Complete characterization of generalized bent and 2^k-bent Boolean functions

Chunming Tang, Can Xiang, Yanfeng Qi, Keqin Feng

Abstract

In this paper we investigate properties of generalized bent Boolean functions and 2^k-bent (i.e., negabent, octabent, hexadecabent, et al.) Boolean functions in a uniform framework. We generalize the work of Stănică et al., present necessary and sufficient conditions for generalized bent Boolean functions and 2^k-bent Boolean functions in terms of classical bent functions, and completely characterize these functions in a combinatorial form. The result of this paper further shows that all generalized bent Boolean functions are regular.

Index Terms

Boolean functions, Walsh-Hadamard transforms, 2^k-bent functions, generalized bent functions, cyclotomic fields

I. Introduction

Throughout this paper, let $\mathbb{Z}_{2^k}$ be the ring of integers modulo 2^k, $\mathbb{Z}_2^n$ be the n-dimensional vector space over $\mathbb{Z}_2$, and $\mathbb{C}$ the field of complex numbers, where k, n are positive integers. If $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$ are two vectors in $\mathbb{Z}_2^n$, we define the scalar (or inner) product by $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$. For a complex $z = a + b\sqrt{-1}$, the absolute value of z is $|z| = \sqrt{a^2 + b^2}$ and $\overline{z} = a - b\sqrt{-1}$ denotes the complex conjugate of z, where a and b are real numbers.

A function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{2^k}$ is called a generalized Boolean function on n variables [11], whose set is denote by $\mathcal{GB}_n^k$. If $k = 1$, a function in $\mathcal{GB}_n^1$ is a classical Boolean function on n variables. An important tool in the analysis of generalized Boolean function is the (generalized) Walsh-Hadamard transform, which is the function $\mathcal{H}_g : \mathbb{Z}_2^n \to \mathbb{C}$, defined by

$$\mathcal{H}_g(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} \zeta_{2^k}^{g(\mathbf{x})}, \tag{1}$$

where $g \in \mathcal{GB}_n^k$, $\mathbf{u} \in \mathbb{Z}_2^n$, and $\zeta_{2^k} = e^{\frac{2\pi\sqrt{-1}}{2^k}}$ is the complex 2^k-primitive root of unity. The inverse Walsh-Hadamard transform of such g is

$$\zeta_{2^k}^{g(\mathbf{x})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u} \in \mathbb{Z}_2^n} \mathcal{H}_g(\mathbf{u}) (-1)^{\mathbf{u}\cdot\mathbf{x}}. \tag{2}$$

The function g is said to be a generalized bent function if $|\mathcal{H}_g(\mathbf{u})| = 1$ for any $\mathbf{u} \in \mathbb{Z}_2^n$. A generalized bent function g is regular if there exists some generalized Boolean function g^* satisfying $\mathcal{H}_g(\mathbf{u}) = \zeta_{2^k}^{g^*(\mathbf{u})}$ for any $\mathbf{u} \in \mathbb{Z}_2^n$. Such function g^* is called the dual of g. From Equation (2), the dual g^* of a regular generalized bent function g is also regular. When $k = 1$, the generalized bent function g is just classical Boolean bent functions which have been introduced by Rothaus [8]. These bent functions only exist for n even. If n is odd, a function $g \in \mathcal{GB}_n^1$ is said to be a semibent function if and only if $|\mathcal{H}_g(\mathbf{u})| \in \{0, \sqrt{2}\}$ for any $\mathbf{u} \in \mathbb{Z}_2^n$. Such Boolean functions have been extensively studied, as they have important applications in cryptograph(stream ciphers [1]), sequences [6] and coding theory (Reed-Muller codes [3]). We refer to [2], [4], [5], [16] for more on cryptographic Boolean function and bent functions. When $k = 2$, generalized Boolean functions in $\mathcal{GB}_n^2$ were studied by Schmidt [10]. Solé and Tokareva [11] discussed the connection between generalized bent functions in $\mathcal{GB}_n^2$ and bent functions in $\mathcal{GB}_n^1$. Stănică et al. [13] characterized generalized bent Boolean functions in $\mathcal{GB}_n^2$ and $\mathcal{GB}_n^3$.

For Boolean functions $f \in \mathcal{GB}_n^1$, the authors in [9], [7], [14], [15] introduced and investigated another transform which was called nega-Hadamard transform. Later, Stănică [12] generalized their results and proposed the 2^k-Hadamard transform of f defined by

$$\mathcal{H}_f^{(2^k)}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{u}\cdot\mathbf{x}} \zeta_{2^k}^{wt(\mathbf{x})}, \tag{3}$$

This work was supported by the National Natural Science Foundation of China (Grant No. 11401480, 11531002). C. Tang also acknowledges support from 14E013 and CXTD2014-4 of China West Normal University. Y. Qi also acknowledges support from KSY075614050 of Hangzhou Dianzi University. The research of K. Feng was supported by NSFC No. 11471178, 11571007 and the Tsinghua National Lab. for Information Science and Technology.

C. Tang is with School of Mathematics and Information, China West Normal University, Nanchong, Sichuan, 637002, China. e-mail: tangchunming-math@163.com

C. Xiang is with the College of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China. Email: cxiangcxiang@hotmail.com

Y. Qi is with School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China. e-mail: qiyanfeng07@163.com.

K. Feng is with the Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China. Email: kfeng@math.tsinghua.edu.cn.

where $\mathbf{u} \in \mathbb{Z}_2^n$ and $wt(\mathbf{x}) = \#\{i : 1 \leq i \leq n, x_i \neq 0\}$ is the Hamming weight of $\mathbf{x}$. A function f is called a 2^k-bent function if the 2^k-Hadamard transform are flat in absolute value, that is, $|\mathcal{H}_f^{(2^k)}(\mathbf{u})| = 1$, for any $\mathbf{u} \in \mathbb{Z}_2^n$. We call a function f a strong 2^k-bent function if and only if f is a 2^l-bent function for any $l \leq k$. Stănică [12] completely characterized the octabent (2^3-bent) and hexadecabent (2^4-bent) functions in terms of bent functions.

