Construction of a New Class of Bent and Semi-bent Functions

P. L. Sharma
Department of Mathematics
Himachal Pradesh University,
Shimla 171005

Neetu Dhiman
Department of Mathematics
Himachal Pradesh University,
Shimla 171005

ABSTRACT
Bent functions play an important role in the designing of S-boxes. 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 a new infinite class of bent and semi-bent functions using few Walsh transform values.

Keywords
Boolean functions, Walsh-Hadamard transform, Bent functions, Semi-bent functions.

1. INTRODUCTION
Rothaus [1] had introduced the bent functions in 1976. Due to the highest non-linearity of bent functions, they have gained importance in the design of stream ciphers and block ciphers. Kumar et al. [2] extended Rothaus’s definition of bent functions to generalized bent functions and also discussed their properties. Since 1974, bent functions are extensively studied because of their significant applications in cryptography (in the design of stream ciphers and in the substitution boxes of block ciphers) [3], coding theory [4], sequence design [5] and graph theory [6, 7]. The new structure introduced in the literature of mathematics known as Rhotrix is gaining importance for making the cryptosystems more secure, see [8, 9, 10, 11]. Irreducible polynomial play an important role in the structure of finite fields which is an essential tool in cryptography, see [12]. 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 [13, 14, 15, 16]. Several constructions of bent functions are discussed in [17, 18]. Some constructions and characterizations of g bent functions are discussed in [19, 20]. Some new constructions of bent and semi-bent functions are recently introduced by Xu et al. [21]. We here present a new construction of bent functions.

Any function \( f(x): F_{2^n} \rightarrow \mathbb{F}_2 \) is called a Boolean function. Let \( n = 2m \) be a positive integer and \( F_{2^n} \) be the finite field with \( 2^n \) elements. Let \( F_{2^n}^* = F_{2^n} \setminus \{0\} \). For any positive integer \( n \), and \( r \) dividing \( n \), the trace function from \( F_{2^n} \rightarrow F_{2^r} \), denoted by \( Tr_{2^r}(x) \), is the mapping defined for every \( x \in F_{2^n} \) as:

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

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

\[
\widehat{f}(w) = \sum_{x \in F_{2^n}} (-1)^{f(x) + Tr_{2^r}(wx)}, \text{ for all } w \in F_{2^r}.
\]

The values \( \widehat{f}(w) \), for all \( w \in F_{2^r} \) are called the Walsh coefficients of \( f \) and the multiset \( \{ \widehat{f}(w), w \in F_{2^r} \} \) is called the Walsh spectrum of a Boolean function \( f \). If \( n \) is even, a Boolean function \( f: F_{2^n} \rightarrow F_2 \) is said to be bent if \( \widehat{f}(w) = \pm 2^{n/2} \), for all \( w \in F_{2^r} \) and \( f \) is said to be semi-bent if \( \widehat{f}(w) = \{0, \pm 2^{n/2-1}\} \) for all \( w \in F_{2^r} \).

2. MAIN RESULTS
We discuss the Walsh-Hadamard transform of a Boolean function \( f(x) \) in the following Lemma.

**Lemma 2.1** Let \( n \) be a positive integer and \( a, b, c \in F_{2^n}^* \). Let \( \mathcal{g}(x) \) be a Boolean function over \( F_{2^n} \). Define the Boolean function \( f(x) \) by

\[
f(x) = \mathcal{g}(x) + Tr_{2^r}(ax)Tr_{2^r}(bx) + Tr_{2^r}(ax)Tr_{2^r}(cx),
\]

then for all \( w \in F_{2^n}^* \)

\[
\widehat{f}(w) = \frac{1}{2}\left[ \widehat{\mathcal{g}}(w) + \widehat{f}(w + a) + \widehat{f}(w + b) + \widehat{f}(w + a + b + c) \right].
\]

**Proof.** For \( i, j \in \{0, 1\} \) and \( a, b \in F_{2^n} \), define

\[
T_{\langle i, j \rangle}(w) = \{ x \in F_{2^n} : Tr_{2^r}(ax) = i, Tr_{2^r}(bx) = j \}
\]

and denote

\[
S_{\langle i, j \rangle}(w) = \sum_{x \in T_{\langle i, j \rangle}(w)} \mathcal{g}(x) + Tr_{2^r}(wx)
\]

and

\[
Q_{\langle i, j \rangle}(w + c) = \sum_{x \in T_{\langle i, j \rangle}(w + c)} \mathcal{g}(x) + Tr_{2^r}(w + c + x).
\]

