Direct Sum of Non Normal and Normal Bent Functions Always Produces Non Normal Bent Functions

Sugata Gangopadhyay and Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute
203, B. T. Road, Calcutta 700 108, INDIA
Email : sugata70@rediffmail.com, subho@isical.ac.in

Abstract

In this paper we analyse a subclass of normal Boolean functions which when composed to a non normal function by direct sum produces non normal functions. Take $f(x)$ to be a non normal function on n-variables and $g(y)$ to be a normal function on m-variables. It is then important to find out what are the conditions such that $f(x) + g(y)$ is non normal too. We identify a subclass (call this subclass $\mathcal{S}_m$) of m-variable normal function such that when $n > m$, both even, then $f(x) + g(y)$, the direct sum, is non normal when $g(y) \in \mathcal{S}_m$. In a recent paper by Canteaut, Daum, Dobbertin and Leander (WCC 2003) non normal bent functions are identified for the first time. The bent functions, which are inside $\mathcal{S}_m$, when composed with non normal bent functions, produce a wide range of non normal bent functions on higher number of variables. We prove that all the normal bent functions on m-variables belong to $\mathcal{S}_m$ and hence direct sum of non normal and normal bent functions always produces non normal bent functions.

Keyword : Boolean Function, Nonlinearity, Normality, Non normality, Bent Functions.

1 Introduction

Given a Boolean function on n-variables (n even), one important question is if there exists a flat of dimension $\frac{n}{2}$ such that the function is constant on this space. If such a space exists, we call the function *normal*. Prior to 2003, the existence of non normal bent function was not known, though the question has been posed by Dobbertin as early as in 1994 [8]. Very recently such functions could be constructed [1] for $n \geq 10$. The case for $n = 10$ has been demonstrated by the following example [1]. Let $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2 \subset \mathbb{F}_{2^{10}}$. Then there exists $\beta \in \mathbb{F}_{2^{10}}$ such that the function $f : \mathbb{F}_{2^{10}} \rightarrow \mathbb{F}_2$ with $f(x) = Tr(\alpha x^{57} + \beta x)$ is non normal. That this function is non normal was proved by running the algorithm presented in [5]. For the cases $n \geq 12$, existence of non normal bent function has been shown [1] by the

simple recursive construction $h(x,y) = f(x) + g(y)$, where $g(y)$ is basically a two variable function $g(y_1, y_2) = y_1 y_2$.

In this paper we try to achieve further generalization. We could identify a subclass of normal functions which when composed to non normal functions by direct sum always produce non normal functions.

Let $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, f : \mathbb{F}_2^n \to \mathbb{F}_2, g : \mathbb{F}_2^m \to \mathbb{F}_2$ and $h(x,y) = f(x) + g(y)$. If $f(x), g(y)$ are normal, then it is clear that $h(x,y)$ is also normal. However, the other direction is not completely answered yet. It is not clear that when $g(y), h(x,y)$ are normal then what is the status of $f(x)$. Therefore one would be interested to identify a subclass of m-variable normal functions such that for any $g(y)$ is in that class, $f(x)$ is normal. In this paper, we present an important sufficient condition on $g(y)$'s and identify a subclass of normal functions (call it $\mathcal{S}_m$) satisfying this.

Thus if $f(x)$ is non normal and $g(y) \in \mathcal{S}_m$, then $h(x,y)$ is also non normal (see Theorem 2 for more details). Further if $f(x), g(y)$ are both bent, then $h(x,y)$ is a non normal bent function. As a major contribution we show that all the normal bent functions belong to $\mathcal{S}_m$. Hence the direct sum of non normal and normal bent functions always produces non normal bent functions.

1.1 Preliminaries

In this section we present some definitions and notations following [1]. In this paper we always consider m, n as two positive integers. By an n-variable Boolean function we mean $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the function

$$a \in \mathbb{F}_2^n \mapsto f^w(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<a,x>}$$

is called the Walsh transform of f. Moreover, the $f^w(a)$, $a \in \mathbb{F}_2^n$ are called the Walsh coefficients of f. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called bent [9] if for all $a \in \mathbb{F}_2^n$, $f^w(a) = \pm 2^{\frac{n}{2}}$. These functions possess maximum possible nonlinearity on even number of variables. It is also known that

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+\alpha)} = 0$$

for any nonzero $\alpha \in \mathbb{F}_2^n$ iff f is bent [9].

A flat of dimension d of $\mathbb{F}_2^n$ is a coset of one of its d dimensional subspaces. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called normal (respectively weakly normal) if there exists a flat of dimension $\frac{n}{2}$ such that f is constant (respectively affine) on this flat. It is clear that a function f is weakly normal if and only if there exists an element $a \in \mathbb{F}_2^n$ such that $f(x) + < a, x >$ is normal.

