On the Lower Bounds of the Second Order Nonlinearity of some Boolean Functions

Sugata Gangopadhyay[1], Sumanta Sarkar[2], Ruchi Telang[1],
[1]Mathematics Department, Indian Institute of Technology
Roorkee - 247 667 Uttarakhand INDIA
[2]Projet SECRET, INRIA
B. P. 105, 78153 Le Chesnay Cedex FRANCE
gsugata@gmail.com, sumanta.sarkar@inria.fr, telang.ruchi82@gmail.com

March 16, 2009

Abstract

The r-th order nonlinearity of a Boolean function is an important cryptographic criterion in analyzing the security of stream as well as block ciphers. It is also important in coding theory as it is related to the covering radius of the Reed-Muller code $\mathcal{R}(r, n)$. In this paper we deduce the lower bounds of the second order nonlinearity of the following two types of Boolean functions:

1. $f_\lambda(x) = Tr_1^n(\lambda x^d)$ with $d = 2^{2r} + 2^r + 1$ and $\lambda \in \mathbb{F}_{2^n}$ where $n = 6r$.
2. $f(x, y) = Tr_1^t(xy^{2^i+1})$ where $x, y \in \mathbb{F}_{2^t}, n = 2t, n \geq 6$ and i is an integer such that $1 \leq i < t$, $\gcd(2^t - 1, 2^i + 1) = 1$.

For some λ, the functions of the first type are bent functions whereas Boolean functions of the second type are all bent functions, i.e., they possess maximum first order nonlinearity. It is demonstrated that in some cases our bounds are better than the previously obtained bounds.

Keywords: Boolean functions, derivative, second order nonlinearity.

1 Introduction

Boolean functions are important building blocks in the design of stream ciphers as well as block ciphers. Let f be an n-variable Boolean function. The r-th order nonlinearity of f, $nl_r(f)$, is the minimum Hamming distance between f and all n-variable Boolean functions of degree at most r. The sequence of values $nl_r(f)$ for r ranging from 1 to $n-1$ is said to be the nonlinearity profile of f. Nonlinearity profile of a Boolean function is a cryptographic criterion that plays an important role in the security of the cipher systems in which it is used. On the other hand, $nl_r(f)$ is exactly the distance from f to the Reed-Muller code, $\mathcal{R}(r,n)$, of size 2^n and order r. Therefore, the maximum value of $nl_r(f)$, while f varies over the set of all n-variable Boolean functions, is the covering radius of $\mathcal{R}(r,n)$.

The first order nonlinearity of f, $nl_1(f)$, is referred to as the nonlinearity of f and denoted by $nl(f)$. The value $nl(f)$ is the minimum of the Hamming distances between f and all the n-variable affine functions. There has been extensive research on the first order nonlinearity of Boolean functions. For results on construction of Boolean functions with high (first order) nonlinearity we refer to [1, 11, 12, 14, 15, 16].

It is to be noted that very little is known about $nl_r(f)$ for $r > 1$. The best known asymptotic upper bound on $nl_r(f)$ is found in [5] which is as follows:

$$nl_r(f) = 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{\frac{n}{2}} + O(n^{r-2}).$$

Computation of the r-th order nonlinearity for $r > 1$ is itself a difficult problem. Efforts are made to compute second order nonlinearity by using decoding techniques of the second order Reed-Muller codes. The algorithms developed till date [6, 7, 10] compute second order nonlinearity for $n \leq 11$ and for $n \leq 13$ for some special cases. Thus there is a need to find out lower bounds of the second order nonlinearity of Boolean functions and in general lower bounds for r-th order nonlinearity of Boolean functions (for $r \geq 1$) which is satisfied for all values of n. In [9] Boolean functions have been constructed whose lower bound of the r-th order nonlinearity is $2^{n-r-3}(r+5)$.

Recently Carlet [4] has introduced a method to determine lower bound of the r-th order nonlinearity of a function from the upper bound of the $(r-1)$-th order nonlinearity of its first derivatives. He has applied this to obtain lower bounds of some functions including Welch function and multiplicative inverse function. These functions have very high first order nonlinearity. In another paper, Sun and Wu [17] have obtained lower bounds of the second order nonlinearity of some functions whose first order nonlinearities are very high.

