Bent and semi-bent functions via linear translators

Neşe Koçak[1,2], Sihem Mesnager[3,4,5], Ferruh Özbudak[2,6]

[1] ASELSAN Inc. Ankara, Turkey
[2] Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
[3] Department of Mathematics, University of Paris VIII, France
[4] University of Paris XIII, LAGA, UMR 7539, CNRS, France
[5] Telecom ParisTech, France
[6] Department of Mathematics, Middle East Technical University, Ankara, Turkey

Abstract. The paper is dealing with two important subclasses of plateaued functions: bent and semi-bent functions. In the first part of the paper, we construct mainly bent and semi-bent functions in the Maiorana-McFarland class using Boolean functions having linear structures (linear translators) systematically. Although most of these results are rather direct applications of some recent results, using linear structures (linear translators) allows us to have certain flexibilities to control extra properties of these plateaued functions. In the second part of the paper, using the results of the first part and exploiting these flexibilities, we modify many secondary constructions. Therefore, we obtain new secondary constructions of bent and semi-bent functions not belonging to the Maiorana-McFarland class. Instead of using bent (semi-bent) functions as ingredients, our secondary constructions use only Boolean (vectorial Boolean) functions with linear structures (linear translators) which are very easy to choose. Moreover, all of them are very explicit and we also determine the duals of the bent functions in our constructions. We show how these linear structures should be chosen in order to satisfy the corresponding conditions coming from using derivatives and quadratic/cubic functions in our secondary constructions.

Keywords: Boolean functions, Bent functions, Semi-bent functions, Walsh-Hadamard transform, Linear structures, Linear translators and Derivatives.

1 Introduction

The classes of bent and semi-bent functions are special subclasses of the so-called plateaued functions [**?**]. They are studied in cryptography because, besides having low Walsh-Hadamard transform magnitude which provides protection against fast correlation attacks and linear cryptanalysis, they can also possess other desirable properties. For their relations to coding theory and applications in cryptography bent and semi-bent functions have attracted a lot of research.

Bent functions are nice combinatorial objects. They are maximally nonlinear Boolean functions with an even number of variables. They were defined by Rothaus [**?**] in 1976 but already studied by Dillon [**?**] since 1974. A book devoted especially to binary bent functions and containing a complete survey on bent functions is [**?**]. Open problems on binary bent functions can be found in [**?**]. The term semi-bent function was introduced by Chee, Lee and Kim at Asiacrypt' 94 [**?**]. These functions had been previously investigated under the name of 3-valued almost optimal Boolean functions. A survey containing open problems on semi-bent functions can be found in [**?**]. Despite the amount of research in the theory of bent and semi-bent functions, the classification of those functions is

still elusive, therefore, not only their characterization, but also their construction are challenging problems. Several constructions of explicit bent and semi-bent functions have been proposed in the literature but investigation of such kind of functions is still needed.

The concept of a linear translator exists of p-ary function (see for instance [**?**]) but it was introduced in cryptography, mainly for Boolean functions (see for instance [**?**]). Functions with linear structures are considered as weak for some cryptographic applications. For instance, a recent attack on hash functions proposed in [**?**] exploits a similar weakness of the involved mappings. All Boolean functions using a linear translator have been characterized by Lai [**?**]. Further, Charpin and Kyureghyan have done the characterization for the functions in univariate variables from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of the form $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(F(x))$, where $F(x)$ is a function over $\mathbb{F}_{p^n}$ and $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}$ denotes the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The result of Lai in [**?**] has been formulated recently by Charpin and Sarkar [**?**].

For a Boolean map, linear structures or linear translators are not desirable and are generally considered as a defect. In this paper, we show that one can recycle such Boolean functions to get Boolean functions with optimal or very high nonlinearity. More precisely, we show that one can obtain primary constructions of bent and semi-bent functions from Boolean maps having linear structures or linear translator in Sections **??**, **??** and **??**. All the primary constructions proposed in the paper belong to the well-known class of Maiorana-McFarland. However, an important feature of the bent functions presented in this paper is that their dual functions can be explicitly computed. Next, we focus on secondary constructions presented in [**?**,**?**,**?**] and show how to obtain new secondary constructions by reusing bent functions presented in the paper. Our new secondary constructions are very explicit and they use Boolean functions (vectorial Boolean functions) with certain linear structures (linear translators) as ingredients instead of bent or semi-bent functions. The conditions on such linear structures (linear translators) in our secondary constructions are easily satisfied. Finally, we show that one can construct bent functions from bent functions of Sections **??** and **??** by adding a quadratic or cubic function appropriately chosen.

This paper is organized as follows: We provide a short background in Section **??**. We present explicit constructions of bent and semi-bent functions in Maiorana-McFarland type in Sections **??**, **??** and **??**. We give various secondary constructions in Sections **??**, **??** and **??**.

2 Notation and Preliminaries

For any set E, $E^\star = E \setminus \{0\}$ and $\#E$ will denote the cardinality of E. A Boolean function on the finite field $\mathbb{F}_{2^n}$ of order 2^n is a mapping from $\mathbb{F}_{2^n}$ to the prime field $\mathbb{F}_2$. Recall that for any positive integers k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined for every $x \in \mathbb{F}_{2^k}$ as $Tr_r^k(x) := x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}$. For a Boolean function f on $\mathbb{F}_{2^n}$, the Walsh-Hadamard transform of f is the discrete Fourier transform of the sign function $\chi_f := (-1)^f$ of f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as $\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}$.

Definition 1. *Let n be an even integer. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be bent if its Walsh transform satisfies $\widehat{\chi_f}(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$.*

Bent functions come in pairs. For a bent function f on $\mathbb{F}_{2^n}$, we define its *dual function* $\widetilde{f}$ as a Boolean function on $\mathbb{F}_{2^n}$ satisfying the equation : $(-1)^{\widetilde{f}(x)} 2^{\frac{n}{2}} = \widehat{\chi_f}(x)$ for all $x \in \mathbb{F}_{2^n}$.

The dual $\widetilde{f}$ of a bent function is also bent.

Definition 2. *Let n be an even integer. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be semi-bent if its Walsh transform satisfies $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$.*

Definition 3. *[?] A Boolean function f on $\mathbb{F}_{2^n}$ is said to be k-plateaued if its Walsh transform satisfies $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+k}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$ and for some fixed k, $0 \leq k \leq n$.*

When n is even, bent functions correspond to 0-*plateaued* functions and semi-bent functions correspond to 2-*plateaued* functions.

We refer to [**?**] for further background and important notions like algebraic representation, trace representation and bivariate representation of Boolean functions. We will mainly use bivariate representation of bent and semi-bent functions in this paper.

Next we recall definitions of linear translator and linear structure.

Definition 4. *Let $n = rk$, $1 \leq k \leq n$. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, $\gamma \in \mathbb{F}_{2^n}^*$ and b be a constant of $\mathbb{F}_{2^k}$. Then γ is a b-linear translator of f if $f(x) + f(x + u\gamma) = ub$ for all $x \in \mathbb{F}_{2^n}$ and $u \in \mathbb{F}_{2^k}$. If $f(x) + f(x + \gamma) = b$ for all $x \in \mathbb{F}_{2^n}$, then γ is called a b-linear structure of f.*

The notion of *b-linear translator* is well known in the literature (see for example [**?**]). The notion of *b-linear structure is usually given for functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, that is $k = 1$ (see for example [?]).*

Remark 1. Note that being b-linear translator is stronger than being b-linear structure if $k > 1$ and they are the same if $k = 1$. For example, let $f : \mathbb{F}_{2^4} \to \mathbb{F}_{2^2}$ be a function defined as $f(x) = Tr_2^4(x^2 + \gamma x)$ where $\gamma \in \mathbb{F}_{2^4} \backslash \mathbb{F}_{2^2}$. Then, γ is a 0-linear structure of f but it is not a 0-linear translator of f as $f(x + u\gamma) \neq f(x)$ for $u \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$.

