A new construction of bent functions based on $\mathbb{Z}$-bent functions

Sugata Gangopadhyay[1], Anand Joshi[2], Gregor Leander[3], and Rajendra Kumar Sharma[2]

[1] Department of Mathematics, Indian Institute of Technology Roorkee
Roorkee 247667 INDIA
gsugata@gmail.com
[2] Department of Mathematics, Indian Institute of Technology Delhi
New Delhi 110016 INDIA
{anadjoshi111, rksharmaiitd}@gmail.com
[3] Department of Mathematics, Technical University of Denmark
DENMARK
g.leander@dtu.mat.dk

Abstract. Dobbertin has embedded the problem of construction of bent functions in a recursive framework by using a generalization of bent functions called $\mathbb{Z}$-bent functions. Following his ideas, we generalize the construction of partial spreads bent functions to partial spreads $\mathbb{Z}$-bent functions of arbitrary level. Furthermore, we show how these partial spreads $\mathbb{Z}$-bent functions give rise to a new construction of (classical) bent functions. We underline the variety given by this construction by showing that all bent function in 6 variables can be constructed in this way.

1 Introduction

Bent functions, first introduced in [5, 9], have maximal distance to the set of all affine function. This outstanding property, with connection to coding theory and cryptography, makes them interesting objects to study. Since the introduction of bent functions substantial efforts have been directed towards their study in the last three decades. Many primary and secondary constructions are known but a general understanding of bent functions is still missing. Even the set of all 8 variable bent functions could not be completely classified so far. We refer the reader to the excellent survey chapter by Carlet [3] for detailed information on what is known about bent functions in general.

In [4] the problem of constructing bent functions has been embedded into a recursive framework by generalizing the notion of bent functions to integer-valued functions with certain properties.

Those functions are referred to as $\mathbb{Z}$-bent functions for level r, where r can be any non-negative integer. The union of all such functions is said to be the set of $\mathbb{Z}$-bent functions and the classical bent function correspond to $\mathbb{Z}$-bent functions of level 0.

Most importantly, $\mathbb{Z}$-bent functions of level r on n variables can be used to construct all $\mathbb{Z}$-bent functions of level $r-1$ on $n+2$ variables by a "gluing" technique. Continuing in this way eventually all $\mathbb{Z}$-bent functions of level 0 on $n+2r$ variables are obtained (which are same as classical bent functions on $n+2r$ variables).

Mathematics Subject Classification: 06E30, 94C10
Key Words: Boolean functions; $\mathbb{Z}$-bent functions; Fourier transform.

The motivation for our work is that one can hope to find new (primary) construction of bent functions following this gluing process. For this, one could first construct (new) $\mathbb{Z}$-bent functions of level 1 and than demonstrate that those can be glued together to classical bent functions.

After fixing our notations and recalling some results on $\mathbb{Z}$-bent functions in Section 2, we generalize the construction of partial spreads bent functions to partial spreads $\mathbb{Z}$-bent functions of level r for any $r \geq 1$ (see Section 3). Based on a suitable subclass of those $\mathbb{Z}$-bent functions we give a new primary construction of (classical) bent functions in Section 4. To demonstrate the variety of bent functions that can efficiently be constructed this way, we argue that all bent functions on 6 variables, up to affine equivalence, can be obtained by our construction (see Section 4.1).

2 Preliminaries

Let $\mathbb{F}_2$ be the finite field with two elements and $\mathbb{F}_2^n$ be the n-dimensional vectorspace over $\mathbb{F}_2$. Any function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ is said to be a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. Let us denote the set of integers by $\mathbb{Z}$. Suppose $F \in \mathcal{B}_n$.

Throughout this paper $n = 2k$ is a positive integer.

The *Walsh transform* of a Boolean function F at a point $a \in \mathbb{F}_2^n$ is defined as

$$F^W(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)} (-1)^{\langle a,x \rangle},$$

where $\langle a, x \rangle$ is the canonical inner product on $\mathbb{F}_2^n$, that is $\langle a, x \rangle = \sum a_i x_i$.

