# A note on constructions of bent functions from involutions

Sihem Mesnager*

October 13, 2015

**Abstract**

Bent functions are maximally nonlinear Boolean functions. They are important functions introduced by Rothaus and studied firstly by Dillon and next by many researchers for four decades. Since the complete classification of bent functions seems elusive, many researchers turn to design constructions of bent functions. In this note, we show that linear involutions (which are an important class of permutations) over finite fields give rise to bent functions in bivariate representations. In particular, we exhibit new constructions of bent functions involving binomial linear involutions whose dual functions are directly obtained without computation.

## 1 Introduction

Bent functions were introduced by Rothaus [31] in 1976 but already studied by Dillon [13] since 1974. A bent function is a Boolean function with an even number of variables which achieves the maximum possible nonlinearity. For their own sake as interesting combinatorial objects, but also for their relations to coding theory (e.g. Reed-Muller codes, Kerdock codes), combinatorics (e.g. difference sets), design theory (any difference set can be used to construct a symmetric design), sequence theory, and applications in cryptography (design of stream ciphers and of S-boxes for block ciphers), bent functions have attracted a lot of research for four decades. Despite their simple and natural definition, bent functions turned out to admit a very complicated structure in general. Since the complete classification of bent functions seems elusive, many researchers turn to design constructions of bent functions and an important focus of research in the twenty past years was then to find constructions. Many methods are known and some of them allow explicit constructions and numerous constructions have been obtained. A non-exhaustive list of references dealing with constructions of binary bent Boolean functions is [16] [21],[13], [3], [4], [14],[18],[15], [32], [19], [11], [2], [10], [6], [25], [22], [23], [24], [8], [1], [30], [20], [26], [27]. Open problems on binary bent functions can be found in [7]. A jubilee survey paper on bent functions

*Department of Mathematics, University of Paris VIII, University of Paris XIII, LAGA, UMR 7539, CNRS and Telecom ParisTech, Paris, France, email: smesnager@univ-paris8.fr

giving an historical perspective, and making pertinent connections to designs, codes and cryptography is [9]. A book devoted especially to bent functions and containing a complete survey (including variations, generalizations and applications) is [28].

Bent functions $f$ are often better viewed in their bivariate representation in the form $f(x, y)$ where $x$ and $y$ belong to $\mathbb{F}_2^m$ or $\mathbb{F}_{2^m}$. The aim of this note is to provide more constructions of bent functions in bivariate representation. To this end, we use the results of a recent joint work with Charpin and Sarkar [12] in which we have provided a detailed mathematical study of involutions which are an important class of permutations. More precisely, we have provided in [12] a systematic study of involutions that are defined over finite field of characteristic 2, characterized the involution property of several classes of polynomials and propose several constructions. In particular the corpus of binary involutions has been fully described. This note shows that the former involutions lead to the construction of bent functions. Involutions have been used for the first time in a very recent joint work with Cohen and Madore [29] for designing bent functions in bivariate representations. We have showed that the construction of the bent functions (involving nonlinear monomial involutions) presented in [29] is based on an arithmetical problem and that the existence of those bent functions can be proved using algebraic and geometric tools such as Fermat hypersurfaces and Lang-Weil estimates.

This note is organized as follows. Formal definitions and necessary preliminaries are introduced in Section 2. In Section 3, we recall previous methods used in [26] and [27] on the constructions of binary bent functions based on special permutations satisfying a condition $(\mathcal{A}_m)$. We highlight that involutions are appropriate in this context since for this class the condition of bentness $(\mathcal{A}_m)$ is reduced to the problem of finding three involutions such that their sum is again an involution. In Section 4 we focus on linear involutions and show how one can construct bent functions from general linear involutions involving linear structures and binomial linear involutions. We shall prove the existence of such bent functions using algebraic arguments by solving equations over finite fields. We also show the non-existence of some bent functions of a particular form while considering monomial linear involutions.

## 2 Notation and Preliminaries

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 $\mathbb{F}_2$. It can be represented as a polynomial in one variable $x \in \mathbb{F}_{2^n}$ of the form $f(x) = \sum_{j=0}^{2^n-1} a_j x^j$ where the $a_j$'s are elements of the field. Such a function $f$ is Boolean if and only if $a_0$ and $a_{2^n-1}$ belong to $\mathbb{F}_2$ and $a_{2j} = a_j^2$ for every $j \notin \{0, 2^n - 1\}$ (where $2j$ is taken modulo $2^n - 1$). This leads to a unique representation which we call the *polynomial form* (for more details, see e.g. [6]). First, 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:

$$Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}.$$

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. We make use of some known properties of the trace function such as $Tr_1^n(x) = Tr_1^n(x^2)$ and for every integer $r$ dividing $k$, the mapping $x \mapsto Tr_r^k(x)$ is $\mathbb{F}_{2^k}$-linear.

