Connections between Quaternary and Binary Bent Functions

Patrick Solé[1] and Natalia Tokareva[2]

[1] CNRS LTCI, Telecom ParisTech, Dept Comelec
46 rue Barrault, 75 013 Paris, France
patrick.sole@telecom-paristech.fr,
[2] Sobolev Institute of Mathematics,
4 Acad. Koptyug avenue, 630090 Novosibirsk, Russia
tokareva@math.nsc.ru

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 direct links between Boolean bent functions, generalized Boolean bent functions (Schmidt, 2006) and quaternary bent functions (Kumar, Scholtz, Welch, 1985) are explored. We also study Gray images of bent functions and notions of generalized nonlinearity for functions that are relevant to generalized linear cryptanalysis.

Key words: 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 [17] 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 [12–14]. In that context bent functions are the ones which are the worst approximated by affine functions, or, equivalently have the worst possible nonlinearity. Recently several researchers [15, 16, 3, 6] 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 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 [18]. We shall 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. For example, to study bent functions on a finite abelian group [9, 20] (later these results were rediscovered in [4]), etc. See a survey of distinct generalizations in [21].

The material is organized as follows. Necessary definitions are given in section 2. In section 3 we show how Boolean bent functions, generalized Boolean bent functions ($q = 4$) and quaternary bent functions can be transformed each to other. In section 4.1 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. In Section 4.2 we show that the Gray image of a quaternary bent function is a binary Boolean semi bent function. Section 5 characterizes bent functions by their nonlinearity. Section 6 illustrates our results by a survey of the known constructions of generalized and quaternary bent functions and their Gray images.

2 Definitions and Notation

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

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_2^n} (-1)^{f(y)+x.y} = \sum_{y \in \mathbb{Z}_2^n} F_y (-1)^{x.y}. \qquad (1)$$

Here $x.y$ is a usual inner product of vectors. 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 partial case of *plateaued functions* [22]. 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

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

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 his paper [18]. 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

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

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] have studied q-ary bent functions in 1985. They proved that such functions exist for any even n and $q \neq 2 (\bmod 4)$. 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.

3 Connections between bent functions

Let $f : \mathbb{Z}_2^{2n} \to \mathbb{Z}_4$ be any 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. Define a quaternary function $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ as $g(x + 2y) = f(x, y)$. In this section we establish connections between properties of bentness for such functions.

The following lemmas are instrumental in what follows.

Lemma 31 *Between Walsh—Hadamard transforms of f, $a + b$, b there is the relation*

$$|\widehat{F}(x, y)|^2 = \frac{1}{2}\left(\widehat{B}^2(x, y) + \widehat{A+B}^2(x, y)\right). \tag{4}$$

Proof. Study the Walsh Hadamard Transform of f. According to (2) we have

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

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

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

From this we directly get what we need. □

Note that Lemma 31 holds for any (not only even) number of variables of the function f.

Theorem 32 *The following statements are equivalent*:
(i) *the generalized Boolean function f is bent in $2n$ variables*;
(ii) *the Boolean functions of $2n$ variables b and $a + b$ are both bent.*

Proof. By Lemma 31 we have $|\widehat{F}(x, y)|^2 = \frac{1}{2}\left(\widehat{B}^2(x, y) + \widehat{A+B}^2(x, y)\right)$. If $a + b$ 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 $\widehat{B}^2(x, y) + \widehat{A+B}^2(x, y) = 2^{2n+1}$. Since WHT coefficients of a Boolean function are integer, this equality has the unique solution $\widehat{B}^2(x, y) = \widehat{A+B}^2(x, y) = 2^{2n}$ (see [8] for detail). So, functions $a + b$ and b are bent. □

Lemma 33 *Between WHT coefficients of g, $a+b$, b there is the relation*

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

Proof. Study the Walsh Hadamard Transform of g. As far as for any $x, x', y, y' \in \mathbb{Z}_2^n$ it holds $(x+2y).(x'+2y') = x.x' + 2x.y' + 2y.x'$ modulo 4, then by (3) it is true

$$\widehat{G}(x+2y) = \sum_{x',y'} (-1)^{x.y'+y.x'+b(x',y')}\, i^{\,a(x',y')+x.x'}.$$

