Composition construction of new bent functions from known dually isomorphic bent functions

Guangpu Gao, Weiguo Zhang, and Yongjuan Wang *

Abstract. Bent functions are optimal combinatorial objects and have been studied over the last four decades. Secondary construction plays a central role in constructing bent functions since it may generate bent functions outside the primary classes of bent functions. In this study, we improve a theoretical framework of the secondary construction of bent functions in terms of the composition of Boolean functions. Based on this framework, we propose several constructions of bent functions through the composition of a balanced Boolean function and dually isomorphic (DI) bent functions defined herein. In addition, we present a construction of self-dual bent functions.

Keywords: Bent function, Boolean function, composition, dual isomorphism, Walsh spectrum.

1 Introduction

Boolean functions (including vectorial cases) play a central role in building nonlinear components of symmetric ciphers. As one of the most effective attacking methods, linear cryptanalysis makes use of the correlation between the input and output of the component to recover the key of the cipher. To resist linear cryptanalysis, high nonlinearity is a primary requirement for Boolean functions used in symmetric cryptosystems [5, 11]. The nonlinearity of a Boolean function f is defined as the minimum Hamming distance between f and affine functions. It can be efficiently computed by the Walsh transform of the constituent functions.

However, the computation is generally more difficult in the scenario of the composition of functions. Some progress was made independently by Bernasconi in [1, Lemma 2.17] and Nyberg in [17]. Three correlation theorems were presented and then were applied to the cryptanalysis of some block ciphers and stream

* G. Gao and Y. Wang are with PLA Strategic Support Force Information Engineering University and Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China, guangpu.gao@gmail.com.

W. Zhang is with State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China, zwg@xidian.edu.cn.

ciphers. Gupta and Sarkar [8] refined Nyberg's work and proposed a concise and lucid formula related to the Walsh transform of the composition of Boolean functions, which they called the "Composition Theorem."

Bent functions are maximally nonlinear Boolean functions with an even number of variables and were introduced by Rothaus [18]. Such functions have been extensively studied for their wide applications in cryptography, spread spectrum, coding theory, and combinatorial design [7]. Since the complete classification of bent functions seems elusive, many researchers have focused on constructing bent functions. Bent functions constructed from scratch are called primary constructions [4, 16], and bent functions constructed from known bent functions are called secondary constructions. The two well-known primary constructions are the Maiorana-McFarland class of bent functions [16] and the partial spread ($\mathcal{PS}$) class of bent functions [4]. As there are so few primary constructions in the literature, secondary constructions are often used to obtain new bent functions.

Two interesting secondary constructions of bent functions are those developed by Rothaus [18] with extension of the number of variables and by Carlet [2] without extension of the number of variables. A series of constructions have been obtained by revisiting or generalizing these results [12–15, 21, 23]. It was proved in [6] that some well-known secondary constructions of bent functions can be described by the composition of a Boolean function and some bent functions. Then a relationship between the secondary constructions and the composition of Boolean functions was established, and two constructions of bent functions were proposed. From the composite view of point, Hodžić et.al. recently [9] presented several new classes of bent or plateaued Boolean functions with some slight conditions. But it is difficult to determine whether these constructed bent functions belong to the completed versions of primary classes up to affine equivalence. More details may be found in a recently published book [13].

The present study is devoted to developing a general theory of secondary constructions of bent functions under the framework of a composition of Boolean functions. The paper is organized as follows. After introducing some formal notations and necessary preliminaries in Section 2, we introduce the definition of dually isomorphic (DI) bent functions in Section 3. We prove that the composition of any balanced Boolean function and the DI bent function is also a bent function without extension of the number of variables. We show that vectorial

bent functions in the $\mathcal{PS}$ class are DI bent functions. By using this conclusion, we give a positive answer to the open problem proposed by Mesnager. We then consider the secondary constructions of bent functions with extension of the number of variables. In Section 4, we present construction of the self-dual bent functions. Finally, we list our conclusions in Section 5.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2 = \{0, 1\}$. An n-variable Boolean function $f(x)$, where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, which can be represented in a unique way as an n-variable polynomial whose degree relative to each variable is at most 1, called its *algebraic normal form* (ANF):

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1, \cdots, n\}} \lambda_I \prod_{i \in I} x_i, \quad \lambda_I \in \mathbb{F}_2.$$

Let $\mathcal{B}_n$ denote the set of Boolean functions of n variables. The binary sequence defined by $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$ is called the *truth table* of a Boolean function $f \in \mathcal{B}_n$, where $v_0 = (0, \ldots, 0, 0)$, $v_1 = (0, \ldots, 0, 1)$, …, $v_{2^n-1} = (1, \ldots, 1, 1)$ are ordered by lexicographical order. The *Lagrange interpolation formula* in terms of Boolean function is defined as

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{2^n-1} f(v_i)(x_1 + v_{i,1} + 1)(x_2 + v_{i,2} + 1) \cdots (x_n + v_{i,n} + 1). \quad (1)$$

By applying the Lagrange interpolation method, it is a simple matter to obtain the ANF of every Boolean function from its truth table. The support of f is defined as $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. If $|\mathrm{supp}(f)| = 2^{n-1}$, then we call $f(x)$ balanced.