The *bivariate representation* of Boolean functions makes sense only when $n$ is an even integer. It plays an important role for defining bent functions and is obtained as follows: we identify $\mathbb{F}_{2^n}$ (where $n = 2m$) with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and consider then the input to $f$ as an ordered pair $(x, y)$ of elements of $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial

$$\sum_{0 \le i,j \le 2^m-1} a_{i,j} x^i y^j$$

over $\mathbb{F}_{2^m}$ such that $f$ is the bivariate polynomial function over $\mathbb{F}_{2^m}$ associated to it. Then the algebraic degree of $f$ equals $\max_{(i,j)\,|\,a_{i,j}\neq 0}(w_2(i)+w_2(j))$. The function $f$ being Boolean, its bivariate representation can be written in the (non unique) form $f(x,y) = Tr_1^m(P(x,y))$ where $P(x,y)$ is some polynomial in two variables over $\mathbb{F}_{2^m}$. There exist other representations of Boolean functions not used in this note (see e.g. [6]) in which we shall only consider functions in their bivariate representation.

If $f$ is a Boolean function defined on $\mathbb{F}_{2^n}$, then 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 follows:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}.$$

Bent functions can be defined in terms of the Walsh transform as follows.

**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 occur in pair. In fact, given a bent function $f$ over $\mathbb{F}_{2^n}$, we define its *dual function*, denoted by $\widetilde{f}$, when considering the signs of the values of the Walsh transform $\widehat{\chi_f}(x)$ ($x \in \mathbb{F}_{2^n}$) of $f$. More precisely, $\widetilde{f}$ is defined by the equation:

$$(-1)^{\widetilde{f}(x)} 2^{\frac{n}{2}} = \widehat{\chi_f}(x). \tag{2.1}$$

Due to the involution law the Fourier transform is self-inverse. Thus the dual of a bent function is again bent.

## 3 Constructions of bent functions from special families of permutations

It has been shown in [26] and next in [27] that it is possible to construct bent functions from three special permutations satisfying a condition $(\mathcal{A}_m)$ introduced by the author in [27].

**Definition 2.** Let $m$ be a positive integer. Three permutations $\phi_1$, $\phi_2$ and $\phi_3$ of $\mathbb{F}_{2^m}$ are said to satisfy $(\mathcal{A}_m)$ if the two following conditions hold

1. Their sum $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation of $\mathbb{F}_{2^m}$.
2. $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

From three permutations satisfying condition $(\mathcal{A}_m)$, one can construct easily bent functions in bivariate representation as follows.

**Theorem 1.** *([26]) Let $m$ be a positive integer. Let $\phi_1$, $\phi_2$ and $\phi_3$ be three permutations of $\mathbb{F}_{2^m}$. Then,*

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

*is bent if and only if $\phi_1$, $\phi_2$ and $\phi_3$ satisfy $(\mathcal{A}_m)$. Furthermore, its dual function $\tilde{g}$ is given by*

$$\tilde{g}(x,y) = Tr_1^m(\phi_1^{-1}(x)y)Tr_1^m(\phi_2^{-1}(x)y) + Tr_1^m(\phi_1^{-1}(x)y)Tr_1^m(\phi_3^{-1}(x)y) + Tr_1^m(\phi_2^{-1}(x)y)Tr_1^m(\phi_3^{-1}(x)y). \tag{3.1}$$

Several new bent functions have been exhibited from monomial permutations satisfying $(\mathcal{A}_m)$ (see [26]) and from more families of new permutations of $\mathbb{F}_{2^m}$ satisfying $(\mathcal{A}_m)$ (see [27]). In this note we are interested on permutations which are *involutions*. An involution is a special permutation, but the involution property includes the bijectivity as it appears in the classical definition.

**Definition 3.** Let $F$ be any function over $\mathbb{F}_{2^n}$. We say that $F$ is an involution if $F \circ F(x) = x, \quad \text{for all } x \in \mathbb{F}_{2^n}$.

In an extended version of [12], Charpin, Mesnager and Sarkar have provided a detailed mathematical study of involutions. In [12], the authors have considered several classes of polynomials and characterized when they are involutions. They characterized monomials as well as linear involutions and presented several constructions of involutions. New involutions constructed from the known ones have also been derived. The following statement is a straightforward consequence of Theorem 1 showing that one can derive bent functions in bivariate representation from involutions.

**Corollary 2.** *Let $m$ be a positive integer. Let $\phi_1$, $\phi_2$ and $\phi_3$ be three involutions of $\mathbb{F}_{2^m}$. Then,*

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

*is bent if and only if $\psi = \phi_1 + \phi_2 + \phi_3$ is an involution.*
*Furthermore, its dual function $\tilde{g}$ is given by $\tilde{g}(x,y) = g(y,x)$.*

Notice that this gives a very handy way to compute the dual (namely, transpose the two arguments), in stark contrast with the univariate case.

# 4 Constructions of bent functions from some linear involutions

In [29], the authors have investigated bent functions from monomial involutions. They have showed that the construction of such bent functions is closely related to an arithmetical problem. The authors have therefore studied in [29] the existence of such bent functions and partially solved the problem from algebraic and geometric point of view using Fermat hypersurface and Lang-Weil estimations.

In this section we focus on linear involutions.

