Secondary Constructions on Generalized Bent Boolean Functions

Brajesh Kumar Singh*

Department of Mathematics,
Indian Institute of Technology Roorkee,
Roorkee 247667, INDIA
Email: bksingh0584@gmail.com

Abstract. *In this paper, we construct generalized bent Boolean functions in $n+2$ variables from given some generalized Boolean functions in n variables. We also show that the direct sum of two generalized bent Boolean functions is also generalized bent Boolean function.*

Key words: Generalized Boolean functions; generalized bent functions; Walsh–Hadamard transform.

1 Introduction

In the recent years several authors have proposed generalizations of Boolean functions [8, 11, 12] and studied the effect of Walsh–Hadamard transform on these classes. As in the Boolean case, in the generalized setup the functions which have flat spectra with respect to the Walsh–Hadamard transform are said to be generalized bent and are of special interest. The classical notion of bent was invented by Rothaus [10].

The generalization due to Schmidt [11] is defined as follows:

Definition 1. *[11, Schmidt] A function defined from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ ($\mathbb{Z}_q$ is ring of integers modulo q), for any positive integer $q \geq 2$, is called* generalized Boolean function *on n variables, where $\mathbb{Z}_2^n = \{\mathbf{x} = (x_n, \ldots, x_1) : x_\ell \in \mathbb{Z}_2, \ell = 1, 2, \ldots, n\}$ denotes a vector space over $\mathbb{Z}_2$ with the standard operations. The set of such functions denoted by $\mathcal{GB}_n^q$.*

The generalized bent Boolean functions are used for constructing the constant amplitude codes for the q valued version of multicode Code Division Multiple Access (MC-CDMA). For $q = 4$, Schmidt [11] studied the relations between generalized bent functions, constant amplitude codes, and $\mathbb{Z}_4$-linear codes. For some problems concerning cyclic codes, Kerdock codes, and Delsarte-Goethals codes, Schmidt's generalization of Boolean function seems more natural than the generalization due to Kumar et al. [8]. Solé and Tokareva [12] investigate systematically the links between Boolean bent functions [10], generalized bent Boolean functions [11], and quaternary bent functions [8]. Schmidt generalized

* Research supported by CSIR, INDIA.

the classical notion of Maiorana-McFarland class of bent functions, for $q = 4$. Recently, Stanica, Gangopadhyay and Singh [13] studied several properties generalized bent Boolean functions, characterized generalized bent Boolean functions symmetric with respect to two variables. They further generalized the classical notion of Maiorana-McFarland class of bent functions for any even positive integer q. The collections of the functions in this class is denoted by GMMF. They also provide the analogous of Dillon partial spreads type bent functions [7] in generalized setup and this class of generalized bent functions is termed as generalized Dillon's class (GD). In the same paper, authors provide an analogous of GPS class [1, 4, 5] in generalized setup which they refer as generalized spread class (GS) and proved that $GD \cup GMMF \subseteq GS$.

1.1 Preliminaries

Let us denote the set of integers, real numbers and complex numbers by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, respectively. By '+' we denote the addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, whereas '$\oplus$' denotes the addition over $\mathbb{Z}_2^n$ for all $n \geq 1$. Addition modulo q is denoted by '+' and it is understood from the context. For any $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1) \in \mathbb{Z}_2^n$, the scalar (or inner) product is defined by $\mathbf{x} \cdot \mathbf{y} := x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. The conjugate of a bit b denoted by $\bar{b}$. If $z = a + b\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\overline{z} = a - b\imath$ denotes the complex conjugate of z, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. $Re[z]$ denotes the real part of z. $\mathbb{R}\imath = \{a\imath : a \in \mathbb{R}\}$, denotes the set of purely imaginary numbers.

Let $\zeta = e^{2\pi\imath/q}$ be the complex q-primitive root of unity. The (generalized) *Walsh–Hadamard transform* of $f \in \mathcal{GB}_n^q$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is the complex valued function

$$\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

A function $f \in \mathcal{GB}_n^q$ is a *generalized bent* (*gbent*) function if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. Generalized bent Boolean functions exists for even integers and odd integers both whereas the bent Boolean functions ($q = 2$) exists only for even integers [10].

The sum

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x}) - g(\mathbf{x} \oplus \mathbf{u})}$$

is the *crosscorrelation* between $f, g \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$. The *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$.