The notions of linear structures, linear translators and derivatives are related.

Definition 5. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. For $a \in \mathbb{F}_{2^n}$, the function D_aF given by $D_aF(x) = F(x) + F(x + a), \forall x \in \mathbb{F}_{2^n}$ is called the derivative of F in the direction of a.*

Note that $D_\gamma f(x) = b$ for each $x \in \mathbb{F}_{2^n}$ if and only if γ is a b-linear structure of f. Similarly, $D_{u\gamma} f(x) = ub$ for each $x \in \mathbb{F}_{2^n}$ and each $u \in \mathbb{F}_{2^k}$ if and only if γ is a b-linear translator of f.

3 Constructions of bent and semi-bent Boolean functions from the class of Maiorana-McFarland using one linear structure

A function $H : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ is said to be in the class of Maiorana-McFarland if it can be written in bivariate form as

$$H(x, y) = Tr_1^m (x\phi(y)) + h(y) \tag{3.1}$$

where ϕ is a map from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ and h is a Boolean function on $\mathbb{F}_{2^m}$. It is well-known that we can choose ϕ so that H is bent or H is semi-bent. Indeed, it is well-known that bent functions of the form (**??**) comes from one-to-one maps while 2-to-1 maps leads to semi-bent functions.

Proposition 1. *([?,?,?]) Let H be defined by (??). Then,*

1. *H is bent if and only if ϕ is a permutation and its dual function is $\tilde{H}(x, y) = Tr_1^m \left(y\phi^{-1}(x)\right) + h(\phi^{-1}(x))$.*
2. *H is semi-bent if ϕ is 2-to-1.*

As a first illustration of Proposition **??**, let us consider a first class of maps from $\mathbb{F}_{2^m}$ to itself: $\phi : y \mapsto y+\gamma f(y)$ where γ is a linear structure of f. This class has the property that it only contains one-to-one maps or 2-to-1 maps. Therefore, by Proposition **??**, one can obtain the following infinite families of bent and semi-bent functions.

Proposition 2. *Let f and h be two Boolean functions over $\mathbb{F}_{2^m}$.*
Let H be the Boolean function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$H(x,y) = Tr_1^m(xy + \gamma x f(y)) + h(y),\ \gamma \in \mathbb{F}_{2^m}.$$

H is bent (resp. semi-bent) if and only if γ is a 0-linear (resp. 1-linear) structure of f. Furthermore, if H is bent, then its dual is

$$\tilde{H}(x,y) = Tr_1^m\big(yx + \gamma y f(x))\big) + h(x + \gamma f(x)).$$

Proof. Properties of $\phi : y \mapsto y+\gamma f(y)$ are well-known and firstly developed in [**?**,**?**] (see also [**?**,**?**]). Bijectivity is given by Theorem 2 of [**?**]. For the 2-to-1 property, see Theorems 3,6 in [**?**]. The proof is then immediately obtained. Also, note that since ϕ is an involution (see also [**?**,**?**,**?**]), we have $\tilde{H}(x,y) = Tr_1^m\big(y\phi(x))\big) + h(\phi(x))$.

In order to show that the hypotheses of Proposition **??** hold in certain cases, we give the following examples which are direct applications of Theorems 3, 4 in [**?**].

Example 1. Let $\gamma \in \mathbb{F}_{2^m}^\star$ and $\beta \in \mathbb{F}_{2^m}$ such that $Tr_1^m(\beta\gamma) = 0$ (resp. $Tr_1^m(\beta\gamma) = 1$). Let $H : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be an arbitrary mapping and h be any Boolean function on $\mathbb{F}_{2^m}$. Then the function g defined over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$g(x,y) = Tr_1^m(xy + \gamma x Tr_1^m(H(y^2 + \gamma y) + \beta y)) + h(y)$$

is bent (resp. semi-bent).

Example 2. Let $0 \le i \le m-1$, $i \notin \{0, \frac{m}{2}\}$ and δ, $\gamma \in \mathbb{F}_{2^m}$ such that $\delta^{2^i-1} = \gamma^{1-2^{2i}}$. Let h be any Boolean function on $\mathbb{F}_{2^m}$ and g be the Boolean function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$g(x,y) = Tr_1^m(xy + \gamma x Tr_1^m(\delta y^{2^i+1})) + h(y).$$

If $Tr_1^m(\delta\gamma^{2^i+1}) = 0$ (resp. $Tr_1^m(\delta\gamma^{2^i+1}) = 1$) then g is bent (resp. semi-bent).

Observe that if we compose ϕ at left by a linearized permutation polynomial L, any output have the same number of preimages under ϕ than under $L \circ \phi$. Hence, one can slightly generalizes Proposition **??** as follows.

Proposition 3. *Let f and h be two Boolean functions over $\mathbb{F}_{2^m}$ and $\gamma \in \mathbb{F}_{2^m}$. Let L be a linearized permutation polynomial of $\mathbb{F}_{2^m}$. The Boolean function H defined by*

$$H(x,y) = Tr_1^m\left(xL(y) + L(\gamma)xf(y)\right) + h(y)$$

is bent (resp. semi-bent) if and only if γ is a 0-linear (resp. 1-linear) structure of f. Moreover, if H is bent then its dual function $\tilde{H}$ is given by

$$\tilde{H}(x,y) = Tr_1^m(yL^{-1}(x) + \gamma y f(L^{-1}(x)) + h(L^{-1}(x) + \gamma f(L^{-1}(x))).$$

4 Constructions of bent and semi-bent Boolean functions from the class of Maiorana-McFarland using two linear structures

In this section we consider the functions H of the form (**??**) :

$$H(x,y) = Tr_1^m\left(x\phi(y)\right) + h(y) \text{ with } \phi(y) = \pi_1\left(\pi_2(y) + \gamma f(\pi_2(y)) + \delta g(\pi_2(y))\right) \tag{4.1}$$

where f, g and h be Boolean functions over $\mathbb{F}_{2^m}$, $\gamma, \delta \in \mathbb{F}_{2^m}^{\star}$, $\gamma \neq \delta$ and π_1, π_2 are permutations of $\mathbb{F}_{2^m}$ (not necessarily linear). The class (**??**) contains the functions involved in Proposition **??** and in Proposition **??** (which correspond to the case where $f = g$). In the line of Section **??**, we study the cases where γ and δ are linear structures of the Boolean functions involved in ϕ. Then one can exhibit conditions of bentness or semi-bentness as those of Propositions **??** and **??** that we present in the following two propositions. We indicate that, despite their similarities with Proposition **??** and **??**, we obtain bent functions that do not fall in the scope of Proposition **??** and **??**.

Proposition 4. *Let H be defined by equation (**??**). Then H is bent if one of the following conditions holds:*

(i) γ is a 0-linear structure of f, δ is a 0-linear structure of f and g,
(ii) γ is a 0-linear structure of f, δ is a 1-linear structure of f and $\delta + \gamma$ is a 0-linear structure of g,
(iii) δ is a 0-linear structure of g, γ is a 0-linear structure of f and g,
(iv) δ is a 0-linear structure of g, γ is a 1-linear structure of g and $\delta + \gamma$ is a 0-linear structure of f,
(v) δ is a 1-linear structure of f, γ is a 1-linear structure of f and g,
(vi) γ is a 1-linear structure of g, δ is a 1-linear structure of f and g.