A Boolean function is called bent if for all $a \in \mathbb{F}_2^n$ it holds that $F^W(a) = \pm 2^k$. The identity

$$\mathrm{wt}((F(x) + \langle a, x \rangle + \epsilon)_{x \in \mathbb{F}_2^n}) = 2^{n-1} - (-1)^{\epsilon} \frac{F^W(a)}{2}. \tag{1}$$

provides the link between the Walsh-transform and the distance of the function F to the linear function $\langle a, \cdot \rangle$. It follows from Parseval's identity

$$\sum_{a \in \mathbb{F}_2^n} F^W(a)^2 = 2^{2n}$$

that $\max_{a \in \mathbb{F}_2^n} |F^W(a)| \geq 2^k$ and therefore bent functions are exactly those Boolean functions (on an even number of variables) that have the maximal distance to the set of all affine functions.

2.1 From Bent to $\mathbb{Z}$-bent functions and back

In order to generalize bent functions to $\mathbb{Z}$-bent functions it is most convenient to replace Boolean, that is $\{0, 1\}$ valued functions by ± 1 valued functions. Given a Boolean function F we consider the function

$$\begin{aligned} f : \mathbb{F}_2^n &\to \{-1, 1\} \subseteq \mathbb{Z} \\ f(x) &= (-1)^{F(x)} \end{aligned}$$

Clearly there is a one-to-one correspondence between the functions defined in these two ways. Throughout this paper we denote by F, G Boolean functions and by f, g the integer-valued function $f(x) = (-1)^{F(x)}$, $g(x) = (-1)^{G(x)}$ associated with F and G. By abuse of terminology we shall refer to these functions from $\mathbb{F}_2^n$ to $\{-1, 1\}$ as Boolean functions as well.

For an integer-valued (or more general real- or complex-valued) function f the *Fourier transform* defined by

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle}$$

is an important tool. Note the close relation to the Walsh-transform given by

$$\hat{f}(a) = \frac{1}{2^k} F^W(a).$$

With this notation at hand a function f is bent if and only if both f and $\hat{f}$ are $\{-1, 1\}$-valued. From this viewpoint, the generalization to $\mathbb{Z}$-bent function, to be discussed below, is almost natural.

In order to put the construction of bent functions in a recursive framework, Dobbertin (see [4]) generalized the notion of bent functions to $\mathbb{Z}$-bent functions. Consider the following sequence of subsets of $\mathbb{Z}$

$$W_0 = \{-1, 1\}$$
$$W_r = \{w \in \mathbb{Z} | -2^{r-1} \leq w \leq 2^{r-1}\} \text{ for } r > 0.$$

Definition 1. *A function $f : \mathbb{F}_2^n \longrightarrow W_r$ is said to be a $\mathbb{Z}$-bent function of* size k *(equivalently on n variables) and* level r *if and only if $\hat{f}$ is also a function into W_r. The set of all $\mathbb{Z}$-bent functions of size k and level r is denoted by $\mathcal{B}F_r^k$. Any function belonging to $\cup_{r \geq 0} \mathcal{B}F_r^k$ is said to be a $\mathbb{Z}$-bent function.*

Next, we recall how $\mathbb{Z}$-bent function of size k and level r can be decomposed into four $\mathbb{Z}$-bent function of size $k-1$ and level $r+1$ (cf. Proposition 2 of [4]).

Suppose $f \in \mathcal{B}F_r^k$,

$$U_{\epsilon_1 \epsilon_2} = \{(\epsilon_1, \epsilon_2, y) | y \in \mathbb{F}_2^{n-2}\}, \epsilon_1, \epsilon_2 \in \mathbb{F}_2.$$

and

$$h_{\epsilon_1 \epsilon_2}(y) = f(\epsilon_1, \epsilon_2, y), y \in \mathbb{F}_2^{n-2}.$$

Define functions $f_{\epsilon_1 \epsilon_2}$ as follows:
Case 1 For $r \geq 1$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \tag{2}$$

Case 2 For $r = 0$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \tag{3}$$

Proposition 2 in [4] states that the functions $f_{\epsilon_1 \epsilon_2}$ are $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$ (that is $f_{\epsilon_1 \epsilon_2} \in \mathcal{B}F_{r+1}^{k-1}$), for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$.

