On construction of non-weakly-normal bent functions

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

Abstract

Given two non-weakly-normal bent functions on n-variables a new method is proposed to construct a non-weakly-normal bent function on $(n+2)$-variables.

1 Introduction

Let $n = 2m$ be an even positive integer. Any function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ is called a Boolean functions on n variables. A bent function on n variables is a function whose Hamming distance is maximum from the set of all affine functions. The Walsh Hadamard transform of f at at $\lambda \in \mathbb{F}_2^n$ is given by $W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle \lambda, x \rangle}$ where $\langle x, \lambda \rangle$ is an inner product of x and λ on $\mathbb{F}_2^n$. A Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is bent if and only if $|W_f(\lambda)| = 2^m$ for all $\lambda \in \mathbb{F}_2^n$. Bent functions were first constructed by Rothaus [8] and Dillon [4, 5].

Definition 1 *A Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is called normal (weakly-normal) if f is constant (affine) on an $\frac{n}{2}$-dimensional flat of $\mathbb{F}_2$.*

Dobbertin [6] introduced the notion of normality and used normal bent functions to construct balanced functions with high nonlinearity. However for a long time no non-normal or non-weakly-normal bent function was known. Non-normal and non-weakly-normal bent functions for $n = 10$ and $n = 14$, respectively were first constructed by Canteaut, Daum, Dobbertin and Leander [1]. Further they proved that

Theorem 1 *(Lemma 10, [1]) Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be a Boolean function. The following properties are equivalent:*

1. *f is (weakly) normal.*
2. *The function*
$$g : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2$$
defined by
$$g(x, y, z) = f(x) + yz$$
is (weakly) normal.

By using this result it is possible to construct non-(weakly)-normal bent functions on higher dimensional spaces starting from a non-(weakly)-normal function on $\mathbb{F}_n$ for some n. Carlet, Dobbertin and Leander [2] proved that the direct sum of a non-(weakly)-normal bent function with any (weakly)-normal one is non-(weakly)-normal. Considering the difficulty of deciding non-(weak)-normality of bent functions any such secondary construction which guarantees non-(weak)-normality is extremely important.

2 Main Result

In this section we present our main result, a generalization of theorem 1.

Theorem 2 *Let $f_1, f_2 : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be two Boolean functions. The following statements are equivalent:*

1. *f_1 or f_2 is weakly-normal.*
2. *The function*
$$g : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2$$
defined by
$$g(x, y, z) = f_1(x) + yz + (y + z)(f_1(x) + f_2(x))$$
is weakly-normal.

Proof : Suppose g is weakly-normal. Therefore there exists an $\frac{n+2}{2}$ dimensional flat E, $\gamma \in \mathbb{F}_2^n$ and $\alpha, \beta \in \mathbb{F}_2$ such that

$$h(x, y, z) = g(x, y, z) + \alpha y + \beta z + \langle \gamma, x \rangle$$

takes the same value, c, on E. We claim that either $f_1(x)$ of $f_2(x)$ is weakly normal.

For $a, b \in \mathbb{F}_2$ we define

$$E_{ab} = \{x \in \mathbb{F}_2^n | (x, a, b) \in E\}.$$

Suppose $x \in E_{ab}$, then

$$c = h(x, a, b) = f_1(x) + ab + (a + b)(f_1(x) + f_2(x)) + \alpha a + \beta b + \langle \gamma, x \rangle$$

i.e.,

$$f_1(x) + (a + b)(f_1(x) + f_2(x)) = c + ab + \alpha a + \beta b + \langle \gamma, x \rangle.$$

Note that

$$f_1(x) + (a + b)(f_1(x) + f_2(x)) = \begin{cases} f_1(x) & \text{i}fa + b = 0 \\ f_2(x) & \text{i}fa + b = 1 \end{cases}$$

Therefore if $x \in E_{ab}$ then either $f_1(x)$ or $f_2(x)$ is affine on E_{ab}.

If one of the flats E_{ab} has dimension $\geq \frac{n}{2}$ then we are done. If this is not true, all the flats E_{ab} have dimension $\frac{n}{2} - 1$. Furthermore since the union of all E_{ab} is a flat, all E_{ab} are cosets of the same subspace U, we write $E_{ab} = x_{ab} + U$. Moreover, $x_{\alpha,\overline{\beta}} \neq x_{\overline{\beta},\alpha}$. Otherwise for any element $(x, \overline{\alpha}, \beta) \in E$ the element $(x, \alpha, \overline{\beta}) \in E$. Then, if we consider two elements $(x, \overline{\alpha}, \beta)$ and (x', α, β) in E, we obtain that,