We say that two n-variable Boolean functions $f(x)$ and $g(x)$ are affinely equivalent if $g(x) = f(xA + b)$, where $b \in \mathbb{F}_2^n$, A is an $n \times n$ nonsingular binary matrix, and xA is the product of the row-vector x and A. An important tool for studying Boolean functions is the Walsh transform. Given $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $w = (w_1, w_2, \ldots, w_n) \in \mathbb{F}_2^n$, the inner product of w and x is defined as $w \cdot x = w_1 x_1 + \cdots + w_n x_n$. The "sign" function of f is the integer-valued function, usually denoted by $\chi_f(x) = (-1)^{f(x)}$. The *Walsh transform* of f is the discrete

Fourier transform of χ_f associated with this inner product, which is an integer-valued function over $\mathbb{F}_2^n$:

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

It is easy to see that f is balanced if and only if $W_f(\mathbf{0}_n) = 0$, where $\mathbf{0}_n$ denotes the zero vector of $\mathbb{F}_2^n$. We define the support of the Walsh spectrum of f as follows:

$$\mathrm{supp}(W_f) = \{w \mid W_f(w) \neq 0,\ w \in \mathbb{F}_2^n\}.$$

The inverse Walsh transform is given by

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{w \in \mathbb{F}_2^n} W_f(w)(-1)^{w \cdot x}.$$

The *Walsh spectrum* of f is the multiset of values $W_f(w)$, where w ranges over $\mathbb{F}_2^n$. The *nonlinearity* of an n-variable Boolean function can be computed by

$$N_f = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |W_f(w)|.$$

From the *Poisson summation formula,* we can derive the Parseval's relation:

$$\sum_{w \in \mathbb{F}_2^n} {W_f}^2(w) = 2^{2n}.$$

By this relation, we have the upper bound of the nonlinearity of a Boolean function $N_f \leq 2^{n-1} - 2^{n/2}$. Bent functions are those Boolean functions with maximal nonlinearity in even numbers of variables. A function $f \in \mathcal{B}_n$ is called a plateaued function if $W_f(\alpha) \in \{0, \pm 2^\lambda\}$ for any $\alpha \in \mathbb{F}_2^n$, where $\lambda \geq n/2$ is a positive integer.

Definition 1 *Let $n = 2m$ be even. A Boolean function $f \in \mathcal{B}_n$ is bent if its Walsh coefficients satisfy*

$$W_f(w) = \pm 2^m, \quad \text{for all } w \in \mathbb{F}_2^n.$$

The dual function of a bent function $f \in \mathcal{B}_n$, denoted by $\tilde{f}$, is the Boolean function of n variables defined by

$$W_f(w) = 2^{n/2}(-1)^{\widetilde{f(w)}}. \tag{2}$$

Let n, k be two positive integers, where $k \leq n$. We call $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^k$,

$$F = \big(f_1, f_2, \ldots, f_k\big),$$

an (n, k) function, where $f_1, f_2, \ldots, f_k \in \mathcal{B}_n$. Suppose $f_1, f_2, \ldots, f_k$ are bent functions. We define the (n, k) function $\widetilde{F}$ as follows:

$$\widetilde{F} = (\widetilde{f_1}, \widetilde{f_2}, \ldots, \widetilde{f_k}).$$

For $v = (v_1, \ldots, v_k) \in \mathbb{F}_2^{k^*}$, let

$$f_v = v \cdot F = v_1 f_1 + \ldots + v_k f_k.$$

If f_v is balanced for any $v \in \mathbb{F}_2^{k^*}$, then we call F a balanced (n, k) function. If f_v is a bent function for any $v \in \mathbb{F}_2^{k^*}$, then we call F an (n, k) bent function.

The composition of a Boolean function $g \in \mathcal{B}_k$ and an (n, k) function F, denoted by $g \circ F$, is an n-variable Boolean function, defined by

$$g \circ F = g\big(F(x)\big) = g\big(f_1(x), f_2(x), \ldots, f_k(x)\big).$$

3 Main construction

In [17], Nyberg considered composite applications for the cryptanalysis of block ciphers and stream ciphers. Gupta and Sarkar [8] generalized Nyberg's work and obtained the Walsh spectrum of the composition of Boolean functions by computing the corresponding inverse Walsh transform.