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

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

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

We see that for any $s \in \mathbb{Z}_4$ it holds

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

Using this formula for $s = x.x' + a(x', y')$ we obtain

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

where

$$S_1 = \sum_{x',y'} (-1)^{x.y'+y.x'+b(x',y')+\beta(x.x'+a(x',y'))},$$

$$S_2 = \sum_{x',y'} (-1)^{x.y'+y.x'+x.x'+b(x',y')+a(x',y')+\beta(x.x'+a(x',y'))}.$$

Here we used also that $\gamma(x.x' + a(x', y')) = x.x' + a(x', y')$, where $+$ is modulo 4 in brackets and modulo 2 on the right side of the equality. One can check it easily.

Now let $\mathbb{Z}_2^n = M_0 \cup M_1$, where $M_\delta = \{\, x' \mid x.x' = \delta \,\}$ for $\delta \in \mathbb{Z}_2$. Note that for x' from M_0 or M_1 the value of $\beta(x.x' + a(x', y'))$ is equal to 0 or $a(x', y')$ respectively. Then we divide every sum S_1, S_2 into two sums of types $\sum\limits_{x' \in M_0, y'}$ and $\sum\limits_{x' \in M_1, y'}$. Grouping items we get

$$S_1 + S_2 = \widehat{B}(x+y,x) + \widehat{A+B}(y,x),$$

$$S_1 - S_2 = \widehat{B}(y,x) - \widehat{A+B}(x+y,x).$$

This completes the proof. $\square$

We say that two Boolean functions c and d in $2n$ variables are *bent correlated* (with respect to dividing variables into two halves) if for any $x, y \in \mathbb{Z}_2^n$, it holds

1) $\widehat{C}^2(x,y) + \widehat{C}^2(x+y,y) + \widehat{D}^2(x,y) + \widehat{D}^2(x+y,y) = 4^{n+1}$;
2) $\widehat{C}(x,y) = \widehat{D}(x+y,y) = \pm 2^n \iff \widehat{C}(x+y,y) = \widehat{D}(x,y) = \pm 2^n$.

Theorem 34 *The following statements are equivalent*:
(i) *the quaternary function g is bent in n variables*;
(ii) *the Boolean functions b and $a+b$ are bent correlated in $2n$ variables.*

Proof. Rewrite the bent correlation property for b and $a+b$ in the form

$$\widehat{B}^2(y,x) + \widehat{B}^2(x+y,x) + \widehat{A+B}^2(y,x) + \widehat{A+B}^2(x+y,x) = 4^{n+1}, \quad (5)$$

$$\widehat{B}(y,x) = \widehat{A+B}(x+y,x) = \pm 2^n \iff \widehat{B}(x+y,x) = \widehat{A+B}(y,x) = \pm 2^n. \quad (6)$$

Applying Lemma 33 we get $4|\widehat{G}(x+2y)|^2 = s^2 + r^2$, where

$$s = \widehat{B}(x+y,x) + \widehat{A+B}(y,x),$$

$$r = \widehat{B}(y,x) - \widehat{A+B}(x+y,x).$$

(ii)$\Rightarrow$(i) Let b and $a+b$ be bent correlated functions. According to the Jacobi Theorem of 1834, see for instance [8], equation (5) has exactly 24 decisions in integer numbers (WHT coefficients). It is easy to obtain all of them. There are 16 decisions, say, *of the first type*, $(\pm 2^n, \pm 2^n, \pm 2^n, \pm 2^n)$. And 8 decisions *of the second type* $(\pm 2^{n+1}, 0, 0, 0)$. Hence integers s and r belong to the set $\{0, \pm 2^{n+1}\}$ for any x, y. We see that $s^2 + r^2$ can take the values 0, 4^{n+1} or $2 \cdot 4^{n+1}$. Let us fix vectors x, y and study these cases.

