On construction of non-normal Boolean functions

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

Abstract

Given two non-weakly k-normal Boolean functions on n variables a method is proposed to construct a non-weakly $(k+1)$-normal Boolean function on $(n+2)$-variables.

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 $\mathcal{B}_n$. 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. In case n is odd finding functions with maximum nonlinearity for $n > 7$ is an open question. 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 [7, 8, 11]. However bent functions are never balanced because of which 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 [9] 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 (non-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] constructed non-normal and non-weakly normal bent functions for $n = 10$ and $n = 14$ for the first time. These functions were proved to be non-normal (non-weakly normal) computationally by using an algorithm developed by Daum, Dobbertin and Leander [6].

Charpin [5] introduced the notion of k-normality. A function is k-normal (weakly k-normal) if it is constant (affine) over a k-dimensional flat irrespective of whether n is odd or even. The concept of normality is also extended to odd variables in [5]. A function is called normal (weakly normal) if there exists a $\lceil \frac{n}{2} \rceil$-dimensional flat on which the function is constant (affine).

It is proved in [1] that the direct sum of a non-normal (non-weakly normal) function $f(x)$ with the function yz is a non-normal (non-weakly normal) function. Subsequently Carlet, Dobbertin and Leander [4] proved that the direct sum of a non-normal (non-weakly normal) bent and a normal bent results in a non-normal (non-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 [9] proved that for increasing dimensions almost all the functions are non-normal we know very few examples of non-normal functions. In this paper we demonstrate that if $f_1(x)$ and $f_2(x)$ are two non-weakly k-normal functions on n variables then $g(x,y,z) = f_1(x)+yz+(y+z)(f_1(x)+f_2(x))$ is a non-weakly $(k+1)$-normal function. This gives a new secondary construction of non-weakly $(k+1)$-normal functions from non-weakly k-normal functions. We prove this fact by using the same technique as given in lemma 10 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 $f_1(x)$ or $f_2(x)$ is weakly normal. For $a, b \in \mathbb{F}_2$ we define
$$E_{ab} = \{x \in \mathbb{F}_2^n | (x,a,b) \in E\}.$$
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 $(x,a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$. If $(\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap H$ is non-empty then

$$E_{ab} = \pi((\mathbb{F}_2^n \times \{a\} \times \{b\}) \cap E) = u + \pi((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H)$$

for some $u \in \mathbb{F}_2^n$. That is all the non-empty E_{ab}'s are cosets of the same subspace $\pi((\mathbb{F}_2^n \times \{0\} \times \{0\}) \cap H)$ and therefore have the same dimension. It can be checked that 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

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

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 $\geq k$ then we are done. If this is not true, it is clear that all the flats E_{ab} have dimension $k-1$. If $E_{\alpha\overline{\beta}} \cap E_{\overline{\alpha}\beta}$ is non-empty then $E_{\alpha\overline{\beta}} = E_{\overline{\alpha}\beta}$, and 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 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 $f_1(x)$ or $f_2(x)$ is weakly normal.

Conversely suppose $f_1(x)$ is weakly normal which implies that there exists a k-dimensional flat E on which $f_1(x)$ is affine. Suppose $f_1(x) = \langle \gamma, x \rangle + c$ on E. Consider the $(k+1)$-dimensional flat
$E' = E \times \{0\} \times \{0\} \cup E \times \{1\} \times \{1\}$.
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 $g(x,y,z) = \langle \gamma, x \rangle + y + c$ for all $(x,y,z) \in E'$.
Suppose that $f_2(x)$ is weakly k-normal which implies that there exists a k-dimensional flat E on which $f_2(x)$ is affine. Suppose $f_2(x) = \langle \gamma, x \rangle + c$ on E. Consider the $(k+1)$-dimensional flat
$E' = E \times \{0\} \times \{1\} \cup E \times \{1\} \times \{0\}.$
As above we check that when $x \in E \times \{0\} \times \{1\}$
$g(x,0,1) = f_2(x) = \langle \gamma, x \rangle + c$
when $x \in E \times \{1\} \times \{0\}$
$g(x,1,0) = f_2(x) = \langle \gamma, x \rangle + c$
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 two non-weakly k-normal functions then the function $g \in \mathcal{B}_{n+2}$ as constructed above is a non-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 (non-weakly normal) bent then g is a non-normal (non-weakly normal) bent. This result is proved by using the notion of normal extensions of bent functions and therefore not applicable in case 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 the techniques used in [1] can be used for secondary constructions which are not direct sum of a function $f(x)$ with yz. Carlet [3] has studied secondary constructions of bent and resilient functions of the following type:

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

where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$. Our construction is a special case of this construction. It is an interesting open problem to find the relationship between non-normality of f_1 and f_2 and properties of g_1, g_2.
Acknowledgement The authors thank Claude Carlet and Subhamoy Maitra for helpful discussions.

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. Two new classes of bent functions. In *Advances in cryptology - EUROCRYPT'93*. Lecture Notes in Computer Science, number 765, pages 77-101, 1994.

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

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

[5] 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.

[6] M. Daum, H. Dobbertin and G. Leander. An algorithm for checking normality of Boolean functions. *Workshop on Coding and Cryptography '03*, pages 133 - 142.

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

[8] 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.

[9] 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.

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

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