*Moreover, if H is bent then its dual is $\tilde{H}(x,y) = Tr_1^m\left(y\phi^{-1}(x)\right) + h(\phi^{-1}(x))$ where $\phi^{-1} = {\pi_2}^{-1} \circ \rho^{-1} \circ {\pi_1}^{-1}$ and ρ^{-1} is given explicitly in the Appendix as Proposition **??**. In particular, choosing $\pi_1(x) = L(x)$ is a linearized permutation polynomial and π_2 is the identity, we get that*

$$H(x,y) = Tr_1^m\left(xL(y) + L(\gamma)xf(y) + L(\delta)xg(y)\right) + h(y) \tag{4.2}$$

is bent in the conditions above and $\tilde{H}(x,y) = Tr_1^m\big(y\rho^{-1}(L^{-1}(x))\big) + h(\rho^{-1}(L^{-1}(x))$.

Proof. We give the proof for only case (i) since the proofs for the other cases are very similar. It suffices to show that $\rho : y \mapsto y + \gamma f(y) + \delta g(y)$ is a permutation. Suppose that $\rho(y) = \rho(z)$, i.e.,

$$y + \gamma f(y) + \delta g(y) = z + \gamma f(z) + \delta g(z). \tag{4.3}$$

Taking f of both sides we obtain $f\big(y + \gamma f(y) + \delta g(y)\big) = f\big(z + \gamma f(z) + \delta g(z)\big)$. Since γ and δ are 0-linear structures of f, we have

$$f(y) = f(z). \tag{4.4}$$

Combining equations (**??**) and (**??**), we get $y + \delta g(y) = z + \delta g(z)$. Taking g of both sides we obtain $g(y + \delta g(y)) = g(z + \delta g(z))$. Since δ is a 0-linear structure of g, we conclude

$$g(y) = g(z). \tag{4.5}$$

Combining equations (**??**), (**??**) and (**??**), we reach that $y = z$. For the dual function, ρ^{-1} is written explicitly in the Appendix as Proposition **??** and the proof for ρ^{-1} for case (i) is given.

Remark 2. The converse of Proposition **??** is not always true. For example, for $f(x) = Tr_1^3(x^3 + \alpha^5 x)$, $g(x) = Tr_1^3(\alpha x^3 + \alpha^5 x)$, $\gamma = \alpha$ and $\delta = \alpha^3$ where α is a primitive element of $\mathbb{F}_{2^3}$, ϕ is a permutation but none of the conditions given in Proposition **??** is satisfied.

The following result shows in which cases ϕ is 2-to-1 and hence H is semi-bent. Also, it can be considered as a generalization of Proposition **??**.

Proposition 5. *Let H be defined by (**??**). Then H is semi-bent if one of the following conditions holds:*

(i) γ, δ are 1-linear structures of f and γ is a 0-linear structure of g,
(ii) δ is a 1-linear structure of f and γ, δ are 0-linear structures of g,
(iii) γ, δ are 0-linear structures of f and δ is a 1-linear structure of g,
(iv) δ is a 0-linear structure of f and γ, δ are 1-linear structures of g,
(v) γ is a 0-linear structure of f, δ is a 1-linear structure of f and $\gamma + \delta$ is a 1-linear structure of g,
(vi) γ is a 1-linear structure of g, δ is a 0-linear structure of g and $\gamma + \delta$ is a 1-linear structure of f.

In particular, choosing $\pi_1(x) = L(x)$ is a linearized permutation polynomial and π_2 is the identity, we get that

$$H(x, y) = Tr_1^m\left(xL(y) + L(\gamma)xf(y) + L(\delta)xg(y)\right) + h(y)$$

is semi-bent in the conditions above.

Proof. We give the proof for case (i) only since the proofs for other cases are similar. Now, we need to show that $\rho(y) : y \mapsto y + \gamma f(y) + \delta g(y)$ is 2-to-1. Let $\rho(y) = a$ for some $a \in \mathbb{F}_{2^m}$. Then, $y \in \{a, a+\gamma, a+\delta, a+\gamma+\delta\}$. As γ is a 1-linear structure of f and 0-linear structure of g, we have $\rho(a) = \rho(a+\gamma)$ and $\rho(a+\delta) = \rho(a+\gamma+\delta)$. Moreover, $\rho(a+\delta) = a + \delta + \gamma f(a+\delta) + \delta g(a+\delta) = a + \delta + \gamma + \gamma f(a) + \delta g(a+\delta)$ where we use that δ is a 1-linear structure of f. We observe that $\rho(a) = a + \gamma f(a) + \delta g(a) \neq \rho(a+\delta)$. Indeed, otherwise if the equality holds, then $\gamma + \delta + \delta\big(g(a) + g(a+\delta)\big) = 0$. This is a contradiction as $\gamma \neq \delta$ and $\gamma \neq 0$. This implies that $\rho^{-1}(a) = \{a, a+\gamma\}$ or $\rho^{-1}(a) = \{a+\delta, a+\gamma+\delta\}$ which shows that ρ is 2-to-1.

Remark 3. The converse of Proposition **??** is not always true. For example, for $f(x) = Tr_1^3(\alpha^4 x^3 + \alpha^4 x)$, $g(x) = Tr_1^3(\alpha x^3 + \alpha^2 x)$, $\gamma = \alpha$ and $\delta = \alpha^3$ where α is a primitive element of $\mathbb{F}_{2^3}$, ϕ is 2-to-1 but none of the conditions given in Proposition **??** is satisfied.

5 Constructions of bent and k-plateaued functions using linear translators

In the preceding sections, we have shown that one can construct bent and semi-bent functions from Boolean functions having linear structures, that is, having constant derivatives. An extension of these constructions is to consider Boolean maps taking its values in a subfield of the ambient field instead of Boolean functions in (**??**). In that case, the natural notion replacing linear structures is the notion of linear translators. We still adopt the approach of the preceding sections and aim to construct bent functions in the class of Maiorana-McFarland. To this end, one can apply results on permutations constructed from Boolean maps having linear translators presented in [**?**] and obtain the following infinite families of bent and plateaued functions.

Proposition 6. *Let m be a positive integer and k be a divisor of m. Let f be a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$ and h be a Boolean function on $\mathbb{F}_{2^m}$. Let H be the function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$H(x,y) = Tr_1^m(xy + \gamma x f(y)) + h(y), \quad \gamma \in \mathbb{F}_{2^m}^\star.$$

(i) If γ is a c-linear translator of f where $c \in \mathbb{F}_{2^m}$ and $c \neq 1$, then H is bent and its dual function is given as

$$\tilde{H}(x,y) = Tr_1^m\left(y\left(x + \gamma\frac{f(x)}{1+c}\right)\right) + h\left(x + \gamma\frac{f(x)}{1+c}\right).$$

Moreover, $H(x,y) = Tr_1^m(xL(y)+L(\gamma)xf(y))+h(y)$ where L is an $\mathbb{F}_{2^k}$-linearized permutation polynomial, is also bent under these conditions and its dual is

$$\tilde{H}(x,y) = Tr_1^m\left(y\left(L^{-1}(x) + \gamma\frac{f(L^{-1}(x))}{1+c}\right)\right) + h\left(L^{-1}(x) + \gamma\frac{f(L^{-1}(x))}{1+c}\right).$$

(ii) If γ is a 1-linear translator of f and $h = 0$ then H is k-plateaued with Walsh transform values

$$\widehat{\chi_H}(a,b) = \begin{cases} \pm 2^{m+k} & \text{if } Tr_k^m(b\gamma) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Note that Proposition **??** generalizes partially Proposition **??** (extending the condition 0-linear structure to c-linear translator with $c \neq 1$). Furthermore, one can derive from Proposition **??** and Proposition **??** similar statements if $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^k}$ instead of being a Boolean function. Indeed, it suffices to change the 0-linear structures (resp. 1-linear structures) with 0-linear translators. (resp. 1-linear translators).