## 4.1 A construction of bent functions from general linear involutions

In the following we show that further bent functions involving linear structures can be simply obtained from general linear involutions. Let us start by recalling the notion of linear structure.

**Definition 4.** Let $f$ be a Boolean function on $\mathbb{F}_{2^n}$. An element $\alpha \in \mathbb{F}_{2^n}^\star$ is said to be an $a$-linear structure for the Boolean function $f$ (where $a \in \mathbb{F}_2$) if $f(x+\alpha) + f(x) = a$, for any $x \in \mathbb{F}_{2^n}$.

Note that 0-linear structures for a Boolean function $f$ are the points for which the derivative of $f$ vanishes : $f(x+\alpha) = f(x)$ for every $x$ is equivalent to say that $D_\alpha f(x) := f(x+\alpha) + f(x) = 0$ for every $x$.

**Proposition 1.** *Let $L : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a $\mathbb{F}_2$-linear involution of $\mathbb{F}_{2^m}$. Let $f$ be a Boolean function over $\mathbb{F}_{2^m}$ and $\alpha$ be a non zero $0$-linear structure of $f$. Then the mapping $\phi$ defined by $\phi(x) = L(x) + L(\alpha)f(x)$, $x \in \mathbb{F}_{2^m}$ is a permutation of $\mathbb{F}_{2^m}$ and*

$$\phi^{-1}(x) = L(x) + \alpha f(L(x)). \tag{4.1}$$

*Proof.* The fact that $\phi$ is a permutation is a straightforward application of ([17], Theorem 1). Note next that

$$\phi(L(x)+\alpha f(L)(x)) = L(L(x)+\alpha f(L)(x)) + L(\alpha)f(L(x)+\alpha f(L(x))).$$

Now, $L$ is a linear involution and $\alpha$ is a 0-linear structure of $f$, therefore

$$\phi(L(x)+\alpha f(L)(x)) = x + L(\alpha)f(L(x)) + L(\alpha)f(L(x)) = x$$

proving (4.1).

$\square$

Let us denote $\mathcal{K}_\alpha(f)$ the set $\{\alpha \in \mathbb{F}_{2^m} \mid D_\alpha f = 0\}$.

**Theorem 3.** *Let $m$ be a positive integer. Let $L$ be a linear involution on $\mathbb{F}_{2^m}$. Let $f$ be a Boolean function over $\mathbb{F}_{2^m}$ such that the set $\mathcal{K}_\alpha(f)$ is of dimension at least two over $\mathbb{F}_2$. Let $(\alpha_1,\alpha_2,\alpha_3)$ be any 3-tuple of pairwise distinct elements of $\mathcal{K}_\alpha(f)$ such that $\alpha_1+\alpha_2+\alpha_3 \neq 0$. Then the Boolean function $g$ defined in bivariate representation on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by*

$$\begin{aligned} g(x,y) = Tr_1^m(xL(y)) + f(y)\Big(&Tr_1^m(L(\alpha_1)x)Tr_1^m(L(\alpha_2)x) \\ &+ Tr_1^m(L(\alpha_1)x)Tr_1^m(L(\alpha_3)x) + Tr_1^m(L(\alpha_2)x)Tr_1^m(L(\alpha_3)x)\Big) \end{aligned} \tag{4.2}$$

*is bent and its dual function $\tilde{g}$ is given by*

$$\begin{aligned} \tilde{g}(x,y) &= Tr_1^m(L(x)y) \\ &\quad + f(L(x))\Big(Tr_1^m(\alpha_1 y)Tr_1^m(\alpha_2 y) + Tr_1^m(\alpha_1 y)Tr_1^m(\alpha_3 y) + Tr_1^m(\alpha_2 y)Tr_1^m(\alpha_3 y)\Big). \end{aligned} \tag{4.3}$$

*Proof.* Set, for $i \in \{1,2,3\}$,

$$\phi_i(y) := L(y) + L(\alpha_i)f(y), y \in \mathbb{F}_{2^m}$$

where $L$ stands for a $\mathbb{F}_2$-linear involution over $\mathbb{F}_{2^m}$. Each map $\phi_i$ is a permutation of $\mathbb{F}_{2^m}$ since $\alpha_i \in \mathcal{K}_0(f)$, according to Proposition 1. Observe next that

$$\psi(y) = \sum_{i=1}^{3}\phi_i(y) = L(y) + L(\alpha_1+\alpha_2+\alpha_3)f(y)$$

by the linearity of $L$. Therefore, $\psi$ is also a permutation of $\mathbb{F}_{2^m}$ since $\alpha_1+\alpha_2+\alpha_3 \in \mathcal{K}_0(f)\setminus\{0\}$, according to Proposition 1. Now, again according to Proposition 1,

$$\psi^{-1}(y) = L(y) + (\alpha_1+\alpha_2+\alpha_3)f(L(y)) = \sum_{i=1}^{3}\phi_i^{-1}(y).$$