For each \( w \in F_{2^n}^* \), we have

\[
\widehat{f}(w) = \sum_{x \in F_{2^n}^*} (-1)^{f(x)}\widehat{f}(wx)
\]

\[
= \sum_{x \in F_{2^n}^*} (-1)^{\mathcal{g}(x) + Tr_{2^r}(ax)Tr_{2^r}(bx) + Tr_{2^r}(ax)Tr_{2^r}(cx) + Tr_{2^r}(cw)}
\]

\[
= \sum_{x \in F_{2^n}^*} (-1)^{f(x)}\widehat{f}(wx).
\]
\[
Q_{(1,0)}(w + c) = \frac{1}{4} [\bar{\gamma}_g(w + c) + \bar{\gamma}_g(w + b + c) - \bar{\gamma}_g(w + a + c) - \bar{\gamma}_g(w + a + b + c)] \tag{2.14}
\]

and
\[
Q_{(1,1)}(w + c) = \frac{1}{4} [\bar{\gamma}_g(w + c) - \bar{\gamma}_g(w + b + c) - \bar{\gamma}_g(w + a + b + c) - \bar{\gamma}_g(w + a + b + c)]. \tag{2.15}
\]

Using (2.12) - (2.15) in (2.7), we get
\[
\bar{\gamma}_g(w) = \bar{\gamma}_g(w) - \frac{1}{4} [\bar{\gamma}_g(w) + \bar{\gamma}_g(w + b) - \bar{\gamma}_g(w + a) - \bar{\gamma}_g(w + a + b) + \frac{1}{4} \{\bar{\gamma}_g(w + a) + \bar{\gamma}_g(w + c) + \bar{\gamma}_g(w + b + c) - \bar{\gamma}_g(w + a + b + c)\} - \frac{1}{4} [\bar{\gamma}_g(w + c) - \bar{\gamma}_g(w + b + c) - \bar{\gamma}_g(w + a + b + c) - \bar{\gamma}_g(w + a + b + c)].
\]

To compute, \(S_{(1,0)}(w)\) and \(S_{(1,1)}(w)\) solving the following system

\[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix}
\begin{bmatrix}
S_{(0,0)}(w) \\
S_{(0,1)}(w) \\
S_{(1,0)}(w) \\
S_{(1,1)}(w)
\end{bmatrix}
= \begin{bmatrix}
\bar{\gamma}_g(w) \\
\bar{\gamma}_g(w + b) \\
\bar{\gamma}_g(w + a) \\
\bar{\gamma}_g(w + a + b)
\end{bmatrix}
\]

that is
\[
S_{(0,0)}(w) + S_{(0,1)}(w) + S_{(1,0)}(w) + S_{(1,1)}(w) = \bar{\gamma}_g(w). \tag{2.8}
\]

\[
S_{(0,0)}(w) - S_{(1,0)}(w) + S_{(0,1)}(w) - S_{(1,1)}(w) = \bar{\gamma}_g(w + b), \tag{2.9}
\]

\[
S_{(0,0)}(w) + S_{(1,0)}(w) - S_{(1,0)}(w) - S_{(1,1)}(w) = \bar{\gamma}_g(w + a), \tag{2.10}
\]

\[
S_{(0,0)}(w) - S_{(1,0)}(w) - S_{(0,1)}(w) + S_{(1,1)}(w) = \bar{\gamma}_g(w + a + b). \tag{2.11}
\]

Solving equations from (2.8) - (2.11), we get
\[
S_{(1,0)}(w) = \frac{1}{4} [\bar{\gamma}_g(w) + \bar{\gamma}_g(w + b) - \bar{\gamma}_g(w + a) - \bar{\gamma}_g(w + a + b)] \tag{2.12}
\]

and
\[
S_{(1,1)}(w) = \frac{1}{4} [\bar{\gamma}_g(w) - \bar{\gamma}_g(w + b) - \bar{\gamma}_g(w + a) + \bar{\gamma}_g(w + a + b)]. \tag{2.13}
\]

Substituting \(w = w + c\) in (2.12) and (2.13), we get
\[ \Delta_2 = \frac{1}{2} \left\{ g_b(\alpha + \beta + \gamma) - g_b(\alpha + \beta + \gamma) \right\}. \]

Using
\[ \overline{g}_b(w) = 2^{2k}(-1)^{T_n^{4k}(\lambda w^{2k+1})} \]
to find the values of \( \Delta_1 \) and \( \Delta_2 \). Therefore,
\[ \Delta_1 = \frac{1}{2} 2^{2k} \left\{ (-1)^{T_n^{4k}(\lambda w^{2k+1})} + (-1)^{T_n^{4k}(\lambda (w + a)^{2k+1})} \right\} \]
\[ = \frac{1}{2} 2^{2k} \left\{ (-1)^{T_n^{4k}(\lambda w^{2k+1})} + \right. \]
\[ \left. (-1)^{T_n^{4k}(\lambda (w + a)^{2k+1})} \right\} \]
\[ = \frac{1}{2} 2^{2k} (-1) \Gamma_n^{4k}(\lambda w^{2k+1}) \left\{ 1 + (-1) \Gamma_n^{4k}(\lambda (w + a)^{2k+1}) \right\} \]
(2.17)

and
\[ \Delta_2 = \frac{1}{2} 2^{2k} \left\{ (-1)^{\Gamma_n^{4k}(\lambda (w + b)^{2k+1})} - (-1)^{\Gamma_n^{4k}(\lambda (w + a + c)^{2k+1})} \right\} \]
\[ = \frac{1}{2} 2^{2k} \left\{ (-1)^{\Gamma_n^{4k}(\lambda (w + b)^{2k+1})} \right. \]
\[ \left. \right\} \]
\[ - \frac{1}{2} 2^{2k} \left\{ (-1)^{\Gamma_n^{4k}(\lambda (w + a + c)^{2k+1})} \right\} \]
(2.18)

