Construction of Some New Classes of Boolean Bent Functions and Their Duals

P. L. Sharma* and Neetu Dhiman

Department of Mathematics and Statistics
Himachal Pradesh University, Shimla 171 005, India
* Corresponding author

Copyright © 2016 P. L. Sharma and Neetu Dhiman. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Bent functions have maximum nonlinearity from the set of all affine functions and are extensively used in the design of stream ciphers and block ciphers. These functions also have significant applications in coding theory, graph theory and sequence design. In the literature of bent functions their complete classification and characterization is still elusive, so the constructions and characterizations of bent functions are challenging problems. Many constructions methods and characterizations of bent functions are discussed in the literature. In this paper we obtain some new infinite families of bent functions and their duals.

Mathematics Subject Classification: 94A60, 06E30, 11T71

Keywords: Boolean functions, Walsh-Hadamard transform, Bent functions, Dual bent functions

1 Introduction

Bent functions were introduced by Rothaus [15] in 1976. Bent functions are the Boolean functions with the highest possible nonlinearity from the set of all affine functions and exist only for even number of variables. Kumar et al. [9] extended Rothaus’s definition of bent functions to generalized bent functions and also discussed their properties. Since 1974, bent functions are extensively
P. L. Sharma and Neetu Dhiman studied because of their significant applications in cryptography (in the design of stream ciphers and in the substitution boxes of block ciphers) [2], coding theory [11], sequence design [14] and graph theory [6,18]. Bent functions are not balanced. A complete classification and characterization of bent functions is still elusive, so the construction and characterization of bent functions are challenging problems. In the recent time most of the research work have been done on the construction of bent functions. Primary and secondary constructions of bent functions are the two kinds of construction of bent functions. In the primary construction, there is no use of previously existing bent functions to construct new ones, while in secondary construction some previously known bent functions are used to construct new bent functions, see [1,5,7,8]. Some constructions and characterizations of bent functions are discussed in [16,17]. Bent functions always occur in pairs and their duals are also bent. Bent functions have two subclasses; self dual bent functions and anti-self dual bent functions, see [3].

Some new constructions of bent functions are recently introduced by Mesnager [12]. We here present some new constructions of bent functions. Any function \( f(x) : \mathbb{F}_{2^n} \to \mathbb{F}_2 \) is called a Boolean function. Let \( n = 2m \) be a positive integer and \( \mathbb{F}_{2^n} \) be the finite field with \( 2^n \) elements. Let \( \mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\} \). For any positive integer \( n \), and \( r \) dividing \( n \), the trace function from \( \mathbb{F}_{2^n} \to \mathbb{F}_r \), denoted by \( \text{Tr}_{n}^{r}(x) \), is the mapping defined for every \( x \in \mathbb{F}_{2^n} \) as:

\[
\text{Tr}_{n}^{r}(x) = \sum_{i=0}^{n-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \ldots + x^{2^{n-r}}.
\]

In particular, the absolute trace occurs for \( r = 1 \). In deriving our results we use some known properties of the trace function such as \( \text{Tr}_{1}^{r}(x) = \text{Tr}_{1}^{r}(x^2) \) and for every integer \( r \) dividing \( n \), the transitivity property of \( \text{Tr}_{n}^{r} \), that is \( \text{Tr}_{1}^{n} = \text{Tr}_{1}^{r} \circ \text{Tr}_{n}^{r} \). The Walsh-Hadamard transform of a Boolean function \( f : \mathbb{F}_{2^n} \to \mathbb{F}_2 \) is the function \( \hat{\chi}_f : \mathbb{F}_{2^n} \to \mathbb{Z} \) defined by

\[
\hat{\chi}_f(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\text{Tr}_{n}^{r}(wx)}, \text{ for all } w \in \mathbb{F}_{2^n}.
\]