In this paper, we consider generalized bent Boolean functions in $\mathcal{GB}_n^k$ and 2^k-bent functions in $\mathcal{GB}_n^1$. Firstly, from the theory of cyclotomic fields we prove that all generalized bent Boolean functions are regular, i.e., their dual exist. Secondly, we completely characterize the generalized bent Boolean functions in $\mathcal{GB}_n^k$ ($k \geq 3$) in terms of bent functions and also describe these functions by a combinatorial form. Finally, we associate every function in $\mathcal{GB}_n^1$ with a function in $\mathcal{GB}_n^k$. Consequently, we completely characterize the 2^k ($k \geq 3$) bent Boolean functions in $\mathcal{GB}_n^1$ in terms of bent functions and also describe these functions by a combinatorial form.

II. Some results on cyclotomic fields and the regularity of generalized bent Boolean functions

In this section we will give some results on cyclotomic fields, which will be used in the following sections. We also prove that any generalized bent Boolean function in $\mathcal{GB}_n^k$ ($k \geq 3$) is always regular. Firstly, we state some basic facts on the cyclotomic field $K = \mathbb{Q}(\zeta_{2^k})$, which can be found in any book on algebraic number theory, such as [17] for example.

Let $\mathcal{O}_K$ be the ring of integers of $K = \mathbb{Q}(\zeta_{2^k})$. Any nonzero ideal A of $\mathcal{O}_K$ can be uniquely(up to the order) expressed as

$$A = P_1^{a_1} \cdots P_s^{a_s},$$

where $P_1, \cdots, P_s$ are distinct(nonzero) prime ideals of $\mathcal{O}_K$ and $a_i \geq 1 (1 \leq i \leq s)$. In other words, the set $S(K)$ of all nonzero ideals of $\mathcal{O}_K$ is a free multiplicative commutative semigroup with a basis $B(K)$, the set of all nonzero prime ideals of $\mathcal{O}_K$. Such semigroup $S(K)$ can be extended to the commutative group $I(K)$, called the group of fractional ideals of K. Each element of $I(K)$, called a fractional ideal, has the form AB^{-1}, where A, B are ideals of $\mathcal{O}_K$. For each $\alpha \in K^* = K \backslash \{0\}$, $\alpha\mathcal{O}_K$ is a fractional ideal, called a principal fractional ideal. And we have $(\alpha\mathcal{O}_K)(\beta\mathcal{O}_K) = \alpha\beta\mathcal{O}_K$ and $(\alpha\mathcal{O}_K)^{-1} = (\alpha^{-1})\mathcal{O}_K$. Therefore, the set $P(K)$ of all principal fractional ideals is a subgroup of $I(K)$. Some results on K are given in the following lemmas.

Lemma 2.1: Let $k \geq 2$ and $K = \mathbb{Q}(\zeta_{2^k})$, then

(i) The field extension $K/\mathbb{Q}$ is Galois of degree 2^{k-1} and the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_j : j \in \mathbb{Z}, j \equiv 1 \mod 2\}$, where the automorphism σ_j of K is defined by $\zeta_{2^k} \mapsto \zeta_{2^k}^j$. Moreover, $\sigma_{-1}(\alpha) = \overline{\alpha}$ for any $\alpha \in K$.

(ii) The ring of integers in K is $\mathcal{O}_K = \mathbb{Z}[\zeta_{2^k}]$ and $\{\zeta_{2^k}^j : 0 \leq j \leq 2^{k-1} - 1\}$ is an integral basis of $\mathcal{O}_K$. The group of roots of unity in $\mathcal{O}_K$ is $W_K = \{\zeta_{2^k}^j : 0 \leq j \leq 2^k - 1\}$.

(iii) Let $\varepsilon \in \mathcal{O}_K^*$(the units of $\mathcal{O}_K$). Then $\varepsilon \in W_K$ if and only if $|\varepsilon| = 1$.

(iv) The principal ideal $(1 - \zeta_{2^k})\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ and the rational prime 2 is totally ramified in $\mathcal{O}_K$, i.e., $2\mathcal{O}_K = ((1 - \zeta_{2^k})\mathcal{O}_K)^{2^{k-1}}$.

Lemma 2.2: Let n be a positive integer, $k \geq 3$, $\alpha \in \mathcal{O}_K$, and $|\frac{\alpha}{2^{\frac{n}{2}}}| = 1$. Then $\frac{\alpha}{2^{\frac{n}{2}}} \in W_K$.

Proof: From the condition (i) of Lemma 2.1 and $|\frac{\alpha}{2^{\frac{n}{2}}}| = 1$, we have

$$\alpha\sigma_{-1}(\alpha) = \alpha\overline{\alpha} = 2^n.$$

From the condition (iv) of Lemma 2.1, we have

$$(\alpha\mathcal{O}_K)\sigma_{-1}(\alpha\mathcal{O}_K) = ((1 - \zeta_{2^k})\mathcal{O}_K)^{n \cdot 2^{k-1}}.$$

According to the uniqueness of the decomposition of $(\alpha\mathcal{O}_K)\sigma_{-1}(\alpha\mathcal{O}_K)$ and the condition (iv) of Lemma 2.1, we have

$$\alpha\mathcal{O}_K = \sigma_{-1}(\alpha\mathcal{O}_K) = ((1 - \zeta_{2^k})\mathcal{O}_K)^{n \cdot 2^{k-2}}.$$

Note that $k \geq 3$ and $2^{\frac{1}{2}} = \zeta_8 + \zeta_8^{-1} \in \mathcal{O}_K$. From the condition (iv) of Lemma 2.1, we have

$$(2^{\frac{n}{2}}\mathcal{O}_K)^2 = (2\mathcal{O}_K)^n = ((1 - \zeta_{2^k})\mathcal{O}_K)^{n \cdot 2^{k-1}}.$$

We immediately have

$$\alpha\mathcal{O}_K = 2^{\frac{n}{2}}\mathcal{O}_K = ((1 - \zeta_{2^k})\mathcal{O}_K)^{n \cdot 2^{k-2}}$$

and

$$\frac{\alpha}{2^{\frac{n}{2}}} \in \mathcal{O}_K^*.$$

From the condition (iii) of Lemma 2.1, this lemma follows. ■

Theorem 2.3: Let $k \geq 3$. Then every generalized bent Boolean function in $\mathcal{GB}_n^k$ is always regular.