Let
\[ c_1 = \Gamma_n^{4k}\left\{ \lambda(\alpha^2 + \beta + \gamma) \right\}, \]
(2.19)
\[ c_2 = \Gamma_n^{4k}\left\{ \lambda(\alpha^2 + \beta + \gamma) \right\}, \]
(2.20)
\[ t_1 = \Gamma_n^{4k}\left\{ \lambda(\alpha^2 + \beta + \gamma) \right\}, \]
(2.21)
\[ t_2 = \Gamma_n^{4k}\left\{ \lambda(\beta^2 + \gamma) \right\}, \]
(2.22)
and
\[ t_3 = \Gamma_n^{4k}\left\{ \lambda(\alpha^2 + \beta + \gamma) \right\}. \]
(2.23)

Using (2.19) - (2.23) in (2.17) and (2.18), we have
\[ \Delta_1 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})}(1 + (-1)^{c_1}) \]
(2.24)

and
\[ \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})} + c_2((-1)^{c_1} - \\
\left((-1)^{c_1 - 1 + t_1 + t_2 + t_3}) \right). \]
(2.25)

For \( t_1 = t_2 = t_3 = 0 \), we have
\[ \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})} + c_2((-1)^{c_1} \]
(2.26)

If \( c_2 = 0 \), then from (2.24) and (2.26), we have
\[ \overline{g}_f(w) = \Delta_1 + \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})}(1 + (-1)^{c_1} + \\
\left((-1)^{c_1} \right) \]
\[ = 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})} \]

Therefore, \( f(x) \) is a bent function.

If \( c_2 = 1 \), then from (2.24) and (2.26), we have
\[ \overline{g}_f(w) = \Delta_1 + \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})}(1 + (-1)^{c_1} + \\
\left((-1)^{c_1} \right) \]
\[ \left((-1)^{c_1} \right) \]
\[ = 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})} \]

Therefore, \( f(x) \) is a bent function.

Let us suppose that \( t_1 = 1, t_2 = t_3 = 0 \), then
\[ \Delta_1 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})}(1 + (-1)^{c_1}) \]

and
\[ \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})} + c_2((-1)^{c_1} + \\
\left((-1)^{c_1} \right) \]
(2.27)

If \( c_2 = 0 \), then (2.27) becomes
\[ \overline{g}_f(w) = \Delta_1 + \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})}(1 + (-1)^{c_1} + \\
\left((-1)^{c_1} \right) \]
(2.28)

If \( c_2 = 1 \), then (2.27) becomes
\[ \overline{g}_f(w) = \Delta_1 + \Delta_2 = \frac{1}{2} 2^{2k} (-1)^{\Gamma_n^{4k}(\lambda w^{2k+1})}(1 + (-1)^{c_1} - \\
\left((-1)^{c_1} \right) \]
(2.29)
\[ \frac{1}{2} \sum_{\alpha} \chi(2^k \cdot \alpha) = 0 \]

From (2.28) and (2.29), it is clear that \( f(x) \) is semi-bent and its Walsh spectrum is \( \{0, \pm 2^{k+1}\} \) when \( t_1 = 1, t_2 = t_3 = 0 \).

In a similar manner, we can prove that \( f(x) \) is semi-bent when either \( t_1 = t_2 = 0, t_3 = 1 \) or \( t_1 = t_3 = 0, t_2 = 1 \).

Example 2.3 Let \( k = 2 \) and \( \zeta \) be the primitive element of \( \mathbb{F}_2^8 \) generated by the primitive polynomial \( x^8 + x^4 + x^3 + x^2 + 1 \).

If \( \lambda = \zeta^{34}, a = \zeta^{248}, b = \zeta^{15} \) and \( c = \zeta^{143} \), then the function \( f(x) \) defined as

\[
f(x) = \sum_{\alpha} \chi(2^k \cdot \alpha) + \sum_{\alpha} \chi(2^{k+1} \cdot \alpha) = 0,
\]

is a bent function. If we take \( a = \zeta^{248}, b = \zeta^{15} \) and \( c = \zeta^{238} \), then we have \( T_{r}^{k}(\lambda(a^2 b + ab^2)) = 0, T_{r}^{k}(\lambda(a^2 c + ac^2 b)) = 0 \) and \( T_{r}^{k+1}(\lambda b^2 c + bc^2 b) = 1 \).

So, the function \( f(x) \) as defined in (2.30) is a semi-bent function.

3. ACKNOWLEDGMENTS

Authors acknowledge the support of UGC-SAP.

4. REFERENCES