On bent functions with zero second derivatives

Sugata Gangopadhyay
Department of Mathematics
Indian Institute of Technology
Roorkee - 247 667 INDIA

Abstract

It is proved that a bent function has zero second derivative with respect to a, b, $a \neq b$, if and only if it is affine on all the flats parallel to the two dimensional subspace $V = \langle a, b \rangle$.

1 Introduction

Bent functions were first constructed by Dillon and Rothaus [6, 7, 9]. They introduced two classes of bent functions namely Maiorana-McFarland class, $\mathcal{M}$ and partial spreads class, $\mathcal{PS}$. Carlet [3] constructed two new classes of bent functions. Another class of bent functions is due to Dobbertin [8], in the same paper he introduced the notion of non-normality of bent functions. Canteaut and Charpin [1] have proved that the Walsh-Hadamard spectra of restrictions of a bent function f to the affine subspaces of codimension 2 can be explicitly derived from the Hamming weights of the second derivatives of the dual function of f. It is observed that these restricted functions have high nonlinearity. However restrictions of bent functions to affine subspaces of low dimensions, e.g., dimension 2 subspaces, can be affine functions. For example given an $\mathcal{M}$ type bent function, by lemma 33 of [2], it is possible to find a subspace V of dimension 2 such that the restriction of the function to each flat parallel to V is affine. Let us denote the set of all bent functions which are affine on all the flats parallel to a 2 dimensional subspace V by $\mathcal{E}$. In this paper primarily by using results of [1, 5] it is proved that a bent function is in $\mathcal{E}$ if and only if it has a zero second derivative with respect to two distinct elements of its domain.

2 Preliminaries

Let $\mathbb{F}_2$ be the prime field of characteristic two. A function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ is said to be a Boolean function on n variables. The set of all such functions is denoted by $\mathcal{B}_n$. Let the cardinality of any set S be denoted by $|S|$. The function $d : \mathcal{B}_n \times \mathcal{B}_n \longrightarrow \mathbb{Z}$ defined by $d(f, g) = |\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}|$, for all $f, g \in \mathcal{B}_n$, is called the Hamming distance between

f and g. The inner product of two vectors $u, v \in \mathbb{F}_2^n$ is denoted by $\langle u, v \rangle$. The dual, $V^\perp$, of any subspace $V \subseteq \mathbb{F}_2^n$ is defined by

$$V^\perp = \{x \in \mathbb{F}_2^n | \forall y \in V, \langle x, y \rangle = 0\}.$$

A function $l \in \mathcal{B}_n$ is affine if and only if there exists $u \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $f(x) = \langle u, x \rangle + \epsilon$. Let $\mathcal{A}_n$ denote the set of affine functions in $\mathcal{B}_n$. The minimum Hamming distance of $f \in \mathcal{B}_n$ from the set $\mathcal{A}_n$ that is $\min\{d(f, l) | l \in \mathcal{A}_n\}$ is called the nonlinearity of f. The Walsh-Hadamard transform $W_f(\lambda)$ of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_2^n$ is defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle \lambda, x \rangle}$$

and the multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_2^n]$ is called the Walsh-Hadamard spectrum of f. The nonlinearity, $nl(f)$ of f is related to the Walsh-Hadamard spectrum of f by the following expression:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |W_f(\lambda)|.$$

The derivative of f with respect to $a \in \mathbb{F}_2^n$ is defined by

$$D_a f(x) = f(x + a) + f(x).$$

Definition 1 *A Boolean function $f \in \mathcal{B}_n$, n even, is said to be bent if and only if its nonlinearity is equal to $2^{n-1} - 2^{\frac{n}{2}-1}$. The Walsh-Hadamard transform of a bent function consists of only two values namely $\pm 2^{\frac{n}{2}}$.*

The dual $\tilde{f}$ of a bent function f is again a bent function defined by the relation

$$W_f(x) = (-1)^{\tilde{f}(x)} 2^{\frac{n}{2}}$$

for all $x \in \mathbb{F}_2^n$.