6 Bent functions not belonging to the class of Maiorana-McFarland using linear translators

In the following we are now interested in investigating constructions of bent functions that do not belong to the class of Maiorana- McFarland contrary to the preceding sections. To this end, we are particularly interested in the secondary constructions presented in [**?**,**?**]. In those papers, several secondary constructions of bent functions of the form $f(x) = \phi_1(x)\phi_2(x)+\phi_1(x)\phi_3(x)+\phi_2(x)\phi_3(x)$ are presented. More precisely, it is shown that f is bent provided that it holds $\tilde{\psi}+\tilde{\phi_1}+\tilde{\phi_2}+\tilde{\phi_3} = 0$ where $\psi := \phi_1+\phi_2+\phi_3$. In this section, we show that one can reuse Boolean functions of the shape presented in the preceding sections in the construction of [**?**,**?**].

Firstly, one can derive easily bent functions f, whose dual functions are very simple, by choosing functions H_i in the class of Maiorana-McFarland such that the permutation involving in each H_i is built in terms of an involution and a linear translator. More explicitly, each H_i is a Boolean function over $\mathbb{F}_{2^m}$ defined by $H_i(y) = Tr_1^m\Big(L(y)+L(\gamma_i)h(g(y))\Big)$ where L is a $\mathbb{F}_{2^k}$-linear involution on $\mathbb{F}_{2^m}$ (k being a divisor of m); carefully chosen according to the hypothesis of [**?**, Corollary 2], g is a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$, h is a mapping from $\mathbb{F}_{2^k}$ to itself, and γ_1, γ_2 and γ_3 are three pairwise distinct elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear translators of g such that $\gamma_1+\gamma_2+\gamma_3 \neq 0$. Bent functions f are therefore obtained from a direct application of [**?**, Theorem 4] and [**?**, Corollary 2].

Secondly, we extend a result from [**?**] by considering two linear structures instead of one. This result uses linear structures as in the first case of Proposition **??**. Similarly, for the other five cases we can construct bent functions and their duals. Due to space limitations these results are presented in the Appendix as Propositions **??**, **??**, **??**, **??**, **??**.

Proposition 7. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y+\gamma_i f(y)+\delta_i g(y)$ where*

(i) δ_1, δ_2, δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f and g;
(ii) γ_1, γ_2 and γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f;
(iii) $\gamma_1+\gamma_2$ and $\gamma_1+\gamma_3$ are 0-linear structures of g.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$h(x,y) = Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)$$

is bent and the dual of h is given by

$$\tilde{h}(x,y) = Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)$$

where $\phi_i^{-1}(x) = x+\gamma_i f(x)+\delta_i\left[g(x)\big(1+f(x)\big)+g(x+\gamma_i)f(x)\right]$.

Proof. Let $\psi_i(x,y) = Tr_1^m\Big(x\phi_i(y)\Big)$. Then by Proposition **??**, ψ_i is bent for $i=1,2,3$. Let $\gamma = \gamma_1+\gamma_2+\gamma_3$ and $\delta = \delta_1+\delta_2+\delta_3$. Then, $\psi(x,y) = Tr_1^m\Big(x(y+\gamma f(y)+\delta g(y))\Big)$ is bent since γ is a 0-linear structure of f and δ is a 0-linear structure of f and g. Now, it remains to show that $\tilde{\psi} = \tilde{\psi_1}+\tilde{\psi_2}+\tilde{\psi_3}$. $\tilde{\psi} = Tr_1^m\Big(x\phi^{-1}(y)\Big)$ and $\phi^{-1}(x)$ is given in Proposition **??** in the Appendix.

Note that $\tilde{\psi} = \tilde{\psi_1}+\tilde{\psi_2}+\tilde{\psi_3}$ if and only if $g(x+\gamma_1)$=$g(x+\gamma_2)$=$g(x+\gamma_3)$=$g(x+\gamma_1+\gamma_2+\gamma_3)$ which means $\gamma_1+\gamma_2$ and $\gamma_1+\gamma_3$ are 0-linear structures of g.

7 A secondary construction of bent and semi-bent functions using derivatives and linear translators

In this section, we consider a new kind of secondary construction. That construction has been proposed by Carlet and Yucas [**?**] and is presented below.

Theorem 1. *Let f and g be two bent functions over $\mathbb{F}_{2^n}$. Assume that there exists $a \in \mathbb{F}_{2^n}$ such that $D_a f = D_a g$. Then the function $h:\mathbb{F}_{2^n}\to\mathbb{F}_2$ defined by $h(x) = f(x)+D_a f(x)\big(f(x)+g(x)\big)$ is bent and its dual is $\tilde{h}(x) = \tilde{f}(x)+Tr_1^n(ax)(\tilde{f}(x)+\tilde{g}(x))$.*

In the line of Theorem **??** and of the preceding sections, we shall derive from Theorem **??** new secondary constructions of bent and semi-bent functions in Theorem **??** and Theorem **??**. To this end, we will use the following lemma.

Lemma 1. *Let $b \in \mathbb{F}_{2^m}$ and $\mathcal{W} \subseteq \mathbb{F}_{2^m}$ be an $m-1$ dimensional linear subspace with $b \notin \mathcal{W}$. Let $\mu:\mathbb{F}_{2^m}\to\mathbb{F}_2$ be a Boolean function such that b is a 0-linear structure of μ. Choose arbitrary functions $h_1:\mathbb{F}_{2^m}\to\mathbb{F}_2$ and $u:\mathcal{W}\to\mathbb{F}_2$ and define the Boolean function $h_2:\mathbb{F}_{2^m}\to\mathbb{F}_2$ by $h_2(w) = u(w)+h_1(w)$ and $h_2(w+b) = u(w)+h_1(w+b)+\mu(w)$ for $w\in\mathcal{W}$. Then $D_b h_1(y)+D_b h_2(y) = \mu(y)$ for all $y\in\mathbb{F}_{2^m}$.*

Proof. We observe that $h_2(w+b)+h_2(w)=h_1(w+b)+h_1(w)+\mu(w)$ for all $w\in\mathcal{W}$ by definition. Using the fact that b is a 0-linear structure of μ we complete the proof.

Note that Lemma **??** gives a construction of a Boolean function $h_2:\mathbb{F}_{2^m}\to\mathbb{F}_2$ with the property $D_bh_1(y)+D_b(h_2(y)=\mu(y)$ for all $y\in\mathbb{F}_{2^m}$ for given $b\in\mathbb{F}_{2^m}$, $h_1:\mathbb{F}_{2^m}\to\mathbb{F}_2$ and μ having b with 0-linear structure. The construction uses $m-1$ free variables in the form of the function $u:\mathcal{W}\to\mathbb{F}_2$.

Using Lemma **??**, Theorem **??** and results from Section **??**, we present below a new secondary construction of bent functions.