If $q = 2$ (in Definition 1), we obtain the classical Boolean functions on n variables, whose set will be denoted by $\mathcal{B}_n$. The Walsh-Hadamard transform of any function $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is defined by

$$W_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}}.$$

A function $f \in \mathcal{B}_n$ for even n is bent if and only if $W_f(\mathbf{u}) = \pm 2^{\frac{n}{2}}$ for all $\mathbf{u} \in \mathbb{Z}_2^n$.

There are several ways to construct bent Boolean functions in $\mathcal{B}_{n+m}$ starting from bent functions in $\mathcal{B}_n$ and $\mathcal{B}_m$ [10]. Direct sum of two bent functions [6, pp. 81] is bent. Preneel et al. [9] constructed bent functions in $n+2$ variables from 4 bent functions in n variables. The construction due to Preneel et al. [9] is given in the following

Proposition 1. *[9, Theorem 7] The concatenation $f \in \mathcal{B}_{n+2}$ of 4 bent functions $f_\ell \in \mathcal{B}_n$ ($\ell = 0, 1, 2, 3$) is bent if and only if*

$$W_{f_0}(\mathbf{u})W_{f_1}(\mathbf{u})W_{f_2}(\mathbf{u})W_{f_3}(\mathbf{u}) = -2^{2n}, \text{ for all } \mathbf{u} \in \mathbb{Z}_2^n.$$

Proposition 2. *[9, Corollary 2] The order of the f_ℓ's has no importance, i.e., suppose $f = f_0||f_1||f_2||f_3$ with $f_\ell \in \mathcal{B}_n$.*

(i) If f, f_0, f_1 and f_2 are bent, then f_3 is bent.
(ii) If $f_0 = f_1$, then $f_2 = 1 \oplus f_3$, and if $f_0 = f_1 = f_2$, then $f_3 = 1 \oplus f_1$.

In this paper, we provide a secondary construction on generalized bent Boolean functions in $n+2$ variables from the generalized Boolean functions in $\mathcal{GB}_n^q$. We further prove that the direct sum of two generalized bent functions is also generalized bent.

2 Properties of Walsh–Hadamard transform on generalized Boolean functions

We gather in the current section several properties of the Walsh–Hadamard transform on generalized Boolean functions discussed in [13] are similar to the Boolean function case.

Theorem 1. *We have:*

(i) Let $f \in \mathcal{GB}_n^q$. The inverse of the Walsh–Hadamard transform is given by

$$\zeta^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u} \in \mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{y}}.$$

(ii) If $f, g \in \mathcal{GB}_n^q$, then

$$\sum_{\mathbf{u} \in \mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})},$$
$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

Further, $\mathcal{C}_{f,g}(\mathbf{u}) = \overline{\mathcal{C}_{g,f}(\mathbf{u})}$ for all $\mathbf{u} \in \mathbb{Z}_2^n$, which implies that $\mathcal{C}_f(\mathbf{u})$ is always real.

(iii) Taking the particular case $f = g$ we obtain

$$\mathcal{C}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2(-1)^{\mathbf{u}\cdot\mathbf{x}}. \quad (1)$$

(iv) If $f \in \mathcal{GB}_n^q$, then f is a gbent function if and only if

$$\mathcal{C}_f(\mathbf{u}) = \begin{cases} 2^n & \text{if } \mathbf{u} = 0, \\ 0 & \text{if } \mathbf{u} \neq 0. \end{cases}$$

(v) Moreover, the (generalized) Parseval's identity holds

$$\sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 = 2^n. \tag{2}$$

The properties of these transforms for $q = 2$ can be derived from the previous theorem. For more resuts on Boolean functions, the interested reader can consult [2, 3, 6].

3 Direct Sum of two Generalized Bent Boolean Functions

Theorem 2. *Suppose f_1 and f_2 are two arbitrary generalized Boolean functions on $\mathbb{Z}_2^r$ and $\mathbb{Z}_2^s$ respectively. Then a function $g : \mathbb{Z}_2^r \times \mathbb{Z}_2^s \to \mathbb{Z}_q$ expressed as*

$$g(\mathbf{x}, \mathbf{y}) = f_1(\mathbf{x}) + f_2(\mathbf{y}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^r, \mathbf{y} \in \mathbb{Z}_2^s,$$

is generalized bent if and only if f_1 and f_2 both are generalized bents.