Suppose U is a codimension 2 subspace of $\mathbb{F}_2^n$ and let the four distinct flats parallel to U be denoted by $a_i + U$, where $i = 0, 1, 2, 3$. The 4-decomposition of $g \in \mathcal{B}_n$ is the sequence of functions (g_1, g_2, g_3, g_4) where $g_i = g|_{a_i + U}$, the restrictioin of g to $a_i + U$, for $i = 0, 1, 2, 3$. It is proved by Canteaut and Charpin [1] that if $g \in \mathcal{B}_n$ is bent then each g_i is either bent, three valued almost optimal or a Boolean function with five distinct values in the Walsh-Hadamard spectrum belonging to the set $\{0, \pm 2^{\frac{n-2}{2}}, \pm 2^{\frac{n}{2}}\}$. The weight distribution of the Walsh-Hadamard spectrum of each g_i is given below,

$\lvert W_{g_i}(u) \rvert$	number of $u \in \mathbb{F}_2^{n-2}$
0	$3(2^{n-4} - 2^{-4}\lambda)$
$2^{\frac{n-2}{2}}$	$\frac{\lambda}{4}$
$2^{\frac{n}{2}}$	$2^{n-4} - 2^{-4}\lambda$

where $\lambda = \mathrm{wt}(D_a D_b \tilde{g})$. For proof we refer to theorem 7 [1]. Charpin proved that a function $f \in \mathcal{B}_n$ is affine on a coset $c + V$, where V is a subspace of $\mathbb{F}_2^n$, if and only if:

$$T_{a,c} = \sum_{v \in V^\perp} (-1)^{\langle c,v \rangle} W_f(a+v) = \pm 2^n \tag{1}$$

for some $a \in W$ where $V^\perp \times W = \mathbb{F}_2^n$, lemma 3, [5]. We make use of this result in the next section to prove the main result.

3 Main Result

In this section we prove the main result which characterizes bent functions which are affine on all the flats parallel to a subspace of dimension 2.

Theorem 1 *If $f \in \mathcal{B}_n$ is a bent function and V is a two dimensional subspace of $\mathbb{F}_2^n$ then f is affine on all the flats parallel to V if and only if $\tilde{f}$ has three valued almost optimal 4-decomposition with respect to $V^\perp$*

Proof : If $f \in \mathcal{B}_n$ is bent then

$$\begin{aligned} T_{a,c} &= \sum_{v \in V^\perp} (-1)^{\langle c,v \rangle} W_f(a+v) = \sum_{v \in V^\perp} (-1)^{\langle c,v \rangle} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle x,(a+v) \rangle} \\ &= 2^{\frac{n}{2}} \sum_{v \in V^\perp} (-1)^{\langle c,v \rangle} (-1)^{\tilde{f}(a+v)} = 2^{\frac{n}{2}} \sum_{v \in V^\perp} (-1)^{\tilde{f}(a+v)+\langle c,v \rangle} = 2^{\frac{n}{2}} W_{\tilde{f}|_{a+V^\perp}}(c). \end{aligned}$$

Let the flats parallel to $V^\perp$ be denoted by $a_i + V^\perp$ where $i \in \{0,1,2,3\}$.

If $\tilde{f}$ has bent 4-decomposition with respect to $V^\perp$ then for all a and all c:

$$T_{a,c} = \pm 2^{\frac{n}{2}} 2^{\frac{n-2}{2}} = \pm 2^{\frac{2n-2}{2}} \neq \pm 2^n.$$

Thus the condition (1) is not satisfied. Hence by lemma 3 [5] f is not affine on any two dimensional flat.