Conversely, under certain conditions, it is possible to construct bent functions of size k and level r from bent functions of size $k-1$ and level $r+1$. This is refereed to as *gluing* in [4] (cf. Theorem 3 of [4]). The following theorem summarizes these result in the special case of level 1 functions being glued together to a classical bent function. Note that our notation differs slightly from the one in [4] as we avoid to introduce so called bent squares.

Theorem 1 ([4], Theorem 3). *Let four $\mathbb{Z}$-bent functions $f_{00}, f_{01}, f_{10}, f_{11}$ of level 1 and size k be given such that*

$$f_{00}(x) \equiv f_{01}(x) + 1 \bmod 2 \tag{4}$$
$$f_{10}(x) \equiv f_{11}(x) + 1 \bmod 2 \tag{5}$$
$$\widehat{f_{00}}(x) \equiv \widehat{f_{10}}(x) + 1 \bmod 2 \tag{6}$$
$$\widehat{f_{01}}(x) \equiv \widehat{f_{11}}(x) + 1 \bmod 2. \tag{7}$$

Then the function

$$h : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^n \to \{-1, 1\}$$
$$h(x, y, z) = h_{x,y}(z)$$

where

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}$$

is a bent function (of level 0).

Especially in light of this gluing process, the construction of $\mathbb{Z}$-bent functions becomes an interesting problem.

3 Generalization of partial spreads bent functions to partial spreads $\mathbb{Z}$-bent functions of arbitrary level

Let E be any subset of $\mathbb{F}_2^n$. The function ϕ_E defined by

$$\phi_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

is the indicator function of E. Suppose $\{E_i : i = 1, 2, \cdots, s\}$ is a set of mutually disjoint k-dimensional subspaces of $\mathbb{F}_2^n$. Here mutually disjoint means $E_i \cap E_j = \{0\}$ whenever $i \neq j$. The partial spreads class of bent functions (PS) consists of two sub-classes PS^- and PS^+. These functions were first constructed by Dillon [5]. The elements of PS^- are those functions whose supports are unions of 2^{k-1} disjoint k-dimensional subspaces of $\mathbb{F}_2^n$ excluding 0, whereas the elements of PS^+ are those whose supports are unions of $2^{k-1}+1$ disjoint k-dimensional subspaces of $\mathbb{F}_2^n$. A function $F \in \mathcal{B}_n$ belonging to the class PS can be expressed as

$$F(x) = \sum_{i=1}^{s} \phi_{E_i}(x) - 2^{k-1}\phi_{\{0\}}(x) \text{ for all } \ x \in \mathbb{F}_2^n,$$

where $s = 2^{k-1}$ if $F \in PS^-$ and $s = 2^{k-1}+1$ if $F \in PS^+$ and the sum is taken over the integers.

Note that, in general, this construction is not efficient in the sense that it is difficult to find those disjoint k-dimensional subspaces. For $n = 8$ a complete classification of all partial spreads bent functions has been obtained in [7]. However, there is a special choice of subspaces where the construction becomes effective. This leads to the class of PS_{ap} bent functions and is explained next.

Here, we consider function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ instead, that is we consider the finite field with 2^n elements instead of the vectorspace only. Furthermore, let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$, and $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$. Clearly the set $\mathcal{S} = \{V_i : i = 0, \ldots, 2^k\}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$. A subclass of PS type bent functions is obtained by constructing functions whose supports are union of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.

Based on the parial spread class of bent function we propose a construction technique of $\mathbb{Z}$-bent functions of level $r \geq 1$, on n variables. However it should be noted that the functions considered so far in this section are from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, whereas the functions considered below are integer valued, that is functions from $\mathbb{F}_2^n$ into $\mathbb{Z}$, the set of integers.