If $s^2 + r^2 = 0$ then $\widehat{B}(x+y,x) = -\widehat{A+B}(y,x)$ and $\widehat{B}(y,x) = \widehat{A+B}(x+y,x)$. According to (5) all these WHT coefficients should be $\pm 2^n$ (decision of the first type), but then we get a contradiction to (6).

Suppose that $s^2 + r^2 = 2 \cdot 4^{n+1}$. Then $\widehat{B}(x+y,x) + \widehat{A+B}(y,x) = \pm 2^{n+1}$ and $\widehat{B}(y,x) - \widehat{A+B}(x+y,x) = \pm 2^{n+1}$. Again from (5) it follows that $\widehat{B}(x+y,x) = \widehat{A+B}(y,x) = \pm 2^n$ and $\widehat{B}(y,x) = -\widehat{A+B}(x+y,x) = \pm 2^n$ (decision of the first type). Irrespective of the signs it again contradicts to (6).

Thus, the case $s^2 + r^2 = 4^{n+1}$ is only possible. Hence $|\widehat{G}(x+2y)|^2 = 4^n$ for any x, y and g is a bent function.

(i)$\Rightarrow$(ii) Let g be a bent function. For fixed x, y we have $4^{n+1} = s^2 + r^2$. This equality has the following possible decisions: $(\pm 2^{n+1}, 0)$ and $(0, \pm 2^{n+1})$. Let us study them.

Case 1 for (s, r). If $s = \pm 2^{n+1}$, $r = 0$ then we have $\widehat{B}(y', x) + \widehat{A+B}(x + y', x) = \pm 2^{n+1}$ and $\widehat{B}(x+y', x) = \widehat{A+B}(y', x)$, where $y' = x + y$. Denote by s' and r' the respecting numbers for the vectors x, y', i. e. $4|\widehat{G}(x+2y')|^2 = s'^2 + r'^2 = 4^{n+1}$. Study again two distinct cases.

Case 1 for (s', r'). Since $s' = \pm 2^{n+1}$, $r' = 0$ we get $\widehat{B}(x+y', x) + \widehat{A+B}(y', x) = \pm 2^{n+1}$ and $\widehat{B}(y', x) = \widehat{A+B}(x+y', x)$. From the four equations obtained we see that $\widehat{B}(x+y, x) = \widehat{A+B}(y, x) = \pm 2^n$ and $\widehat{B}(y, x) = \widehat{A+B}(x+y, x) = \pm 2^n$. So, in this case conditions (5) and (6) are satisfied for the given x, y.

Case 2 for (s', r'). It holds $s' = 0$ and $r' = \pm 2^{n+1}$. Then we get $\widehat{B}(x+y', x) = -\widehat{A+B}(y', x)$ and $\widehat{B}(y', x) - \widehat{A+B}(x+y', x) = \pm 2^{n+1}$. From the new four equations we obtain $\widehat{B}(y, x) = \widehat{A+B}(x+y, x) = 0$ and $\widehat{B}(x+y, x), \widehat{A+B}(y, x) \in \{0, \pm 2^{n+1}\}$ with the property that $\widehat{B}(x+y, x)$ is nonzero iff $\widehat{A+B}(y, x)$ is zero. Again for the vectors x, y conditions (5) and (6) are satisfied.

Case 2 for (s, r) is similar to Case 1. We have $s = 0$, $r = \pm 2^{n+1}$ and then $\widehat{B}(y', x) = -\widehat{A+B}(x+y', x)$ and $\widehat{B}(x+y', x) - \widehat{A+B}(y', x) = \pm 2^{n+1}$ for $y' = x + y$. Analyzing again both cases for (s', r') we see that (5) and (6) are true every time.

We have shown that for any vectors x, y the conditions (5), (6) hold, hence functions b and $a + b$ are bent correlated. □

Let us analyze the property of bent correlation. If functions c and d are bent then 1) is always true. Property 2) gives us some conformity between signs of WH coefficients for c and d. It is easy to note that if c and d are bent correlated then they are bent or not bent simultaneously.

