AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **38** (2007), Pages 267–272

On construction of non-normal Boolean functions

Sugata Gangopadhyay   Deepmala Sharma

Department of Mathematics
Indian Institute of Technology Roorkee – 247 667
INDIA

Abstract

A method is given to construct a Boolean function on $(n+2)$ variables which is not weakly $(k+1)$-normal given two Boolean functions on n variables neither of which is weakly k-normal.

1 Introduction

A function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ is called 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 $\langle u, v\rangle$. 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 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 A_n that is $\min\{d(f,l)|l \in A_n\}$ is called the nonlinearity of f. A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if and only if $|\{x \in \mathbb{F}_2^n | f(x) = 1\}| = |\{x \in \mathbb{F}_2^n | f(x) = 0)\}| = 2^{n-1}$.

Boolean functions find extensive applications in designing stream ciphers and block ciphers. High nonlinearity and balancedness are possibly the most important properties that a Boolean function which is being used in cipher systems must possess. When n is odd finding functions with maximum nonlinearity for $n > 7$ is an open problem. For n even the maximum nonlinearity attainable is $2^{n-1} - 2^{\frac{n}{2}-1}$ and functions having this nonlinearity are called bent functions [6, 7, 9]. However bent functions are never balanced, and so it is not possible to use a bent function directly as a component of a cipher system. Carlet [2] proved that if a bent function on n variables is constant over an $\frac{n}{2}$-dimensional flat then it is balanced on all the other flats of the same subspace. Dobbertin [8] used this idea to construct highly nonlinear, balanced Boolean functions. In the same paper he introduced the notion of non-normality, a function is called non-normal (not weakly normal) if it is not constant (affine) over any $\frac{n}{2}$-dimensional flat, otherwise the function is called normal (weakly normal). Canteaut, Daum, Dobbertin and Leander [1] gave the first examples of bent functions of $n = 10$ and $n = 14$ variables which are not normal and not weakly normal respectively. These functions were proved to be non-normal (not weakly normal) computationally by using an algorithm developed by Canteaut, Daum, Dobbertin and Leander [1].

Charpin [5] introduced the notion of k-normality and extended the notion of normality to odd n. For any n, a Boolean function on n variables is called k-normal if it is constant on a k-dimensional flat and weakly k-normal if it is affine on a k-dimensional flat. A function is called normal if it is $\lceil\frac{n}{2}\rceil$-normal, and weakly normal if it is weakly $\lceil\frac{n}{2}\rceil$-normal.

It is proved in [1] that if f is a non-normal (not weakly normal) Boolean function, then its direct sum with yz, the Boolean function g defined by $g(x, y, z) = f(x) + yz$, is non-normal (not weakly normal). Carlet, Dobbertin and Leander [4] proved that the direct sum of a non-normal (not weakly normal) bent and a normal bent results in a non-normal (not weakly normal) bent. This proof is done by introducing the notion of normal extension of a bent function and is restricted to the case when n is even and the functions are bent. While Dobbertin [8] proved that for increasing dimensions almost all Boolean functions are non-normal we know very few examples of non-normal functions. In this paper we demonstrate that if f_1 and f_2 are two Boolean functions on n variables which are not weakly k-normal then $g(x, y, z) = f_1(x) + yz + (y + z)(f_1(x) + f_2(x))$ is not a weakly $(k + 1)$-normal function. This gives a new secondary construction of $(n + 2)$-variable Boolean functions which are not weakly $(k + 1)$-normal from n-variable Boolean functions which are not weakly k-normal. We prove this fact by using the same technique as given in Lemma 25 of [1].

2 Main result

In this section we present our main result.

Theorem 1 *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 k-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 $(k + 1)$-normal.

Proof : Suppose g is weakly $(k + 1)$-normal. Therefore there exists a $(k + 1)$-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 or f_2 is weakly normal. For $a, b \in \mathbb{F}_2$ we define

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

Since E is a $(k+1)$-dimensional flat there exists an element $v \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$ and a $(k+1)$-dimensional subspace H of $\mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$ such that $E = v + H$. Let $\pi : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2^n$ be the projection map defined by $\pi(x, a, b) = x$ for all $(x, a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$.