Proof: From the definition of generalized bent Boolean functions and Lemma 2.2, this lemma follows. ■

Lemma 2.4: Let $\gamma_{\mathbf{a}} = \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{a}\cdot\mathbf{v}} \zeta_{2^k}^{\sum_{j=1}^{k-1} v_j 2^{k-1-j}}$, where $\mathbf{a} \in \mathbb{Z}_2^{k-1}$ and $\mathbf{v} = (v_1, v_2, \cdots, v_{k-1})$. Then

$$\zeta_{2^k}^{e} = \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}},$$

where $e = \sum_{j=1}^{k-1} u_j 2^{k-1-j}$, $\mathbf{u} = (u_1, u_2, \cdots, u_{k-1})$, and $u_j \in \mathbb{Z}_2$. Further, $\{\gamma_{\mathbf{a}} : \mathbf{a} \in \mathbb{Z}_2^{k-1}\}$ is a basis of $K = \mathbb{Q}(\zeta_{2^k})$ over $\mathbb{Q}$.

Proof: For simplicity, denote

$$A = \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}}.$$

Then we have

$$\begin{aligned} A =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{u}\cdot\mathbf{a}} \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{v}\cdot\mathbf{a}} \zeta_{2^k}^{\sum_{j=1}^{k-1} v_j 2^{k-1-j}} \\ =& \frac{1}{2^{k-1}} \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}} \zeta_{2^k}^{\sum_{j=1}^{k-1} v_j 2^{k-1-j}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{a}\cdot(\mathbf{u}+\mathbf{v})}. \end{aligned}$$

Since $\sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{a}\cdot(\mathbf{u}+\mathbf{v})} = \begin{cases} 0, & v \neq u \\ 2^{k-1}, & v = u \end{cases}$. This leads to

$$A = \frac{1}{2^{k-1}} \cdot 2^{k-1} \zeta_{2^k}^{\sum_{j=1}^{k-1} u_j 2^{k-1-j}} = \zeta_{2^k}^{e}.$$

This completes the proof. ∎

Lemma 2.5: Let $\gamma_{\mathbf{a}} = \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{a}\cdot\mathbf{v}} \zeta_{2^k}^{\sum_{j=1}^{k-1} v_j 2^{k-1-j}}$, where $\mathbf{a} \in \mathbb{Z}_2^{k-1}$ and $\mathbf{v} = (v_1, v_2, \cdots, v_{k-1})$.Then

$$\zeta_{2^k}^{e} + \zeta_{2^k}^{e+2^{k-2}} = \frac{1}{2^{k-2}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}, a_1 = u_1} (-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}},$$

where $e = \sum_{j=1}^{k-1} u_j 2^{k-1-j}$, $\mathbf{u} = (u_1, u_2, \cdots, u_{k-1})$, and $u_j \in \mathbb{Z}_2$.

Proof: When $u_1 = 0$, from Lemma 2.4 we have

$$\begin{aligned} \zeta_{2^k}^{e} + \zeta_{2^k}^{e+2^{k-2}} =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} ((-1)^{\mathbf{u}\cdot\mathbf{a}} + (-1)^{a_1+\mathbf{u}\cdot\mathbf{a}}) \gamma_{\mathbf{a}} \\ =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (1 + (-1)^{a_1})(-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}} \\ =& \frac{1}{2^{k-2}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}, a_1 = u_1} (-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}}. \end{aligned}$$

When $u_1 = 1$, from $\zeta_{2^{k-1}}^{e+2^{k-2}} = -\zeta_{2^{k-1}}^{e-2^{k-2}}$ and Lemma 2.4 we have

$$\begin{aligned} \zeta_{2^k}^{e} + \zeta_{2^k}^{e+2^{k-2}} =& \zeta_{2^k}^{e} - \zeta_{2^k}^{e-2^{k-2}} \\ =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} ((-1)^{\mathbf{u}\cdot\mathbf{a}} - (-1)^{\mathbf{u}\cdot\mathbf{a}-a_1}) \gamma_{\mathbf{a}} \\ =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (1 - (-1)^{a_1})(-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}} \\ =& \frac{1}{2^{k-2}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}, a_1 = u_1} (-1)^{\mathbf{u}\cdot\mathbf{a}} \gamma_{\mathbf{a}}. \end{aligned}$$

This completes the proof. ∎

Lemma 2.6: Let $\mathbf{a} \in \mathbb{Z}_2^{k-1}$ and $\gamma_{\mathbf{a}} = \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{a}\cdot\mathbf{v}} \zeta_{2^k}^{\sum_{j=1}^{k-1} v_j 2^{k-1-j}}$. Then

$$\gamma_{\mathbf{a}} = \prod_{j=1}^{k-1} (1 + (-1)^{a_j} \zeta_{2^{j+1}}).$$

Proof: For simplicity, denote

$$A=\prod_{j=1}^{k-1}(1+(-1)^{a_j}\zeta_{2^{j+1}}).$$

Then we have

$$\begin{aligned}A&=\prod_{j=1}^{k-1}(\sum_{v_j\in\mathbb{Z}_2}(-1)^{a_jv_j}\zeta_{2^k}^{v_j2^{k-1-j}})\\&=\sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}}(-1)^{\mathbf{a}\cdot\mathbf{v}}\zeta_{2^k}^{\sum_{j=1}^{k-1}v_j2^{k-1-j}}.\end{aligned}$$

This completes the proof. ■

III. Complete characterization of generalized bent Boolean functions

In this section, we present the complete characterization of generalized bent Boolean functions in terms classical Boolean bent functions.

Let $g:\mathbb{Z}_2^n\to\mathbb{Z}_{2^k}$ be a generalized Boolean function. It turns out that the generalized Walsh-Hadamard spectrum of g can be described (albeit, in a comlicated manner) in terms of the Walsh-Hadamard spectrum of its Boolean components g_i.