Proof. Let $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s$ be arbitrary. We compute,

$$\begin{aligned} \mathcal{H}_g(\mathbf{u}, \mathbf{v}) &= 2^{-\frac{r+s}{2}} \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s} \zeta^{g(\mathbf{x},\mathbf{y})} (-1)^{\mathbf{u}\cdot\mathbf{x} + \mathbf{v}\cdot\mathbf{y}} \\ &= 2^{-\frac{r}{2}} \sum_{(\mathbf{x}) \in \mathbb{Z}_2^r} \zeta^{f_1(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} \left(2^{-\frac{s}{2}} \sum_{(\mathbf{y}) \in \mathbb{Z}_2^s} \zeta^{f_2(\mathbf{y})} (-1)^{\mathbf{v}\cdot\mathbf{y}} \right) \\ &= \mathcal{H}_{f_1}(\mathbf{u}) \mathcal{H}_{f_2}(\mathbf{v}). \end{aligned} \tag{3}$$

Suppose f_1 and f_2 are two arbitrary generalized bent Boolean functions on $\mathbb{Z}_2^r$ and $\mathbb{Z}_2^s$ respectively, then we have $|\mathcal{H}_{f_1}(\mathbf{u})| = 1$ and $|\mathcal{H}_{f_2}(\mathbf{v})| = 1$. Therefore, from (3), $|\mathcal{H}_g(\mathbf{u}, \mathbf{v})| = |\mathcal{H}_{f_1}(\mathbf{u})||\mathcal{H}_{f_2}(\mathbf{v})| = 1$ for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s$, this implies that g is generalized bent Boolean function.

Conversely, we assume g is generalized bent Boolean function, our aim is to show that the functions f_1 and f_2 are generalized bent Boolean functions. Let us suppose that f_1 is not bent, then there exists $\mathbf{u} \in \mathbb{Z}_2^r$ such that $|\mathcal{H}_{f_1}(\mathbf{u})| = \ell \neq 1$. Therefore, from (3), $|\mathcal{H}_{f_2}(\mathbf{v})| = \frac{1}{\ell}$ for every $\mathbf{v} \in \mathbb{Z}_2^s$. This implies

$$\sum_{\mathbf{v} \in \mathbb{Z}_2^s} |\mathcal{H}_{f_2}(\mathbf{v})|^2 = \frac{2^s}{\ell^2} \neq 2^s.$$

Which is a contradiction. Hence result. □

4 Generalized Bent Boolean Functions in $\mathcal{GB}_{n+2}^q$ From the Functions in $\mathcal{GB}_n^q$

Let $\mathbf{v} = (v_r, \ldots, v_1)$. We define

$$f_{\mathbf{v}}(x_{n-r}, \ldots, x_1) = f(x_n = v_r, \ldots, x_{n-r+1} = v_1, x_{n-r}, \ldots, x_1).$$

Let $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_2^r$ and $\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{Z}_2^{n-r}$. We define the vector concatenation by

$$\mathbf{uw} := (u_r, \ldots, u_1, w_{n-r}, \ldots, w_1).$$

Lemma 1. *Let $\mathbf{u} \in \mathbb{Z}_2^r$, $\mathbf{w} \in \mathbb{Z}_2^{n-r}$ and f be an n-variable generalized Boolean function. Then*

$$\mathcal{C}_f(\mathbf{uw}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^r} \mathcal{C}_{f_{\mathbf{v}}, f_{\mathbf{v} \oplus \mathbf{u}}}(\mathbf{w}).$$

In particular, for $r = 1$, $\mathcal{C}_f(0\mathbf{w}) = \mathcal{C}_{f_0}(\mathbf{w}) + \mathcal{C}_{f_1}(\mathbf{w})$, and $\mathcal{C}_f(1\mathbf{w}) = 2Re[\mathcal{C}_{f_0,f_1}(\mathbf{w})]$.

Theorem 3. *A function $f \in \mathcal{GB}_{n+2}^q$ expressed as*

$$f(z, y, \mathbf{x}) = f_0(\mathbf{x})(1 \oplus z)(1 \oplus y) + f_1(\mathbf{x})(1 \oplus z)y + f_2(\mathbf{x})(1 \oplus y)z + f_3(\mathbf{x})yz,$$

where $f_\ell \in \mathcal{GB}_n^q$, $(\ell = 0, 1, 2, 3)$, is generalized bent if and only if

(a) $\sum_{\ell=0}^3 \mathcal{C}_{f_\ell}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{0\}$, and

(b) $\mathcal{C}_{f_0,f_1}(\mathbf{u}) + \mathcal{C}_{f_2,f_3}(\mathbf{u}), \mathcal{C}_{f_0,f_2}(\mathbf{u}) + \mathcal{C}_{f_1,f_3}(\mathbf{u}), \mathcal{C}_{f_0,f_3}(\mathbf{u}) + \mathcal{C}_{f_1,f_2}(\mathbf{u}) \in \mathbb{R}\imath$ for all $\mathbf{u} \in \mathbb{Z}_2^n$.