The values \( \hat{\chi}_f(w) \), for all \( w \in \mathbb{F}_{2^n} \) are called the Walsh coefficients of \( f \) and the multiset \( \{\hat{\chi}_f(w), w \in \mathbb{F}_{2^n}\} \) is called the Walsh spectrum of a Boolean function \( f \). If \( n \) is even, a Boolean function \( f : \mathbb{F}_{2^n} \to \mathbb{F}_2 \) is said to be bent if \( \hat{\chi}_f(w) = \pm 2^{n/2} \), for all \( w \in \mathbb{F}_{2^n} \) and \( f \) is said to be semi-bent if \( \hat{\chi}_f(w) = \{0, \pm 2^{n/2-1}\} \) for all \( w \in \mathbb{F}_{2^n} \). For a bent function with \( n \) variables, its dual is denoted by \( \tilde{f} \) and is defined by the equation

\[
(-1)^{\tilde{f}(x)}2^{n/2} = \hat{\chi}_f(x).
\]
The first derivative of a Boolean function $f(x)$ in the direction of $\alpha \in \mathbb{F}_{2^n}$ is defined as
$$D_{\alpha}(x) = f(x) + f(x + \alpha).$$

The second order derivative of $f(x)$ with respect to $(\alpha, \beta) \in \mathbb{F}_{2^n}^2$ is defined as
$$D_\beta D_{\alpha}f(x) = f(x) + f(x + \alpha) + f(x + \beta) + f(x + \alpha + \beta).$$

## 2 Main Results

**Lemma 2.1.** Let $h(x)$ be a bent function defined on $\mathbb{F}_{2^n}$ whose dual function $\tilde{h}(x)$ has a null second order derivative with respect to $a, b, c \in \mathbb{F}_{2^n}$ such that $a \neq b \neq c$. Then the Boolean function $g'(x)$ defined by
$$g'(x) = h(x) + Tr^n_1(ax)Tr^n_1(bx) + Tr^n_1(ax)Tr^n_1(cx), \quad \text{for all } x \in \mathbb{F}_{2^n}$$
is a bent function and its dual bent function $\tilde{g}'(x)$ is given by
$$\tilde{g}'(x) = \tilde{h}(x)\tilde{h}(x + a) + \tilde{h}(x + a)\tilde{h}(x + b + c) + \tilde{h}(x)\tilde{h}(x + b + c).$$

**Proof.** Let $a_i(x)$ be defined by
$$a_i(x) = h(x) + Tr^n_1(\lambda_i x) \quad \text{for } i \in \{1, 2, 3\}$$
and the Boolean function $g(x)$ be defined by
$$g(x) = h(x) + Tr^n_1(\lambda_1 x)Tr^n_1((\lambda_1 + a)x) + Tr^n_1(\lambda_1 x)Tr^n_1((\lambda_1 + b + c)x)$$
$$+ Tr^n_1((\lambda_1 + a)x)Tr^n_1((\lambda_1 + b + c)x)$$
$$= h(x) + Tr^n_1(\lambda_1 x)Tr^n_1(\lambda_1 x) + Tr^n_1(\lambda_1 x)Tr^n_1(ax) + Tr^n_1(\lambda_1 x)Tr^n_1(\lambda_1 x)$$
$$+ Tr^n_1(\lambda_1 x)Tr^n_1(bx) + Tr^n_1(\lambda_1 x)Tr^n_1(cx)$$
$$+ Tr^n_1(\lambda_1 x)Tr^n_1(ax) + Tr^n_1(\lambda_1 x)Tr^n_1(bx) + Tr^n_1(\lambda_1 x)Tr^n_1(cx)$$
$$= h(x) + Tr^n_1(ax)Tr^n_1(bx) + Tr^n_1(ax)Tr^n_1(cx) + Tr^n_1(\lambda_1 x)$$
$$= g'(x) + Tr^n_1(\lambda_1 x).$$
Since \( h \) is bent, therefore, the functions \( a_i(x), i \in \{1, 2, 3\} \) and \( a_4(x) = \sum_{i=1}^{3} a_i(x) \) are also bent. Therefore, by Theorem 4 [12], the Boolean function \( g(x) \) is bent if
\[
\tilde{h}(x + \lambda_1) + \tilde{h}(x + \lambda_2) + \tilde{h}(x + \lambda_3) + \tilde{h}(x + \lambda_1 + \lambda_2 + \lambda_3) = 0. \tag{2.2}
\]
Substituting above defined values of \( \lambda_1, \lambda_2 \) and \( \lambda_3 \) in equation (2.2), we get
\[
\tilde{h}(x + \lambda_1) + \tilde{h}(x + \lambda_1 + a) + \tilde{h}(x + \lambda_1 + b + c) + \tilde{h}(x + \lambda_1 + a + \lambda_1 + b + c) = 0
\]
\[
\Rightarrow \tilde{h}(x + \lambda_1) + \tilde{h}(x + \lambda_1 + a) + \tilde{h}(x + \lambda_1 + b + c) + \tilde{h}(x + \lambda_1 + a + b + c) = 0
\]
\[
\Leftrightarrow D_{b+c}D_a \tilde{h}(x + \lambda_1 + a + b + c) = 0
\]
\[
\Leftrightarrow D_{b+c}D_a \tilde{h}(x) = 0.
\]
Also
\[
\sum_{i=1}^{4} \tilde{a}_i(x) = 0, \text{ for all } x \in \mathbb{F}_{2^n},
\]
where \( \tilde{a}_i(x) \) denotes the dual function of bent functions \( a_i(x) \). Thus the conditions of Theorem 4 [12] are fulfilled. Therefore, \( g(x) \) is a bent function and hence \( g'(x) \) is bent.

