Lower Bound on Covering Radius of Reed-Muller Codes in Set of Balanced Functions

Brajesh Kumar Singh and Sugata Gangopadhyay
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee–247667, INDIA
Email: {singh.brajesho584, gsugata}@gmail.com

October 6, 2011

Abstract

In this paper, we derive a general lower bound on covering radius, $\hat{\rho}(0,2,n)$ of Reed-Muller code $RM(2,n)$ in $R_{0,n}$, set of balanced Boolean functions on n variables where $n = 2t+1$, t is an odd prime satisfying one of the following conditions

(i) $ord_t(2) = t-1$;

(ii) $t = 2s+1$, s is odd, and $ord_t(2) = s$.

Further, it is proved that $\hat{\rho}(0,2,11) \geq 806$, which is improved upon the bound obtained by Kurosawa et al.'s bound (*IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 468-475, 2004).

Keywords: Bent functions, Walsh–Hadamard transform, second-order nonlinearity.

1 Introduction

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n. A function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables. The set of Boolean functions on n variables is denoted by $\mathcal{B}_n$. The set of all n-tuples of elements of $\mathbb{F}_2$, $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_2, i \in \{1,2,\ldots,n\}\}$, is isomorphic to $\mathbb{F}_{2^n}$ as $\mathbb{F}_2$-vector spaces. Thus, the Boolean functions can also be thought of as functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. An element in $x \in \mathbb{F}_{2^n}$ can be uniquely associated to an element $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ once a basis of $\mathbb{F}_{2^n}$ is fixed. Let $\mathbb{Z}$ be the set of integers. We denote $|S|$ the cardinality of S. The additions in both $\mathbb{Z}$ and $\mathbb{F}_{2^n}$ are denoted by '$+$', whereas '$\oplus$' denotes the addition in $\mathbb{F}_2^n$. The Hamming weight of any element $\mathbf{x} \in \mathbb{F}_2^n$, $w_H(\mathbf{x}) := \sum_{i=1}^n x_i$, where the sum is over $\mathbb{Z}$. The algebraic normal form (ANF) of a Boolean function, $f \in \mathcal{B}_n$ is

$$f(x_1, x_2, \ldots, x_n) = \sum_{\mathbf{a}=(a_1,a_2,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \prod_{i=1}^{n} x_i^{a_i}, \text{ where } \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

The algebraic degree of a Boolean function, $f \in \mathcal{B}_n$ is denoted by $\deg(f)$ and defined as $\deg(f) = \max\{w_H(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0, \mathbf{a} \in \mathbb{F}_2^n\}$. For any $f, g \in \mathcal{B}_n$, the Hamming distance between f and g is $d(f,g) = |\{x \in \mathbb{F}_{2^n} | f(x) \neq g(x)\}|$.

The trace function $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as follows:

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

The functions $(x, y) \mapsto Tr_1^n(xy)$ and $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \cdot \mathbf{y} = \oplus_{i=1}^n x_i\, y_i$ are both inner products on $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$, respectively.

Definition 1. *The set of all Boolean functions in $\mathcal{B}_n$ with algebraic degrees less than or equal to r is said to be the Reed–Muller code of order r and length 2^n and denoted by $RM(r, n)$.*

The covering radius of $RM(r, n)$ is defined as:

$$\rho(r, n) = \max_{f \in \mathcal{B}_n} \min_{h \in RM(r,n)} d(f, h).$$

Definition 2. *A function $f \in \mathcal{B}_n$ is t-th order correlation immune if and only if its Walsh-Hadamard transform $W_f : \mathbb{F}_{2^n} \to [-2^n, 2^n]$ satisfies $W_f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_{2^n}$ with $1 \leq w_H(\alpha) \leq t$. A balanced t-th order correlation immune functions is called t-resilient function (any $f \in \mathcal{B}_n$ is balanced if $w_H(f) = 2^{n-1}$, i.e., $W_f(0) = 0$). Let $\mathcal{R}_{t,n}$ denote the set of t-resilient Boolean functions of n variables.*

Kurosawa et al. [9] have introduced a new covering radius, which measure the the maximum distance between t-resilient functions to Reed–Muller code of order r and length 2^n i.e.,

$$\hat{\rho}(t, r, n) = \max_{f \in \mathcal{R}_{t,n}} \min_{h \in RM(r,n)} d(f, h).$$

The rth-order nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$nl_r(f) = \min_{h \in RM(r,n)} d(f, h).$$

Therefore the maximum of the rth-order nonlinearities of the Boolean functions is $\rho(r, n)$, $\hat{\rho}(t, r, n))$, the covering radius of $RM(r, n)$ in the sets $\mathcal{B}_n$, $\mathcal{R}_{t,n}$ respectively.

.....

Therefore the maximum of the rth-order nonlinearities of the Boolean functions is $\rho(r, n)$ (respectively $\hat{\rho}(t, r, n))$, the covering radius of $RM(r, n)$ in the set $\mathcal{B}_n$ (respectively $\mathcal{R}_{t,n}$).