In this paper we deduce the lower bounds of the second order nonlinearity of the following two types of Boolean functions:

1. $f_\lambda(x) = Tr_1^n(\lambda x^d)$ with $d = 2^{2r} + 2^r + 1$ and $\lambda \in \mathbb{F}_{2^n}$ where $n = 6r$.
2. $f(x,y) = Tr_1^t(xy^{2^i+1})$ where $x, y \in \mathbb{F}_{2^t}, n = 2t, n \geq 6$ and i is an integer such that $1 \leq i < t$, $\gcd(2^t-1, 2^i+1) = 1$.

For some λ, the functions of the first type are bent functions whereas Boolean functions of the second type are all bent functions, i.e., they possess maximum first order nonlinearity. It is demonstrated that in some cases our bounds are better than the previously obtained bounds.

2 Preliminaries

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and $\mathbb{F}_{2^n}$ be the extension field of degree n over $\mathbb{F}_2$. The finite field $\mathbb{F}_{2^n}$ can be considered as an n dimensional vector space over $\mathbb{F}_2$. The set containing all invertible elements of $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}^*$. Any function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is called a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. For any set S the cardinality of S is denoted by $|S|$. For any two functions $f, g \in \mathcal{B}_n$, $d(f, g) = |\{x : f(x) \neq g(x), x \in \mathbb{F}_{2^n}\}|$ is said to be the Hamming distance between f and g. The trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is defined by

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$$

for all $x \in \mathbb{F}_{2^n}$. Given any $x, y \in \mathbb{F}_{2^n}$, $Tr_1^n(xy)$ is an inner product of x and y. Let $f_\lambda(x) = Tr_1^n(\lambda x)$ for all $x \in \mathbb{F}_{2^n}$. The set of affine functions $\mathcal{A}_n$ is defined as follows:

$$\mathcal{A}_n = \{f_\lambda + \epsilon : \lambda \in \mathbb{F}_{2^n}, \epsilon \in \mathbb{F}_2\}.$$

Suppose $B = \{b_1, \ldots, b_n\}$ is a basis of $\mathbb{F}_{2^n}$. Then any $x \in \mathbb{F}_{2^n}$ can be written as

$$x = x_1 b_1 + \ldots + x_n b_n \text{ where } x_i \in \mathbb{F}_2, \text{ for all } i = 1, \ldots, n.$$

Once a basis B of $\mathbb{F}_{2^n}$ is fixed any function $f \in \mathcal{B}_n$ can be written as a function of $x_1, \ldots, x_n$ as follows

$$f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a(\prod_{i=1}^{n} x_i^{a_i}), \text{ where } \mu_a \in \mathbb{F}_2.$$

The algebraic degree of f, denoted by $\deg(f)$, is the maximal value of weight of a, $wt(a)$, such that $\mu_a \neq 0$. The weight of a, $wt(a) = \sum_{i=1}^n a_i$ where the sum is over integers.

Definition 1 *The derivative of f with respect to $a \in \mathbb{F}_{2^n}$, is denoted by $D_a f$ and is the Boolean function $D_a f(x) = f(x) + f(x + a)$ for all $x \in \mathbb{F}_{2^n}$.*

The higher order derivatives are defined as follows:

Definition 2 *Let V be a m dimensional subspace of $\mathbb{F}_{2^n}$ generated by $a_1, \ldots, a_m$, that is $V = \langle a_1, \ldots, a_m\rangle$. The m-th order derivative of $f \in \mathcal{B}_n$ is defined by*

$$D_V f(x) = D_{a_1} \ldots D_{a_m} f(x) \textit{ for all } x \in \mathbb{F}_{2^n}.$$

It is to be noted that the m-th order derivative of f depends only on the choice of the m dimensional subspace V and independent of the choice of the basis of V. The Walsh transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\lambda) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}.$$

Nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l \in \mathcal{A}_n}\{d(f,l)\}$. The multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}]$ is said to be the Walsh spectrum of f. Nonlinearity and Walsh spectrum of $f \in \mathcal{B}_n$ is related as follows:

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

Using Parseval's identity

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_f(\lambda)^2 = 2^{2n}$$

it can be shown that $|W_f(\lambda)| \geq 2^{n/2}$ as a consequence $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 3 *Suppose n is an even integer. A function $f \in \mathcal{B}_n$ is said to be a bent function if and only if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ (i.e., $W_f(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$).*

Clearly for even n the bent functions are Boolean functions with maximum nonlinearity and therefore optimally resistant to best affine approximation attacks. Next we introduce a generalization of the notion of nonlinearity.