Theorem 3.1: Let $g(\mathbf{x})=\sum_{i=0}^{k-1}g_i(\mathbf{x})2^{k-1-i}$, where $g\in\mathcal{GB}_n^k$ and $g_i\in\mathcal{GB}_n^1$. Then

$$\mathcal{H}_g(\mathbf{u})=\frac{1}{2^{k-1}}\sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}}\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u})\gamma_{\mathbf{a}},$$

where $\gamma_{\mathbf{a}}=\sum_{\mathbf{v}\in\mathbb{Z}_2^{k-1}}(-1)^{\mathbf{a}\cdot\mathbf{v}}\zeta_{2^k}^{\sum_{j=1}^{k-1}v_j2^{k-1-j}}$.

Proof: According to the definition of $\mathcal{H}_g(\mathbf{u})$, we have

$$\begin{aligned}2^{\frac{n}{2}}\mathcal{H}_g(\mathbf{u})&=\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta_{2^k}^{g(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\\&=\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta_{2^k}^{\sum_{i=0}^{k-1}g_i(\mathbf{x})2^{k-1-i}}(-1)^{\mathbf{u}\cdot\mathbf{x}}\\&=\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta_{2^k}^{\sum_{i=0}^{k-1}g_i(\mathbf{x})2^{k-1-i}}(-1)^{\mathbf{u}\cdot\mathbf{x}}\\&=\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{\mathbf{u}\cdot\mathbf{x}}\prod_{i=0}^{k-1}\zeta_{2^{i+1}}^{g_i(\mathbf{x})}\\&=\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\prod_{i=1}^{k-1}\zeta_{2^{i+1}}^{g_i(\mathbf{x})}\\&=\frac{1}{2^{k-1}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\cdot\prod_{i=1}^{k-1}((1+(-1)^{g_i(\mathbf{x})})+(1-(-1)^{g_i(\mathbf{x})})\zeta_{2^{i+1}})\\&=\frac{1}{2^{k-1}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\cdot\prod_{i=1}^{k-1}((1+\zeta_{2^{i+1}})+(1-\zeta_{2^{i+1}})(-1)^{g_i(\mathbf{x})}).\end{aligned}$$

Note that

$$(1+(-1)^{a_i}\zeta_{2^{i+1}})(-1)^{a_ig_i(\mathbf{x})}=\begin{cases}1+\zeta_{2^{i+1}} & \text{if } a_i=0,\\(1-\zeta_{2^{i+1}})(-1)^{g_i(\mathbf{x})} & \text{if } a_i=1.\end{cases}$$

Therefore, we have

$$\begin{aligned}2^{\frac{n}{2}}\mathcal{H}_g(\mathbf{u})&=\frac{1}{2^{k-1}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\cdot\sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}}(-1)^{\sum_{i=1}^{k-1}\mathbf{a}_ig_i(\mathbf{x})}\prod_{i=1}^{k-1}(1+(-1)^{a_i}\zeta_{2^{i+1}})\\&=\frac{1}{2^{k-1}}\sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}}\prod_{i=1}^{k-1}(1+(-1)^{a_i}\zeta_{2^{i+1}})\cdot\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}+\sum_{i=1}^{k-1}\mathbf{a}_ig_i(\mathbf{x})}.\end{aligned}$$

According to the definition of $\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u})$, we have

$$\mathcal{H}_g(\mathbf{u}) = \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} \mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) \cdot \prod_{i=1}^{k-1}(1+(-1)^{a_i}\zeta_{2^{i+1}}).$$

From Lemma 2.6, this theorem follows. ■

Theorem 3.2: Let $k \geq 3$ and $g(\mathbf{x}) = \sum_{i=0}^{k-1} g_i(\mathbf{x})2^{k-1-i}$, where $g \in \mathcal{GB}_n^k$ and $g_i \in \mathcal{GB}_n^1$. Then g is generalized bent if and only if condition (i), for n even, respectively, (ii), for n odd hold, where:

(i) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = (-1)^{\mathbf{v}\cdot\mathbf{a}+b_0}, \text{for all } \mathbf{a} \in \mathbb{Z}_2^{k-1}.$$

(ii) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = \frac{1+(-1)^{a_1+v_1}}{2}(-1)^{\widetilde{\mathbf{v}}\cdot\widetilde{\mathbf{a}}+b_0}\sqrt{2},$$

for all $\mathbf{a} \in \mathbb{Z}_2^{k-1}$, where $\widetilde{\mathbf{v}} = (v_2, \cdots, v_{k-1})$ and $\widetilde{\mathbf{a}} = (a_2, \cdots, a_{k-1})$.

Proof: If g is generalized bent, then for any $\mathbf{u}$, $|\mathcal{H}_g(\mathbf{u})| = 1$. From Lemma 2.2, one has $\mathcal{H}_g(\mathbf{u}) \in W_K$. Thus, $\mathcal{H}_g(\mathbf{u}) = \zeta_{2^k}^e$ or $-\zeta_{2^k}^e$, where $e = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$ and $v_j \in \mathbb{Z}_2$.