Lemma 1 *[8] (Composition Theorem): Let $g \in \mathcal{B}_k$ and F be an (n, k) function. Then for any $w \in \mathbb{F}_2^n$,*

$$W_{g \circ F}(w) = \frac{1}{2^k} \sum_{v \in \mathbb{F}_2^k} W_g(v) \cdot W_{v \cdot F}(w). \tag{3}$$

We next introduce a hypothetical property, the "dual isomorphism" of an (n, k) function, which will play an important role in the construction of new bent functions by dint of the composition theorem.

Definition 2 *Let $F = (f_1, f_2, \ldots, f_k)$ be an (n, k) function and the set $S \subseteq F_2^{k^*}$. If there exists an (n, k) function $H = (h_1(x), h_2(x), \ldots, h_k(x))$ such that for any $v \in S$,*

– $v \cdot F$ *is a bent function, and*
– $\widetilde{v \cdot F} = v \cdot H$,

then we call the vectorial functions F *and* H *a pair of dually isomorphic (DI)* (n, k) *bent functions on* S*. Functions* F *and* H *are called DI* (n, k) *bent functions on* S*, respectively.*

Theorem 1 *Let* $g(z) \in \mathcal{B}_k$ *be any balanced Boolean function, and let* F *and* H *be a pair of DI* (n, k) *bent functions on* $\mathrm{supp}(W_g)$*. Then the composition function* $g \circ F$ *is a bent function, and its dual is* $g \circ H$*.*

Proof. Since the Boolean function g is balanced, then $\mathbf{0}_n \notin \mathrm{sup}(W_g)$. For any $w \in \mathbb{F}_2^n$, we have

$$\begin{aligned} W_{g\circ F}(w) &= \frac{1}{2^k} \sum_{v \in \mathbb{F}_2^k} W_{g(z)}(v) \cdot W_{v\cdot F}(w) \\ &= 2^{\frac{n}{2}} \left(\frac{1}{2^k} \sum_{v \in \mathrm{sup}(W_g)} W_{g(z)}(v) (-1)^{\widetilde{v\cdot F}(w)} \right) \\ &= 2^{\frac{n}{2}} \left(\frac{1}{2^k} \sum_{v \in \mathrm{sup}(W_g)} W_{g(z)}(v) (-1)^{v\cdot H(w)} \right) \\ &= 2^{\frac{n}{2}} (-1)^{g\circ H(w)}. \end{aligned}$$

The last equation holds because it can be dealed by the inverse Walsh transform of g at the vector $H(w)$. We conclude that the composition function $g \circ F$ is a bent function with its dual $g \circ H$.

It is worth noting that it is unnecessary for each f_i, $i = 1, 2, \ldots, k$, to be bent in Definition 2. In this study, we mainly explore the particular case where f_i, $i = 1, 2, \ldots, k$, are all bent functions, and $H = \widetilde{F} = (\widetilde{f_1}, \widetilde{f_2}, \ldots, \widetilde{f_k})$.

Example 1. Let $g \in \mathcal{B}_3$ with $g(z_1, z_2, z_3) = z_1 z_2 + z_1 z_3 + z_2 z_3$, where $(z_1, z_2, z_3) \in \mathbb{F}_2^3$. Note that g is balanced, and its Walsh support is $\mathrm{supp}(W_g) = \{(001), (010), (100), (111)\}$. Let $F = (f_1, f_2, f_3)$ be a DI $(n, 3)$ bent function on $\mathrm{supp}(W_g)$. Then $g(f_1, f_2, f_3)$ is an n-variable bent function.

The method to obtain a bent function in Example 1 is in fact a construction in [2], and this method has been generalized in [12, 19, 20].

The result of Theorem 1 can be generalized to construct vectorial bent functions.

Corollary 1 *Let G be a balanced (k,r)-function with $1 \le r \le k$. If F is a DI (n,k) bent function on*

$$\mathrm{supp}(W_{\alpha\cdot G})$$

for any $\alpha \in \mathbb{F}_2^{r*}$, then the composition function $G \circ F$ is an (n,r) bent function.

Proof. Note that G is a balanced (k,r)-function. Then $g_\alpha = \alpha \cdot G$ is balanced for any $\alpha \in \mathbb{F}_2^{r*}$. Since F is a DI (n,k) bent function on $\mathrm{supp}(W_{\alpha\cdot G})$, by Theorem 1, $g_\alpha \circ F$ is a bent function. This implies $G \circ F$ is an (n,r) bent function.