According to Theorem 4 [12], the dual function \( \tilde{g}(x) \) of \( g(x) \) is given by
\[
\tilde{g}(x) = \tilde{h}(x + \lambda_1)\tilde{h}(x + \lambda_2) + \tilde{h}(x + \lambda_2)\tilde{h}(x + \lambda_3) + \tilde{h}(x + \lambda_1)\tilde{h}(x + \lambda_3).
\]
On substituting values of \( \lambda_1, \lambda_2 \) and \( \lambda_3 \) in above equation, we get
\[
\tilde{g}(x) = \tilde{h}(x + \lambda_1)\tilde{h}(x + \lambda_1 + a) + \tilde{h}(x + \lambda_1 + a) + \tilde{h}(x + \lambda_1 + b + c) + \tilde{h}(x + \lambda_1 + b + c).
\]
Since the duals of \( g(x) \) and \( g'(x) \) are linked by the relation
\[
\tilde{g}'(x) = \tilde{g}(x + \lambda_1).
\]
So
\[
\tilde{g}'(x) = \tilde{h}(x)\tilde{h}(x + a) + \tilde{h}(x + a)\tilde{h}(x + b + c) + \tilde{h}(x)\tilde{h}(x + b + c).
\]
3 Infinite families of Bent functions via Kasami function and Niho exponents.

Let $h(x)$ be the monomial Niho quadratic bent function defined as

$$h(x) : x \in \mathbb{F}_{2^n} \rightarrow Tr_m^1(\lambda x^{2^m+1}),$$

(3.1)

where $\lambda \in \mathbb{F}_{2^n}^*$, $x \in \mathbb{F}_{2^n}$ and $n = 2m$, $m$ be a positive integer. The dual function $\tilde{h}(x)$ of $h(x)$ is discussed in [13] as

$$\tilde{h}(x) = Tr_m^1(\lambda^{-1}x^{2^m+1}) + 1.$$  

(3.2)

In the following theorem we have constructed a new infinite family of bent functions from Kasami bent function $h(x)$.

**Theorem 3.1.** Let $n = 2m$ be a positive integer and $\lambda \in \mathbb{F}_{2^n}^*$. Let $a, b, c \in \mathbb{F}_{2^n}$ be such that $Tr_m^1(\lambda^{-1}a^{2^m}b) = Tr_m^1(\lambda^{-1}a^{2^m}c)$. Then the Boolean function $f(x)$ defined on $\mathbb{F}_{2^n}$ as

$$f(x) = Tr_m^1(\lambda x^{2^m+1}) + Tr_m^1(ax)Tr_m^1(bx) + Tr_m^1(ax)Tr_m^1(cx)$$

is a bent function and its dual function $\tilde{f}(x)$ is given by

$$\tilde{f}(x) = 1 + h'(x) + (h'(a) + Tr_m^1(\lambda^{-1}a^{2^m}x))(h'(b) + h'(c) + Tr_m^1(\lambda^{-1}b^{2^m}x) + Tr_m^1(\lambda^{-1}c^{2^m}x) + Tr_m^1(\lambda^{-1}(b^{2^m}c + bc^{2^m})).$$