$$(x, \overline{\alpha}, \beta) + (x, \alpha, \overline{\beta}) + (x', \alpha, \beta) = (x', \overline{\alpha}, \overline{\beta})$$

belongs to E implying that $h(x', \alpha, \beta) = h(x', \overline{\alpha}, \overline{\beta})$. But,

$$\begin{aligned} h(x', \overline{\alpha}, \overline{\beta}) &= f_1(x') + \overline{\alpha}\overline{\beta} + (\overline{\alpha} + \overline{\beta})(f_1(x') + f_2(x')) + \alpha\overline{\alpha} + \beta\overline{\beta} + \langle \gamma, x \rangle \\ &= f_1(x') + \alpha\beta + (\alpha + \beta)(f_1(x') + f_2(x')) + \alpha + \beta + \langle \gamma, x \rangle \\ &= h(x', \alpha, \beta) + 1 \end{aligned}$$

which leads to a contradiction. Therefore since $x_{\alpha,\overline{\beta}} \neq x_{\overline{\alpha},\beta}$, the set $E_{\alpha,\overline{\beta}} \cup E_{\overline{\alpha},\beta}$ is a flat of dimension $\frac{n}{2}$. Moreover we deduce the following:
For all $x \in E_{\alpha,\overline{\beta}}$
$c = h(x, \alpha, \overline{\beta}) = f_1(x) + \alpha\overline{\beta} + (\alpha + \overline{\beta})(f_1(x) + f_2(x)) + \alpha\alpha + \beta\overline{\beta} + \langle \gamma, x \rangle$
i.e., $f_1(x) + (\alpha + \beta + 1)(f_1(x) + f_2(x)) = c + \alpha\beta + \langle \gamma, x \rangle$.
Similarly for all $x \in E_{\overline{\alpha},\beta}$
$c = h(x, \overline{\alpha}, \beta) = f_1(x) + \overline{\alpha}\beta + (\overline{\alpha} + \beta)(f_1(x) + f_2(x)) + \alpha\overline{\alpha} + \beta\beta + \langle \gamma, x \rangle$
i.e., $f_1(x) + (\alpha + \beta + 1)(f_1(x) + f_2(x)) = c + \alpha\beta + \langle \gamma, x \rangle$.
Therefore when $x \in E_{\alpha,\overline{\beta}} \cup E_{\overline{\alpha},\beta}$
$f_1(x) + (\alpha + \beta + 1)(f_1(x) + f_2(x)) = c + \alpha\beta + \langle \gamma, x \rangle$.
Thus either $f_1(x)$ or $f_2(x)$ is weakly normal.

Conversely suppose $f_1(x)$ is weakly normal which implies that there exists an $\frac{n}{2}$ dimensional space E on which $f_1(x)$ is affine. Suppose $f_1(x) = \langle \gamma, x \rangle + c$ on E. Consider the $\frac{n+2}{2}$ dimensional subspace
$E' = E \times \{0\} \times \{0\} \cup E \times \{1\} \times \{1\}$.
It can be checked that
$g(x, 0, 0) = f_1(x) = \langle \gamma, x \rangle + c$
and
$g(x, 1, 1) = f_1(x) + 1 = \langle \gamma, x \rangle + c + 1$
Therefore we can write $g(x, y, z) = \langle \gamma, x \rangle + y + c$ for all $(x, y, z) \in E'$. Thus g is weakly normal. ■

Thus if we start with two non-weakly-normal bent functions f_1 and f_2 on n variables then the function $g(x, y, z)$ is a non-weakly-normal function on $n + 2$ variables. The construction given in 1 cannot increase the algebraic degree of the bent function on $n + 2$ variables whereas our construction increases degree by 1 if algebraic degree of f_1 and $f_1 + f_2$ are same. Thus unlike the construction in [1] starting from two non-weakly-normal bent functions on n variables and algebraic degree $\frac{n}{2}$ with $deg(f_1) = deg(f_1 + f_2)$ if is possible to construct a non-weakly-normal bent function of algebraic degree $\frac{n+2}{2}$, which is optimal.

References

[1] A. Canteaut, M. Daum, H. Dobbertin and G. Leander. Normal and Non Normal Bent Functions. *Workshop on Coding and Cryptography '03*, pages 91 - 100.

[2] C. Carlet, H. Dobbertin and G. Leander. Normal Extensions of Bent Functions. *IEEE Trans. on Information Theory*, number 11 pages 2880 - 2885, 2004.

[3] Pascale Charpin. Normal Boolean functions. Journal of Complexity , "Complexity Issue in Cryptography and Coding Theory", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday.

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

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

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

[7] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.

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