3.1 A class of dually isomorphic (n,k) bent functions

In this subsection, we will show that there is an infinite class of bent functions that satisfy the hypothesis of Definition 2. That is, there exist DI (n,k) bent functions. More precisely, a $\mathcal{PS}$ (n,k) bent function is a kind of DI (n,k) bent function.

Below we describe the construction of $\mathcal{PS}$ bent functions, introduced by Dillon [4], in terms of disjoint linear codes.

Definition 3 *[10] For $1 \le i \le N$, let E_i be a set of $[n,m]$ linear codes. The set $\mathcal{E} = \{E_1, E_2, \ldots, E_N\}$ such that*

$$E_i \cap E_j = \{\mathbf{0}_n\}, \quad 1 \le i < j \le N \tag{4}$$

is called a set of (n,m) disjoint linear codes of cardinality N.

Lemma 2 *Let $f \in \mathcal{B}_n$, where $n = 2m$. Let $\mathcal{E} = \{E_0, E_1, \ldots, E_{2^m}\}$ be a set of (n,m) disjoint linear codes with $\bigcup_{i=0}^{2^m} E_i = \mathbb{F}_2^n$. Then f is a $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) bent function when it satisfies (a) (resp. (b)):*

(a) $\mathrm{supp}(f) = \bigcup_{i=0}^{2^{m-1}-1} {E_i}^*$, *where* $E_i^* = E_i \backslash \{\mathbf{0}_n\}$;
(b) $\mathrm{supp}(f) = \bigcup_{i=0}^{2^{m-1}} E_i$.

Definition 4 *The (n,k) function F is called a $\mathcal{PS}$ (n,k) bent function if for any $v \in \mathbb{F}_2^{k*}$, if $v \cdot F$ is a $\mathcal{PS}$ ($\mathcal{PS}^-$ or $\mathcal{PS}^+$) bent function.*

In the following lemma, we describe a construction method of $\mathcal{PS}$ (n,k) bent functions based on disjoint linear codes.

Lemma 3 *[22] Let n be even, and let $\{E_0, E_1, \cdots, E_{2^{n/2}-1}, E_{2^{n/2}}\}$ be a set of $(n, n/2)$ disjoint linear codes of cardinality $2^{n/2}+1$. Let $H = (h_1, \ldots, h_k)$ be a balanced $(n/2, k)$-function, where $2 \le k \le n/2$, and $h_i \in \mathcal{B}_{n/2}$, $i = 1, \ldots, k$. Define the functions $f_i \in \mathcal{B}_n$ by*

$$\mathrm{supp}(f_i) = \bigcup_{y \in \mathrm{supp}(h_i)} E^*_{[y]}, \tag{5}$$

where $[y]$ denotes the decimal representation of y. Then, $F = (f_1, \ldots, f_k)$ is an (n, k) bent function.

Proof. By Lemma 2, for $i = 1, \ldots, m$, f_i is obviously a $\mathcal{PS}^-$ bent function. Since H is a balanced $(n/2, k)$-function, then $h_v = v_1 h_1 + \cdots + v_k h_k$ is a balanced Boolean function, where $v = (v_1, \ldots, v_k) \in \mathbb{F}_2^{k^*}$. Let $f_v = v_1 f_1 + \cdots + v_k f_k$ be a nonzero linear combination of $f_1, \ldots, f_k$. Notice that

$$\mathrm{supp}(f_v) = \bigcup_{y \in \mathrm{supp}(h_v)} E^*_{[y]}. \tag{6}$$

By Lemma 2, f_v is also a $\mathcal{PS}^-$ bent function, and therefore $F = (f_1, \ldots, f_k)$ is an (n, k) bent function.

Theorem 2 *Let n be even, and $k \le n/2$. A function F constructed as in Lemma 3 is a DI (n, k) bent function on $\mathbb{F}_2^{k^*}$.*

Proof. Let $F = \big(f_1(x), f_2(x), \ldots, f_k(x)\big)$ be an (n, k) bent function as in Lemma 3. For any $v \in \mathbb{F}_2^{k^*}$, $v \cdot F$ is a bent function. Let

$$S_v = \{[y] \mid y \in \mathrm{supp}(h_v)\}.$$

For any $w \in \mathbb{F}_2^n$, we have

$$\begin{aligned} W_{v\cdot F}(w) &= (-1)^0 + \sum_{i=0}^{2^{n/2}} \sum_{x \in E_i^*} (-1)^{v\cdot F(x) + w\cdot x} \\ &= 1 + \sum_{y \notin S_v} \sum_{x \in E_i^*} (-1)^{0 + w\cdot x} + \sum_{y \in S_v} \sum_{x \in E_i^*} (-1)^{1 + w\cdot x} \\ &= \sum_{i \notin S_v} \sum_{x \in E_i} (-1)^{w\cdot x} - \sum_{i \in S_v} \sum_{x \in E_i} (-1)^{w\cdot x}. \end{aligned}$$