It is not hard to get that between all 2^8 quaternary functions g in one variable there are precisely 24 bent functions. To obtain all of them get function $a(x_1, x_2)$ equal to 0, x_1 or $x_1 + 1$ and function b being arbitrary bent in two variables (8 possibilities).

We have got that among all 2^{32} quaternary functions g in 2 variables there are exactly $200\,704 = 49 \times 2^{12}$ bent functions. For $53\,248 = 13 \times 2^{12}$ such quaternary bent functions we obtained that Boolean functions $a + b$ and b are bent. For the rest $147\,456 = 36 \times 2^{12}$ functions $a + b$ and b are both not bent.

4 Gray images of bent functions

4.1 Generalized Boolean 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 [18, Th. 3.5] and is omitted.

Proposition 41 *For the WHTs of functions f and $\phi(f)$ it holds*

$$\widehat{\Phi(f)}(u, v) = 2\Re(i^{-v}\widehat{F}(u)) = \widehat{B}(u) + (-1)^v \widehat{A+B}(u), \text{ where } u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2. \quad (7)$$

Here $\Re$ denotes real part of a complex number. As far as the left side of equation (7) is a WH coefficient of a Boolean function, we easily get

Corollary 42 *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 43 *If f is 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. [8]. The obvious solutions for n odd are $X = Y = 2^{(n-1)/2}$ and $Y = 0,\ X = 2^{n/2}$ 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 43. The proof is immediate.

Proposition 44 *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.*

4.2 Quaternary bent functions

For a quaternary function $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ the Gray map $\phi(g)$ may be defined as the binary Boolean function in $2n+1$ variables $\phi(g)(x,y,z) := a(x,y)z+b(x,y)$, where $x, y \in \mathbb{Z}_2^n$ and $z \in \mathbb{Z}_2$. In other words this is the Gray map of f (with $2n$ variables) in the definition given above. From Proposition 41 we have

$$\widehat{\Phi(g)}(x,y,z) = \widehat{B}(x,y) + (-1)^z\widehat{A+B}(x,y), \text{ where } x,y \in \mathbb{Z}_2^n, z \in \mathbb{Z}_2. \quad (8)$$

Proposition 45 *If g is quaternary bent in n variables then $\phi(g)$ is a binary Boolean semi bent function in $2n+1$ variables.*

Proof. By Theorem 34 we know that b and $a+b$ are bent correlated. In the same way as in the proof of this theorem we can study possible values for $\widehat{B}(x,y)$ and $\widehat{A+B}(x,y)$. From the condition 1) of bent correlation property it follows that $\widehat{B}(x,y) + (-1)^z\widehat{A+B}(x,y)$ can get values 0 and $\pm 2^{n+1}$ only. According to (8) it means that $\phi(g)$ is semi bent. □

5 Notions of nonlinearity

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

5.1 Generalized Boolean functions

Let $RM(r,k)$ be the Reed Muller code of length 2^k and of order r, see [11]. 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 [5] for detail. We introduce the **nonlinearity** $N(f)$ of a generalized bent Boolean function f in n variables as

$$N(f) := 2^n - \frac{1}{2} \max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\widehat{\Phi(f)}(u,v)|. \tag{9}$$

We denote by $d_L(\cdot,\cdot)$ the Lee distance on $\mathbb{Z}_4^N$. Analogously, let $d_H(\cdot,\cdot)$ be the Hamming distance on $\mathbb{Z}_2^{2N}$. According to Corollary 42 we have

Proposition 51 *For any generalized Boolean function f in n variables it is true $N(f) \leqslant 2^n - 2^{(n-1)/2}$.*

Proposition 52 *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

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

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 $\widehat{\tilde{F}}(u) = \sum_{y \in \mathbb{Z}_2^n} i^{f(y)+2u.y}$. The second equality holds by the isometry property of the Gray map [5]. $\square$

Hence, using Propositions 51 and 52 we can reformulate one partial case from Corollary 43 and Proposition 44 as follows.