Theorem 2. *Let $m_1, m_2, \cdots, m_s$ be integers and $E_1, E_2, \cdots, E_s$ be k-dimensional subspaces of $\mathbb{F}_2^n$, then the function*

$$f(x) = \sum_{i=1}^{s} m_i \phi_{E_i}(x)$$

is a $\mathbb{Z}$-bent function and its dual is given by $\sum_{i=1}^{s} m_i \phi_{E_i^\perp}(x)$.

Proof. All we have to show is that both f and $\hat{f}$ are integer valued. For f this is clear by definition. The Fourier transform of f at $a \in \mathbb{F}_2^n$ is as follows

$$\begin{aligned}
\hat{f}(a) &= \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle} \\
&= \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} \sum_{i=1}^{s} m_i \phi_{E_i}(x)(-1)^{\langle a,x \rangle} \\
&= \frac{1}{2^k} \sum_{i=1}^{s} m_i \sum_{x \in E_i} (-1)^{\langle a,x \rangle} \\
&= \frac{1}{2^k} \sum_{i=1}^{s} m_i 2^k \phi_{E_i^\perp}(a) \\
&= \sum_{i=1}^{s} m_i \phi_{E_i^\perp}(a)
\end{aligned}$$

Thus, $\hat{f}$ is also an integer valued function and the result follows.

While the previous theorem is quite general, it is difficult to specify the exact level of the $\mathbb{Z}$-bent functions constructed. In order to be able to construct bent functions of a specific level r the following technical lemma is useful.

Lemma 1. *Let U and V be k-dimension subspaces of $\mathbb{F}_2^n$ such that*

$$U \cap V = \{0\}$$

then

$$U^\perp \cap V^\perp = \{0\}$$

Proof. As U and V are k-dimensional $U \cap V = \{0\}$ is equivalent to $\mathbb{F}_2^n = U \oplus V$, that is $\mathbb{F}_2^n$ is the direct sum of U and V. Now let $x \in U^\perp \cap V^\perp$ be given. Then,

$$\begin{aligned} \langle x, u\rangle &= 0 \quad \forall u \in U \\ \langle x, v\rangle &= 0 \quad \forall v \in V \end{aligned}$$

and as $\mathbb{F}_2^n = U \oplus V$ we conclude that

$$\langle x, w\rangle = 0 \quad \forall w \in \mathbb{F}_2^n$$

implying that $x = 0$ as claimed.

With this lemma at hand we now can construct bent functions of any specific level.

Corollary 1. *Suppose $\{E_i : i = 1, 2, \cdots, s\}$ is a set of k-dimensional subspace of $\mathbb{F}_2^n$ with the property that $E_i \cap E_j = \{0\}$ whenever $i \neq j$. The function*

$$f(x) = \sum_{i=1}^{s} c_i \phi_{E_i}(x), \text{ for all } x \in \mathbb{F}_2^n, \tag{8}$$

where $c_i \in W_r$, for all $i = 1, 2, \ldots, s$, is a $\mathbb{Z}$-bent function of level r, for any $r \geq 1$, if and only if $\sum_{i=1}^{s} c_i \in W_r$.

Proof. From Theorem 2 we already know that f is a $\mathbb{Z}$-bent function. To prove that it is a bent function of level r we have to show that $f(x) \in W_r$ and $\hat{f}(a) \in W_r$ for all $x, a \in \mathbb{F}_2^n$. While the first part follows immediately from the construction of f we elaborate a bit on the second part.

Applying Theorem 2 yields that

$$\hat{f}(a) = \sum_{i=1}^{s} m_i \phi_{E_i^\perp}(a)$$

and Lemma 1 implies that the k-dimensional spaces $E_i^\perp$ are pairwise disjoint. Thus for $a \neq 0$ we conclude

$$\hat{f}(a) \in \{c_i \mid 1 \leq i \leq s\} \cup \{0\} \subseteq W_r$$

and for $a = 0$

$$\hat{f}(0) = \sum_{i=1}^{s} c_i \in W_r$$

by construction.