Theorem 2. *Let $1\leq k<m$ be integers with $k\mid m$. Let f, g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$. Assume that $\gamma,\delta\in\mathbb{F}_{2^m}^\star$ are 0-linear translators of f and g, respectively. Further assume that $b\in\mathbb{F}_{2^m}$ is a 0-linear structure of f and g. Let $a\in\mathbb{F}_{2^m}$ be an arbitrary element. For arbitrary function $h_1:\mathbb{F}_{2^m}\to\mathbb{F}_2$ construct $h_2:\mathbb{F}_{2^m}\to\mathbb{F}_2$ satisfying $D_bh_1(y)=D_bh_2(y)+Tr_1^m\big(a(\gamma f(y+b)+\delta g(y+b))\big)$ for all $y\in\mathbb{F}_{2^m}$ using Lemma **??**. Set $F(x,y):=Tr_1^m(xy+\gamma xf(y))+h_1(y)$ and $G(x,y):=Tr_1^m(xy+\delta xg(y))+h_2(y)$. The function defined by*

$$H(x,y)=F(x,y)+D_{a,b}F(x,y)\big(F(x,y)+G(x,y)\big)$$

is bent and its dual is

$$\begin{aligned}\tilde{H}(x,y)=&Tr_1^m\big(yx+\gamma yf(x)\big)+h_1(x+\gamma f(x))\\&+Tr_1^m(ax+by)\left[Tr_1^m\big(y(\gamma f(x)+\delta g(x))\big)+h_1(x+\gamma f(x))+h_2(x+\delta g(x))\right].\end{aligned}$$

Proof. F and G are bent by Proposition **??**. Using the fact that b is a 0-linear structure of f and g we get that $D_{a,b}F(x,y)=Tr_1^m\big(xb+a(y+b+\gamma f(y+b))\big)+D_bh_1(y)$ and $D_{a,b}G(x,y)=Tr_1^m\big(xb+a(y+b+\delta g(y+b))\big)+D_bh_2(y)$. Hence $D_{a,b}F(x,y)=D_{a,b}G(x,y)$ and the proof follows from Theorem **??** and Proposition **??**.

Using [**?**, Theorem 16] instead of Theorem **??** we obtain the following secondary construction of semi-bent functions.

Theorem 3. *Under notation and assumptions of Theorem **??** we construct $h_2:\mathbb{F}_{2^m}\to\mathbb{F}_2$ satisfying $D_bh_1(y)=D_bh_2(y)+Tr_1^m\big(a(\gamma f(y+b)+\delta g(y+b))\big)+1$ (instead of $D_bh_1(y)=D_bh_2(y)+Tr_1^m\big(a(\gamma f(y+b)+\delta g(y+b))\big)$) for all $y\in\mathbb{F}_{2^m}$. Set F and G in the same way. Then the function defined by*

$$H(x,y)=F(x,y)+G(x,y)+D_{a,b}F(x,y)+D_{a,b}FG(x,y)$$

is semi-bent.

Note that Theorem **??** gives a secondary construction of semi-bent functions of high degree by choosing the arbitrary function $h_1:\mathbb{F}_{2^m}\to\mathbb{F}_2$ of large degree. Moreover it gives a different construction than the one given in [**?**, Section 4.2.5] and hence it is an answer to Problem 4 of [**?**].

8 A secondary construction of bent functions using certain quadratic and cubic functions together with linear structures

In this section we consider Boolean functions that are the sum of a bent function of Section **??** or Section **??** and a quadratic or cubic function. We show that one can choose appropriately the

quadratic and cubic function so that those Boolean functions are bent again. Furthermore, the dual functions of those bent functions can be explicitly computed as in the preceding sections. The main results are Theorems **??**, **??**, **??** and **??**.

Theorem **??** is based on [**?**, Lemma 1]. We note that the bent functions of Theorem **??** is different from the two classes of plateaued functions in Section 6 of [**?**]. First of all we obtain bent functions while two classes of functions in Section 6 of [**?**] produce only plateaued functions.

Theorem **??** is a further generalization of Theorem **??** using cubic functions instead of quadratic functions.

Lemma 2. *[**?**] Let $w_1, w_2, u \in \mathbb{F}_{2^m}$ with $\{w_1, w_2\}$ linearly independent over $\mathbb{F}_{2^m}$. We have*

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(w_1x)Tr_1^m(w_2x)+Tr_1^m(ux)} = \begin{cases} 0 & \text{if } u \notin \langle w_1, w_2\rangle = \{0, w_1, w_2, w_1+w_2\}, \\ 2^{m-1} & \text{if } u \in \{0, w_1, w_2\}, \\ -2^{m-1} & \text{if } u = w_1 + w_2. \end{cases}$$

In Lemma **??**, for any given $\mathbb{F}_2$-linearly independent set, the Boolean function on $\mathbb{F}_{2^m}$ given by $x \mapsto Tr_1^m(w_1x)Tr_1^m(w_2x)$ is a quadratic function.

Theorem 4. *Let $w_1, w_2, \gamma \in \mathbb{F}_{2^m}$ with $\{w_1, w_2\}$ linearly independent over $\mathbb{F}_2$. Assume that $f, h : \mathbb{F}_{2^m} \to \mathbb{F}_2$ are Boolean functions such that w_1 and w_2 are 0-linear structures of f and h. Moreover, we assume that γ is a 0-linear structure of f. Then the Boolean function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2) + Tr_1^m\big(xy + \gamma x f(y)\big) + h(y) \tag{8.1}$$

is bent and its dual function is

$$\tilde{F}(x, y) = Tr_1^m(yw_1)Tr_1^m(yw_2) + Tr_1^m\big(yx + \gamma y f(x)\big) + h(x + \gamma f(x)).$$

Moreover, $F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2) + Tr_1^m\big(xL(y) + L(\gamma)xf(y)\big) + h(y)$ where L is a linearized permutation polynomial of $\mathbb{F}_{2^m}$ is also bent under the same conditions and its dual function is

$$\tilde{F}(x, y) = Tr_1^m(yw_1)Tr_1^m(yw_2) + Tr_1^m\big(yL^{-1}(x) + \gamma y f(L^{-1}(x))\big) + h(L^{-1}(x) + \gamma f(L^{-1}(x))).$$

Proof. One has for every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,

$$\widehat{\chi_F}(a, b) = \sum_{y\in\mathbb{F}_{2^m}} (-1)^{h(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xw_1)Tr_1^m(xw_2)+Tr_1^m\left(xy+\gamma xf(y)+ax\right)}$$

Let $\phi(y) = y + \gamma f(y)$ and $\mathcal{S} = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xw_1)Tr_1^m(xw_2)+Tr_1^m\left(x(\phi(y)+a)\right)}$. Then by Lemma **??**, we have

$$\mathcal{S} = \begin{cases} 0 & \text{if } \phi(y) + a \notin \{0, w_1, w_2, w_1 + w_2\}, \\ 2^{m-1} & \text{if } \phi(y) + a \in \{0, w_1, w_2\}, \\ -2^{m-1} & \text{if } \phi(y) + a = w_1 + w_2. \end{cases}$$

Now, $f(a) = f(a + w_1) = f(a + w_2) = f(a + w_1 + w_2)$ since w_1 and w_2 are 0-linear structures of f. We have two cases, namely $f(a) = 0$ and $f(a) = 1$. Here, only the proof for the case $f(a) = 0$ is given since the proof for the other case is very similar.

