehat{G'}(x + 2(x \oplus y)) = \frac{1}{2}\left(\widehat{A \cdot B}(y, x) + \widehat{B}(x \oplus y, x) - 2c_{a\oplus b}(y, x) - 2c_b(x \oplus y, x)\right) +$$

$$+\frac{i}{2}\left(\widehat{A \cdot B}(x \oplus y, x) - \widehat{B}(y, x) + 2c_b(y, x) - 2c_{a\oplus b}(x \oplus y, x)\right),$$

with

$$c_f(u, x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle},$$

where f is a Boolean function in $2n$ variables, $V_x = \{\, x' \mid \langle x, x' \rangle \neq x.x' \,\}$, and $u \in \mathbb{Z}_2^n$.

Let $\Re$ and $\Im$ be real and imaginary parts of a complex number respectively. Then $\Re(\widehat{G}(x + 2y)) = \Re(\widehat{G'}(x + 2(x \oplus y)))$, $\Im(\widehat{G}(x + 2y)) = -\Im(\widehat{G'}(x + 2(x \oplus y)))$.

As it was mentioned in section 2 all quaternary bent functions are regular. Therefore, each of Walsh–Hadamard coefficients of a quaternary bent function has only real or imaginary part. Hence, if g is bent then $|\widehat{G'}(x+2(x\oplus y))| = |\widehat{G}(x+2y)| = 4^{n/2}$. By the same way we can prove that if g' is bent then $|\widehat{G}(x+2y)| = |\widehat{G'}(x+2(x\oplus y))| = 4^{n/2}$. This completes the proof. □

9. Conclusion and open problems

In the present work we have shown how generalizations of the notion of bent functions involving the ring $\mathbb{Z}_4$ could produce, by Gray map or by base 2 expansion, bent Boolean functions in the classical sense. We have proved that the approach of Kumar et al. and that of Schmidt are not equivalent at least in quaternary case. Schmidt's definition fits better $\mathbb{Z}_4$-cyclic codes constructions. Conversely classical binary bent functions (but perhaps not semi bent functions) can yield generalized bent functions by inverse Gray map. These results motivate to explore further algebraic constructions of generalized bent functions. Although the results show that there is no direct connection between quaternary and Boolean bent functions it is still might be possible to connect these notions if we will ask for additional conditions. For instance, it would be interesting to solve the problem that we mentioned at the end of section 4.3. It is also possible that notions of q-ary and Boolean bent functions are more connected for $q > 4$.

Acknowledgment

Authors wish to thank Sihem Mesnager and Alexander Kutsenko for helpful discussions. The work of the first and the second authors was supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

References

[1] S.V. Agievich, *Bent rectangles*, in Preneel, Bart (ed.) et al., *Boolean functions in cryptology and information security. Selected papers based on the presentations at the NATO-Russia Advanced Study Institute on Boolean functions in cryptology and information security, Zvenigorod, Russia, September 8–18, 2007*, 2008, 3–22. Zbl 1167.94004

[2] A.S. Ambrosimov, *Properties of bent functions of q-valued logic over finite fields*, Discrete Math. Appl., **4**:4 (1994), 341–350. Zbl 0816.03010

[3] T. Baignères, P. Junod, S. Vaudenay, *How far can we go beyond linear cryptanalysis?,* in Lee, Pil Joong, *Advances in Cryptology — ASIACRYPT 2004*, Lecture Notes in Computer Science, **3329**, 432-450, 2004, Zbl 1094.94025

[4] S. Gangopadhyay, E. Pasalic, P. Stănică, *A note on generalized bent criteria for Boolean functions*, IEEE Trans. Inf. Theory, **59**:5 (2013), 3233–3236. Zbl 1364.94799

[5] S. Gangopadhyay, C. Riera, P. Stănică, *Gowers U2 norm of Boolean functions and their generalizations*, Workshop on Cryptography and Coding, Rennes, France 2019.

[6] L. Granboulan, É. Levieil, G. Piret, *Pseudorandom permutation families over abelian groups*, in Robshaw, Matthew (ed.), *Fast Software Encryption — FSE 2006*, Graz, Austria. March 15–17, 2006, Lecture Notes in Computer Science, **4047**, 2006, 57–77. Zbl 1234.94043

[7] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inf. Theory, **40**:2 (1994), 301–319. Zbl 0811.94039

[8] S. Hodžić, W. Meidl, E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image*, IEEE Trans. Inf. Theory, **64**:7 (2018), 5432–5440. Zbl 1401.94263

[9] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, GTM, **84**, Springer, New York etc., 1990. Zbl 0712.11001

[10] P.V. Kumar, R.A. Scholtz, L.R. Welch, *Generalized bent functions and their properties*, J. Comb. Theory, Ser. A, **40**:1 (1985), 90–107. Zbl 0585.94016

[11] N. Li, X. Tang, T. Helleseth, *New constructions of quadratic bent functions in polynomial form*, IEEE Trans. Inf. Theory, **60**:9 (2014), 5760–5767. Zbl 1360.94479