Remark 1. It is to be noted that in the binary case we obtain bent functions if and only if $s \in \{2^{k-1}, 2^{k-1} + 1\}$ while the integer valued case is more flexible. We refer to these integer valued functions as PS type $\mathbb{Z}$-bent functions of level r.

Remark 2. It is possible to construct the analogue of PS_{ap} type bent function by considering the functions of the form

$$f(x) = \sum_{i=0}^{2^k} c_i \phi_{V_i}(x), \text{ for all } x \in \mathbb{F}_{2^n}, \tag{9}$$

where $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 0, \ldots, 2^k$, $c_i \in W_r$ for all $i = 1, 2, \ldots, 2^k$ and $\sum_{i=1}^{s} c_i \in W_r$. We shall refer to these functions as PS_{ap} type $\mathbb{Z}$-bent functions of level r. In the next section we use those functions together with Theorem 1 to give a new general construction of bent functions. In particular, we demonstrate that all the bent functions on 6 variables, up to affine equivalence, can be constructed by "gluing" PS_{ap} type $\mathbb{Z}$-bent functions of level 1 on 4 variables.

Remark 3. It is to be noted that for each $i \in \{0, 1, \ldots, 2^k\}$ there exists $j \in \{0, 1, \ldots, 2^k\}$ such that $V_i^{\perp} = V_j$. Therefore the dual of a PS_{ap} type $\mathbb{Z}$-bent function of level r is also a PS_{ap} type $\mathbb{Z}$-bent function of level r.

4 A New Construction of Bent functions

In this section we describe a new construction of (classical) bent functions based on the bent functions of level 1 presented in Corollary 1 and the gluing Theorem 1.

While, in general, fulfilling only the conditions given in Theorem 1 on the functions f_{ij} *or* on their duals $\widehat{f_{ij}}$ is easy, fulfilling all four conditions at the same time seems difficult. However, bent functions of level 1 described in Corollary 1, lead to a special case where things are a lot easier.

We start by letting $\mathcal{S} = \{S_i\}$ be a spread, i.e. a collection of $2^k + 1$ subspaces of dimension k with the condition that

$$S_j \cap S_i = \{0\} \text{ and } \cup_i S_i = \mathbb{F}_2^n .$$

Next, we partition this spread $\mathcal{S}$ into two parts, $\mathcal{A}$ and $\mathcal{B}$, i.e. $\mathcal{A} \cap \mathcal{B} = \emptyset$ and $\mathcal{A} \cup \mathcal{B} = \mathcal{S}$ and select four collections of coefficients, each in $\{-1, 1\}$

$$\begin{aligned}
(m_A)_{A\in\mathcal{A}} &\text{ such that } \sum m_A \in \{-1, 0, 1\} \\
(m'_A)_{A\in\mathcal{A}} &\text{ such that } \sum m'_A \in \{-1, 0, 1\} \\
(n_B)_{B\in\mathcal{B}} &\text{ such that } \sum n_B \in \{-1, 0, 1\} \\
(n'_B)_{B\in\mathcal{B}} &\text{ such that } \sum n'_B \in \{-1, 0, 1\}.
\end{aligned}$$

Given those coefficients, we are ready to construct our four $\mathbb{Z}$ bent functions of level 1 as follows

$$\begin{aligned}
f_{00}(x) &= \sum_{A\in\mathcal{A}} m_A \phi_A(x) \\
f_{10}(x) &= \sum_{B\in\mathcal{B}} n_B \phi_B(x) \\
f_{01}(x) &= \sum_{B\in\mathcal{B}} n'_B \phi_B(x) \\
f_{11}(x) &= \sum_{A\in\mathcal{A}} m'_A \phi_A(x).
\end{aligned}$$

In order to apply Theorem 1 we have to verify that the four conditions (4) to (7) are fulfilled. To verify the first condition, let $x \in \mathbb{F}_2^n$ be given. We compute

$$\begin{aligned} f_{00}(x) + f_{01}(x) &= \sum_{A \in \mathcal{A}} m_A \phi_A(x) + \sum_{B \in \mathcal{B}} n'_B \phi_B(x) \\ &= \sum_{A \in \mathcal{A}} \phi_A(x) + \sum_{B \in \mathcal{B}} \phi_B(x) \pmod 2 \\ &= \sum_{S_i \in \mathcal{S}} \phi_{S_i}(x) \pmod 2 \end{aligned}$$