Definition 4 *Suppose f is a Boolean function on n variables. For every non-negative integer $r \leq n$, we denote by $nl_r(f)$ the r-th order nonlinearity of f, which is the minimum Hamming distance of f and all functions of algebraic degree at most r.*

The following two propositions are due to Carlet [4].

Proposition 1 ([4], Proposition 2) *Let f be any n-variable Boolean function and r be a positive integer smaller than n, we have*

$$nl_r(f) \geq \frac{1}{2}\max_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f)$$

In particular for $r = 2$, we have

$$nl_2(f) \geq \frac{1}{2}\max_{a \in \mathbb{F}_{2^n}} nl(D_a f).$$

Proposition 2 ([4], Proposition 3) *Let f be any n-variable boolean function and r be a positive integer smaller than n. We have*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f)}$$

In [4], Carlet remarked that in general, the lower bound given in Proposition 2 is better than that given in Proposition 1. If one does not know the exact values of $nl_{r-1}(D_a f)$ for all a, but some lower bound is known, then we have the following corollary.

Corollary 1 ([4], Corollary 2) *Let f be any n-variable function and r be a positive integer smaller than n. Assume that for some nonnegative integers M and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_{2^n}$, then*

$$\begin{array}{rcl} nl_r(f) & \geq & 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)M2^{m+1}+2^n} \\ & \approx & 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}} \end{array}$$

In this paper we use these results to obtain lower bounds of second order nonlinearities of some cubic bent functions. The derivative of any cubic function has algebraic degree at most 2. It is to be noted that the Walsh spectrum of a quadratic Boolean function (degree 2 Boolean function) is completely characterized by the dimension of the kernel of the bilinear form associated to it. We refer to [13, 3] for details. Below we state only the results which we use in this paper. Suppose $f \in \mathcal{B}_n$ is a quadratic function. The bilinear form associated to f is defined by $B(x,y) = f(0) + f(x) + f(y) + f(x+y)$. The kernel [3] of $B(x,y)$ is the subspace defined by

$$\mathcal{E}_f = \{x \in \mathbb{F}_{2^n} : B(x,y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

Following lemma is obtained from the definitions.

Lemma 1 ([3], Lemma 1) *Let f be any quadratic boolean function. The kernel, $\mathcal{E}_f$, is the subspace of $\mathbb{F}_2^n$ consisting of those a such that the derivative D_af is constant. That is*

$$\mathcal{E}_f = \{a \in \mathbb{F}_2^n | D_af = \mathit{constant}\}$$

The Walsh spectrum of any quadratic function $f \in \mathcal{B}_n$ is given below

Lemma 2 ([3], page 224) *If $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ is a quadratic Boolean function and $B(x,y)$ is the quadratic form associated to it, then the Walsh Spectrum of f depends only on the dimension, k, of the kernel, $\mathcal{E}_f$, of $B(x,y)$. The weight distribution of the Walsh spectrum of f is:*

$W_f(\alpha)$	*number of* α
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)}2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)}2^{(n-k-2)/2}$

3 Lower bound of second order nonlinearity

First we consider a class of cubic Boolean function studied by Canteaut, Charpin and Kyureghyan [3] of the form $f_\lambda(x) = Tr_1^n(\lambda x^d)$ with $d = 2^{2r} + 2^r + 1$ and $\lambda \in \mathbb{F}_{2^n}$ where $n = 6r$. Canteaut, Charpin and Kyureghyan [3] have characterized those λ for which f_λ is bent.