**Proof.** Let $h(x)$ and $\tilde{h}(x)$ be as defined in (3.1) and (3.2) respectively. The derivative of $\tilde{h}(x)$ in the direction of $a \in \mathbb{F}_{2^n}$ is

$$D_a\tilde{h}(x) = Tr_m^1(\lambda^{-1}x^{2^m+1}) + Tr_m^1(\lambda^{-1}(x+a)^{2^m+1})$$

$$= Tr_m^1(\lambda^{-1}x^{2^m+1}) + Tr_m^1(\lambda^{-1}(x^{2^m+1} + a^{2^m+1} + x^{2^m}a + xa^{2^m}))$$

$$= Tr_m^1(\lambda^{-1}x^{2^m+1}) + Tr_m^1(\lambda^{-1}x^{2^m+1}) + Tr_m^1(\lambda^{-1}a^{2^m+1})$$

$$+ Tr_m^1(\lambda^{-1}(x^{2^m}a + xa^{2^m}))$$

$$= Tr_m^1(\lambda^{-1}a^{2^m+1}) + Tr_m^1(\lambda^{-1}(Tr_m^1(a^{2^m}x)))$$

$$= Tr_m^1(\lambda^{-1}a^{2^m+1}) + Tr_m^1(Tr_m^1(\lambda^{-1}(a^{2^m}x)))$$

$$= Tr_m^1(\lambda^{-1}a^{2^m+1}) + Tr_m^1(\lambda^{-1}(a^{2^m}x)).$$

The second order derivative of $\tilde{h}(x)$ with respect to “$b + c$” is given by

$$D_{b+c}D_a\tilde{h}(x) = Tr_m^1(\lambda^{-1}a^{2^m+1}) + Tr_m^1(\lambda^{-1}(a^{2^m}x))$$

$$+ Tr_m^1(\lambda^{-1}a^{2^m+1}) + Tr_m^1(\lambda^{-1}(a^{2^m}(x + b + c)))$$

$$= Tr_m^1(\lambda^{-1}(a^{2^m}x)) + Tr_m^1(\lambda^{-1}(a^{2^m}x))$$

$$+ Tr_m^1(\lambda^{-1}(a^{2^m}b)) + Tr_m^1(\lambda^{-1}(a^{2^m}c))$$

$$= Tr_m^1(\lambda^{-1}(a^{2^m}b)) + Tr_m^1(\lambda^{-1}(a^{2^m}c)).$$
Since $a, b$ and $c$ are such that $Tr_1^m(\lambda^{-1}(a^{2m}b)) = Tr_1^m(\lambda^{-1}(a^{2m}c))$. Therefore,

$$D_{b+c}D_a\tilde{h}(x) = 0.$$ 

So, by Lemma 2.1 $f(x)$ is a bent function. The dual of $f(x)$ is given by

$$\tilde{f}(x) = \tilde{h}(x)\tilde{h}(x+a) + \tilde{h}(x+a)\tilde{h}(x+b+c) + \tilde{h}(x)\tilde{h}(x+b+c)$$

$$= (Tr_1^m(\lambda^{-1}x^{2m+1}) + 1)(Tr_1^m(\lambda^{-1}(x+a)^{2m+1}) + 1)$$

$$+ (Tr_1^m(\lambda^{-1}(x+a)^{2m+1}) + 1)(Tr_1^m(\lambda^{-1}(x+b+c)^{2m+1}) + 1)$$

$$+ (Tr_1^m(\lambda^{-1}x^{2m+1}) + 1)(Tr_1^m(\lambda^{-1}(x+b+c)^{2m+1}) + 1). \quad (3.3)$$