The last equation holds in view of the balanced h_v-function. For a fixed j, $0 \leq j \leq 2^{n/2}$, if $\mathbf{0}_n \neq w \in E_j^{\perp}$, then

$$\sum_{x \in E_i} (-1)^{w \cdot x} = \begin{cases} +2^{n/2}, & \text{if } i = j,\ i \notin S_v \\ -2^{n/2}, & \text{if } i = j,\ i \in S_v \\ 0, & \text{if } i \neq j. \end{cases}$$

We have

$$W_{v \cdot F}(w) = \begin{cases} +2^{n/2}, & \text{if } i \notin S_v \\ -2^{n/2}, & \text{if } i \in S_v. \end{cases} \tag{7}$$

Combining (2), (6), and (7), we obtain

$$\operatorname{supp}(\widetilde{v \cdot F}) = \bigcup_{i \in S_v} E_i^{\perp *} \ \Leftrightarrow \ \operatorname{supp}(v \cdot F) = \bigcup_{i \in S_v} E_i^{*} \ \Leftrightarrow \ \operatorname{supp}(v \cdot \widetilde{F}) = \bigcup_{i \in S_v} E_i^{\perp *}. \tag{8}$$

This implies $\widetilde{v \cdot F} = v \cdot \widetilde{F}$. Thus, F is a DI (n, k) bent function on $\mathbb{F}_2^{k*}$.

In Lemma 3, the nonzero linear combinations of F are limited to $\mathcal{PS}^-$ bent functions. In fact, for a $\mathcal{PS}$ (n, k) bent function, the result of Theorem 2 is still correct.

Corollary 2 *Let F be a $\mathcal{PS}$ (n, k) bent function. Then for any balanced Boolean function $g \in \mathcal{B}_k$, the composition function $g \circ F$ is a $\mathcal{PS}$ type bent function and its dual is $g \circ \widetilde{F}$.*

The previously constructed bent functions are bent functions without extension of variables of the ingredient functions. In the remainder of this subsection, we build a framework of the composition construction of bent functions with extension of variables of the ingredient functions.

Theorem 3 *Let k, s be two positive integers. Let $g(z, y) \in \mathcal{B}_{k+s}$, $z \in \mathbb{F}_2^k$, $y \in \mathbb{F}_2^s$ be a balanced Boolean function, and let $F = (f_1(x), f_2(x), \ldots, f_k(x))$ be an (n, k) function satisfying the condition that the component $v \cdot F$ is bent for any $(v, e) \in \operatorname{supp}(W_g) \subseteq \mathbb{F}_2^{k+s*}$, where $v \in \mathbb{F}_2^{k*}$ and $e \in \mathbb{F}_2^s$. Then the composition function $g\big(f_1(x), f_2(x), \ldots, f_k(x), y\big)$ is an $(n + s)$-variable bent function if the following conditions hold:*

- *$g(z, y)$ is plateaued with amplitude $2^{k+\frac{s}{2}}$ (s is even);*
- *For any $(v, e) \in \operatorname{supp}(W_g)$ and $(v', e') \in \operatorname{supp}(W_g)$, where $v, v' \in \mathbb{F}_2^{k*}$ and $e, e' \in \mathbb{F}_2^s$, $v = v'$ if any only if $e = e'$.*

Proof. Since g is balanced, then $\mathbf{0}_{k+s} \notin \mathrm{supp}(W_g)$. If the conditions of Theorem 3 hold, then for any $w \in \mathbb{F}_2^n, e \in \mathbb{F}_2^s$, we have

$$\begin{aligned} W_{g(f_1,f_2,\ldots,f_k,y)}(w,e) &= \frac{1}{2^{k+s}} \sum_{(v,u)\in\mathbb{F}_2^{k+s}} W_{g(z,y)}(v,u) \cdot W_{v\cdot F+u\cdot y}(w,e) \\ &= \frac{1}{2^{k+s}} \left(\sum_{(v,u)\in \mathrm{supp}(W_g)} W_{g(z,y)}(v,u) W_{v\cdot F}(w) W_{u\cdot y}(e) \right) \\ &= \frac{1}{2^{k}} \left(\sum_{(v,e)\in \mathrm{supp}(W_g)} W_{g(z,y)}(v,e) W_{v\cdot F}(w) \right) \\ &= \pm 2^{\frac{n+s}{2}}. \end{aligned} \tag{9}$$

Therefore, $g(f_1(x), f_2(x), \ldots, f_k(x), y)$ is a bent function.