Assume $f(a)=0$. Then $\phi(y)+a \in \{0, w_1, w_2\}$ when $y \in \mathcal{A}=\{a, a+w_1, a+w_2\}$ and $\phi(y)+a = w_1+w_2$ when $y=a+w_1+w_2$. Hence,

$$\widehat{\chi_F}(a,b) = 2^{m-1}\left[\sum_{y\in\mathcal{A}} (-1)^{h(y)+Tr_1^m(by)} - (-1)^{h(a+w_1+w_2)+Tr_1^m(b(a+w_1+w_2))}\right].$$

Since w_1 and w_2 are 0-linear structures of h, we obtain

$$\widehat{\chi_F}(a,b) = 2^{m-1}\left[(-1)^{h(a)+Tr_1^m(ba)}\right]\mathcal{S}_1$$

where

$$\mathcal{S}_1 = \left[1+(-1)^{Tr_1^m(bw_1)}+(-1)^{Tr_1^m(bw_2)}-(-1)^{Tr_1^m(b(w_1+w_2))}\right]. \tag{8.2}$$

Note that

$$\mathcal{S}_1 = \begin{cases} 2 \text{ if } Tr_1^m(bw_1)Tr_1^m(bw_2)=0, \\ -2 \text{ if } Tr_1^m(bw_1)Tr_1^m(bw_2)=1. \end{cases}$$

Combining these we obtain that F is bent and its dual $\tilde{F}$ satisfies that

$$\tilde{F}(x,y) = Tr_1^m(yw_1)Tr_1^m(yw_2)+Tr_1^m\big(yx+y\gamma f(x)\big)+h(x+\gamma f(x)).$$

Remark 4. In Theorem **??**, for given $\mathbb{F}_2$-linearly independent subset $\{w_1, w_2\}$, the Boolean function on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ given by $(x,y)\mapsto Tr_1^m(xw_1)Tr_1^m(xw_2)$ is a quadratic function, which is used as the first summand in the definition of $F(x,y)$ in equation (**??**). In the proof of Theorem **??**, we apply Lemma **??** for this quadratic function. Note that if $\gamma\neq 0$ and $1+deg(f)$, $deg(h)$ and 2 are distinct, then the degree of $F(x,y)$ is $max\{1+deg(f), deg(h), 2\}$, which may be much larger than 2.

In the following we present a straightforward generalization of Theorem **??**.

Theorem 5. *Let $w_1, w_2, \gamma, \delta \in \mathbb{F}_{2^m}$ with $\{w_1, w_2\}$ linearly independent over $\mathbb{F}_2$. Assume that $f, g, h : \mathbb{F}_{2^m}\to\mathbb{F}_2$ are Boolean functions such that w_1 and w_2 are 0-linear structures of f, g and h. Moreover, we assume that γ is a 0-linear structure of f and δ is a 0-linear structure of f and g. Then the Boolean function F defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by*

$$F(x,y) = Tr_1^m(xw_1)Tr_1^m(xw_2)+Tr_1^m\big(x(L(y)+L(\gamma)f(y)+L(\delta)g(y))\big)+h(y)$$

is bent and its dual function is

$$\tilde{F}(x,y) = Tr_1^m(yw_1)Tr_1^m(yw_2)+Tr_1^m\big(y\rho^{-1}(x)\big)+h(\rho^{-1}(x)) \text{ where}$$

$$\rho^{-1}(x) = L^{-1}(x)+\gamma f(L^{-1}(x))+\delta\left[g(L^{-1}(x))\big(1+f(L^{-1}(x))\big)+g(L^{-1}(x)+\gamma)f(L^{-1}(x))\right].$$

We now give the analogue of Lemma **??** which improves Lemma 1 of [**?**].

Lemma 3. *Let $w_1, w_2, w_3, u \in \mathbb{F}_{2^m}$ with $\{w_1, w_2, w_3\}$ linearly independent over $\mathbb{F}_{2^m}$. We have*

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(w_1x)Tr_1^m(w_2x)Tr_1^m(w_3x)+Tr_1^m(ux)} = \begin{cases} 0 & \text{if } u\notin\langle w_1,w_2,w_3\rangle, \\ 3.2^{m-2} & \text{if } u=0, \\ 2^{m-2} & \text{if } u\in\{w_1,w_2,w_3,w_1+w_2+w_3\}, \\ -2^{m-2} & \text{if } u\in\{w_1+w_2, w_1+w_3, w_2+w_3\}. \end{cases}$$

Proof. Let $\mathcal{T}$ denotes the sum in the statement of the lemma. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be the sums as

$$\mathcal{T}_1 = \sum_{x\in\mathbb{F}_{2^m}|Tr_1^m(w_1x)=0} (-1)^{Tr_1^m(ux)}$$

and

$$\mathcal{T}_2 = \sum_{x\in\mathbb{F}_{2^m}|Tr_1^m(w_1x)=1} (-1)^{Tr_1^m(w_2x)Tr_1^m(w_3x)+Tr_1^m(ux)}.$$

We have that $\mathcal{T} = \mathcal{T}_1 + \mathcal{T}_2$. It is clear that

$$\mathcal{T}_1 = \begin{cases} 0 & \text{if } u \notin \langle 0, w_1\rangle = \{0, w_1\}, \\ 2^{m-1} & \text{if } u \in \{0, w_1\}. \end{cases}$$

Using Lemma **??** we obtain that

$$\mathcal{T}_2 = \begin{cases} 0 & \text{if } u \notin \langle w_1, w_2, w_3\rangle, \\ 2^{m-2} & \text{if } u \in \{0, w_1, w_2, w_3, w_1+w_2+w_3\}, \\ -2^{m-2} & \text{if } u \in \{w_1+w_2, w_1+w_3, w_2+w_3\}. \end{cases}$$

Combining $\mathcal{T}_1$ and $\mathcal{T}_2$ we complete the proof.

Remark 5. This remark is analogous to Remark **??**. In Theorem **??**, for given $\mathbb{F}_2$-linearly independent subset $\{w_1, w_2, w_3\}$, the Boolean function on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ given by

$$(x, y) \mapsto Tr_1^m(xw_1)Tr_1^m(xw_2)Tr_1^m(xw_3)$$

is a cubic function, which is used as the first summand in the definition of $F(x, y)$ in equation (**??**). In the proof of Theorem **??**, we apply Lemma **??** for this cubic function. As in Remark **??**, the degree of $F(x, y)$ is $max\{1 + deg(f), deg(h), 3\}$ under suitable conditions, which may be much larger than 3.

Theorem 6. *Let f and h be two Boolean functions on $\mathbb{F}_{2^m}$. Let $w_1, w_2, w_3 \in \mathbb{F}_{2^m}$ be linearly independent and $\gamma \in \mathbb{F}_{2^m}$. Assume that γ is a 0-linear structure of f, and w_1, w_2, w_3 are 0-linear structures of f and h. Then, the function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2)Tr_1^m(xw_3) + Tr_1^m\big(x(L(y) + L(\gamma)f(y))\big) + h(y) \tag{8.3}$$

is bent and its dual is

$$\begin{aligned}\tilde{F}(x, y) = {} & Tr_1^m(yw_1)Tr_1^m(yw_2)Tr_1^m(yw_3) + Tr_1^m\big(y(L^{-1}(x) + \gamma f(L^{-1}(x)))\big) \\ & + h(L^{-1}(x) + \gamma f(L^{-1}(x))).\end{aligned}$$

Proof. Let $\phi(y) = y + \gamma f(y)$. For every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,

$$\widehat{\chi_F}(a, b) = \sum_{y\in\mathbb{F}_{2^m}} (-1)^{h(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(w_1x)Tr_1^m(w_2x)Tr_1^m(w_3x)+Tr_1^m\left(x(\phi(y)+a)\right)}.$$

For the case $f(a) = 0$,

- $\phi(y) + a = 0$ when $y = a$,

– $\phi(y) + a \in \{w_1, w_2, w_3, w_1 + w_2 + w_3\}$ when
$y \in \mathcal{A}_1 = \{a + w_1, a + w_2, a + w_3, a + w_1 + w_2 + w_3\}$
– $\phi(y) + a \in \{w_1 + w_2, w_1 + w_3, w_2 + w_3\}$
when $y \in \mathcal{A}_2 = \{a + w_1 + w_2, a + w_1 + w_3, a + w_2 + w_3\}$.