Theorem 1 *Let $f_\lambda(x) = Tr_1^n(\lambda x^d)$ with $d = 2^{2r} + 2^r + 1$ and $\lambda \in \mathbb{F}_{2^n}$ where $n = 6r$. Then*

$$\begin{array}{ll} nl_2(f_\lambda) & \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n}{2}+2r}+2^n} \\ & \approx 2^{n-1} - 2^{\frac{3n+4r-4}{4}}. \end{array}$$

Proof : It is known ([3], Proposition 3) that $D_a f_\lambda$ is always quadratic for all nonzero $a \in \mathbb{F}_{2^n}$. It is also proved that the dimension of the kernel of the bilinear form associated to $D_a f_\lambda$ is either $2r$ or $4r$ ([3], Proposition 4). Therefore, by Lemma 2 we get, $nl(D_a(f_\lambda))$ is either $2^{n-1} - \frac{1}{2}2^{\frac{n+2r}{2}}$ or $2^{n-1} - \frac{1}{2}2^{\frac{n+4r}{2}}$. Therefore,

$$\max_{a \in \mathbb{F}_{2^n}} (nl(D_a(f_\lambda))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+2r}{2}}.$$

Hence using Proposition 1 we get

$$nl_2(f_\lambda) \geq \frac{1}{2}(2^{n-1} - \frac{1}{2}2^{\frac{n+2r}{2}}).$$

For all nonzero $a \in \mathbb{F}_{2^n}$, we also have

$$\begin{array}{rcl} nl(D_a f_\lambda) & \geq & 2^{n-1} - \frac{1}{2}2^{\frac{n+4r}{2}} \\ & = & 2^{n-1} - 2^{\frac{n}{2}+2r-1}. \end{array} \quad (1)$$

Therefore, we have a scope to get better bound by using Corollary 1. Comparing the inequality (1) and Corollary 1, we get $M = 1$ and $m = \frac{n}{2} + 2r - 1$. So,

$$\begin{array}{rcl} nl_2(f_\lambda) & \geq & 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n}{2}+2r}+2^n} \\ & \approx & 2^{n-1} - 2^{\frac{3n+4r-4}{4}}. \end{array} \quad (2)$$

It is quite obvious that for large n, the bound given in (2) is better than that of (1). Therefore we conclude that

$$\begin{array}{ll} nl_2(f_\lambda) & \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n}{2}+2r}+2^n} \\ & \approx 2^{n-1} - 2^{\frac{3n+4r-4}{4}}. \end{array}$$

■

Next we consider the functions of the form

$$f(x,y) = Tr_1^t(xy^{2^i+1})$$

where $x, y \in \mathbb{F}_{2^t}, n = 2t, n \geq 6$ and i is an integer such that $1 \leq i < t$, $\gcd(2^t-1, 2^i+1) = 1$. It is to be noted that $y \rightarrow y^{2^i+1}$ where $\gcd(2^t-1, 2^i+1) = 1$ is a quadratic permutation over $\mathbb{F}_{2^t}$. The function f is a Maiorana-MacFarland type bent function of algebraic degree 3. Canteaut and Charpin [2] proved that functions of this form do not have affine derivatives. We determine the lower bound of the second order nonlinearity of these functions.

Theorem 2 *If* $f(x,y)= Tr_1^t(xy^{2^i+1})$*, where* $x, y \in \mathbb{F}_{2^t}, n = 2t, n \geq 6$ *and* i *is an integer such that* $1 \leq i < t$*,* $\gcd(2^t-1, 2^i+1) = 1$ *and* $\gcd(i,t) = e$ *then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{(\frac{3n}{2}+e)} - 2^{(\frac{3n}{4}+\frac{e}{2})} + 2^n(2^{(\frac{n}{4}+\frac{e}{2})} - 2^e + 1)}.$$

Proof : The derivative of f at $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$, $D_{(a,b)}f$, is a quadratic function ([2], Lemma 1).