Remark 1. The constructions of bent functions in [18] and [6, Thorem 6,7] are special cases of Theorem 3. We can also compute the dual of the bent function $g(f_1, f_2, \ldots, f_k, y)$ by Lagrange interpolation as in [6], if the signs of the Walsh spectra $W_{g(z,y)}(v,e)$, $(v,e) \in \mathrm{supp}(W_g)$, are known.

3.2 An answer to an open problem bent functions in univariate form

We identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$. For any positive integer k dividing n, we denote the trace function $z + z^{2^k} + \cdots + z^{2^{n-k}}$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ by Tr_k^n. It satisfies the transitivity property $\mathrm{Tr}_1^n = \mathrm{Tr}_1^k \circ \mathrm{Tr}_k^n$.

Every function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ has a unique univariate representation of the form $f(z) = \sum_{i=0}^{2^n-1} u_i z^i$, where $u_i \in \mathbb{F}_{2^n}$. When f is Boolean (i.e., valued in $\mathbb{F}_2$), that is, it satisfies $(f(z))^2 = f(z) \pmod{z^{2^n} + z}$, its univariate representation can be written in the form

$$f(z) = \sum_{j\in\Gamma_n} \mathrm{Tr}_1^{o(j)}(a_j z^j) + a_{2^n-1} z^{2^n-1},, \tag{10}$$

called its trace representation, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$, $o(j)$ is the size of the corresponding cyclotomic coset containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$, and $a_{2^n-1} \in \mathbb{F}_2$. The algebraic degree of f (i.e., the degree of its ANF when its input vector is decomposed over some basis) equals $\max\{w_2(j) \mid a_j \neq 0\}$, where the 2-weight

$w_2(j)$ of j is the Hamming weight of its binary expansion [3]. Taking the inner product $u \cdot z = \mathrm{Tr}_1^n(uz)$, the Walsh transform of f is defined as

$$W_f(u) = \sum_{z \in \mathbb{F}_{2^n}} (-1)^{f(z)+\mathrm{Tr}_1^n(uz)}, \quad u \in \mathbb{F}_{2^n}.$$

For any Boolean function $f(x)$ over $\mathbb{F}_{2^n}$, choosing a normal basis $(\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}})$ of $\mathbb{F}_{2^n}$ and decomposing x over this basis gives a Boolean function f over $\mathbb{F}_2^n$.

Mesnager proposed two open problems about the secondary construction of some class of bent functions [12]. The first problem was solved in [19], and we present the second problem as follows.

Problem 1. Let n be an even positive integer and r be a positive integer with $r \leq n/2$. Let F be a bent vectorial map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$. For $b \in \mathbb{F}_{2^r}$, denote by f_b a component of F and by f_b its dual. Find (a_1, a_2, a_3) a 3-tuple of pairwise distinct elements of $\mathbb{F}_{2^r}^*$ with $a_3 \neq a_1 + a_2$ such that $\widetilde{f_{a_1+a_2+a_3}} = \widetilde{f_{a_3}} + \widetilde{f_{a_1}} + \widetilde{f_{a_2}}$.

The existence of such a vectorial bent function will lead to the construction of a bent function as $g(x) = f_{a_1} f_{a_2} + f_{a_2} f_{a_3} + f_{a_1} f_{a_3}$. By identifying the finite fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^r}$ with the vectorial spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^r$, we will give a positive answer to this problem.

Proof. Let vectors $a_1, a_2, a_3 \in \mathbb{F}_2^{r*}$ with $a_3 \neq a_1 + a_2$, and let F be an (n, r)-function constructed by Lemma 3. According to Theorem 2, the function F is a DI (n, r) bent function on $\mathbb{F}_2^{r*}$. Then

$$\begin{aligned}
\widetilde{f_{a_1+a_2+a_3}} &= \widetilde{(a_1 + a_2 + a_3) \cdot F} \\
&= (a_1 + a_2 + a_3) \cdot \widetilde{F} \\
&= a_1 \cdot \widetilde{F} + a_2 \cdot \widetilde{F} + a_3 \cdot \widetilde{F} \\
&= \widetilde{a_1 \cdot F} + \widetilde{a_2 \cdot F} + \widetilde{a_3 \cdot F} \\
&= \widetilde{f_{a_1}} + \widetilde{f_{a_2}} + \widetilde{f_{a_3}}.
\end{aligned}$$

This implies that the open problem is solved.