Then, following the steps in proof of Theorem **??** and using Lemma **??**, we get

$$\begin{aligned}\widehat{\chi_F}(a,b) &= 3.2^{m-2}(-1)^{Tr_1^m(ba)+h(a)} + 2^{m-2}\sum_{y\in\mathcal{A}_1}(-1)^{Tr_1^m(by)+h(y)} \\ &\quad -2^{m-2}\sum_{y\in\mathcal{A}_2}(-1)^{Tr_1^m(by)+h(y)} \\ &= 2^{m-2}\left[(-1)^{Tr_1^m(ba)+h(a)}\right]\mathcal{S}\end{aligned}$$

where

$$\mathcal{S} = [3 + \mathcal{S}_1 + \mathcal{S}_2], \tag{8.4}$$

$\mathcal{S}_1 = (-1)^{Tr_1^m(bw_1)} + (-1)^{Tr_1^m(bw_2)} + (-1)^{Tr_1^m(bw_3)} + (-1)^{Tr_1^m(b(w_1+w_2+w_3)}$ and
$\mathcal{S}_2 = (-1)^{Tr_1^m(b(w_1+w_2))} + (-1)^{Tr_1^m(b(w_1+w_3))} + (-1)^{Tr_1^m(b(w_2+w_3))}$. Let $(-1)^{Tr_1^m(bw_i)} = c_i$ where $c_i \in \mathbb{F}_2$, for $i = 1, 2, 3$. Then, $3 + \mathcal{S}_1 + \mathcal{S}_2 = \pm 4$ and hence $\widehat{\chi_F}(a, b) = \pm 2^m$.
The proof for the case $f(a) = 1$ is very similar.

As in Theorem **??**, in the following we get a modification of Theorem **??** using two linear structures instead of one linear structure.

Theorem 7. *Let f, g and h be Boolean functions on $\mathbb{F}_{2^m}$. Let $w_1, w_2, w_3 \in \mathbb{F}_{2^m}$ be linearly independent and $\gamma, \delta \in \mathbb{F}_{2^m}$, $\gamma \neq \delta$. Assume that γ is a 0-linear structure of f, δ is a 0-linear structure of f and g. Moreover, assume that w_1, w_2, w_3 are 0-linear structures of f, g and h. Then, the function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$F(x,y) = Tr_1^m(xw_1)Tr_1^m(xw_2)Tr_1^m(xw_3) + Tr_1^m\big(x(L(y) + L(\gamma)f(y) + L(\delta)g(y))\big) + h(y)$$

is bent and its dual is

$$\tilde{F}(x,y) = Tr_1^m(yw_1)Tr_1^m(yw_2)Tr_1^m(yw_3) + Tr_1^m\big(y\rho^{-1}(x)\big) + h(\rho^{-1}(x)) \text{ where}$$

$$\rho^{-1}(x) = L^{-1}(x) + \gamma f(L^{-1}(x)) + \delta\left[g(L^{-1}(x))\big(1 + f(L^{-1}(x))\big) + g(L^{-1}(x) + \gamma)f(L^{-1}(x))\right].$$

Acknowledgment

The authors would like to thank the anonymous reviewers and the program committee for the detailed and constructive comments which improved the paper a lot.

References

1. A. Canteaut and M. Naya-Plasencia. Structural weakness of mappings with a low differential uniformity. In *Conference on Finite Fields and Applications*, 2009.
2. C. Carlet, E. Prouff. On plateaued functions and their constructions. In *Fast Software Encryption*, Springer Berlin Heidelberg, pages 54-73, 2003.
3. C. Carlet, J. L. Yucas. Piecewise constructions of bent and almost optimal Boolean functions. *Des. Codes Cryptography*, Vol. 37, No. 3, pages 449-464, 2005.
4. C. Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer Berlin Heidelberg, pages 1-28, 2006.
5. C. Carlet. Boolean functions for Cryptography and Error Correcting Codes. In Yves Crama and Peter L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Cambridge University Press, pages 257-397, 2010.
6. C. Carlet. Open problems on binary bent functions. In *Open Problems in Mathematics and Computational Science*, Springer, pages 203-241, 2014.
7. P. Charpin and G. M. Kyureghyan. On a class of permutation polynomials over $\mathbb{F}_{2^n}$. SETA 2008, in: Lecture Notes in Comput. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368-376.
8. P. Charpin and G. M. Kyureghyan. When does $G(x) + \gamma\, Tr(H(x))$ permute $\mathbb{F}_2$? *Finite Fields Appl.*, 15(5) (2009) 615-632.
9. P. Charpin and G. Kyureghyan. Monomial functions with linear structure and permutation polynomials. In *Finite Fields: Theory and Applications - Fq9 - Contemporary Mathematics, AMS*, Vol. 518, pages 99-111, 2010.
10. P. Charpin, G. M. Kyureghyan and V. Suder. Sparse Permutations with Low Differential Uniformity. *Finite Fields and Their Applications*, 28(2014), pp. 214-243.
11. P. Charpin, S. Mesnager and S. Sarkar. On involutions of finite fields. In *Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT 2015.*
12. P. Charpin and S. Sarkar. Polynomials With Linear Structure and Maiorana-McFarland Construction. In *IEEE Trans. Inf. Theory*, Vol. 57, No. 6, pages 3796-3804, 2011.
13. S. Chee, S. Lee and K. Kim. Semi-bent Functions. In *Advances in Cryptology-ASIACRYPT'94*, LNCS, Vol. 917, pages 107-118, 1994.
14. J. Dillon. Elementary Hadamard Difference Sets. In *Ph.D. dissertation, Univ. of Maryland, College Park*, 1974.
15. G. Kyureghyan. Constructing permutations of finite fields via linear translators. *Journal of Combinatorial Theory Series A*, Vol. 118, No. 3, pages 1052-1061, 2011.
16. X. Lai. Additive and linear structures of cryptographic functions. In *Fast Software Encryption*, LNCS, Vol. 1008, pages 75-85, 1995.
17. S. Mesnager. Semi-bent functions from oval polynomials. In *Proceedings of Fourteenth International Conference on Cryptography and Coding, IMACC 2013*, LNCS 8308, Springer, Heidelberg, pages 1-15, 2013.
18. S. Mesnager. Several new infinite families of bent functions and their duals. *IEEE Trans. Inf. Theory*, Vol. 60, No. 7, pages 4397-4407, 2014.
19. S. Mesnager. On semi-bent functions and related plateaued functions over the Galois field F_{2^n}. In *Open Problems in Mathematics and Computational Science*, Springer, pages 243-273, 2014.
20. S. Mesnager. Further constructions of infinite families of bent functions from new permutations and their duals. *Journal of Cryptography and Communications (CCDS)*, Springer. To appear.
21. S. Mesnager. Bent functions: fundamentals and results. *Springer* 2015. To appear.
22. O-S. Rothaus. On bent functions. *J. Combin. Theory Ser. A*, Vol. 20, pages 300-305, 1976.
23. G. Sun, C. Wu. Construction of semi-bent Boolean functions in even number of variables. *Chin. J. Electron.*, Vol. 18, No. 2, pages 231-237, 2009.
24. Y. Zheng, X. M. Zhang. Plateaued functions. In *Advances in Cryptology-ICICS*, LNCS, Vol. 1726, pages. 284-300, 1999.