It is to be noted that

$$E_{ab} = \pi((\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E).$$

Consider the case E_{ab} non-empty or equivalently

$$(\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E \neq \phi.$$

Suppose $(x, a, b), (y, a, b) \in (\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E$. Since $E = v + H$, $(x, a, b) - (y, a, b) = (x - y, 0, 0) \in (\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H$. Again if $(x, a, b) \in (\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E$ and $(z, 0, 0) \in (\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H$ then $(x, a, b) + (z, 0, 0) = (x + z, a, b) \in (\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E$. Therefore $(\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E$ is a coset of the subspace $(\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H$ for any $a, b \in \mathbb{F}_2$. Hence all non-empty E_{ab}'s are flats of the same subspace $\pi((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H)$ and therefore have the same dimension.

Let $\rho : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2 \times \mathbb{F}_2$ be the projection map $\rho(x, a, b) = (a, b)$, then $((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H)$ is the kernel of ρ restricted to H. Thus

$$\dim((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H) = k + 1 - \dim(\rho(H)).$$

The $\dim(\rho(H)) \in \{0, 1, 2\}$. Because π restricted to $\mathbb{F}_2^n \times \{0\} \times \{0\}$ is bijective

$$\dim(\pi((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H)) = \dim((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H).$$

Hence the dimension of $\pi((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H)$ is either $k + 1$ or k or $k - 1$.

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

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

Therefore if $E_{ab} \neq \phi$, either f_1 or f_2 is affine on E_{ab}.

If one of the flats E_{ab} has dimension $\geq k$ then we are done. If this is not true then for any $a, b \in \mathbb{F}_2$ the number of elements in E_{ab}, $|E_{ab}| \in \{0, 2^{k-1}\}$. Since $|E_{ab}| = |\{(x, a, b) | x \in E_{ab}\}|$, we have $|E| = \sum_{b \in \mathbb{F}_2} \sum_{a \in \mathbb{F}_2} |E_{ab}| = 2^{k+1}$. This is possible if and only if $|E_{ab}| = 2^{k-1}$, for all $a, b \in \mathbb{F}_2$. Suppose $E_{\alpha\overline{\beta}} = E_{\overline{\alpha}\beta}$, so that for any element $(x, \overline{\alpha}, \beta) \in E$ the element $(x, \alpha, \overline{\beta}) \in E$, where for any $\epsilon \in \mathbb{F}_2$, $\overline{\epsilon}$ denotes the complement of ϵ, i.e., $\overline{0} = 1$ and $\overline{1} = 0$. If we consider two elements $(x, \overline{\alpha}, \beta)$ and (x', α, β) in E, we find 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,

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

which contradicts h constant on E. Since $E_{\alpha\overline{\beta}}$ and $E_{\overline{\alpha}\beta}$ are distinct parallel flats of dimension $k-1$ in an $\mathbb{F}_2$-vector space the set $E_{\alpha\overline{\beta}} \cup E_{\overline{\alpha}\beta}$ is a flat of dimension k. 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 or f_2 is weakly normal.

Conversely suppose f_1 or f_2 is weakly normal. Suppose first f_1 is weakly normal, that is there is a k-dimensional flat E on which f_1 is affine. Suppose $f_1(x) = \langle \gamma, x \rangle + c$ on E, where $\gamma \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. Consider the $(k+1)$-dimensional flat

$$E' = (E \times \{0\} \times \{0\}) \cup (E \times \{1\} \times \{1\}).$$

It is to be noted that if E is a coset of the subspace H then E' is a coset of the subspace $H' = (H \times \{0\} \times \{0\}) \cup (H \times \{1\} \times \{1\})$. It can be checked that for $x \in E$,

$$g(x, 0, 0) = f_1(x) = \langle \gamma, x \rangle + c$$

and

$$g(x, 1, 1) = f_1(x) + 1 = \langle \gamma, x \rangle + c + 1.$$

Therefore $g(x, y, z) = \langle \gamma, x \rangle + y + c$ for all $(x, y, z) \in E'$.