One can therefore apply Corollary 1 to $\phi_1$, $\phi_2$ and $\phi_3$ since $\phi_1$, $\phi_2$ and $\phi_3$ satisfy $(\mathcal{A}_m)$. After calculations, the result follows by combining Corollary 1 and Proposition 1. $\square$

To apply Theorem 3, one has to find a Boolean function $f$ such that $\mathcal{K}_\alpha(f)$ is of dimension at least 2. If $m = rk$ with $r$ even and $k \geq 2$, candidates are functions of the form $f(x) = h(Tr_k^m(x))$ where $h$ is a Boolean function over $\mathbb{F}_{2^k}$. Indeed note that, for every $\alpha \in \mathbb{F}_{2^k}$, $f(x+\alpha) = g(Tr_k^m(x) + Tr_k^m(\alpha)) = h(Tr_k^m(x) + \alpha Tr_k^m(1)) = h(Tr_k^m(x))$ since $Tr_k^m(1) = 0$.

### 4.2 Bent functions from monomial linear involutions

Let $\phi(x) = \lambda x^{2^i}$ be a linear monomial mapping where $0 < i < n$ and $\lambda \in \mathbb{F}_2^*$. In [12], the authors have characterized linear monomials that are involutions. More precisely, $\phi(x)$ is an involution if and only if $m = \frac{n}{2}$ with $n$ even and $\lambda^{2^m+1} = 1$. It has been shown that there is no linear monomial involution when $n$ is odd.

A natural question is to wonder if linear monomials involutions give rise to bent functions $g$ of the form (3.1) or not. The next lemma gives a negative answer.

**Lemma 4.** *Let $n = 2m$ be an even integer and $\lambda_i$ ($1 \leq i \leq 3$) three pairwise distinct elements of $\mathbb{F}_{2^n}^\star$. Set $\lambda_0 := \lambda_1 + \lambda_2 + \lambda_3$. Then there is no 3-tuple $(\lambda_1, \lambda_2, \lambda_3)$ satisfying ${\lambda_i}^{2^m+1} = 1$, for $0 \leq i \leq 3$.*

*Proof.* Let $U$ be the cyclic subgroup of $\mathbb{F}_{2^n}^\star$ of $(2^m+1)$-st roots of unity. By hypothesis $\lambda_i$ belongs to $U$ for all $i$ with $0 \leq i \leq 3$. Set $\lambda_2 = a\lambda_1$ and $\lambda_3 = b\lambda_1$ with $(a,b) \in U^2$. Note that $a \neq b$, $a \neq 1$ and $b \neq 1$. Now we have

$$\begin{aligned}
{\lambda_0}^{2^m+1} = 1 &\iff \lambda_1^{2m+1}(1+a+b)^{2^m+1} = 1 \\
&\iff a^{2^m} + a + b^{2^m} + b + a^{2^m}b + ab^{2^m} = 0 \\
&\iff a^{-1} + a + b^{-1} + b + a^{-1}b + ab^{-1} = 0 \\
&\iff b + a^2b + a + ab^2 + b^2 + a^2 = 0 \\
&\iff (a+b)(1+ab+b+a) = 0 \\
&\iff b(1+a) = 1+a
\end{aligned}$$

leading to a contradiction with $b \neq 1$. Therefore there are no three distinct elements of $U$ such that their sum belongs to $U$. $\square$

Consequently, according to Corollary 2 and Lemma 4, there is no bent function of the form (3.1) with $\phi_i$'s linear monomial involutions.

### 4.3 Bent functions from binomial linear involutions

In this section, we focus on some binomial involutions. Recall the following result given in [12] which characterizes linear binomials that are involutions.

**Proposition 2.** *(Proposition 5, [12])*
*Let $Q(x) = ax^{2^i} + bx^{2^j}$, $a \in \mathbb{F}_2^*$ and $b \in \mathbb{F}_2^*$, where $i < j < n$. Then we have:*

- *For odd $n$, $Q$ can never be an involution.*
- *For even $n$, $n = 2m$, $Q$ is an involution if and only if $j = i + m$ and either*

$$i = 0,\ a^2 + b^{2^m+1} = 1;$$

*or $m$ is even,*

$$i = m/2,\ ab^{2^i} + a^{2^j}b = 1 \quad and \quad a^{2^i+1} + b^{2^j+1} = 0.$$

Using Corollary 2 and the first part of Proposition 2 one deduces the following construction of bent functions.

**Theorem 5.** *Let $n = 2m$ be an even integer. Let $\Phi_1$, $\Phi_2$ and $\Phi_3$ be three linear mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by*

$$\Phi_i(x) = \alpha_i x + \beta_i x^{2^m}$$

*for all $i \in \{0, 1, 2, 3\}$ where $(\alpha_i, \beta_i) \in (\mathbb{F}_{2^n}^\star)^2$ satisfy the following condition (C)*

$${\alpha_i}^2 + {\beta_i}^{2^m+1} = 1$$

*where $\alpha_0 := \alpha_1 + \alpha_2 + \alpha_3$ and $\beta_0 := \beta_1 + \beta_2 + \beta_3$. Then the Boolean function $g$ defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by (3.1) is bent and its dual is given by $\tilde{g}(x, y) = g(y, x)$.*