Let the dimension of the kernel of the bilinear form associated to $D_{(a,b)}f$, that is the subspace $\mathcal{E}_{D_{(a,b)}f}$, be denoted by $k(a,b)$. By Lemma 1

$$\mathcal{E}_{D_{(a,b)}f} = \{(c,d) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} | D_{(c,d)}D_{(a,b)}f = \text{ constant}\}.$$

Consider a 2-dimensional subspace V generated by two vectors (a,b) and (c,d).The second derivative of f at V is as follows:

$$\begin{aligned} D_V f(x,y) &= D_{(c,d)}D_{(a,b)}f(x,y) \\ &= Tr_1^t(((ad+cb) + (ad^{2^i} + cb^{2^i})^{2^i})y^{2^i}) + Tr_1^t((bd^{2^i} + b^{2^i}d)x) \\ &\quad + Tr_1^t(ad^{2^i+1} + cb^{2^i+1}) + Tr_1^t((a+c)(bd^{2^i} + b^{2^i}d)). \end{aligned}$$

Case 1: Consider the case $b = 0$.
Subcase 1: $b = 0$, $d \neq 0$. The second derivative of f at $V = \langle (a,b),(c,d) \rangle$ is

$$\begin{aligned} D_V f(x,y) &= D_{(c,d)}D_{(a,0)}f(x,y) \\ &= Tr_1^t((ad + (ad^{2^i})^{2^i})y^{2^i}) + Tr_1^t(ad^{2^i+1})). \end{aligned}$$

$D_V f(x,y)$ is constant if and only if
$ad + (ad^{2^i})^{2^i} = 0$
i.e., $ad + a^{2^i}d^{2^{2i}} = 0$
i.e., $a^{2^i-1}d^{2^{2i}-1} = 1$
i.e., $(ad^{2^i+1})^{2^i-1} = 1$
i.e., $ad^{2^i+1} \in \mathbb{F}_{2^e}^*$, since $(ad^{2^i+1})^{2^t-1} = 1$ and $\gcd(i,t) = e$
i.e., $d^{2^i+1} \in a^{-1}\mathbb{F}_{2^e}^*$

Thus given any $a \in \mathbb{F}_{2^t}^*$ and $b = 0$, it is possible to choose d in $2^e - 1$ ways and for each choice of d, c in 2^t ways so that $D_{(c,d)}D_{(a,b)}f$ is constant. Therefore, the total number of ways in which (c,d) can be chosen so that $D_{(c,d)}D_{(a,0)}f$ is constant is $(2^e-1)2^t$.
Subcase 2: $b = 0$, $d = 0$. In this case the second derivative of f, $D_{(c,0)}D_{(a,0)} = 0$ for all $c \in \mathbb{F}_{2^t}$. Therefore, the total number of ways in which $(c,0)$ can be chosen so that $D_{(c,0)}D_{(a,0)}f$ is constant is 2^t.

We conclude the **Case 1** by observing that if $b = 0$ the total number of ways in which (c,d) can be chosen such that $D_{(c,d)}D_{(a,b)}f =$ constant is $(2^e-1)2^t + 2^t = 2^{e+t}$. Therefore, $\mathcal{E}_{D_{(a,0)}f}$ contains exactly 2^{e+t} elements which implies that $k(a,0) = e + t$.
Case 2: $b \neq 0$.

Subcase 1: $b \neq 0$ and $d = 0$. In this case we obtain

$$D_{(c,0)}D_{(a,b)}f(x,y) \;=\; Tr_1^t((cb + (cb^{2^i})^{2^i})y^{2^i}) + Tr_1^t(cb^{2^i+1})).$$

$D_{(c,0)}D_{(a,b)}f$ is constant if and only if
$cb + (cb^{2^i})^{2^i} = 0$
i.e., $cb + c^{2^i}b^{2^{2i}} = 0$
i.e., $c^{2^i-1}b^{2^{2i}-1} = 1$ assuming that $c \neq 0$.
i.e., $(cb^{2^i+1})^{2^i-1} = 1$
i.e., $cb^{2^i+1} \in \mathbb{F}_{2^e}^*$, since $(cb^{2^i+1})^{2^i-1} = 1$ and $\gcd(i,t) = e$
i.e., $c \in (b^{2^i+1})^{-1}\mathbb{F}_{2^e}^*$.

Thus the total number of ways in which $(c,0)$ can be chosen is so that $D_{(c,0)}D_{(a,b)}f$ is constant is 2^e (including the case $c = 0$).