When n is even, suppose $\mathcal{H}_g(\mathbf{u}) = \zeta_{2^k}^e$ and $e = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$. According to Theorem 3.1 and Lemma 2.4, we have

$$\begin{aligned}\mathcal{H}_g(\mathbf{u}) =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} \mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u})\gamma_{\mathbf{a}} \\ =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (-1)^{\mathbf{v}\cdot\mathbf{a}}\gamma_{\mathbf{a}}.\end{aligned}$$

From the uniqueness of the expansion of $\mathcal{H}_g(\mathbf{u})$ by the basis $\{\gamma_{\mathbf{a}} : \mathbf{a} \in \mathbb{Z}_2^{k-1}\}$, we have

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = (-1)^{\mathbf{v}\cdot\mathbf{a}}, \text{for any } \mathbf{a} \in \mathbb{Z}_2^{k-1},$$

where $\mathbf{v}$ only depends on g and $\mathbf{u}$. Suppose $\mathcal{H}_g(\mathbf{u}) = -\zeta_{2^k}^e$ and $e = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$, by the same technique used in the case $e = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$, it can be verified that

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = (-1)^{\mathbf{v}\cdot\mathbf{a}+1}, \text{for any } \mathbf{a} \in \mathbb{Z}_2^{k-1}.$$

When n is odd, suppose $\mathcal{H}_g(\mathbf{u}) = \zeta_{2^k}^e$. Note that $\sqrt{2}\zeta_{2^k}^e = \zeta_{2^k}^e(\zeta_8 + \zeta_8^{-1}) = \zeta_{2^k}^{e-2^{k-3}} + \zeta_{2^k}^{(e-2^{k-3})+2^{k-2}}$. If $\mathcal{H}_g(\mathbf{u}) = \zeta_{2^k}^{e-2^{k-3}}$ and $e - 2^{k-3} = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$, by Theorem 3.1 and Lemma 2.5, we have

$$\begin{aligned}\sqrt{2}\mathcal{H}_g(\mathbf{u}) =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}} (\sqrt{2}\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}))\gamma_{\mathbf{a}} \\ =& \frac{1}{2^{k-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^{k-1}, a_1=v_1} 2(-1)^{\mathbf{v}\cdot\mathbf{a}}\gamma_{\mathbf{a}}.\end{aligned}$$

From the uniqueness of the expansion of $\sqrt{2}\mathcal{H}_g(\mathbf{u})$ by the basis $\{\gamma_{\mathbf{a}} : \mathbf{a} \in \mathbb{Z}_2^{k-1}\}$ and $\sqrt{2}\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) \in \mathbb{Q}$, we have

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = \begin{cases}\sqrt{2}(-1)^{\mathbf{v}\cdot\mathbf{a}}, & a_1 = v_1, \\ 0, & a_1 \neq v_1.\end{cases}$$

Hence, we obtain

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = \begin{cases}\sqrt{2}(-1)^{\widetilde{\mathbf{v}}\cdot\widetilde{\mathbf{a}}+v_1}, & a_1 = v_1, \\ 0, & a_1 \neq v_1,\end{cases}$$

where $\widetilde{\mathbf{v}} = (v_2, \cdots, v_{k-1})$ and $\widetilde{\mathbf{a}} = (a_2, \cdots, a_{k-1})$.

If $\mathcal{H}_g(\mathbf{u}) = -\zeta_{2^k}^{e-2^{k-3}}$ and $e - 2^{k-3} = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$, by the same technique used in the case $\mathcal{H}_g(\mathbf{u}) = \zeta_{2^k}^{e-2^{k-3}}$ and $e - 2^{k-3} = \sum_{j=1}^{k-1} v_j 2^{k-1-j}$, it can be verified that

$$\mathcal{H}_{g_0+\sum_{i=1}^{k-1}a_ig_i}(\mathbf{u}) = \begin{cases}\sqrt{2}(-1)^{\widetilde{\mathbf{v}}\cdot\widetilde{\mathbf{a}}+v_1+1}, & a_1 = v_1, \\ 0, & a_1 \neq v_1,\end{cases}$$

where $\widetilde{\mathbf{v}} = (v_2, \cdots, v_{k-1})$ and $\widetilde{\mathbf{a}} = (a_2, \cdots, a_{k-1})$.

If the condition (i) or (ii) in this theorem holds, then from the definition of generalized bent functions a simple computation shows that g is generalized bent.

Hence, the theorem follows. ■

Remark The cases $k = 2$ and $k = 3$ in Theorem 3.2 are investigated by Stănică, et al. in [13].

Corollary 3.3: Let $k \geq 3$ and $g(\mathbf{x}) = \sum_{i=0}^{k-1} g_i(\mathbf{x})2^{k-1-i}$ be generalized bent, where $g \in \mathcal{GB}_n^k$ and $g_i \in \mathcal{GB}_n^1$. Then, conditions (i), for n even, respectively, (ii), for n odd hold, where

(i) $g_0 + \sum_{i=1}^{k-1} a_i g_i$ is bent for all $\mathbf{a} \in \mathbb{Z}_2^{k-1}$;

(ii) $g_0 + \sum_{i=1}^{k-1} a_i g_i$ is semibent, for all $\mathbf{a} \in \mathbb{Z}_2^{k-1}$.

Proof: From Theorem 3.2, this corollary follows. ■

Corollary 3.4: Let $k \geq 3$ and $g(\mathbf{x}) = \sum_{i=0}^{k-1} g_i(\mathbf{x})2^{k-1-i}$ be generalized bent, where $g \in \mathcal{GB}_n^k$ and $g_i \in \mathcal{GB}_n^1$. Then, g_π is always generalized bent, where g_π is defined as (i), for n even, respectively, (ii), for n odd, where

(i) $g_\pi(\mathbf{x}) = g_0(\mathbf{x})2^{k-1} + \sum_{i=1}^{k-1} g_{\pi(i)}(\mathbf{x})2^{k-1-i}$ for any permutation π of $\{1, 2, \cdots, k-1\}$;

(ii) $g_\pi(\mathbf{x}) = g_0(\mathbf{x})2^{k-1} + g_1(\mathbf{x})2^{k-2} + \sum_{i=2}^{k-1} g_{\pi(i)}(\mathbf{x})2^{k-1-i}$ for any permutation π of $\{2, 3, \cdots, k-1\}$.