To prove the existence of bent functions given by Theorem 5, we show that there exist $(\alpha_i, \beta_i) \in (\mathbb{F}_{2^n}^\star)^2$ satisfying condition (C) of Theorem 5. To that end, we use the polar decomposition. Let $x$ be an element of $\mathbb{F}_{2^n}$. The conjugate of $x$ over a subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$ will be denoted by $\bar{x} = x^{2^m}$ and the relative norm with respect to the quadratic field extension $\mathbb{F}_{2^n}/\mathbb{F}_{2^m}$ by $norm(x) = x\bar{x}$. Also, we denote by $U$ the set $\{u \in \mathbb{F}_{2^n} \mid norm(u) = 1\}$, which is the group of $(2^m + 1)$-st roots of unity. Note that since the multiplicative group of the field $\mathbb{F}_{2^n}$ is cyclic and $2^m + 1$ divides $2^n - 1$, the order of $U$ is $2^m + 1$. Finally, note that the unit 1 is the single element in $\mathbb{F}_{2^m}$ of norm one and every non-zero element $x$ of $\mathbb{F}_{2^n}$ has a unique decomposition as: $x = \lambda u$ with $\lambda \in \mathbb{F}_{2^m}$ and $u \in U$.

**Lemma 6.** *If $\beta_1$, $\beta_2$, $\beta_3$, $\alpha_1$, $\alpha_2$, $\alpha_3$ satisfy condition (C) of Theorem 5, then $\beta_{\sigma(1)}$, $\beta_{\sigma(2)}$, $\beta_{\sigma(3)}$, $\alpha_{\sigma(1)}$, $\alpha_{\sigma(2)}$, $\alpha_{\sigma(3)}$ is again a solution for any permutation $\sigma$ of the set $\{1, 2, 3\}$. Up to a permutation of the indices, the only solutions of condition (C) of Theorem 5 are :*

- *either $\beta_1 = a$, $\beta_2 = b$ and $\beta_3 = \frac{ab^{2^m}+c}{(a+b)^{2^m}}$ where $a$, $b$ are two distinct elements of $\mathbb{F}_{2^n}^\star$ and $c$ is an element of $\mathbb{F}_{2^m}$ such that $c \neq ab^{2^m}$;*
- *or $\beta_1 = \beta_2 = a$ and $\beta_3 = b$ where $a$, $b$ are two elements of $\mathbb{F}_{2^n}^\star$.*

*Furthermore, $\alpha_i := \lambda_i + 1$, for $i = 1, 2, 3$, where the $\lambda_i$'s are defined by : $\beta_i = \lambda_i u_1$, with the $\lambda_i$'s in $\mathbb{F}_{2^m}$ and the $u_i$'s in the cyclic group $U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$.*

*Proof.* Note that the condition (C) of Theorem 5 implies the $\alpha_i$'s are in $\mathbb{F}^\star_{2^m}$. Let us now observe that condition (C) is equivalent to

$$\beta_i^{2^m+1} = 1 + \alpha_i^2 \iff \beta_i = (1 + \alpha_i)u_i$$

where $u_i$ belongs to $U$. This proves that $\alpha_i = 1 + \lambda_i$ where $\lambda_i$ is the unique element of $\mathbb{F}_{2^m}$ such that $\beta_i = \lambda_i u_i$ with $u_i \in U$. The last point is to find when the following equality holds :

$$(\alpha_1 + \alpha_2 + \alpha_3)^2 + (\beta_1 + \beta_2 + \beta_3)^{2^m+1} = 1. \tag{4.4}$$

To this end, observe that

$$\begin{aligned}
&(\alpha_1 + \alpha_2 + \alpha_3)^2 + (\beta_1 + \beta_2 + \beta_3)^{2^m+1} \\
&= \alpha_1^2 + \beta_1^{2^m+1} + \alpha_2^2 + \beta_2^{2^m+1} + \alpha_3^2 + \beta_3^{2^m+1} \\
&\quad + \beta_1\beta_2^{2^m} + \beta_1^{2^m}\beta_2 + \beta_1\beta_3^{2^m} + \beta_1^{2^m}\beta_3 + \beta_2\beta_3^{2^m} + \beta_2^{2^m}\beta_3. \\
&= 1 + Tr_m^n\left(\beta_1\beta_2^{2^m} + \beta_3(\beta_1 + \beta_2)^{2^m}\right).
\end{aligned}$$

Therefore

$$\begin{aligned}
(\alpha_1 + \alpha_2 + \alpha_3)^2 + (\beta_1 + \beta_2 + \beta_3)^{2^m+1} = 1 &\iff Tr_m^n\left(\beta_1\beta_2^{2^m} + \beta_3(\beta_1 + \beta_2)^{2^m}\right) = 0 \\
&\iff \beta_1\beta_2^{2^m} + \beta_3(\beta_1 + \beta_2)^{2^m} \in \mathbb{F}_{2^m}.
\end{aligned}$$

If $\beta_2 = \beta_1$, (4.4) is trivially true for any $\beta_1$ since $\beta_1^{2^m+1} \in \mathbb{F}_{2^m}$ for any $\beta_1$, while, if $\beta_2 \neq \beta_1$, (4.4) is satisfied if and only if $\beta_3 = \frac{\beta_1\beta_2^{2^m}+c}{(\beta_1+\beta_2)^{2^m}}$ with $c \in \mathbb{F}_{2^m}$ different from $ab^{2^m}$. $\square$

Using Corollary 2 and the second part of Proposition 2 one deduces the following construction of bent functions.