Proof. Let F_ℓ $(\ell \in \mathbb{Z}_2)$ be the restriction of f on the hyperplane $\{\ell\} \times \mathbb{Z}_2 \times \mathbb{Z}_2^n \equiv \mathbb{Z}_2^{n+1}$. Then $F_0(y, \mathbf{x}) = f(0, y, \mathbf{x}) = f_0(\mathbf{x})(1 \oplus y) + f_1(\mathbf{x})y$ and $F_1(y, \mathbf{x}) = f(1, y, \mathbf{x}) = f_2(\mathbf{x})(1 \oplus y) + f_3(\mathbf{x})y$. Now,

$$\begin{aligned}
\mathcal{C}_{F_0,F_1}(0, \mathbf{u}) &= \sum_{(y,\mathbf{x}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^n} \zeta^{F_0(y,\mathbf{x}) - F_1((y,\mathbf{x}) \oplus (0,\mathbf{u}))} \\
&= \sum_{(y,\mathbf{x}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^n} \zeta^{F_0(y,\mathbf{x}) - F_1((y,\mathbf{x} \oplus \mathbf{u}))} \\
&= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{F_0(0,\mathbf{x}) - F_1((0,\mathbf{x} \oplus \mathbf{u}))} + \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{F_0(1,\mathbf{x}) - F_1((1,\mathbf{x} \oplus \mathbf{u}))} \qquad (4) \\
&= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f_0(\mathbf{x}) - f_2(\mathbf{x} \oplus \mathbf{u})} + \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f_1(\mathbf{x}) - f_4(\mathbf{x} \oplus \mathbf{u})} \\
&= \mathcal{C}_{f_0,f_2}(\mathbf{u}) + \mathcal{C}_{f_1,f_3}(\mathbf{u}).
\end{aligned}$$

Similarly we compute,

$$\begin{aligned}\mathcal{C}_{F_0,F_1}(1,\mathbf{u}) &= \sum_{(y,\mathbf{x})\in\mathbb{Z}_2\times\mathbb{Z}_2^n} \zeta^{F_0(y,\mathbf{x})-F_1((1\oplus y,\mathbf{x}\oplus\mathbf{u}))}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{F_0(0,\mathbf{x})-F_1((1,\mathbf{x}\oplus\mathbf{u}))} + \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{F_0(1,\mathbf{x})-F_1((0,\mathbf{x}\oplus\mathbf{u}))}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f_0(\mathbf{x})-f_3(\mathbf{x}\oplus\mathbf{u})} + \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f_1(\mathbf{x})-f_2(\mathbf{x}\oplus\mathbf{u})}\\ &= \mathcal{C}_{f_0,f_3}(\mathbf{u}) + \mathcal{C}_{f_1,f_2}(\mathbf{u}).\end{aligned} \tag{5}$$

Using Lemma 1 for $r = 1$, we have

$$\mathcal{C}_f(0,b,\mathbf{u}) = \mathcal{C}_{F_0}(b,\mathbf{u}) + \mathcal{C}_{F_1}(b,\mathbf{u}), b\in\mathbb{Z}_2, \mathbf{u}\in\mathbb{Z}_2^n, \text{ and} \tag{6}$$

$$\mathcal{C}_f(1,b,\mathbf{u}) = \mathcal{C}_{F_0,F_1}(b,\mathbf{u}) + \overline{\mathcal{C}_{F_0,F_1}(b,\mathbf{u})}, b\in\mathbb{Z}_2, \mathbf{u}\in\mathbb{Z}_2^n. \tag{7}$$

Further, using Lemma 1 in (6), we have

$$\mathcal{C}_f(0,0,\mathbf{u}) = \mathcal{C}_{f_0}(\mathbf{u}) + \mathcal{C}_{f_1}(\mathbf{u}) + \mathcal{C}_{f_2}(\mathbf{u}) + \mathcal{C}_{f_3}(\mathbf{u}), \text{ and} \tag{8}$$

$$\begin{aligned}\mathcal{C}_f(0,1,\mathbf{u}) &= \mathcal{C}_{F_0}(1,\mathbf{u}) + \mathcal{C}_{F_1}(1,\mathbf{u})\\ &= \mathcal{C}_{f_0,f_1}(\mathbf{u}) + \overline{\mathcal{C}_{f_0,f_1}(\mathbf{u})} + \mathcal{C}_{f_2,f_3}(\mathbf{u}) + \overline{\mathcal{C}_{f_2,f_3}(\mathbf{u})},\\ &= 2Re\left[\mathcal{C}_{f_0,f_1}(\mathbf{u}) + \mathcal{C}_{f_2,f_3}(\mathbf{u})\right].\end{aligned} \tag{9}$$