Let $h'(x)$ be defined on $\mathbb{F}_{2^n}$ as

$$h'(x) = Tr_1^m(\lambda^{-1}x^{2m+1}). \quad (3.4)$$

Now

$$Tr_1^m(\lambda^{-1}(x+a)^{2m+1}) = Tr_1^m(\lambda^{-1}(x^{2m+1} + a^{2m+1} + x^{2m}a + xa^{2m}))$$

$$= Tr_1^m(\lambda^{-1}x^{2m+1}) + Tr_1^m(\lambda^{-1}a^{2m+1})$$

$$+ Tr_1^m(\lambda^{-1}(Tr_1^m(a^{2m}x)))$$

$$= h'(x) + h'(a) + Tr_1^m(\lambda^{-1}(a^{2m}x)) \quad (3.5)$$

and

$$Tr_1^m(\lambda^{-1}(x+b+c)^{2m+1}) = Tr_1^m(\lambda^{-1}(x^{2m+1} + b^{2m+1} + c^{2m+1} + x^{2m}b + x^{2m}c + bx^{2m} + xc^{2m} + bc^{2m}))$$

$$= Tr_1^m(\lambda^{-1}x^{2m+1}) + Tr_1^m(\lambda^{-1}b^{2m+1}) + Tr_1^m(\lambda^{-1}c^{2m+1})$$

$$+ Tr_1^m(\lambda^{-1}(Tr_1^m(b^{2m}x)))$$

$$= h'(x) + h'(b) + h'(c) + Tr_1^m(\lambda^{-1}(b^{2m}x))$$

$$+ Tr_1^m(\lambda^{-1}(c^{2m}x)) + Tr_1^m(\lambda^{-1}(b^{2m}c + bc^{2m}))$$

$$= h'(x) + h'(b) + h'(c) + Tr_1^m(\lambda^{-1}(b^{2m}x))$$

$$+ Tr_1^m(\lambda^{-1}(c^{2m}x)) + Tr_1^m(\lambda^{-1}(b^{2m}c + bc^{2m})). \quad (3.6)$$

Using (3.4) - (3.6) in (3.3), we get

$$\tilde{f}(x) = (h'(x) + 1)(h'(x) + h'(a) + Tr_1^m(\lambda^{-1}a^{2m}x) + 1)$$

$$+ (h'(x) + h'(a) + Tr_1^m(\lambda^{-1}a^{2m}x) + 1)$$

$$+ (h'(x) + h'(b) + h'(c) + Tr_1^m(\lambda^{-1}b^{2m}x)$$

$$+ Tr_1^m(\lambda^{-1}c^{2m}x) + Tr_1^m(\lambda^{-1}(b^{2m}c + bc^{2m})) + 1)$$

$$+ ((h'(x) + 1)(h'(x) + h'(b) + h'(c)$$

$$+ Tr_1^m(\lambda^{-1}b^{2m}x) + Tr_1^m(\lambda^{-1}c^{2m}x$$

$$+ Tr_1^m(\lambda^{-1}(b^{2m}c + bc^{2m})))) + 1)$$
Construction of some new classes of Boolean bent functions