Subcase 2: $b \neq 0$ and $d \neq 0$. In this case we have

$$\begin{aligned} D_{(c,d)}D_{(a,b)}f(x,y) \;=\; & Tr_1^t(((ad+cb) + (ad^{2^i} + cb^{2^i})^{2^i})y^{2^i}) \\ & + Tr_1^t((bd^{2^i} + b^{2^i}d)x) + Tr_1^t((ad^{2^i+1} + cb^{2^i+1}) \\ & + Tr_1^t((a+c)(bd^{2^i} + b^{2^i}d)) \end{aligned}$$

$D_{(c,d)}D_{(a,b)}f$ is constant if and only if
$(ad+cb) + (ad^{2^i} + cb^{2^i})^{2^i} = 0$
and $bd^{2^i} + b^{2^i}d = 0$.
From the second condition we obtain $(b^{-1}d)^{2^i-1} = 1$. We have
$(b^{-1}d)^{2^t-1} = 1$
therefore,
$(b^{-1}d)^{2^e-1} = 1$, since $\gcd(i,t) = e$
i.e., $b^{-1}d \in \mathbb{F}_{2^e}^*$ or $d \in b\mathbb{F}_{2^e}^*$
$d = \gamma b, \gamma \in \mathbb{F}_{2^e}^*$.
Substituting $d = \gamma b$ in first condition, we get $b(a\gamma + c) + (b^{2^i}(a\gamma + c))^{2^i} = 0$
i.e., $b^{2^{2i}}(a\gamma + c)^{2^i} = b(a\gamma + c)$
i.e., $b^{2^{2i}-1}(a\gamma + c)^{2^i-1} = 1$ assuming $a\gamma + c \neq 0$
i.e., $(b^{2^i+1}(a\gamma + c))^{2^i-1} = 1$ which implies $b^{2^i+1}(a\gamma + c) \in \mathbb{F}_{2^i}$. Since $(b^{2^i+1}(a\gamma + c))^{2^t-1} = 1$ and $\gcd(i,t) = e$ we have
$(b^{2^i+1}(a\gamma + c))^{2^e-1} = 1$.
i.e., $b^{2^i+1}(a\gamma + c) \in \mathbb{F}_{2^e}^*$.
Suppose (a,b) is fixed. Since $0 \neq d = \gamma b$ and $\gamma \in \mathbb{F}_{2^e}^*$, it is possible to choose γ in $2^e - 1$ ways. For each choice of d that is γ the second derivative $D_{(c,d)}D_{(a,b)}f$ is constant if and only if c is such that
$b(a\gamma + c) + (b^{2^i}(a\gamma + c))^{2^i} = 0$.
This is possible if either $c = a\gamma$ or $c = a\gamma + \alpha$ where $0 \neq \alpha \in b^{-(2^i+1)}\mathbb{F}_{2^e}^*$. Thus for each choice of γ there exists 2^e choice of c such that $D_{(c,d)}D_{(a,b)}f$ is constant.

Combining the two subcases of **Case 2** we infer that the total number of ways in which (c,d) can be chosen for so that $D_{(c,d)}D_{(a,b}f$ is constant for any given (a,b) such that $b \neq 0$ is $(2^e-1)2^e + 2^e = 2^{2e}$, therefore, $k(a,b) = 2e$. So we can write:

$$k(a,b) = \begin{cases} e+t, & b=0 \\ 2e, & b \neq 0 \end{cases}$$

The nonlinearity of $D_{(a,b)}f$ is,

$$\begin{aligned} nl(D_{(a,b)}f) &= 2^{n-1} - \frac{1}{2} \max_{(\lambda,\mu)\in\mathbb{F}_2^t\times\mathbb{F}_2^t} |W_{D_{(a,b)}f}(\lambda,\mu)| \\ &= 2^{n-1} - \frac{1}{2} 2^{\frac{n+k(a,b)}{2}}. \end{aligned}$$

Since, $1 \leq i < t$ and $e = gcd(i,t)$, we have $e < t$. Therefore,

$$\max_{(a,b)\in\mathbb{F}_2^t\times\mathbb{F}_2^t} (nl(D_{(a,b)}f)) = 2^{n-1} - \frac{1}{2} 2^{\frac{n+2e}{2}}.$$

By Proposition 1, we get

$$nl_2(f) \geq \frac{1}{2}(2^{n-1} - \frac{1}{2} \cdot 2^{\frac{n+2e}{2}}). \tag{3}$$