Proof: From Theorem 3.2, this corollary follows. ■

Corollary 3.5: Let $k \geq 3$, $l \leq k$, and $g(\mathbf{x}) = \sum_{i=0}^{k-1} g_i(\mathbf{x})2^{k-1-i}$ be generalized bent, where $g \in \mathcal{GB}_n^k$ and $g_i \in \mathcal{GB}_n^1$. Then, g_I is always generalized bent in $\mathcal{GB}_n^l$, where g_I is defined as (i), for n even, respectively, (ii), for n odd, where

(i) $g_I(\mathbf{x}) = g_0(\mathbf{x})2^{l-1} + \sum_{j=1}^{l-1} g_{i_j}(\mathbf{x})2^{l-1-j}$ for any subset $I = \{i_1, \cdots, i_{l-1}\}$ of $\{1, 2, \cdots, k-1\}$, where $\#I = l - 1$;

(ii) $g_I(\mathbf{x}) = g_0(\mathbf{x})2^{l-1} + g_1(\mathbf{x})2^{l-2} + \sum_{j=2}^{l-1} g_{i_j}(\mathbf{x})2^{l-1-j}$ for any subset $I = \{i_2, \cdots, i_{l-1}\}$ of $\{2, 3, \cdots, k-1\}$, where $\#I = l - 2$.

Proof: From Theorem 3.2, this corollary follows. ■

Theorem 3.6: Let $k \geq 3$ and $g(\mathbf{x}) = \sum_{i=0}^{k-1} g_i(\mathbf{x})2^{k-1-i}$, where $g \in \mathcal{GB}_n^k$ and $g_i \in \mathcal{GB}_n^1$. For any $\mathbf{w} \in \mathbb{Z}_2^{k-1}$, we define the set

$$\Gamma_{\mathbf{w}} = \{\mathbf{x} \in \mathbb{Z}_2^n : (g_1(\mathbf{x}), \cdots, g_{k-1}(\mathbf{x})) = \mathbf{w}\}.$$

Then g is generalized bent if and only if conditions (i), for n even, respectively, (ii), for n odd hold, where

(i) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} = \begin{cases} (-1)^{b_0} 2^{\frac{n}{2}}, & \mathbf{w} = \mathbf{v}, \\ 0, & otherwise. \end{cases}$$

(ii) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} = \begin{cases} \frac{(-1)^{b_0}}{\sqrt{2}} 2^{\frac{n}{2}}, & \mathbf{w} = (0, \widetilde{\mathbf{v}}), \\ \frac{(-1)^{b_0+v_1}}{\sqrt{2}} 2^{\frac{n}{2}}, & \mathbf{w} = (1, \widetilde{\mathbf{v}}), \\ 0, & otherwise, \end{cases}$$

where $\mathbf{v} = (v_1, \widetilde{\mathbf{v}})$.

Proof: Let $A = 2^{\frac{n}{2}} \mathcal{H}_{g_0+\sum_{i=1}^{k-1} a_i g_i}(\mathbf{u})$. According to the definition of $\mathcal{H}_{g_0+\sum_{i=1}^{k-1} a_i g_i}(\mathbf{u})$, one obtains

$$\begin{aligned} A &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}+\sum_{i=1}^{k-1} g_i(\mathbf{x})a_i} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} (-1)^{\sum_{i=1}^{k-1} g_i(\mathbf{x})a_i} \\ &= \sum_{\mathbf{w}\in\mathbb{Z}_2^{k-1}} \Big(\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} \Big) (-1)^{\mathbf{w}\cdot\mathbf{a}}. \end{aligned}$$

Suppose g is generalized bent. When n is even, from Theorem 3.2, we have

$$\begin{aligned} A = &\sum_{\mathbf{w}\in\mathbb{Z}_2^{k-1}} \Big(\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} \Big) (-1)^{\mathbf{w}\cdot\mathbf{a}} \\ = &2^{\frac{n}{2}} (-1)^{b_0} (-1)^{\mathbf{v}\cdot\mathbf{a}}, \end{aligned}$$

where $\mathbf{a} \in \mathbb{Z}_2^{k-1}$. Since $(-1)^{\mathbf{w}\cdot\mathbf{a}} (\mathbf{w} \in \mathbb{Z}_2^{k-1})$ as functions from $\mathbb{Z}_2^{k-1}$ to $\mathbb{C}$ $(\mathbf{a} \mapsto (-1)^{\mathbf{w}\cdot\mathbf{a}})$ are linear independent over $\mathbb{C}$. Hence, we obtain

$$\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} = \begin{cases} (-1)^{b_0} 2^{\frac{n}{2}}, & \mathbf{w} = \mathbf{v}, \\ 0, & otherwise. \end{cases}$$

When n is odd, from Theorem 3.2 we have

$$\begin{aligned}A=&\sum_{\mathbf{w}\in\mathbb{Z}_2^{k-1}}(\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}})(-1)^{\mathbf{w}\cdot\mathbf{a}}\\ =&2^{\frac{n}{2}}\frac{1+(-1)^{a_1+v_1}}{2}(-1)^{\widetilde{\mathbf{v}}\cdot\widetilde{\mathbf{a}}+b_0}\sqrt{2}.\end{aligned}$$

where $\mathbf{a}\in\mathbb{Z}_2^{k-1}$, $\mathbf{v}=(v_1,\widetilde{\mathbf{v}})$, and $\mathbf{a}=(a_1,\widetilde{\mathbf{a}})$. Let $c_{\mathbf{w}}=\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}$. Then one gets

$$\begin{aligned}A=&\sum_{\mathbf{w}\in\mathbb{Z}_2^{k-1}}c_{\mathbf{w}}(-1)^{\mathbf{w}\cdot\mathbf{a}}\\ =&\sum_{w_1\in\mathbb{Z}_2,\widetilde{\mathbf{w}}\in\mathbb{Z}_2^{k-2}}c_{\mathbf{w}}(-1)^{w_1\cdot a_1}(-1)^{\widetilde{\mathbf{w}}\cdot\widetilde{\mathbf{a}}}\\ =&\sum_{\widetilde{\mathbf{w}}\in\mathbb{Z}_2^{k-2}}(c_{(0,\widetilde{\mathbf{w}})}+c_{(1,\widetilde{\mathbf{w}})}(-1)^{a_1})(-1)^{\widetilde{\mathbf{w}}\cdot\widetilde{\mathbf{a}}}\\ =&2^{\frac{n}{2}}\frac{1+(-1)^{a_1+v_1}}{\sqrt{2}}(-1)^{b_0}(-1)^{\widetilde{\mathbf{v}}\cdot\widetilde{\mathbf{a}}}.\end{aligned}$$