Suppose second that f_2 is weakly k-normal, that is that there is a k-dimensional flat E on which f_2 is affine. Suppose $f_2(x) = \langle \gamma, x \rangle + c$ on E, where $\gamma \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. Consider the $(k+1)$-dimensional flat

$$E' = (E \times \{0\} \times \{1\}) \cup (E \times \{1\} \times \{0\}).$$

The flat E' constructed as above is a coset of the subspace $H' = (H \times \{0\} \times \{0\}) \cup (H \times \{1\} \times \{1\})$. As above we check that when $x \in E$,

$$g(x, 0, 1) = f_2(x) = \langle \gamma, x \rangle + c$$

and

$$g(x, 1, 0) = f_2(x) = \langle \gamma, x \rangle + c.$$

Therefore

$g(x, y, z) = \langle \gamma, x \rangle + c$ for all $(x, y, z) \in E'$. Thus g is weakly $(k + 1)$-normal. ■

By using the above theorem we can conclude that if f_1, $f_2 \in \mathcal{B}_n$ are not weakly k-normal functions then the function $g \in \mathcal{B}_{n+2}$ as constructed above is not a weakly $(k + 1)$-normal function. In case the $\deg(f_1 + f_2) = \max\{\deg(f_1), \deg(f_2)\}$ then $\deg(g) = \max\{\deg(f_1), \deg(f_2)\} + 1$, whereas in case of direct sum with the function yz the algebraic degree of the resulting function does not increase.

Remark 1 *It is to be noted that if f_1 and f_2 are bent functions, then by Proposition 8,* [4]*, it can be proved that if one of them is non-normal (not weakly normal) bent, then g is a non-normal (not weakly normal) bent. This result is proved by using the notion of normal extension of bent functions and therefore is not applicable when the functions are not bent. Our result on the other hand is applicable to k-normal functions on n variables, n even or odd.*

3 Conclusion

In this paper we demonstrate that techniques used in [1] can be used for secondary constructions which are not the direct sum of a function f with yz. Carlet [3] has studied secondary constructions of bent and resilient functions of the following type:

$$g(x,y) = f_1(x) + g_1(y) + (g_1 + g_2)(y)(f_1 + f_2)(x)$$

where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$. Our construction is a special case of this construction. It is an interesting open problem to find relationships between non-normality of f_1 and f_2 and properties of g_1, g_2.

Acknowledgment

The authors thank Claude Carlet and Subhamoy Maitra for helpful discussions. The authors are grateful to the reviewers for their careful reading of the paper and critical comments which helped to improve the paper substantially.

References

[1] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, Finding nonnormal bent functions, *Discrete Appl. Math.* **154** (2006), 202–218.

[2] C. Carlet, Two new classes of bent functions, In *Advances in cryptology—EUROCRYPT '93*, Lec. Notes Comp. Sc. **765** (1994), 77–101.

[3] 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.

[4] C. Carlet, H. Dobbertin and G. Leander, Normal Extensions of Bent Functions, *IEEE Trans. Inf. Theory* **50** no. 11 (2004), 2880–2885.

[5] Pascale Charpin, Normal Boolean functions, *J. 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 *Proc. 6th S.E. Conf. Combin., Graph Theory, and Computing*, Congressus Numerantium XIV, Utilitas Math., Winnipeg (1975), 237–249.

[8] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption—FSE '94*, Lec. Notes Comp. Sc. **1008** (1995), 61–74.

[9] O. S. Rothaus, On bent functions. *J. Combin. Theory (Ser. A)* **20** (1976), 300–305.

(Received 31 May 2006; revised 11 Dec 2006)