\( h'(x)h'(x) + h'(x)h'(a) + h'(x)T_{r_1}^n(\lambda^{-1} a^{2^m} x) \\
+ h'(x) + h'(x) + h'(a) \\
+ T_{r_1}^n(\lambda^{-1} a^{2^m} x) + 1 + h'(x)h'(x) + h'(x)h'(b) \\
+ h'(x)h'(c) + h'(x)T_{r_1}^n(\lambda^{-1} b^{2^m} x) \\
+ h'(x)T_{r_1}^n(\lambda^{-1} c^{2^m} x) + h'(x)T_{r_1}^m(\lambda^{-1} (b^{2^m} c + bc^{2^m})) \\
+ h'(x) + h'(a)h'(b) + h'(a)h'(c) \\
+ h'(a)T_{r_1}^n(\lambda^{-1} b^{2^m} x) + h'(a)T_{r_1}^n(\lambda^{-1} c^{2^m} x) \\
+ h'(a)T_{r_1}^m(\lambda^{-1} (b^{2^m} c + bc^{2^m})) + h'(a) \\
+ T_{r_1}^n(\lambda^{-1} a^{2^m} x)h'(x) + T_{r_1}^n(\lambda^{-1} a^{2^m} x)h'(b) \\
+ T_{r_1}^n(\lambda^{-1} a^{2^m} x)h'(c) + T_{r_1}^n(\lambda^{-1} a^{2^m} x)T_{r_1}^n(\lambda^{-1} b^{2^m} x) \\
+ T_{r_1}^n(\lambda^{-1} a^{2^m} x)T_{r_1}^n(\lambda^{-1} c^{2^m} x) + T_{r_1}^n(\lambda^{-1} a^{2^m} x)T_{r_1}^m(\lambda^{-1} a^{2^m} x) + T_{r_1}^n(\lambda^{-1} b^{2^m} x) \\
+ h'(b) + h'(c) + T_{r_1}^n(\lambda^{-1} b^{2^m} x) + T_{r_1}^n(\lambda^{-1} c^{2^m} x) + T_{r_1}^m(\lambda^{-1} (b^{2^m} c + bc^{2^m})) \\
+ 1 + h'(x)h'(x) + h'(x)h'(b) + h'(x)h'(c) + h'(x)T_{r_1}^n(\lambda^{-1} b^{2^m} x) \\
+ h'(x)T_{r_1}^n(\lambda^{-1} c^{2^m} x) + h'(x) + h'(a) + h'(c) \\
+ T_{r_1}^n(\lambda^{-1} b^{2^m} x) + T_{r_1}^n(\lambda^{-1} c^{2^m} x) + T_{r_1}^m(\lambda^{-1} b^{2^m} c + bc^{2^m})) + 1 \\
= h'(a)h'(b) + h'(a)h'(c) + h'(a)T_{r_1}^n(\lambda^{-1} b^{2^m} x) + h'(a)T_{r_1}^n(\lambda^{-1} c^{2^m} x) \\
+ h'(a)T_{r_1}^m(\lambda^{-1} b^{2^m} c + bc^{2^m})) + h'(b) + h'(a)T_{r_1}^n(\lambda^{-1} a^{2^m} x) \\
+ h'(c)T_{r_1}^n(\lambda^{-1} a^{2^m} x) + T_{r_1}^n(\lambda^{-1} a^{2^m} x)T_{r_1}^n(\lambda^{-1} b^{2^m} x) \\
+ T_{r_1}^n(\lambda^{-1} a^{2^m} x)T_{r_1}^n(\lambda^{-1} c^{2^m} x) + T_{r_1}^n(\lambda^{-1} a^{2^m} x)T_{r_1}^m(\lambda^{-1} (b^{2^m} c + bc^{2^m})) \\
+ h'(x)h'(x) + 1 \\
= 1 + h'(x) + (h'(a) + T_{r_1}^n(\lambda^{-1} a^{2^m} x)) \\
(\lambda^{-1} b^{2^m} x) + T_{r_1}^n(\lambda^{-1} c^{2^m} x) + T_{r_1}^m(\lambda^{-1} (b^{2^m} c + bc^{2^m})).

Example 3.2. Let \( m = 2, n = 4 \) and \( \alpha \) be the primitive element over \( \mathbb{F}_{16} \) such that \( \alpha^4 + \alpha + 1 = 0 \). Let \( \lambda = \alpha, a = \alpha^{10}, b = \alpha^{4}, c = \alpha^{2} \) such that \( T_{r_1}^n(\lambda^{-1} a^{4} b) = T_{r_1}^n(\lambda^{-1} a^{4} c) \), then the Boolean function \( f(x) \) defined by

\[
 f(x) = T_{r_1}^m(\lambda x^{2^m+1}) + T_{r_1}^n(\alpha^{10} x)T_{r_1}^4(\alpha^{4} x) + T_{r_1}^4(\alpha^{10} x)T_{r_1}^4(\alpha^{2} x)
\]

is a bent function.

The bent function, given by Leander and Kholosha [10], defined on \( \mathbb{F}_{2^n} \) via 2\( n \) Niho exponents by with \( r > 1 \) satisfying \( gcd(r, m) = 1 \) and \( a \in \mathbb{F}_{2^n} \) such that \( a + a^{2^m} = 1 \). For \( a \in \mathbb{F}_{2^n} \) such that \( a + a^{2^m} = 1 \), we have

\[
 T_{r_1}^n(ax^{2^m+1}) = T_{r_1}^m(x^{2^m+1}T_{r_1}^n(a)) = T_{r_1}^m(x^{2^m+1}).
\]