**Theorem 7.** *Let $n = 4k$ be an integer with $k \in \mathbb{N}^\star$. Let $\Phi_1$, $\Phi_2$ and $\Phi_3$ be three linear mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by*

$$\Phi_i(x) = \alpha_i x^{2^k} + \beta_i x^{2^{3k}}$$

*for all $i \in \{0, 1, 2, 3\}$ where $(\alpha_i, \beta_i) \in (\mathbb{F}^\star_{2^n})^2$ satisfy the following conditions*

1. $\alpha_i\beta_i^{2^k} + \alpha_i^{2^{3k}}\beta_i = 1$;
2. ${\alpha_i}^{2^k+1} + {\beta_i}^{2^{3k}+1} = 0$;

*where $\alpha_0 := \alpha_1 + \alpha_2 + \alpha_3$ and $\beta_0 := \beta_1 + \beta_2 + \beta_3$. Then the Boolean function $g$ defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by (3.1) is bent and its dual is given by $\tilde{g}(x, y) = g(y, x)$.*

The main question remaining in the construction of bent functions derived from Theorem 7 is the existence of $(\alpha_i, \beta_i) \in (\mathbb{F}_{2^n}^\star)^2$ satisfying the conditions 1 and 2. The next lemma gives an answer of the existence's problem.

**Lemma 8.** *Consider the following system* $(S)$ *of equations (4.5) and (4.6) in* $\mathbb{F}_{2^n}^\star$ *where* $n = 4k$ *with* $k \in \mathbb{N}^\star$ *and whose unknowns are* $x$ *and* $y$*:*

$$\begin{cases} xy^{2^k} + x^{2^{3k}} y = 1 & (4.5) \\ x^{2^k+1} + y^{2^{3k}+1} = 0 & (4.6) \end{cases}$$

*Then* $(x, y)$ *be a solution of the system* $(S)$ *if and only if* $x = Auv^{2^{3k}}$ *and* $y = (A+1)uv^{2^k}$ *where* $A \in \mathbb{F}_{2^n}$ *is such that* $A^{2^k} = A + 1$*,* $u \in U_k := \{u \in \mathbb{F}_{2^{4k}} \mid u^{2^k+1} = 1\}$ *and* $v \in U_{2k} := \{u \in \mathbb{F}_{2^{4k}} \mid u^{2^{2k}+1} = 1\}$*.*

*Proof.* Note that $U_k$ is s subgroup of $\mathbb{F}_{2^n}^\star$ since $2^n - 1 = (2^k + 1)(2^{3k} - 2^{2k} + 2^k - 1)$. We have

$$(4.6) \iff y^{2^{3k}+1} = x^{2^k+1} \iff y^{2^k+1} = (x^{2^k})^{2^k+1} \iff \left(\frac{y}{x^{2^k}}\right)^{2^k+1} = 1.$$

Hence, $y = x^{2^k} u$ where $u \in U_k$.

Set $z = xy^{2^k}$. Note that (4.5) can be rewritten as $z + z^{2^{3k}} = 1$. That implies that, raising the preceding equation to the power $2^{2k}$: $z^{2^{2k}} + z^{2^k} = 1$. Summing up the two preceding equations leads to $z^{2^k} + z^{2^{2k}} + z + z^{2^{3k}} = 0$, that is, $Tr_k^{4k}(z) = 0$. Hence $z = \rho + \rho^{2^k}$ for some $\rho \in \mathbb{F}_{2^n}$.

Now, one has

$$1 = z + z^{2^{3k}} = \rho^{2^k} + \rho^{2^{3k}} = (\rho + \rho^{2^{2k}})^{2^k}.$$

Therefore, $z = \rho + \rho^{2^k}$ with $\rho + \rho^{2^{2k}} = Tr_{2k}^{4k}(\rho) = 1$.
Conversely, suppose that $z = \rho + \rho^{2^k}$ with $Tr_{2k}^{4k}(\rho) = 1$. Then,

$$z + z^{2^{3k}} + \rho + \rho^{2^k} + \rho^{2^{3k}} + \rho = (Tr_{2k}^{4k}(\rho))^{2^k} = 1.$$

Basically, the system $(S)$ is equivalent to $y = x^{2^k} u$ and $xy^{2^k} = \rho + \rho^{2^k}$ with $Tr_{2k}^{4k}(\rho) = 1$ and $u \in U_k$.