Since $(-1)^{\widetilde{\mathbf{w}}\cdot\widetilde{\mathbf{a}}}(\widetilde{\mathbf{w}}\in\mathbb{Z}_2^{k-2})$ as functions from $\mathbb{Z}_2^{k-2}$ to $\mathbb{C}$ $(\widetilde{\mathbf{a}}\mapsto(-1)^{\widetilde{\mathbf{w}}\cdot\widetilde{\mathbf{a}}})$ are linear independent over $\mathbb{C}$. Hence, we obtain

$$c_{(0,\widetilde{\mathbf{w}})}+c_{(1,\widetilde{\mathbf{w}})}(-1)^{a_1}=\begin{cases}\frac{1+(-1)^{a_1+v_1}}{\sqrt{2}}(-1)^{b_0}2^{\frac{n}{2}}, & \widetilde{\mathbf{w}}=\widetilde{\mathbf{v}},\\ 0, & otherwise,\end{cases}$$

where $a_1\in\mathbb{Z}_2$. This implies that

$$\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}}(-1)^{g_0(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}=\begin{cases}\frac{(-1)^{b_0}}{\sqrt{2}}2^{\frac{n}{2}}, & \mathbf{w}=(0,\widetilde{\mathbf{v}}),\\ \frac{(-1)^{b_0+v_1}}{\sqrt{2}}2^{\frac{n}{2}}, & \mathbf{w}=(1,\widetilde{\mathbf{v}}),\\ 0, & otherwise.\end{cases}$$

If the condition (i) or (ii) holds, from the definition of generalized bent functions, g is generalized bent.
Hence, this theorem follows. ■

IV. Complete characterization of 2^k-bent Boolean functions

In this section, we consider the characterization of 2^k-bent Boolean functions, connect 2^k-bent Boolean functions with generalized bent functions, and characterize 2^k-bent Boolean functions in terms of bent Boolean functions.

For any $f\in\mathcal{GB}_n^1$, we give a unique generalized boolean function $g\in\mathcal{GB}_n^k$ such that

$$g(\mathbf{x})=f(\mathbf{x})2^{k-1}+wt(\mathbf{x}). \tag{4}$$

Suppose $g(\mathbf{x})=\sum_{i=0}^{k-1}g_i(\mathbf{x})2^{k-1-i}$, where $g_i\in\mathcal{GB}_n^1$. From Lemma 5 of [12], we have

$$g_i(\mathbf{x})=\begin{cases}f(\mathbf{x})+s_{2^{k-1}}(\mathbf{x}), & i=0,\\ s_{2^{k-1-i}}(\mathbf{x}), & 1\le i\le k-1,\end{cases} \tag{5}$$

where $s_{2^{k-1-i}}(\mathbf{x})$ are the elementary symmetric polynomials of degree 2^{k-1-i} (we use the convention that $s_{2^{k-1-i}}(\mathbf{x})=0$, if $\mathbf{x}\in\mathbb{Z}_2^n$, and $2^{k-1-i}>n$). The following theorem gives the relationship between f and g.

Theorem 4.1: Let f and g defined as Equation (4). Then

$$\mathcal{H}_f^{(2^k)}(\mathbf{u})=\mathcal{H}_g(\mathbf{u}).$$

Further, f is 2^k-bent if and only if g is generalized bent.

Proof: According to the definition of $\mathcal{H}_g(\mathbf{u})$, we have

$$\begin{aligned}\mathcal{H}_g(\mathbf{u})=&2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{\mathbf{u}\cdot\mathbf{x}}\zeta_{2^k}^{g(\mathbf{x})}\\ =&2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{\mathbf{u}\cdot\mathbf{x}}\zeta_{2^k}^{f(\mathbf{x})2^{k-1}+wt(\mathbf{x})}\\ =&2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\zeta_{2^k}^{wt(\mathbf{x})}\\ =&\mathcal{H}_f^{(2^k)}(\mathbf{u}).\end{aligned}$$

Then f is 2^k-bent if and only if g is generalized bent. Hence, this theorem follows. ■

Theorem 4.2: Let $k \geq 3$ and $f \in \mathcal{GB}_n^1$. Then f is 2^k-bent if and only if conditions (i), for n even, respectively, (ii), for n odd hold, where

(i) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\mathcal{H}_{f+s_{2^{k-1}}+\sum_{i=1}^{k-1} a_i s_{2^{k-1-i}}}(\mathbf{u}) = (-1)^{\mathbf{v}\cdot\mathbf{a}+b_0},$$

for any $\mathbf{a} \in \mathbb{Z}_2^{k-1}$.

(ii) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\mathcal{H}_{f+s_{2^{k-1}}+\sum_{i=1}^{k-1} a_i s_{2^{k-1-i}}}(\mathbf{u}) = \frac{1+(-1)^{a_1+v_1}}{\sqrt{2}}(-1)^{\widetilde{\mathbf{v}}\cdot\widetilde{\mathbf{a}}+b_0},$$

for any $\mathbf{a} \in \mathbb{Z}_2^{k-1}$, where $\widetilde{\mathbf{v}} = (v_2, \cdots, v_{k-1})$, and $\widetilde{\mathbf{a}} = (a_2, \cdots, a_{k-1})$.

Proof: From Theorem 4.1, Theorem 3.2, and Equation (5), this theorem follows. ■

Remark The case $k = 2$ in Theorem 4.2 was considered by Stănică et al. [14]. Stănică [12] investegated cases $k = 3, 4$ in Theorem 4.2.

Corollary 4.3: Let $k \geq 3$ and $f \in \mathcal{GB}_n^1$ be 2^k-bent. Then, conditions (i), for n even, respectively, (ii), for n odd hold, where
(i) $f + s_{2^{k-1}} + \sum_{i=0}^{k-2} a_i s_{2^i}$ is bent for all $\mathbf{a} \in \mathbb{Z}_2^{k-1}$;
(ii) $f + s_{2^{k-1}} + \sum_{i=0}^{k-2} a_i s_{2^i}$ is semibent for all $\mathbf{a} \in \mathbb{Z}_2^{k-1}$, .