If $x \neq 0$ then, as $\mathcal{S}$ is a spread, there exists exactly one subspace S_k such that $x \in S_k$ and

$$f_{00}(x) + f_{01}(x) = \sum_{S_i \in \mathcal{S}} \phi_{S_i}(x) = \phi_{S_k}(x) = 1 \pmod 2.$$

On the other hand, if $x = 0$ than

$$f_{00}(0) + f_{01}(0) = \sum_{S_i \in \mathcal{S}} 1 = 2^k + 1 = 1 \pmod 2.$$

The other conditions follow in a very similar way. In particular conditions (6) and (7) follow from the fact that, due to Corollary 1, the duals $\widehat{f_{ij}}$ of f_{ij} are again of the same type so the condition carries over to the duals nicely.

4.1 Construction of all 6 variable bents up to affine equivalence

In this section we consider PS_{ap} type $\mathbb{Z}$-bent functions of level 1 on 4 variables. Let ζ be a root of the primitive polynomial $x^4 + x + 1$ on $\mathbb{F}_2$. The finite field

$$\mathbb{F}_{2^4} = \{\zeta^i : i = 0, 1, \ldots, 14\} \cup \{0\}.$$

In this case the elements of $\mathcal{S}$ can be explicitly written as follows.

$$\begin{aligned} V_0 &= \{0, 1, \zeta^5, \zeta^{10}\}, \\ V_1 &= \{0, \zeta, \zeta^6, \zeta^{11}\}, \\ V_2 &= \{0, \zeta^2, \zeta^7, \zeta^{12}\}, \\ V_3 &= \{0, \zeta^3, \zeta^8, \zeta^{13}\}, \\ V_4 &= \{0, \zeta^4, \zeta^9, \zeta^{14}\}. \end{aligned}$$

We generate all the PS_{ap} type $\mathbb{Z}$-bent functions of level 1 on 4 variables and "glue" them to construct bent functions on 6 variables. Then by exhaustive search we find seven PS_{ap} type $\mathbb{Z}$-bent functions of level 1 on 4 variables such that all the 6-variable bent functions up to affine equivalence can be generated by gluing them. We denote these functions by $g_0, g_1, g_2, g_3, g_4, g_5, g_6$ and list them below.

$g_0(x) = 0$,
$g_1(x) = \phi_{V_0}(x)$,
$g_2(x) = -\phi_{V_0}(x) - \phi_{V_1}(x) + \phi_{V_2}(x) + \phi_{V_3}(x) + \phi_{V_4}(x)$,
$g_3(x) = -\phi_{V_0}(x) + \phi_{V_1}(x) - \phi_{V_2}(x) + \phi_{V_3}(x) + \phi_{V_4}(x)$,
$g_4(x) = -\phi_{V_1}(x) - \phi_{V_2}(x) + \phi_{V_3}(x) + \phi_{V_4}(x)$,
$g_5(x) = -\phi_{V_0}(x) - \phi_{V_1}(x) - \phi_{V_2}(x) + \phi_{V_3}(x) + \phi_{V_4}(x)$.
$g_6(x) = -\phi_{V_1}(x) + \phi_{V_2}(x) - \phi_{V_3}(x) + \phi_{V_4}(x)$,

The truth tables of the the above functions are as follows.

g_0	0000000000000000
g_1	1100001100000000
g_2	$1-1-1111-1-11111-11-11$
g_3	$1-111-11-1-1111-1111-1$
g_4	$00-11-1100111-1-11-1-1$
g_5	$-1-1-11-11-1-1111-1-11-1-1$
g_6	$00-111-100-1111-1-1-11$