Set $A = (\rho + \rho^{2^k})^{1/2}$ (where $s^{1/2}$ stands for $s^{2^{n-1}} = s^{2^{4k-1}}$). Observe that

$$A^{2^k} = (\rho^{2^k} + \rho^{2^{2k}})^{1/2} = (1 + \rho + \rho^{2^k})^{1/2} = 1 + A.$$

We therefore have to solve the following system of equations with unknowns $x$ and $y$ in $\mathbb{F}_{2^n}$:

$$\begin{cases} y = x^{2^k} u & (4.7)\\ xy^{2^k} = A^2 & (4.8)\end{cases}$$

where $A^{2^k} = A + 1$ and $u \in U_k$. Raising Equation (4.7) to the power $2^k$, we obtain $y^{2^k} = x^{2^{2k}} u^{2^k} = x^{2^{2k}} u^{-1}$. Dividing Equation (4.8) by the above equation, we obtain $x = \frac{A^2 u}{x^{2^{2k}}}$, that is, $x^{2^{2k}+1} = A^2 u$.

Now, note that $A \in \mathbb{F}_{2^{2k}}$ since $A^{2^{2k}} = (A^{2^k})^{2^k} = (A+1)^{2^k} = A$ and $(u^2)^{2^{2k}} = (u^{2^{2k}})^2 = ((u^{2^k})^{2^k})^2 = ((u^{-1})^{2^k})^2 = u^2$.

Hence $x^{2^{2k}+1} = (Au^{1/2})^{2^{2k}+1}$, equivalently $\left(\frac{x}{Au^{1/2}}\right)^{2^{2k}+1} = 1$, that is, $x = Au^{1/2}v$ with $v \in U_{2k}$ from which we deduce

$$\begin{aligned} y &= x^{2^k} u \\ &= A^{2^k} (u^{2^k})^{1/2} v^{2^k} u \\ &= (A+1) u^{-1/2} u v^{2^k} \\ &= (A+1) u^{1/2} v^{2^k}. \end{aligned}$$

Conversely, suppose $x = Au^{1/2}v$ and $y = (A+1)u^{1/2}v^{2^k}$ where $v \in U_{2k}$, $u \in U_k$ and $A^{2^k} = A + 1$. Then

$$x^{2^k+1} = A^{2^k} A v^{2^k+1} (u^{1/2})^{2^k+1} = A(A+1) v^{2^k+1},$$

and

$$y^{2^{3k}+1} = (A+1)^{2^{3k}} (A+1) (u^{2^{3k}+1})^{1/2} v^{2^k(2^{3k}+1)} = A(A+1) v^{2^k+1}$$

since $(2^{3k}+1) = (2^k+1)(2^{2k}-2^k+1)$ and $A^{2^{3k}} = (A^{2^{2k}})^{2^k} = A^{2^k} = A+1$. Thus $(x, y)$ satisfies Equation (4.6).

Moreover, we have

$$\begin{aligned} xy^{2^k} &= Au^{1/2} v (A+1)^{2^k} u^{2^k/2} v^{2^{2k}} \\ &= A(A+1)^{2^k} u^{(2^k+1)/2} v^{2^{2k}+1} \\ &= A(A+1)^{2^k} = A(A^{2^k}+1) = A^2. \end{aligned}$$

and

$$\begin{aligned} x^{2^{3k}} y &= A^{2^{3k}} u^{2^{3k}/2} v^{2^{3k}} (A+1) u^{1/2} v^{2^k} \\ &= A^{2^{3k}} (A+1) u^{(2^{3k}+1)/2} (v^{2^{2k}+1})^{2^k} \\ &= (A+1)(a+1) = A^2+1. \end{aligned}$$

Thus $(x, y)$ satisfies Equation (4.5), which completes the proof.

□

We can deduce from Lemma 8 that there exist $\alpha_1$, $\alpha_2$, $\alpha_3$, $\beta_1$, $\beta_2$ and $\beta_3$ satisfying conditions 1. and 2. of Theorem 7:

$$\alpha_i = A_i \tilde{u} v^{2^{3k}}, \beta_i = (A_i+1)\tilde{u} v^{2^k}$$

where $A_i^{2^k} = A_i + 1$, $\tilde{u} \in U_k := \{u \in \mathbb{F}_{2^{4k}} \mid u^{2^k+1} = 1\}$ and $v \in U_{2k} := \{u \in \mathbb{F}_{2^{4k}} \mid u^{2^{2k}+1} = 1\}$. By Lemma 8, $\alpha_1$, $\alpha_2$, $\alpha_3$, $\beta_1$, $\beta_2$ and $\beta_3$ satisfy conditions 1 and 2 of Theorem 7. But above, $\alpha_0 := \alpha_1 + \alpha_2 + \alpha_3 = (A_1 + A_2 + A_3)\tilde{u} v^{2^{3k}}$ and $\beta_0 := \beta_1 + \beta_2 + \beta_3 = (A_1 + A_2 + A_3 + 1)\tilde{u} v^{2^k}$. Clearly, $(A_1 + A_2 + A_3)^{2^k} = A_1 + A_2 + A_3 + 1$ and therefore $\alpha_0$ and $\beta_0$ satisfy also conditions 1 and 2 of Theorem 7.