A Appendix

The following proposition is related to Proposition **??** in Section **??**.

Proposition 8. *Let H be defined by equation (**??**), γ and δ be defined as in Proposition **??**. Then the dual of H is $\tilde{H}(x,y) = Tr_1^m\left(y\phi^{-1}(x)\right) + h(\phi^{-1}(x))$ where $\phi^{-1} = {\pi_2}^{-1} \circ \rho^{-1} \circ {\pi_1}^{-1}$ and $\rho^{-1}(x)$ is given as follows.*

(i) If γ is a 0-linear structure of f, δ is a 0-linear structure of f and g, then

$$\rho^{-1}(x) = x + \gamma f(x) + \delta\left[g(x)(1+f(x)) + g(x+\gamma)f(x)\right].$$

(ii) If γ is a 0-linear structure of f, δ is a 1-linear structure of f and $\delta+\gamma$ is a 0-linear structure of g, then

$$\rho^{-1}(x) = x + \gamma\left[g(x) + f(x)\big(1+g(x)+g(x+\gamma)\big)\right] + \delta\left[g(x)(1+f(x)) + g(x+\gamma)f(x)\right].$$

(iii) If δ is a 0-linear structure of g, γ is a 0-linear structure of f and g, then

$$\rho^{-1}(x) = x + \gamma\left[f(x)(1+g(x)) + f(x+\delta)g(x)\right] + \delta g(x).$$

(iv) If δ is a 0-linear structure of g, γ is a 1-linear structure of g and $\delta+\gamma$ is a 0-linear structure of f, then

$$\rho^{-1}(x) = x + \gamma\left[f(x)(1+g(x)) + f(x+\delta)g(x)\right] + \delta\left[f(x)(1+g(x)) + \big(1+f(x+\delta)\big)g(x)\right].$$

(v) If δ is a 1-linear structure of f or δ is a 0-linear structure of g, then

$$\rho^{-1}(x) = x + \gamma\left[f(x)(1+g(x+\delta)) + \big(1+f(x)\big)g(x)\right] + \delta f(x).$$

(vi) If γ is a 1-linear structure of g, δ is a 1-linear structure of f and g, then

$$\rho^{-1}(x) = x + \gamma g(x) + \delta\left[f(x)(1+g(x)) + f(x+\gamma)g(x)\right].$$

Proof. We give only the proof for the case (i). Assume that γ is a 0-linear structure of f, δ is a 0-linear structure of f and g, then we claim that

$$\rho^{-1}(x) = \begin{cases} x & \text{if } f(x)=0 \text{ and } g(x)=0 \\ x+\delta & \text{if } f(x)=0 \text{ and } g(x)=1 \\ x+\gamma & \text{if } f(x)=1 \text{ and } g(x+\gamma)=0 \\ x+\gamma+\delta & \text{if } f(x)=1 \text{ and } g(x+\gamma)=1 \end{cases} \tag{A.1}$$

Let $\rho(y) = a$. Then,

$$y + \gamma f(y) + \delta g(y) = a \tag{A.2}$$

Taking f of both sides gives $f(y+\gamma f(y)+\delta g(y)) = f(a)$. Since γ and δ are 0-linear structures of f, we get

$$f(y) = f(a). \tag{A.3}$$

Note that, $\big(f(a), g(a)\big) \in \{(0,0),(0,1),(1,0),(1,1)\}$. These four cases correspond to the cases in equation (**??**). We prove only the first case in equation (**??**) and the proofs of other cases are similar. Hence, we assume that $(f(a), g(a)) = (0,0)$. Then, by equation (**??**), $f(y) = 0$ and by equation (**??**), $y + \delta g(y) = a$. Taking g of both sides and using that δ is a 0-linear structure of g, we obtain that $g(y + \delta g(y)) = g(y) = g(a)$. As $g(a) = 0$ by our assumption, we get $g(y) = 0$ and putting $f(y) = g(y) = 0$ in equation (**??**) we conclude that $y = a$.
Finally, the equation (**??**) can be written in the form

$$\rho^{-1}(x) = x + \gamma f(x) + \delta\left[g(x)(1 + f(x)) + g(x + \gamma)f(x)\right].$$

The following five propositions are related to Proposition **??** in Section **??**.

Proposition 9. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f;
(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f;
(iii) $\gamma_1 + \delta_1$, $\gamma_2 + \delta_2$, $\gamma_3 + \delta_3$ are 0-linear structures of g;
(iv) $\gamma_1 + \gamma_2$ and $\gamma_1 + \gamma_3$ are 0-linear structures of g.

Then the function h defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} h(x,y) = {} & Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \\ & + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned} \tilde{h}(x,y) = {} & Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \\ & + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \end{aligned}$$

where

$$\begin{aligned} \phi_i^{-1}(x) = {} & x + \gamma\left[g(x) + f(x)\big(1 + g(x) + g(x + \gamma)\big)\right] \\ & + \delta\left[g(x)(1 + f(x)) + g(x + \gamma)f(x)\right]. \end{aligned}$$

Proposition 10. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f and g;
(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of g;
(iii) $\delta_1 + \delta_2$ and $\delta_1 + \delta_3$ are 0-linear structures of f.

Then the function h defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} h(x,y) = {} & Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \\ & + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \end{aligned}$$

is bent and the dual of h is given by

$$\tilde{h}(x,y) = Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)$$

where $\phi_i^{-1}(x) = x + \gamma\left[f(x)(1+g(x)) + f(x+\delta)g(x)\right] + \delta g(x)$.

Proposition 11. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of g;
(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of g;
(iii) $\gamma_1+\delta_1$, $\gamma_2+\delta_2$, $\gamma_3+\delta_3$ are 0-linear structures of f;
(iv) $\delta_1+\delta_2$ and $\delta_1+\delta_3$ are 0-linear structures of f.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$h(x,y) = Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)$$

is bent and the dual of h is given by

$$\tilde{h}(x,y) = Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)$$

where

$$\phi_i^{-1}(x) = x + \gamma\left[f(x)(1+g(x)) + f(x+\delta)g(x)\right] + \delta\left[f(x)(1+g(x)) + \big(1+f(x+\delta)\big)g(x)\right].$$

Proposition 12. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f and g;
(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f;
(iii) $\delta_1+\delta_2$ and $\delta_1+\delta_3$ are 0-linear structures of g.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$h(x,y) = Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)$$

is bent and the dual of h is given by

$$\tilde{h}(x,y) = Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)$$

where $\phi_i^{-1}(x) = x + \gamma\left[f(x)(1+g(x+\delta)) + \big(1+f(x)\big)g(x)\right] + \delta f(x)$.

Proposition 13. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of g;
(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f and g;
(iii) $\gamma_1 + \gamma_2$ and $\gamma_1 + \gamma_3$ are 0-linear structures of f.

Then the function h defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} h(x,y) = {} & Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \\ & + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned} \tilde{h}(x,y) = {} & Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \\ & + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \end{aligned}$$

where $\phi_i^{-1}(x) = x + \gamma g(x) + \delta\left[f(x)(1+g(x)) + f(x+\gamma)g(x)\right]$.