So, \( h(x) \) can be written as

\[
 h(x) = T_{r_1}^m(x^{2^m+1}) + T_{r_1}^n\left( \sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)i+1} \right). \quad (3.7)
\]
For any $u \in \mathbb{F}_{2^n}$ with $u + u^{2^m} = 1$, dual function $\overline{h}(x)$ of $h(x)$ is discussed in [4] as

$$\overline{h}(x) = Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m})(1 + x + x^{2^m})^{1/2^{r-1}} \right\}. \quad (3.8)$$

**Theorem 3.3.** Let $a, b, c$ be three pairwise distinct elements of $\mathbb{F}_{2^m}$. A Boolean function $f(x)$ defined on $\mathbb{F}_{2^n}$ as

$$f(x) = Tr_1^m (x^{2^{m+1}}) + Tr_1^n \left( \sum_{i=1}^{2^{r-1}-1} x^{(2^{m-1})} \right) + Tr_1^n(ax)Tr_1^n(bx) + Tr_1^n(ax)Tr_1^n(cx)$$

is a bent function and its dual is

$$\overline{f}(x) = Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m})(1 + x + x^{2^m})^{1/2^{r-1}} \right\}$$

$$+ Tr_1^m \left\{ (a + b + c)(1 + x + x^{2^m})^{1/2^{r-1}} \right\} +$$

$$Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m} + a)(1 + x + x^{2^m})^{1/2^{r-1}} \right\}$$

$$+ Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m} + b + c)(1 + x + x^{2^m})^{1/2^{r-1}} \right\}.$$

**Proof.** For $a \in \mathbb{F}_{2^m}$, we have

$$a^{2^m} = a$$

$$1 + (x + a) + (x + a)^{2^m} = 1 + x + x^{2^m}.$$

Consider

$$D_a \overline{h}(x) = Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m})(1 + x + x^{2^m})^{1/2^{r-1}} \right\}$$

$$+ Tr_1^m \left\{ (u(1 + (x + a) + (x + a)^{2^m}) + u^{2^{n-r}} + + (x + a)^{2^m})(1 + (x + a) + (x + a)^{2^m})^{1/2^{r-1}} \right\}$$

$$= Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m})(1 + x + x^{2^m})^{1/2^{r-1}} \right\}$$

$$+ Tr_1^m \left\{ (u(1 + x + x^{2^m}) + u^{2^{n-r}} + x^{2^m} + a^{2^m})(1 + x + x^{2^m})^{1/2^{r-1}} \right\}$$

$$= Tr_1^m \left\{ a^{2^m}(1 + x + x^{2^m})^{1/2^{r-1}} \right\}$$

$$= Tr_1^m \left\{ a(1 + x + x^{2^m})^{1/2^{r-1}} \right\}. \quad (3.9)$$

For $b, c \in \mathbb{F}_{2^m}$, we have

$$1 + (x + b + c) + (x + b + c)^{2^m} = 1 + (x + b + c) + x^{2^m} + b^{2^m} + c^{2^m}$$

$$= 1 + x + b + c + x^{2^m} + b + c$$

$$= 1 + x + x^{2^m}.$$
So,

\[
D_a \tilde{h}(x + b + c) = Tr^m_1 \left\{ \begin{array}{l}
(u(1 + (x + b + c) + (x + b + c)^{2^n}) \\
+ u^{2^{n-r}} + (x + b + c)^{2^n} \\
(1 + (x + b + c) + (x + b + c)^{2^n})^{1 \over \varphi - 1}
\end{array} \right\} + Tr^m_1 \left\{ \begin{array}{l}
(u(1 + (x + a + b + c) \\
+ (x + a + b + c)^{2^n}) \\
+ u^{2^{n-r}} + (x + a + b + c)^{2^n} \\
(1 + (x + a + b + c)^{2^n})^{1 \over \varphi - 1}
\end{array} \right\}
\]

\[
= Tr^m_1 \left\{ \begin{array}{l}
(u(1 + x + x^{2^n}) + u^{2^{n-r}} + x^{2m} \\
+ b + c)(1 + x + x^{2^n})^{1 \over \varphi - 1}
\end{array} \right\}
\]

\[
+ Tr^m_1 \left\{ \begin{array}{l}
(u(1 + x + x^{2^n}) + u^{2^{n-r}} + x^{2m} \\
+ a + b + c)(1 + x + x^{2^n})^{1 \over \varphi - 1}
\end{array} \right\}
\]

\[
= Tr^m_1 \left\{ a(1 + x + x^{2^n})^{1 \over \varphi - 1} \right\}. \quad (3.10)
\]