If $\tilde{f}$ has three valued almost optimal decomposition with respect to $V^\perp$ then for any a_i and c,

$$\sum_{v \in a_i + V^\perp} (-1)^{\tilde{f}(v)+\langle c,v \rangle} \in \{0, 2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}.$$

Since $\tilde{f}$ is bent:

$$\begin{aligned} &\sum_{v \in a_0 + V^\perp} (-1)^{\tilde{f}(v)+\langle c,v \rangle} + \sum_{v \in a_1 + V^\perp} (-1)^{\tilde{f}(v)+\langle c,v \rangle} \\ &+ \sum_{v \in a_2 + V^\perp} (-1)^{\tilde{f}(v)+\langle c,v \rangle} + \sum_{v \in a_3 + V^\perp} (-1)^{\tilde{f}(v)+\langle c,v \rangle} = \pm 2^{\frac{n}{2}} \end{aligned} \tag{2}$$

Therefore given any c in order that (2) satisfied there has to exist at least one $i \in \{0,1,2,3\}$ such that

$$T_{a_i,c} = \sum_{v \in a_i + V^{\perp}} (-1)^{\tilde{f}(v)+\langle c,v\rangle} = \pm 2^{\frac{n}{2}}$$

which implies that f is affine on $c+V$. Since c can be arbitrarily chosen this means that f is affine on all the cosets of the two dimensional subspace V.

Suppose $\tilde{f}|_{a+V^{\perp}}$ has Walsh-Hadamard spectrum with five values $0, \pm 2^{\frac{n-2}{2}}, \pm 2^{\frac{n}{2}}$ for each $a \in \mathbb{F}_2^n$.From (2) we obtain:

$$\begin{aligned}(-1)^{\langle a_0,c\rangle} \sum_{v \in V^{\perp}} (-1)^{\tilde{f}(a_0+v)+\langle c,v\rangle} + (-1)^{\langle a_1,c\rangle} \sum_{v \in V^{\perp}} (-1)^{\tilde{f}(a_1+v)+\langle c,v\rangle} & \\ +(-1)^{\langle a_2,c\rangle} \sum_{v \in V^{\perp}} (-1)^{\tilde{f}(a_2+v)+\langle c,v\rangle} + (-1)^{\langle a_3,c\rangle} \sum_{v \in V^{\perp}} (-1)^{\tilde{f}(a_3+v)+\langle c,v\rangle} &= \pm 2^{\frac{n}{2}}. \end{aligned} \quad (3)$$

For $i = 0,1,2,3$, define $g_i(v) = \tilde{f}(a_i + v)$ for all $v \in V^{\perp}$. Since $V^{\perp}$ is an $n-2$ dimensional subspace, if we restrict the linear function $\phi_c(x) = \langle c, x\rangle$ to $V^{\perp}$ then there exists an element $c' \in V^{\perp}$ such that $\phi_c(v) = \langle c', v\rangle$ for all $v \in V^{\perp}$. The above sum can be written as

$$\begin{aligned}(-1)^{\langle a_0,c\rangle} \sum_{v \in V^{\perp}} (-1)^{g_0(v)+\langle c',v\rangle} + (-1)^{\langle a_1,c\rangle} \sum_{v \in V^{\perp}} (-1)^{g_1(v)+\langle c',v\rangle} & \\ +(-1)^{\langle a_2,c\rangle} \sum_{v \in V^{\perp}} (-1)^{g_2(v)+\langle c',v\rangle} + (-1)^{\langle a_3,c\rangle} \sum_{v \in V^{\perp}} (-1)^{g_3(v)+\langle c',v\rangle} &= \pm 2^{\frac{n}{2}}\end{aligned}$$

Consider

$$S_i = \{c' \in V^{\perp} || W_{g_i}(c')| = 2^{\frac{n}{2}}\}$$

where $i = 0,1,2,3$. By theorem 7 [1] stated above

$$|S_i| = 2^{n-4} - \frac{\lambda}{2^4}.$$

Taking union over all S_i we obtain

$$|\cup_{i=0}^{3} S_i| \leq \sum_{i=0}^{3} |S_i| = 2^2(2^{n-4} - \frac{\lambda}{2^4}) = 2^{n-2} - \frac{\lambda}{2^2}.$$

If $\lambda \neq 0$ then $|\cup_{i=0}^{3} S_i| < 2^{n-2}$. Therefore there exists $c' \in V^{\perp}$ such that

$$|\sum_{v \in V^{\perp}} (-1)^{g_i(v)+\langle c',v\rangle}| \neq 2^{\frac{n}{2}} \text{ for all } i = 0,1,2,3.$$