Note that in [4], it was remarked that in general, the bound obtained by Proposition 2 is better than that of Proposition 1. Therefore, we still have scope to improve the lower bound by using Proposition 2, since, the values of $nl(D_{(a,b)}f)$ are all known. We obtain,

$$\begin{aligned} &\sum_{(a,b)\in\mathbb{F}_2^t\times\mathbb{F}_2^t} nl(D_{(a,b)}f) \\ &= nl(D_{(0,0)}f) + \sum_{(a,0)\in\mathbb{F}_2^t\times\mathbb{F}_2^t, a\neq 0} nl(D_{(a,0)}f) + \sum_{(a,b)\in\mathbb{F}_2^t\times\mathbb{F}_2^t, b\neq 0} nl(D_{(a,b)}f) \\ &= (2^t-1)(2^{2t-1} - \tfrac{1}{2}2^{\frac{3t+e}{2}}) + 2^t(2^t-1)(2^{2t-1} - \tfrac{1}{2}2^{\frac{2t+2e}{2}}) \\ &= 2^{4t-1} - 2^{2t-1} + \tfrac{1}{2}(2^{2t+e} + 2^{\frac{3t+e}{2}} - 2^{3t+e} - 2^{\frac{5t+e}{2}}). \end{aligned}$$

Then by using Proposition 2, we get

$$\begin{aligned} nl_2(f) &\geq 2^{2t-1} - \frac{1}{2}\sqrt{2^{4t} - (2^{4t} - 2^{2t} + (2^{2t+e} + 2^{\frac{3t+e}{2}} - 2^{3t+e} - 2^{\frac{5t+e}{2}})} \\ &= 2^{2t-1} - \frac{1}{2}\sqrt{2^{3t+e} - 2^{\frac{3t+e}{2}} + 2^{2t}(2^{\frac{t+e}{2}} - 2^e + 1)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{(\frac{3n}{2}+e)} - 2^{(\frac{3n}{4}+\frac{e}{2})} + 2^n(2^{(\frac{n}{4}+\frac{e}{2})} - 2^e + 1)}. \end{aligned} \tag{4}$$

Let us now calculate the difference between the two lower bounds that we have obtained in (3) and (4) respectively. The difference is as follows.

$$
\begin{aligned}
&2^{n-1} - \tfrac{1}{2}\sqrt{2^{(\frac{3n}{2}+e)} - 2^{(\frac{3n}{4}+\frac{e}{2})} + 2^n(2^{(\frac{n}{4}+\frac{e}{2})} - 2^e + 1)} - \tfrac{1}{2}(2^{n-1} - \tfrac{1}{2}2^{\frac{n+2e}{2}})\\
&= 2^{n-2} + 2^{\frac{n+2e-4}{2}} - \tfrac{1}{2}\sqrt{2^{(\frac{3n}{2}+e)} - 2^{(\frac{3n}{4}+\frac{e}{2})} + 2^n(2^{(\frac{n}{4}+\frac{e}{2})} - 2^e + 1)}\\
&= \tfrac{1}{4}(2^{(e+\frac{n}{2})} + 2^n) - \tfrac{1}{2}\sqrt{2^{\frac{3n}{4}}(2^{(e+\frac{3n}{4})} + 2^{\frac{e+n}{2}} + 2^{\frac{n}{4}} - 2^{\frac{e}{2}} - 2^{(e+\frac{n}{4})})}\\
&> 0,
\end{aligned}
$$

for sufficiently large n. Therefore we conclude that,

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{(\frac{3n}{2}+e)} - 2^{(\frac{3n}{4}+\frac{e}{2})} + 2^n(2^{(\frac{n}{4}+\frac{e}{2})} - 2^e + 1)}.$$