4 Construction of self-dual bent functions

Let $n = 2m = 4t$ for a positive integer t. Mesnager [12] showed that the monomial function $f(x) = \mathrm{Tr}_1^n(\lambda x^{2^t+1})$ is self-dual bent for any fixed $\lambda \notin \{x^{1+2^t}, x \in \mathbb{F}_{2^n}\}$

with $\lambda + \lambda^{2^{3t}} = 1$. The latter equation is equivalent to $\lambda + \lambda^{2^t} = 1$. This implies that $\lambda \in \mathbb{F}_{2^{2t}}$. That is, $f(x)$ is a self-dual bent function if $\lambda \in \mathbb{F}_{2^{2t}}$ and $\mathrm{Tr}_t^{2t}(\lambda) = 1$.

Let k be a positive integer, where $k \leq 2^t - 1$. Let $\lambda_1, \lambda_2, ..., \lambda_k$ be k elements in $\mathbb{F}_{2^{2t}}$ such that $\mathrm{Tr}_1^n(\lambda_i x^{2^t+1})$ is a self-dual bent function for $1 \leq i \leq k$. Define an (n, k) function

$$F(x) = \big(\mathrm{Tr}_1^n(\lambda_1 x^{2^t+1}), \mathrm{Tr}_1^n(\lambda_2 x^{2^t+1}), ..., \mathrm{Tr}_1^n(\lambda_k x^{2^t+1})\big). \tag{11}$$

For any $\mathbf{0}_k \neq v \in \mathbb{F}_2^k$, the component function $v \cdot F(x)$ is a self-dual bent function if the Hamming weight of v is odd. By following these results, we can construct an infinite class of self-dual bent functions.

Theorem 4 *Assume that the vectorial function $F(x)$ is defined as in (11). Let $g(z) \in \mathcal{B}_k$ be a balanced Boolean function whose Walsh support is a set of vectors with odd Hamming weight. Then the compostion function $g \circ F$ is a self-dual bent function.*

The balanced Boolean function $g(x)$ in Theorem 4 can be easily constructed by the so-called *partially bent function* [**?**]. The characterization of the partially bent functions can be described with the following lemma.

Lemma 4 *Let $g \in \mathcal{B}_n$ and let k be an even positive integer. Then g is a partially bent function if and only if there exists a subspace V of dimension k and a vector t of $\mathbb{F}_2^n$ such that*

$$W_g^2(w + t) = \begin{cases} 2^{2n-k}, & w \in V; \\ 0, & \text{otherwise.} \end{cases}$$

Choose k linearly independent vectors of $\mathbb{F}_2^n$ with even Hamming weight and then span the subspace V. For any vector $t \in \mathbb{F}_2^n$ with odd Hamming weight, we construct the partially bent function $g(x)$ as in Lemma 4. Then g is a balanced Boolean function whose Walsh support is a set of vectors with odd Hamming weight.

Example 2. Let

$$V = \begin{bmatrix} 1\,1\,0\,0\,0\,0\,0 \\ 1\,0\,1\,0\,0\,0\,0 \\ 1\,0\,0\,1\,0\,0\,0 \\ 1\,0\,0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,0\,0\,1 \end{bmatrix}.$$

It is easy to check that $\mathrm{rank}(V) = 6$. Choosing any vector t in $\mathbb{F}_2^7$ with odd Hamming weight, we construct $E = \{t + uV, u \in \mathbb{F}_2^6\}$. Then E is a flat of $\mathbb{F}_2^7$, and the Hamming weight of each vector of E is odd. By following the method in [6, Theorem 6], we obtain a partially bent function

$$\begin{aligned} g(z_0, z_1, z_2, z_3, z_4, z_5) = {} & z_0z_2z_3 + z_0z_1z_4 + z_1z_3z_4 + z_1z_2z_5 + z_0z_3z_5 + z_2z_4z_5 + z_0z_1z_6 \\ & + z_0z_2z_6 + z_1z_2z_6 + z_1z_3z_6 + z_2z_3z_6 + z_0z_4z_6 + z_2z_4z_6 + z_3z_4z_6 \\ & + z_0z_5z_6 + z_1z_5z_6 + z_3z_5z_6 + z_4z_5z_6 + z_0z_1 + z_1z_2 + z_0z_3 + z_2z_3 \\ & + z_1z_4 + z_3z_4 + z_0z_5 + z_2z_5 + z_4z_5 + z_0 + z_1 + z_2 + z_5 + 1. \end{aligned}$$

The Walsh support of g is E.