Corollary 53 *Let n be odd. A 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 again more complicated. We have

Corollary 54 *Let n be even. If a function f is bent then $N(f) = 2^n - 2^{n/2}$.*

Proof. By Corollary 43 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 41 and definition (9) we get $N(f) = 2^n - 2^{n/2}$. $\square$

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 $n+1$.

5.2 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 3) 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 52 is immediate.

Proposition 55 *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 determined yet.

6 Examples of Constructions

The degree of a generalized Boolean function g denoted by $\deg(g)$ is understood in the sense of its algebraic normal form (ANF). For computing degrees we require the following lemma.

Lemma 61 *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 [5]. □

6.1 Generalized bent functions

In [18, Th. 4.3] figures a natural generalization of the classical Maiorana McFarland construction.

Proposition 62 *(Schmidt, [18]) 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 43 the Gray map of this function is a binary Boolean semi bent function in $2n+1$ variables. By Lemma 61 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. [5].

Proposition 63 *(Schmidt, [18]) 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 [18, Construction 5.2] upon observing that $ZRM(1, n)$ is described by functions $f(x) = \epsilon + 2Tr(sx)$. The second assertion follows by Corollary 43. $\square$

A monomial construction of bent generalized Boolean function is in [18, Th. 5.3]. Intuitively it detects the generalized bent functions in the dual of the Goethals code.

Proposition 64 *(Schmidt, [18]) Keep the notation of Proposition 63. 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 43 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 61.

6.2 Quaternary bent functions

In [10, Th. 1] figures a natural generalization of the classical Maiorana McFarland construction. We specialize it to the case $q = 4$.

Proposition 65 *(Kumar, Scholtz, Welch, [10]) Let $n = 2m$ denote an even integer. The quaternary function g in n variables defined for x, y in $\mathbb{Z}_4^m$ by*

$$g(x, y) = x.\pi(y) + \tau(y),$$

with τ an arbitrary quaternary function in m variables and π an arbitrary permutation of $\mathbb{Z}_4^m$ is bent.

By Proposition 45 the Gray map $\phi(g)$ of this function is a binary Boolean semi bent function in $2n + 1$ variables. With the notation of Section 3 we see, by Theorem 34 that both b and $a + b$ are binary bent correlated functions in $2n$ variables.

7 Conclusion and open problems

In the present work we have shown how generalizations of the notion of bent function involving the ring $\mathbb{Z}_4$ could produce, by Gray map or by base 2 expansion, bent Boolean functions in the classical sense. The approach of Kumar et al and that of Schmidt do not seem to be equivalent. In the notation of Section 3 the quaternary function g being bent does not seem to imply that the generalized Boolean function f is bent. It would be very interesting to exhibit an example of the situation g bent and f not bent for any admissible number of variables. Both approaches are inspiring. Schmidt's definition fits better $\mathbb{Z}_4$-cyclic codes constructions and Kumar et al approach allows a nice analogue of Maiorana McFarland construction. In both cases an analogue of Dillon construction is lacking. Conversely classical binary bent function (but perhaps not semi bent functions) can yield generalized bent functions by inverse Gray map. These results set a motivation to explore further algebraic constructions of generalized bent functions or of quaternary bent functions. It would be interesting, for instance, to replace the exponent 3 in Proposition 64 by a Gold exponent $2^k + 1$ along the lines of [7]. More generally, monomial bent functions either quaternary or in the generalized sense are worthy of our interest.

Acknowledgment. Authors wish to thank Sihem Mesnager for helpful discussions. The first author was partially supported by ANR grant NUGET. The second author was supported by the RF President grant for young Russian scientists (MK-1250.2009.1), by the Russian Foundation for Basic Research (grants 07-01-00248, 08-01-00671, 09-01-00528) and the Russian Science Support Foundation.