By "gluing" them we obtain four bent functions on 6 variables which can be demonstrate to be affine non-equivalent by using the weight distributions of the second derivative spectrum introduced in [6]. Since by [9] it is known there are only four bent functions on 6-variables, up to affine equivalence, this proves that all the bent functions up to affine equivalence are obtained by our construction. Let us denote the four functions obtained is this way by $h^{(1)}$, $h^{(2)}$, $h^{(3)}$, $h^{(4)}$. Define

$$h^{(i)}_{\epsilon_1\epsilon_2}(y) = h^{(i)}(\epsilon_1, \epsilon_2, y), y \in \mathbb{F}_2^{n-2} \text{ for } \ i = 1, 2, 3, 4.$$

The functions are defined as follows:

$$\begin{pmatrix} h^{(1)}_{00} & h^{(1)}_{10} \\ h^{(1)}_{01} & h^{(1)}_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} g_0 & g_2 \\ g_2 & g_0 \end{pmatrix}.$$

The truth table of the Boolean function $H^{(1)}$ associated to $h^{(1)}$ is

$$0110001100001010100111001111010101100011000010100110001100001010.$$

$$\begin{pmatrix} h^{(2)}_{00} & h^{(2)}_{10} \\ h^{(2)}_{01} & h^{(2)}_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} g_0 & g_3 \\ g_2 & g_0 \end{pmatrix}.$$

The truth table of the Boolean function $H^{(2)}$ associated to $h^{(2)}$ is

$$0110001100001010100111001111010101001011000100010100101100010001.$$

$$\begin{pmatrix} h^{(3)}_{00} & h^{(3)}_{10} \\ h^{(3)}_{01} & h^{(3)}_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} g_0 & g_5 \\ g_2 & g_0 \end{pmatrix}.$$

The truth table of the Boolean function $H^{(3)}$ associated to $h^{(3)}$ is

$$0110001100001010100111001111010111101011000110111110101100011011.$$

$$\begin{pmatrix} h^{(4)}_{00} & h^{(4)}_{10} \\ h^{(4)}_{01} & h^{(4)}_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} g_1 & g_6 \\ g_4 & g_1 \end{pmatrix}.$$

The truth table of the Boolean function $H^{(4)}$ associated to $h^{(4)}$ is

$$0010100000011011000101001110010000100100100011101110011110001110.$$

It can be directly checked that $H^{(i)}$, for $i = 1, 2, 3, 4$ are bent functions. Moreover, it is not hard to see (for example using the techniques presented in [6] to show that all those functions are pairwise inequivalent. Thus we obtain all the bent functions on 6 variables up to affine equivalence.

5 Conclusion

In this paper we generalize the PS type bents to PS type $\mathbb{Z}$-bent functions of level r for any $r \geq 1$. We also identify the natural analogue of the class PS_{ap}. Finally we demonstrate that all the 6-variable bent functions can be constructed by "gluing" PS_{ap} type bent functions of level 1 on 4 variables.

References

1. C. Carlet, "Generalized partial spreads", *IEEE Trans. Inform. Theory* 41 (1995), 1482–1487.
2. C. Carlet, P. Guillot, "A characterization of binary bent functions", *J. Comb. Theory, Ser. A* 76 (1996), 328–335.
3. C. Carlet, Boolean functions for cryptography and error correcting codes. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
4. H. Dobbertin, G. Leander, "Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions", *Des. Codes Cryptogr.* 49 (2008), 3–22.
5. J. F. Dillon, "Elementary Hadamard difference sets", *Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing*, Utility Mathematics, Winnipeg, (1975), 237–249.
6. S. Gangopadhyay, D. Sharma, S. Sarkar and S. Maitra, "On affine (non)equivalence of Boolean functions", *Computing* 85 (2009) 37–55.
7. P. Langevin and X.-D. Hou, "Counting Partial Spread Functions in Eight Variables", *preprint* (2010)
8. F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*. North-Holland, Amsterdam, New York, Oxford, 1977.
9. O. S. Rothaus, "On bent functions", *J. Comb. Theory, Ser. A* 20 (1976), 300–305.