**Acknowledgement.** The author thanks Gérard Cohen and David Madore for interesting discussions. She also thanks Pascale Charpin and Sumanta Sarkar for attractive discussions on involutions.

# References

[1] Budaghyan, L., Carlet, C., Helleseth, T., Kholosha, A., and Mesnager, S.: Further results on Niho bent functions. *IEEE Transactions on Information Theory*, 58(11), pages 6979-6985 (2012)

[2] Canteaut, A., Charpin, P., and Kyureghyan. G.: A new class of monomial bent functions. *Finite Fields and Their Applications*, 14(1), pages 221-241 (2008)

[3] Carlet, C.: Two new classes of bent functions.: In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 77-101 (1994)

[4] Carlet, C.: A construction of bent function.: In *Proceedings of the Third International Conference on Finite Fields and Applications*, pages 47-58. Cambridge University Press (1996)

[5] Carlet, C.: On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Berlin Heidelberg. 1-28 (2006)

[6] Carlet, C.: 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. 257-397 (2010)

[7] C. Carlet.: Open problems on binary bent functions. Proceeding of the conference *Open problems in mathematical and computational sciences*, Sept. 18-20, 2013, in Istanbul, Turkey, pp. 203-241, Springer (2014)

[8] Carlet, C., and Mesnager. S.: On Dillon's class H of bent functions, Niho bent functions and O-polynomials. *Journal of Combinatorial Theory, Series A*, 118(8), pages 2392-2410 (2011)

[9] Carlet, C., and Mesnager, S.: Four decades of research on bent functions. Journal Designs, Codes and Cryptography (to appear)

[10] Charpin, P., and Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans. Inform. Theory, 54(9), pages 4230-4238 (2008)

[11] Charpin, P., and Kyureghyan, G.: Cubic monomial bent functions: A subclass of $\mathcal{M}$. *SIAM Journal on Discrete Mathematics*, 22(2), pages 650-665 (2008)

[12] Charpin, P., Mesnager, S., and Sarkar, S.: On involutions of finite fields. In Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT (2015)

[13] J. Dillon.: *Elementary Hadamard difference sets.* PhD thesis, University of Maryland (1974)

[14] Dillon, J., and Dobbertin, H.: New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3), pages 342-389 (2004)

[15] Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., and Gaborit, P.: Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, 113, pages 779-798 (2006)

[16] Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Transactions on Information Theory*, 14(1), pages 154-156 (1968)

[17] G. Kyureghyan. Constructing permutations of finite fields via linear translators. *Journal of Combinatorial Theory Series A*, 118(3):1052–1061, 2011.

[18] Leander, G.: Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2), pages 738-743 (2006)

[19] Leander, G., and Kholosha, A.: Bent functions with $2^r$ Niho exponents. *IEEE Transactions on Information Theory*, 52(12), pages 5529-5532 (2006)

[20] Li, N., Helleseth, T., Tang, X., and Kholosha, A.: Several new classes of bent functions from Dillon exponents. *IEEE Transactions on Information Theory*, 59(3), pages 1818-1831 (2013)

[21] McFarland, R. L.: A family of noncyclic difference sets. *Journal of Combinatorial Theory, Series A*, 15, pages 1-10 1(973)

[22] Mesnager, S.: A new family of hyper-bent boolean functions in polynomial form. *Proceedings of Twelfth International Conference on Cryptography and Coding*, IMACC 2009, LNCS 5921, pages 402-417, Springer, Heidelberg (2009)

[23] Mesnager, S.: Hyper-bent boolean functions with multiple trace terms. *Proceedings of International Workshop on the Arithmetic of Finite Fields*, WAIFI 2010, LNCS 6087, pages 97-113. Springer, Heidelberg (2010)

[24] Mesnager, S.: Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. *IEEE Transactions on Information Theory*, 57(9), pages 5996-6009 (2011)

[25] Mesnager, S.: A new class of bent and hyper-bent boolean functions in polynomial forms. *Designs, Codes and Cryptography*, 59(1-3), pages 265-279 (2011)

[26] Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory. 60(7), 4397-4407 (2014)

[27] Mesnager, S.: Further constructions of infinite families of bent functions from new permutations and their duals. Journal of Cryptography and Communications (CCDS), Springer (to appear)

[28] Mesnager, S.: Bent functions: fundamentals and results. Springer 2015 (to appear)

[29] Mesnager, S., Cohen. G., and Madore. D.: On existence (based on an arithmetical problem) and constructions of bent functions. Proceedings of the fifteenth International Conference on Cryptography and Coding, Oxford, United Kingdom, IMACC 2015, LNCS, Springer, Heidelberg, 2015 (to appear)

[30] Mesnager, S and Flori, J. P.: Hyper-bent functions via Dillon-like exponents. *IEEE Transactions on Information Theory*, 59(5), pages 3215-3232, (2013)

[31] Rothaus, O.S.: On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20:300–305 (1976).

[32] Yu, N.Y and Gong, G.: Construction of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 52(7), pages 3291-3299, (2006)