■

Remark 1 *The function of Theorem 2 does not have any derivative in $\mathcal{R}(1,n)$ [2]. In [4], a general lower bound has been given on the second order nonlinearity for the n-variable functions which do not have derivatives in $\mathcal{R}(1,n)$ and the bound is $2^{n-1} - 2^{n-\frac{3}{2}}$. Let us calculate the difference between this bound and the one that we have obtained in (3). The difference is*

$$\frac{1}{2}(2^{n-1} - \frac{1}{2}2^{\frac{n+2e}{2}}) - (2^{n-1} - 2^{n-\frac{3}{2}}) = 2^{n-2}(\sqrt{2} - 1 - 2^{-\frac{n-2e}{2}}) > 0,$$

if $\sqrt{2} - 1 > 2^{-\frac{n-2e}{2}}$. Taking logarithm base 2 in both the sides of this inequality we obtain $2e < n + 2\log_2(\sqrt{2}-1)$ that is $2\gcd(i,t) < 2t + 2\log_2(\sqrt{2}-1)$. Therefore, Theorem 2 provides us a class of cubic bent functions with no affine derivatives whose lower bound on second order nonlinearity is greater than the general lower bound provided in [4].

Acknowledgments: The authors would like to thank Pascale Charpin for helpful suggestions. This paper is based on several discussions with her concerning second derivatives of bent functions and properties of quadratic Boolean functions. The authors are also thankful to anonymous reviewers whose comments have improved the technical as well as editorial quality of the paper.

References

[1] E. R. Berlekamp and L. R. Welch. Weight distributions of the cosets of the $(32,6)$ Reed-Muller code. In *IEEE Transactions on Information Theory*, Vol. 18(1), pp. 203–207, January 1972.

[2] A. Canteaut and P. Charpin. Decomposing Bent Functions, In *IEEE Transactions on Information Theory*, Vol. 49(8), pp. 2004-2019, 2003.

[3] A. Canteaut, P. Charpin and G. M. Kyureghyan. A new class of monomial bent functions. In *Finite Fields and their Applications*, Vol. 14, pp. 221-241, 2008.

[4] C. Carlet. Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications. In *IEEE Transactions on Information Theory*, Vol. 54(3), pp. 1262–1272, March 2008.

[5] C. Carlet and S. Mesnager. Improving the upper bounds on the covering radii of binary Reed-Muller codes. In *IEEE Transactions on Information Theory*, Vol. 53(1), January 2007.

[6] I. Dumer, G. Kabatiansky and C. Tavernier. List decoding of second order Reed-Muller codes up to the Johnson bound with almost linear complexity. In Proc. IEEE Int. Symp. Information Theory In *ISIT 2006*, Seattle, WA, Jul. 2006 pp, 138–142, 2006.

[7] R. Fourquet and C. Tavernier. List decoding of second order Reed-Muller codes and its covering radius implications. In *WCC 2007*, pp, 147–156, 2007.

[8] X. -d. Hou. On the norm and covering radius of the first order Reed-Muller codes. In *IEEE Transactions on Information Theory*, 43(3):1025–1027, 1997.

[9] T. Iwata and K. Kurosawa. Probabilistic higher order differential attack and higher order bent functions. In Asiacrypt 1999, Lecture Notes in Computer Science 1716, Springer-Verlag, pp 62–74, 1999.

[10] G. Kabatiansky and C. Tavernier List decoding of second order Reed-Muller codes. In 8th International Symposium of Communication theory and Applications, Ambleside, U. K. Jul. 2005.

[11] S. Kavut, S. Maitra S. Sarkar and M. D. Yücel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240. In *INDOCRYPT - 2006*, Lecture Notes in Computer Science 4329, Springer-Verlag, pp 266–279, 2006.

[12] S. Kavut and M. D. Yücel. Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions - 9 Variable Boolean Functions with Nonlinearity 242 In *AAECC*, Lecture Notes in Computer Science 4851, Springer-Verlag, pp 266–279, 2007.

[13] MacWilliams F. J., Sloane N. J. A., The theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.

[14] J. J. Mykkeltveit. The covering radius of the $(128, 8)$ Reed-Muller code is 56. In *IEEE Transactions on Information Theory*, Vol. 26(3), pp. 359–362, 1980.

[15] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. In *IEEE Transactions on Information Theory*, Vol. 29(3), pp. 354–356, 1983.

[16] O. S. Rothaus. On bent functions. In *Journal of Combinatorial Theory, Series A*,Vol. 20, pp. 300–305, 1976.

[17] G. Sun and C. Wu. The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity. In *Information Sciences*, Vol 179(3), pp. 267–278, January 2009