Combining (4) and (7), we have

$$\begin{aligned}\mathcal{C}_f(1,0,\mathbf{u}) &= \mathcal{C}_{F_0,F_1}(0,\mathbf{u}) + \overline{\mathcal{C}_{F_0,F_1}(0,\mathbf{u})}\\ &= \mathcal{C}_{f_0,f_2}(\mathbf{u}) + \mathcal{C}_{f_1,f_3}(\mathbf{u}) + \overline{\mathcal{C}_{f_0,f_2}(\mathbf{u}) + \mathcal{C}_{f_1,f_3}(\mathbf{u})}\\ &= 2Re\left[\mathcal{C}_{f_0,f_2}(\mathbf{u}) + \mathcal{C}_{f_1,f_3}(\mathbf{u})\right].\end{aligned} \tag{10}$$

Similarly on combining (5) and (7), we have

$$\mathcal{C}_f(1,1,\mathbf{u}) = 2Re\left[\mathcal{C}_{f_0,f_3}(\mathbf{u}) + \mathcal{C}_{f_1,f_2}(\mathbf{u})\right]. \tag{11}$$

Suppose $f\in\mathcal{GB}_{n+2}^q$ such that conditions (a) and (b) holds, then from (8), (9), (10) and (11) we have $\mathcal{C}_f(b,a,\mathbf{u}) = 0$ for all $(b,a,\mathbf{u}) \neq (0,0,\mathbf{0})$ and $\mathcal{C}_f(0,0,\mathbf{0}) = 2^{n+2}$. Therefore f is generalized bent.

Conversely, if f is generalized bent, then $\mathcal{C}_f(b,a,\mathbf{u}) = 0$ for all $(b,a,\mathbf{u}) \neq (0,0,\mathbf{0})$ and $\mathcal{C}_f(0,0,\mathbf{0}) = 2^{n+2}$. Applying (8), (9), (10) and (11) with the above conditions we have (a) and (b). □

References

1. Carlet, C.: *Generalized partial spreads*, IEEE Trans. Inform. Theory 41((1995), 1482–1487.
2. Carlet, C.: *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monograph "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), (2010), 257–397.
3. Carlet, C.: *Vectorial Boolean Functions for Cryptography*, Chapter of the monograph "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), (2010), 398–469.
4. Carlet, C. and Guillot, P.: *A characterization of binary bent functions*, J. Combin. Theory (A) 76(2) (1996), 328–335.
5. Carlet, C. and Guillot, P.: *An alternate characterization of the bentness of binary functions, with uniqueness*, Des. Codes Cryptography 14(2) (1998), 133–140.
6. Cusick, T. W. and Stănică, P.: Cryptographic Boolean functions and applications, Elsevier – Academic Press, 2009.
7. Dillon, J. F.: *Elementary Hadamard difference sets*, Proceedings of Sixth S.E. Conference of Combinatorics, Graph Theory, and Computing, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg 1975, 237–249.
8. Kumar, P. V., Scholtz, R. A. and Welch, L. R.: *Generalized bent functions and their properties*, J. Combin. Theory (A) 40 (1985), 90–107.
9. Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R. and Vandewalle, J.: *Propagation characteristics of Boolean functions.* In: Adv. in Crypt.-Eurocrypt 90. LNCS, 473. Berlin: Springer; 1991. p. 16173.
10. Rothaus, O. S.: *On bent functions*, J. Combinatorial Theory Ser. A 20 (1976), 300–305.
11. Schmidt K-U.: *Quaternary Constant-Amplitude Codes for Multicode CDMA*, IEEE International Symposium on Information Theory, ISIT'2007 (Nice, France, June 24–29, 2007), 2781–2785; available at http://arxiv.org/abs/cs.IT/0611162.
12. Solé, P. and Tokareva, N.: *Connections between Quaternary and Binary Bent Functions*, http://eprint.iacr.org/2009/544.pdf; see also, Prikl. Diskr. Mat. 1 (2009), 16–18.
13. Stanica, P., Gangopadhyay, S. and Singh, B. K.: *Some Results Concerning Generalized Bent Functions*, http://eprint.iacr.org/2011/290.pdf.