5 Conclusion

In this study, we developed a general theory of secondary constructions of bent functions under the framework of composition of Boolean functions. First, we established the relationships between the secondary constructions of bent functions and the composition of Boolean functions in terms of the dually isomorphic bent functions. Next, we proposed various constructions of bent functions, including the self-dual case, according to this framework, and we also derived the dual functions of these bent functions. Subsequently, we demonstrated how the open problem proposed by Mesnager can be solved by the existence of a dually isomorphic bent function. Finding more classes of dually isomorphic bent functions is an interesting direction of this research field to generate more bent functions.

References

1. A. Bernasconi, "Mathematical techniques for the analysis of Boolean functions", Ph. D. dissertation TD-2/98, Universit di Pis-Udine, 1998. 1
2. C. Carlet, "On bent and highly nonlinear balanced/resilient functions and their algebraic immunities", in Proc. AAECC, Berlin, Germany: Springer, vol. 3857, pp. 1-28, 2006. 2, 6
3. C. Carlet, "Boolean Functions for Cryptography and Coding Theory", Cambridge University Press, Cambridge, 2020. 11
4. J. Dillon, "Elementary Hadamard Difference Sets", PhD dissertation, Universtiy of Maryland, 1974. 2, 7
5. C. Ding, G. Xiao, and W. Shan, "The Stability Theory of Stream Ciphers", *LNCS* 561. Berlin, Germany: Springer-Verlag, 1991. 1

6. G. Gao, D. Lin, W. Liu, Y. Wang. "Composition of Boolean functions: An application to the secondary constructions of bent functions". *Discrete Mathematics*, 2020, 343(3):111711. 2, 10, 13
7. G. Gao, X. Zhang, W. Liu, C. Carlet, "Constructions of quadratic and cubic rotation symmetric bent functions", *IEEE Transactions on Information Theory,* 58(7), pp. 4908–4913, 2012. 2
8. K. Gupta, P. Sarkar, "Toward a general correlation theorem", *IEEE Transactions on Information Theory*, 51(9), pp. 3297–3302, 2005. 2, 5
9. Hodžić, Samir, Enes Pasalic and Yongzhuang Wei. "A general framework for secondary constructions of bent and plateaued functions." Designs, Codes and Cryptography, pp.1-29, 2020. 2
10. T. Johansson, E. Pasalic, "A construction of resilient functions with high nonlinearity", *IEEE Transactions on Information Theory*, 49(2), pp. 494–501, 2003. 7
11. M. Matsui, "Linear cryptanalysis method for DES cipher", in Advances in Cryptology—EUROCRYPT'93, (Lecture Notes in Computer Science), vol. 765. Berlin, Germany: Springer-Verlag, 1994, pp. 386-397. 1
12. S. Mesnager, "Several new infinite families of bent functions and their duals" , *IEEE Transactions on Information Theory*, 60(7), pp. 4397–4407, 2014. 2, 6, 11
13. S. Mesnager, "Bent Functions: Fundamentals and Results", Springer-Verlag, 2016. 2
14. S. Mesnager, F. Zhang, "On constructions of bent, semi-bent and five valued spectrum functions from old bent functions", *Advances in Mathematics of Communications*, 11(2), pp. 339–345, 2017. 2
15. S. Mesnager, F. Zhang, Y. Zhou, "On construction of bent functions involving symmetric functions and their duals", *Advances in Mathematics of Communications*, 11(2), pp. 347–352, 2017. 2
16. R. L. McFarland, "A family of noncyclic difference sets", *Journal of Comb. Theory, Series A*, 15, pp. 1–10, 1973. 2
17. K. Nyberg, "Correlation theorems in cryptanalysis", *Discrete Applied Mathematics*, 111, pp. 177–188, 2001. 1, 5
18. O. S. Rothaus, "On bent functions", *Journal of Comb. Theory, Series A*, 20, pp. 300–305, 1976. 2, 10
19. C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth, "Generic Construction of Bent Functions and bent idempotents With Any Possible Algebraic Degrees," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6149-6157, 2017. 6, 11
20. G. Xu, X. Cao, and S. Xu, "Several new classes of Boolean functions with few Walsh transform values", *Appl. Algebra Eng. Commun. Comput.*, vol. 28, no. 2, pp. 155-176, 2017.2 6
21. F. Zhang, C. Carlet, Y. Hu, W. Zhang, "New secondary constructions of bent functions", *Appl. Algebra Eng. Commun. Comput.*, 27, pp. 413–434, 2016. 2
22. W.-G. Zhang, E. Pasalic, "Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes", *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1638-1651, 2014. 8
23. F. Zhang, E. Pasalic, Y. Wei, N. Cepak, "Constructing bent functions outside the Maiorana-McFarland class using a general form of Rothaus", *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5336–5349, 2017. 2