Important characterizations of bent functions were provided by Rothaus in [9]. Different subclasses of normal bent functions have been identified by Dillon in [6, 7]. Carlet has also presented normal bent functions [3] which were not covered by Dillon. See [4, 2] for more recent references on bent functions.

2 The Subclass $\mathcal{S}_m$ of Normal Functions

We first start with a well known simple result for clarity.

Proposition 1 *Let $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, f : \mathbb{F}_2^n \to \mathbb{F}_2, g : \mathbb{F}_2^m \to \mathbb{F}_2$ and $h(x, y) = f(x) + g(y)$. If $f(x), g(y)$ are normal, then $h(x, y)$ is also normal.*

Proof : If f is normal, then there exists an $\frac{n}{2}$ dimensional flat E_1 over which f is constant. Similarly if g is normal, then there exists an $\frac{m}{2}$ dimensional flat E_2 over which g is constant. Then $E_1 \times E_2$ is an $\frac{n+m}{2}$ dimensional flat in $\mathbb{F}_2^n \times \mathbb{F}_2^m$ over which $h(x, y)$ is constant. ∎

However, it is not clear that when $g(y), h(x, y)$ are both normal, then what is the status of $f(x)$. In [1, Lemma 10, Page 94], it has been shown that if $g(y) = g(y_1, y_2) = y_1 y_2$, in that case $f(x)$ is normal. We generalize this result further. For this we need to describe a subset $\mathcal{S}_m$ of the set of normal functions.

Definition 1 *Let $y \in \mathbb{F}_2^m$, m even. Let $g(y)$ be an m-variable normal Boolean function. The function $g(y) \in \mathcal{S}_m$ if there exists an $\frac{m}{2}$ dimensional flat, say $E^{(g)}$, on which $g(y)$ is constant and the following propertry holds:*

given any nonzero $\alpha \in V^{(g)}$, there exists at least one $\beta \in \mathbb{F}_2^m$ such that $g(\beta) \neq g(\alpha + \beta)$ where $E^{(g)} = y^{(g)} + V^{(g)}$, $V^{(g)}$ is an $\frac{m}{2}$ dimensional vector subspace of $\mathbb{F}_2^m$ and $y^{(g)} \in \mathbb{F}_2^m$.

Proposition 2 *Let A be a nonsingular $m \times m$ binary matrix and $b \in \mathbb{F}_2^m$. The function $g(y) \in \mathcal{S}_m$ if and only if $g(Ay + b) \in \mathcal{S}_m$.*

Proof : Suppose $g \in \mathcal{S}_m$. Then g is constant on an $\frac{m}{2}$ dimensional flat $E^{(g)}$ for which the property in Definition 1 holds. It is possible to write $E^{(g)} = y^{(g)} + V^{(g)}$ for some $y^{(g)} \in \mathbb{F}_2^m$ and $\frac{m}{2}$ dimensional subspace $V^{(g)}$. Let $y \mapsto Ay + b$ be any affine transformation on $\mathbb{F}_2^m$. The inverse of this affine transformation can be written as $y \mapsto By + d$ where $B = A^{-1}$ and $d = -A^{-1}b$ (basically $d = A^{-1}b$ since we work on fields of characteristic 2).

Let $\tilde{g}(y) = g(Ay + b)$. Thus in the other direction $\tilde{g}(By + d) = g(y)$. Note that $E^{(\tilde{g})} = (By^{(g)} + d) + BV^{(g)}$ is an $\frac{m}{2}$ dimensional flat over which the function $\tilde{g}(y)$ is constant. Thus $\tilde{g}(y)$ is normal. Note that $V^{(\tilde{g})} = BV^{(g)}$ is also an $\frac{m}{2}$ dimensional subspace of $\mathbb{F}_2^m$.

Since $g(y) \in \mathcal{S}_m$, for any $\alpha \in V^{(g)}$ there exists $\beta \in \mathbb{F}_2^m$ such that $g(\beta) \neq g(\alpha + \beta)$. From this we obtain $\tilde{g}(B\beta + d) \neq \tilde{g}((B\beta + d) + B\alpha)$. When α varies over whole of $V^{(g)}$ then $B\alpha$ varies over whole of $V^{(\tilde{g})}$. Thus, if $g(y) \in \mathcal{S}_m$ then $\tilde{g}(y) \in \mathcal{S}_m$ too. The other direction can be proved similarly. ∎

Now we present the following important result which is a generalization of [1, Lemma 10, Page 94].