Proof: From Theorem 4.2, this corollary follows. ■

Corollary 4.4: Let $k \geq 3$ and $f \in \mathcal{GB}_n^1$ be a strong 2^k-bent function. Then, conditions (i), for n even, respectively, (ii), for n odd hold, where
(i) $f + \sum_{i=0}^{k-1} a_i s_{2^i}$ is bent for all $\mathbf{a} \in \mathbb{Z}_2^k$;
(ii) $f + \sum_{i=0}^{k-1} a_i s_{2^i}$ is semibent for all $\mathbf{a} \in \mathbb{Z}_2^k$.

Proof: The conclusion follows from Corollary 4.3. ■

Theorem 4.5: Let $k \geq 3$ and $f \in \mathcal{GB}_n^1$. For any $\mathbf{w} \in \mathbb{Z}_2^{k-1}$, denote the following set

$$\Gamma_{\mathbf{w}} = \{\mathbf{x} \in \mathbb{Z}_2^n : (s_{2^{k-2}}(\mathbf{x}), \cdots, s_{2^0}(\mathbf{x})) = \mathbf{w}\}.$$

Then, f is 2^k-bent if and only if conditions (i), for n even, respectively, (ii), for n odd hold, where
(i) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{f(\mathbf{x})+s_{2^{k-1}}(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} = \begin{cases} (-1)^{b_0} 2^{\frac{n}{2}}, & \mathbf{w} = \mathbf{v}, \\ 0, & otherwise. \end{cases}$$

(ii) For any $\mathbf{u} \in \mathbb{Z}_2^n$, there exist some $\mathbf{v} \in \mathbb{Z}_2^{k-1}$ and some $b_0 \in \mathbb{Z}_2$ such that

$$\sum_{\mathbf{x}\in\Gamma_{\mathbf{w}}} (-1)^{f(\mathbf{x})+s_{2^{k-1}}(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} = \begin{cases} \frac{(-1)^{b_0}}{\sqrt{2}} 2^{\frac{n}{2}}, & \mathbf{w} = (0, \widetilde{\mathbf{v}}), \\ \frac{(-1)^{b_0+v_1}}{\sqrt{2}} 2^{\frac{n}{2}}, & \mathbf{w} = (1, \widetilde{\mathbf{v}}), \\ 0, & otherwise, \end{cases}$$

where $\mathbf{v} = (v_1, \widetilde{\mathbf{v}})$.

Proof: From Theorem 4.2, this theorem follows. ■

Corollary 4.6: Let $n \geq 3$ and $f \in \mathcal{GB}_n^1$ be 2^k-bent. Then $k \leq \log_2 n + 1$.

Proof: Suppose $k > \log_2 n + 1$. Then $n = \sum_{i=0}^{k-2} w_i 2^i$ and $w_i \in \{0, 1\}$. By the definition of $\Gamma_{\mathbf{w}}$, we have

$$\Gamma_{\mathbf{w}} = \{(\underbrace{1, 1, \cdots, 1}_{n})\}.$$

From Theorem 4.5 and $n \geq 3$, we have

$$1 = \#\Gamma_{\mathbf{w}} \equiv 0 \mod 2.$$

This leads to a contradiction and completes the proof. ■

V. Concluding Remarks

This paper generalized the work of Stănică et al. on generalized Boolean bent functions and 2^k-bent Boolean functions[12], [13], [14] . We showed that every generalized bent Boolean function was regular. A complete characterization for generalized Boolean bent functions and 2^k-bent Boolean functions was presented in terms of bent functions. And we also completely characterized these functions in a combinatoric form. It would be interesting to characterize generalized p-ary bent functions.

REFERENCES

[1] C. Carlet, "Boolean functions for cryptography and error correcting codes," in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257-397.

[2] C. Carlet, "Vectorial boolean functions for cryptography, in: Boolean Methods and Models," Cambridge University Press, Cambridge (2010), 398-469.

[3] C. Charnes, M. Rotteler, T. Beth, "Homogeneous bent functions, invariants," and designs, designs, codes and cryptography, 26(1-3), 139-154, 2002

[4] T. W. Cusick, P. Stănică, Cryptographic Boolean functions and Applications, Elsevier-Academic Press, 2009.

[5] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, New York, to appear.

[6] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," IEEE Trans. Inf. Theory, vol. 28, no. 6, pp. 858-864, Nov. 1982.

[7] M. G. Parker, A. Pott, "On Boolean functions which are bent and negabent." In: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (eds.), SSC 2007, LNCS 4893 (2007), Springer, Heidelberg, 9-23

[8] O. Rothaus, "On bent functions," J. Combin. Theory, Ser. A. 1976. V. 20. N 3. P. 300-305.

[9] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions," IEEE Trans. Inf. Theory 52:9 (2006), 4142-4159.

[10] 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.

[11] P. Solé , N. Tokareva, "Connections Between Quaternary and Binary Bent Functions." http://eprint.iacr.org/ 2009/544.pdf; see also, Prikl. Diskr. Mat. 1, 16-18 (2009).

[12] P. Stănică , "On weak and strong 2^k-bent Boolean functions," DOI 10.1109/TIT.2016.2539971, IEEE Transactions on Information Theory.

[13] P. Stănică, T.Martinsen, S. Gangopadhyay, B.K. Singh, "Bent and generalized bent Boolean functions," Des. Codes Cryptogr.69(1), 77-94 (2013).

[14] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, S. Maitra, "Investigations on bent and negabent functions via the negaHadamard transform," IEEE Trans. Inf. Theory 58 (2012), 4064-4072.

[15] W. Su, A. Pott, X. Tang, "Characterization of Negabent Functions and Construction of Bent-Negabent Functions With Maximum Algebraic Degree," IEEE Trans. Inf. Theory 59:6 (2013), 3387-3395.

[16] N. Tokareva, Bent Functions-Results and Applications to Cryptography, Elsevier-Academic Press, 2015.

[17] L.C. Washington, Introduction to Cyclotomic Fields, GTM 83. Springer, New York (1997).