From (3.9) and (3.10), we have

\[
D_a \tilde{h}(x) = D_a \tilde{h}(x + b + c).
\]

That is

\[
\tilde{h}(x) + \tilde{h}(x + a) = \tilde{h}(x + b + c) + \tilde{h}(x + a + b + c). \quad (3.11)
\]

Now

\[
D_{b+c}D_a \tilde{h}(x) = D_{b+c} \left\{ \tilde{h}(x) + \tilde{h}(x + a) \right\}
\]

\[
= \tilde{h}(x) + \tilde{h}(x + a) + \tilde{h}(x + b + c) + \tilde{h}(x + a + b + c).
\]

Using (3.11), we get

\[
D_{b+c}D_a \tilde{h}(x) = 0.
\]

Therefore, by Lemma 2.1, \( f(x) \) is a bent function. The dual of a function \( f(x) \) is given as

\[
\tilde{f}(x) = \tilde{h}(x)\tilde{h}(x + a) + \tilde{h}(x + a)\tilde{h}(x + b + c) + \tilde{h}(x)\tilde{h}(x + b + c), \quad (3.12)
\]

where \( h(x) \) is defined by (3.7).
So,

\[
\tilde{h}(x)\tilde{h}(x + a) = Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m} + a)}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= \left[ Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\} \right]^2 + Tr_1^m \left\{ a(1 + x + x^{2m})^{\frac{1}{2-r}} \right\}
\]

\[
Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\} \]

(3.13)

\[
\tilde{h}(x + a)\tilde{h}(x + b + c) = Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m} + b + c)}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= \left[ Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\} \right]^2 + Tr_1^m \left\{ (b + c)(1 + x + x^{2m})^{\frac{1}{2-r}} \right\}
\]

\[
Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\} . (3.14)
\]

and

\[
\tilde{h}(x)\tilde{h}(x + b + c) = Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})(1 + x + x^{2m})^{\frac{1}{2-r}}}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m} + b + c)(1 + x + x^{2m})^{\frac{1}{2-r}}}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= \left[ Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\} \right]^2 + Tr_1^m \left\{ (b + c)(1 + x + x^{2m})^{\frac{1}{2-r}} \right\}
\]

\[
Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m})}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\} . (3.15)
\]

Using (3.13) - (3.15) in (3.12), we get

\[
\tilde{f}(x) = Tr_1^m \left\{ \frac{(u(1 + x + x^{2m}) + u^{2n-r} + x^{2m} + b + c)(1 + x + x^{2m})^{\frac{1}{2-r}}}{(1 + x + x^{2m})^{\frac{1}{2-r}}} \right\}
\]

\[
= Tr_1^m \left\{ (a + b + c)(1 + x + x^{2m})^{\frac{1}{2-r}} \right\}
\]

\[
+ Tr_1^m \left\{ (u(1 + x + x^{2m}) + u^{2n-r} + x^{2m} + a)(1 + x + x^{2m})^{\frac{1}{2-r}} \right\}
\]

\[
= Tr_1^m \left\{ (u(1 + x + x^{2m}) + u^{2n-r} + x^{2m} + b + c)(1 + x + x^{2m})^{\frac{1}{2-r}} \right\} .
\]
Construction of some new classes of Boolean bent functions

Example 3.4. Let $r = 2, n = 6$ and $x^6 + x + 1$ be a primitive polynomial over $\mathbb{F}_{64}$. Let $a = 1$, $b = \alpha$ and $c = \alpha^2 + 1 \in \mathbb{F}_8$ such that $a + b + c \neq 0$, then the function $f(x)$ defined by

$$f(x) = Tr_1^3(x^9) + Tr_1^{6}(x^{7\frac{1}{2} + 1}) + Tr_1^{6}(x)Tr_1^{6}(\alpha x) + Tr_1^{6}(x)Tr_1^{6}((\alpha^2 + 1)x)$$

is a bent function.

Acknowledgements. Authors acknowledge the support of UGC-SAP.

References


Received: November 17, 2016; Published: March 11, 2017