References

1. S. V. Agievich, *Bent rectangles*, NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Zvenigorod, Russia. September 8–18, 2007). Proc: Netherlands, IOS Press. 2008. P. 3–22. Available at `http://arxiv.org/abs/0804.0209`.
2. A. S. Ambrosimov, *Properties of q-ary bent functions over finite fields*, Discrete Mathematics and Applications, 1994, V. 4. N 4. P. 341–350.
3. T. Baignères, P. Junod, S. Vaudenay *How Far Can We Go Beyond Linear Cryptanalysis?* Advances in Cryptology — ASIACRYPT '04 (Jeju Island, Korea. December 5–9, 2004). Proc. Berlin: Springer, 2004. P. 432–450 (LNCS 3329).
4. C. Carlet, C. Ding, *Highly nonlinear mappings*, J. of Complexity. 2004. V. 20. N 2–3. P. 205–244.
5. R. Hammons, V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *Kerdock, Preparata, Goethals and others are linear over* $\mathbb{Z}_4$, IEEE Trans. of Information Theory. 1994. V. 40. P. 301–319.
6. L. Granboulan, É. Levieil and G. Piret *Pseudorandom Permutation Families over Abelian Groups*, Fast Software Encryption — FSE 2006 (Graz, Austria. March 15–17, 2006). Springer, 2006. P. 57–77 (LNCS 4047).
7. T. Helleseth, V. Kumar, A. Shanbhag, *Codes with the same weight distribution as the Goethals and the Delsarte-Goethals codes*, Des. Codes and Crypt. 1996. V. 9. P. 257–266.
8. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, GTM 84, Springer. 1990.
9. O. A. Logachev, A. A. Sal'nikov, V. V. Yashenko, *Bent functions on a finite Abelian group*, Discrete Mathematics and Applications. 1997. V. 7. N 6. P. 547–564.
10. P. V. Kumar, R. A. Scholtz and L. R. Welch, *Generalized bent functions and their properties*. J. Combin. Theory Ser. A 40. 1985. P. 90-107.
11. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, Amsterdam: North–Holland, 1977.
12. M. Matsui, A. Yamagishi *A New Method for Known Plaintext Attack of FEAL Cipher*. Advances in Cryptology — EUROCRYPT'92 (Balatonfured, Hungary. May 24–28, 1992). Proc. Berlin: Springer, 1993. P. 81–91 (LNCS 658).
13. M. Matsui *Linear Cryptanalysis Method for DES Cipher*. Advances in Cryptology — EUROCRYPT'93 (Lofthus, Norway. May 23–27, 1993). Proc. Berlin: Springer, 1994. P. 386–397 (LNCS 765).
14. M. Matsui *The First Experimental Cryptanalysis of the Data Encryption Standard*. Advances in Cryptology — CRYPTO'94 (Santa Barbara, California, USA. August 21–25, 1994). Proc. Berlin: Springer, 1994. P. 1–11 (LNCS 839).
15. M. G. Parker and H. Raddum *Z4-Linear Cryptanalysis*. NESSIE Internal Report, 27/06/2002: NES/DOC/UIB/WP5/018/1.
16. M. G. Parker *Generalised S-Box Nonlinearity*. NESSIE Public Document, 11.02.03: NES/DOC/UIB/WP5/020/A.
17. O. Rothaus *On bent functions*, J. Combin. Theory, Ser. A. 1976. V. 20. N 3. P. 300–305.
18. K-U. Schmidt, *Quaternary Constant-Amplitude Codes for Multicode CDMA*. // IEEE International Symposium on Information Theory — ISIT'2007. (Nice, France. June 24–29, 2007). Proc. 2007. P. 2781–2785. Available at `http://arxiv.org/abs/cs.IT/0611162`.

19. *Schmidt K-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // IEEE International Symposium on Information Theory — ISIT'2007. (Nice, France. June 24–29, 2007). Proc. 2007. P. 2781–2785. Available at `http://arxiv.org/abs/cs.IT/0611162`.
20. Solodovnikov V. I. *Bent functions from a finite abelian group into a finite abelian group* // Discrete Mathematics and Applications. 2002. V. 12. N 2. P. 111–126.
21. Tokareva N. N. *Generalizations of bent functions. A survey* // appear soon in Journal of Applied and Industrial Mathematics, 2010.
22. Y. Zheng, X.-M. Zhang *On plateaued functions*, IEEE Trans. of Information Theory. 2001. V. 47. N. 3. P. 1215–1223.