Theorem 1 *Let $n > m$, both even. Let $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, f : \mathbb{F}_2^n \to \mathbb{F}_2, g : \mathbb{F}_2^m \to \mathbb{F}_2$ and $h(x, y) = f(x) + g(y)$. Let $h(x, y)$ be normal. Further if $g(y) \in \mathcal{S}_m$ then $f(x)$ is normal.*

Proof : Since $h(x,y)$ is normal, it has a binary constant value (say c) on an $\frac{n+m}{2}$ dimensional flat E. Define

$$E_y = \{x \in \mathbb{F}_2^n | (x,y) \in E\} \text{ and } E^{(f)} = \bigcup_{y \in E^{(g)}} E_y.$$

Take any $x, x' \in E^{(f)}$. Then there exists $y, y' \in E^{(g)}$ such that $(x,y),(x',y') \in E$. Therefore $h(x,y) = h(x',y') = c$. Since $y, y' \in E^{(g)}$, $g(y) = g(y')$ and hence $f(x) = f(x')$. Thus the function $f(x)$ is constant over $E^{(f)}$.

Let $x, x', x'' \in E_y$. Then $(x,y),(x',y),(x'',y) \in E$ and hence $(x,y)+(x',y)+(x'',y) \in E$, since E is a flat. Thus, $(x+x'+x'',y) \in E$. Therefore, $x+x'+x'' \in E_y$. Thus E_y is a flat. Since E_y is a flat and f is constant on E_y, if the dimension of E_y is $\geq \frac{n}{2}$, then we are done. Otherwise, the dimension of each E_y is equal and the value is $\frac{n}{2} - i$ where $1 \leq i \leq \frac{m}{2}$.

Let $x, x', x'' \in E^{(f)}$. Hence there exists $y, y', y'' \in E^{(g)}$ such that $(x,y),(x',y'),(x'',y'') \in E$. Hence $(x,y)+(x',y')+(x'',y'') \in E$, since E is a flat. $(x+x'+x'', y+y'+y'') \in E$. Hence $x+x'+x'' \in E_{y+y'+y''}$. But $y+y'+y'' \in E^{(g)}$. Thus $x+x'+x'' \in E^{(f)}$. Hence $E^{(f)}$ is a flat.

Now we will show that if $g(y) \in \mathcal{S}_m$ (see Definition 1), then the dimension of $E^{(f)}$ is $\geq \frac{n}{2}$.

For this first we show that for distinct $y, y' \in E^{(g)}$, $E_y \cap E_{y'} = \emptyset$. If possible, let $x \in E_y \cap E_{y'}$. Then both $(x,y),(x,y') \in E$. Put $\alpha = y + y'$. Hence $\alpha \in V^{(g)}$. Since $g(y) \in \mathcal{S}_m$, there exists $\beta \in \mathbb{F}_2^m$ such that $g(\beta) \neq g(\alpha + \beta)$.

Since $n > m$, for any $\beta \in \mathbb{F}_2^m$, there exists $x' \in F_2^n$ such that $(x', \beta) \in E$. Hence $(x,y)+(x,y')+(x',\beta) = (x', \alpha+\beta) \in E$. Also $(x',\beta) \in E$. Hence, $h(x',\beta) = h(x',\alpha+\beta)$. This implies $g(\beta) = g(\alpha+\beta)$, which is a contradiction.

Thus $|E^{(f)}| = \sum_{y \in E^{(g)}} |E_y| = \sum_{y \in E^{(g)}} 2^{\frac{n}{2}-i} = 2^{\frac{m}{2}} 2^{\frac{n}{2}-i} = 2^{\frac{n+m}{2}-i} \geq 2^{\frac{n}{2}}$, since $1 \leq i \leq \frac{m}{2}$. Therefore $E^{(f)}$ is an (at least) $\frac{n}{2}$ dimensional flat. ■

Theorem 1 immediately provides the following result.

Theorem 2 *Let $n > m$, both even. Let $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, f : \mathbb{F}_2^n \to \mathbb{F}_2, g : \mathbb{F}_2^m \to \mathbb{F}_2$. Let $f(x)$ be non normal and $g(y) \in \mathcal{S}_m$. Then $h(x,y) = f(x) + g(y)$ is non normal.*

Proof : Let us consider the following : P : $h(x,y)$ is normal, Q : $g(y) \in \mathcal{S}_m$, and R : $f(x)$ is normal.