Therefore, there exists $c \in \mathbb{F}_2^n$ such that

$$|\sum_{v \in V^{\perp}} (-1)^{\tilde{f}(a_i+v)+\langle c,v\rangle}| \neq 2^{\frac{n}{2}} \text{ for all } i = 0,1,2,3.$$

Since $\mathbb{F}_2^n = \cup_{i=0}^3 (a_i + V)$, there exists $c \in \mathbb{F}_2^n$ such that

$$|\sum_{v \in V^\perp} (-1)^{\tilde{f}(a+v)+\langle c,v\rangle}| \neq 2^{\frac{n}{2}} \text{ for all } a \in \mathbb{F}_2^n.$$

Hence there exist $c \in \mathbb{F}_2^n$ such that $T_{a,c} \neq \pm 2^n$ for all $a \in \mathbb{F}_2^n$. Therefore f is not affine on $c + V$ i.e., there exists at least one flat parallel to V on which the function is not affine.

This proves that $f \in \mathcal{B}_n$ is a bent function and V is a two dimensional subspace of $\mathbb{F}_2^n$ then f is affine on all the cosets of V if and only if $\tilde{f}$ has three valued almost optimal 4-decomposition with respect to $V^\perp$ ■

Corollary 1 *If $f \in \mathcal{B}_n$ is a bent function and V is a two dimensional subspace of $\mathbb{F}_2^n$ then f is affine on all the cosets of V if and only if there exist $a, b \in \mathbb{F}_2^n$ such that $D_a D_b f = 0$.*

Proof : If $f \in \mathcal{B}_n$ is a bent function such that $D_a D_b f = 0$ for some $a, b \in \mathbb{F}_2^n$, $a \neq b$, then by theorem 7 [1] with respect to $V^\perp = \langle a, b\rangle^\perp$, $\tilde{f}$ has three-valued almost optimal 4-decomposition which in turn by theorem 1 above implies that restrictions of f are affine on all the flats parallel to the two dimensional subspace $V = \langle a, b\rangle$.

Conversely, suppose that the restriction of f are affine on all the flats parallel to the two dimensional subspace $V = \langle a, b\rangle$. By theorem 1 $\tilde{f}$ has three valued almost optimal 4-decomposition with respect to $V^\perp$. Again by theorem 7, [1] $D_a D_b f = 0$. ■

Corollary 2 *If $f \in \mathcal{B}_n$ is a cubic bent function then $f \in \mathcal{E}$.*

Proof : By corollary 5 [1], since f is cubic it must have a zero second derivative which implies by corollary 1 that $f \in \mathcal{E}$.

4 Conclusion

In this paper we have characterized the class $\mathcal{E}$ of bent functions which are affine of all the flats corresponding to a given 2 dimensional subspace by using their second derivative. It is to be noted that these are the functions that can be constructed by concatenating 2-variable affine functions. Further it is shown that all cubic bent functions are in this class $\mathcal{E}$ as well as all the functions in $\mathcal{M}$.

References

[1] Anne Canteaut and Pascale Charpin. Decomposing Bent Functions. IEEE Trans. Inform. Theory, **49** no. 8 (2003), 2004 - 2019.

[2] A. Canteaut, M. Daum, H. Dobbertin and G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, **154** (2006), 202 - 218.

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

[4] C. Carlet. On secondary constructions of resilient and bent functions. *Coding, Cryptography and Combinatorics*. Progress in computer science and applied logic, Birkhauser Verlag, Basel, **23** (2004), 3 - 28.

[5] Pascale Charpin. Normal Boolean functions. Journal of Complexity **20** (2004), 245 - 265.

[6] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, (1974).

[7] J. F. Dillon. Elementary Hadamard difference sets. In *Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing*. Utility Mathematics, Winnipeg (1975), 237- 249.

[8] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption - FSE'94*. Lecture Notes in Computer Science **1008** (1995), 61 - 74.

[9] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A* **20** (1976), 300 - 305.