[12] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes. Parts I, II*, North-Holland, Amsterdam etc., 1977. Zbl 0369.94008

[13] T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, in Duquesne, Sylvain (ed.) et al., *Arithmetic of finite fields, WAIFI 2016*, Lect. Notes Comput. Sci., **10064**, 160–173, 2016. Zbl 1409.11135

[14] T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, *Decomposing generalized bent and hyperbent functions*, IEEE Trans. Inf. Theory, **63**:12 (2017), 7804–7812. Zbl 1390.94951

[15] M. Matsui, A. Yamagishi, *A new method for known plaintext attack of FEAL cipher*, in Rueppel, Rainer A. (ed.), *Advances in cryptology — EUROCRYPT'92, Balatonfured, Hungary. May 24–28, 1992, Proc.*, Lect. Notes Comput. Sci. **658**, 81–91, Springer, Berlin, 1993. Zbl 0787.94019

[16] M. Matsui, *Linear cryptanalysis method for DES cipher*, in Helleseth, Tor (ed.), *Advances in Cryptology — EUROCRYPT'93 (Lofthus, Norway. May 23–27, 1993), Proc.*, Lect. Notes Comput. Sci., **765**, 386–397, Springer, Berlin, 1994. Zbl 0951.94519

[17] M. Matsui, *The first experimental cryptanalysis of the Data Encryption Standard.* in Desmedt, Yvo G. (ed.), *Advances in Cryptology — CRYPTO'94 (Santa Barbara, California, USA, August 21–25, 1994), Proc.*, Lect. Notes Comput. Sci., **839**, 1–11, Springer, Berlin, 1994. Zbl 0939.94551

[18] W. Meidl, *A secondary construction of bent functions, octal gbent functions and their duals*, Math. Comput. Simul., **143** (2018), 57–64. Zbl 07316125

[19] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, 2016.

[20] M.G. Parker, H. Raddum, *Z_4-linear cryptanalysis.* NESSIE Internal Report, 27/06/2002: NES/DOC/UIB/WP5/018/1.

[21] M.G. Parker, *Generalised S-Box Nonlinearity.* NESSIE Public Document, 11.02.03: NES/DOC/UIB/WP5/020/A.

[22] C. Riera, P. Stănică, S. Gangopadhyay, *Generalized bent Boolean functions and strongly regular Cayley graphs*, Discrete Appl. Math., **283** (2020), 367–374. Zbl 1442.05250

[23] O. Rothaus, *On bent functions*, J. Comb. Theory, Ser. A., **20**:3 (1976), 300–305. Zbl 0336.12012

[24] K-U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA.* IEEE Trans. Inf. Theory, **55**:4 (2009), 1824–1832. Zbl 1367.94344

[25] D. Singh, M. Bhaintwal, B.K. Singh, *Some results on q-ary bent functions*, Int. J. Comput. Math., **90**:9 (2013), 1761–1773. Zbl 1314.94094

[26] L. Sok, M. Shi, P. Solé, *Classification and construction of quaternary self-dual bent functions*, Cryptogr. Commun., **10**:2 (2018), 277–289. Zbl 1412.94257

[27] P. Solé, N. Tokareva, *Connections between quaternary and binary bent functions*, Cryptology ePrint Archive, Report, **2009/544**, (2009). available at `http://eprint.iacr.org/`.

[28] P. Solé, N. Tokareva, *On quaternary and binary bent functions*, Prikl. Diskr. Mat., Suppl., **1** 2009, 16–18. Zbl 07300366

[29] P. Stănică, T. Martinsen, S. Gangopadhyay, B.K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptography, **69**:1 (2013), 77–94. Zbl 1322.94094

[30] C. Tang, C. Xiang, Y. Qi, K. Feng, *Complete characterization of generalized bent and 2^k-bent Boolean functions*, IEEE Trans. Inf. Theory, **63**:7 (2017), 4668–4674. Zbl 1370.94614

[31] N.N. Tokareva, *Generalizations of bent functions. A survey*, Discretn. Anal. Isslid. Oper., **17**:1 (2010), 34–64. Zbl 1249.94057

[32] N. Tokareva, *Bent functions: results and applications to cryptography*, Acad. Press. Elsevier, Burlington, 2015.

[33] Y. Zheng, X.-M. Zhang, *On plateaued functions*, IEEE Trans. Inf. Theory, **47**:3 (2001), 1215–1223. Zbl 0999.94026

Natalia Nikolaevna Tokareva
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Email address: tokareva@math.nsc.ru

Alexander Sergeyevich Shaporenko
Novosibirsk State University,
2, Pirogova str.,
Novosibirsk, 630090, Russia
Email address: alexandr.shaporenko@gmail.com

Patrick Solé
I2M, CNRS, Aix-Marseille University, Centrale Marseille,
Marseilles, France
Email address: patrick.sole@telecom-paristech.fr