We have shown in Theorem 1 that $P \wedge Q \Rightarrow R$. Now $P \wedge Q \Rightarrow R \equiv \neg(P \wedge Q) \vee R \equiv (\neg P \vee \neg Q) \vee R \equiv (R \vee \neg Q) \vee \neg P \equiv \neg(\neg R \wedge Q) \vee \neg P \equiv \neg R \wedge Q \Rightarrow \neg P$. Thus we have proved that if $f(x)$ is non normal and $g(y) \in \mathcal{S}_m$ then $h(x,y)$ is non normal. ■

In fact the 2-variable function $g(y) = g(y_1, y_2) = y_1 y_2$ described in [1, Lemma 10, Page 94] belongs to $\mathcal{S}_2$. It is clear that the recursive application of the two variable function $g(y) = g(y_1, y_2) = y_1 y_2$ described in [1, Lemma 10, Page 94] provides a general form $g(y) = g(y_1, \ldots, y_m) = y_1 y_2 + \ldots + y_{m-1} y_m$ when applied $\frac{m}{2}$ times. Thus using the arguement of [1, Lemma 10, Page 94] it is clear that if $f(x)$ is non normal bent, then $f(x)+g(y)$ is also non normal bent. It is clear that the function $g(y) = g(y_1, \ldots, y_m) = y_1 y_2 + \ldots + y_{m-1} y_m$ is normal. We will now present a much generalized result that any normal bent function belongs to $\mathcal{S}_m$.

Lemma 1 *Let $g(y)$ be an m-variable normal bent function. Then $g(y) \in \mathcal{S}_m$.*

Proof : Suppose if possible $g(y) \notin \mathcal{S}_m$. Since $g(y)$ is normal, there exists an $\frac{m}{2}$ dimensional flat, say $E^{(g)}$, on which $g(y)$ is constant. Let $E^{(g)} = y^{(g)} + V^{(g)}$, where $V^{(g)}$ is an $\frac{m}{2}$ dimensional vector subspace of $\mathbb{F}_2^m$ and $y^{(g)} \in \mathbb{F}_2^m$.

As we have taken $g(y) \notin \mathcal{S}_m$, there exists a nonzero $\alpha \in V^{(g)}$, such that $g(\beta) = g(\alpha + \beta)$ for all $\beta \in \mathbb{F}_2^m$. Thus $\sum_{y \in \mathbb{F}_2^m} (-1)^{g(y)+g(y+\alpha)} = 2^m$. However, it is known that $\sum_{y \in \mathbb{F}_2^m} (-1)^{g(y)+g(y+\alpha)} = 0$ for any nonzero $\alpha \in \mathbb{F}_2^m$ iff g is bent [9]. Hence we land into a contradiction. Thus the proof. ∎

Thus we get the following important result.

Theorem 3 *Let $n > m$, both even. Let $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, f : \mathbb{F}_2^n \to \mathbb{F}_2, g : \mathbb{F}_2^m \to \mathbb{F}_2$. Let $f(x)$ be non normal bent and $g(y)$ be a normal bent function. Then $h(x, y) = f(x) + g(y)$ is a non normal bent function.*

Proof : The proof follows from Lemma 1 and Theorem 2. ∎

It should be noted that the requirement $n > m$ in Theorem 3 does not pose a serious constraint for construction of non normal bent functions. Suppose we have an n-variable non normal bent function and our requirement is to construct an $(n + m)$-variable non normal bent function, where $m > n$. Then we can write m as a sum $m = m_1 + \ldots + m_k$ with the property $m_1 < n, m_2 < n + m_1, \ldots, m_k < n + m_1 + \ldots + m_{k-1}$, where all m_i's are even. To the initial non normal bent function we add successively m_i-variable normal bent functions for $i = 1, \ldots, k$. Final result is a non normal bent function on $(n + m)$-variables.

References

[1] A. Canteaut, M. Daum, H. Dobbertin and G. Leander. Normal and Non normal Bent Functions. In *Proceedings of Workshop on Coding and Cryptography, WCC 2003*, Pages 91–100, Versailles, France, March 2003.

[2] A. Canteaut and P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, August 2003.

[3] C. Carlet. Two new classes of bent functions. In *Advances in Cryptology - Eurocrypt'93*, number 765, Lecture notes in computer science, pages 77 - 101. Springer - Verlag, 1994

[4] C. Carlet. Recent results on binary bent functions. In *International Conference on Combinatorics, Information Theory and Statistics*, 1997.

[5] M. Daum, H. Dobbertin and G. Leander. An Algorithm for checking Normality of Boolean Functions. In *Proceedings of Workshop on Coding and Cryptography, WCC 2003*, Pages 133–142, Versailles, France, March 2003.

[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, Pages 237–249, 1975.

[8] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption, 1994*, number 1008 in Lecture Notes in Computer Science, pages 61–74. Springer-Verlag, 1995.

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