The exact values of $\rho(1, n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ for all even n and the exact value of $\rho(1, n) = 2^{n-1} - 2^{\frac{n-1}{2}}$ for all odd $n \leq 7$. Borissov, Braeken, Svetla and Preneel [1] proved that the covering radius, $\hat{\rho}(3, 2, n) = 32$. Moreover, they proved that the covering radii of the Reed-Muller code $RM(2, 7)$ in $\mathcal{R}_{0,7}$, $\mathcal{R}_{1,7}$, $\mathcal{R}_{2,7}$ are at least 40, 36, 32 respectively (see Table 2 in [1]). They provided these results computationally. In 2004, Kurosawa, Iwata and Yoshiwara [10] provided the general lower bound on covering radius, $\hat{\rho}(t, r, n)$ of $RM(r, n)$ in sets $\mathcal{R}_{t,n}$. The bound is given in following

Proposition 1. *[10, Theorem 5.2]*

$$\hat{\rho}(t, r, n) \geq \begin{cases} 2\rho(r, n-1) & \text{if } t = 0 \\ 2\hat{\rho}(t-1, r, n-1) & \text{if } t \geq 1. \end{cases} \tag{1}$$

Moreover, Fouquet and Tavernier [7] proved that $d(f, RM(2,10)) = 400$. Using proposition 1, $\hat{\rho}(0,2,11) \geq 800$. In this paper, we prove that $\hat{\rho}(0,2,11) \geq 806$. Further, we give a general lower bound for $\hat{\rho}(0,2,n)$ by computing the lower bounds of second-order nonlinearities for a class of semi-bent Boolean functions for all n, $n = 2t+1$, t is odd prime satisfying one of the following conditions

(i) $ord_t(2) = t-1$;

(ii) $t = 2s+1$, s is odd, and $ord_t(2) = s$.

2 Preliminaries

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_2^n$ is defined as

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

The multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}]$ is said to be the *Walsh–Hadamard spectrum* of f. The frequency distribution of the values in the Walsh–Hadamard spectrum of f is referred to as the *weight distribution* of the Walsh–Hadamard spectrum of f. The first-order nonlinearity of a Boolean function is referred to as the "nonlinearity" of f and denoted by $nl(f)$. The following relationship exists between nonlinearity of a Boolean function $f \in \mathcal{B}_n$ and its Walsh–Hadamard spectrum.

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

By Parseval's identity, $\sum_{\lambda \in \mathbb{F}_2^n} W_f(\lambda)^2 = 2^{2n}$, it can be shown that $\max\{|W_f(\lambda)| : \lambda \in \mathbb{F}_{2^n}\} \geq 2^{\frac{n}{2}}$ which implies that $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

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

Definition 4. *Suppose n is an odd positive integer. A function $f \in \mathcal{B}_n$ is said to be a semi-bent function if and only if $W_f(\lambda) \in \{0, 2^{\frac{n+1}{2}}, -2^{\frac{n+1}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$.*

For detailed study on Boolean functions and error correcting codes and extensive bibliography we refer to the book chapter [4] written by Carlet.

Definition 5. *The derivative of $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as*

$$D_a f(x) = f(x) + f(x+a) \text{ for all } x \in \mathbb{F}_{2^n}.$$

Suppose $a, b \in \mathbb{F}_{2^n}$ are $\mathbb{F}_2$-linearly independent and generate a two-dimensional subspace V in $\mathbb{F}_{2^n}$. The function

$$D_V f(x) = D_a D_b f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b) \text{ for all } x \in \mathbb{F}_{2^n}$$

is said to be the *second-derivative* of f with respect to the subspace V. It can be checked that $D_V f$ is independent of the choice of the basis of V. This notion can be further generalized. For more details we refer to [4].

2.1 Quadratic Boolean functions

Suppose $f \in \mathcal{B}_n$ be a quadratic Boolean function. The bilinear form associated with f is defined [11] by $B(x,y) = f(0) + f(x) + f(y) + f(x+y)$ and the kernel, $\mathcal{E}_f$, of $B(x,y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

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

Canteaut, Charpin and Kyureghyan [2] proved the following

Proposition 2. *[2, Lemma 1] Let $f \in \mathcal{B}_n$ be a quadratic Boolean function. Then*

$$\mathcal{E}_f = \{a \in \mathbb{F}_{2^n} : D_a f = \text{ constant }\}.$$

Any element $c \in \mathcal{E}_f$ is said to be a linear structure of f. If $f \in \mathcal{B}_n$ is a quadratic Boolean function then the weight distribution of the Walsh–Hadamard spectrum to f depends only on the dimension k of $\mathcal{E}_f$ which is given in Table 1 [2, 11].

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

Table 1: The weight distribution of the Walsh–Hadamard spectrum of a quadratic Boolean function $f \in \mathcal{B}_n$.

2.2 Semi-bent Boolean functions

For any prime p and $a \in \mathbb{Z}$, let $ord_p(a)$ denote the multiplicative order of a modulo p. The following result due to Charpin, Pasalić and Tavernier [5] is the main result used by us to obtain the lower bound.

Proposition 3. *[5, Lemma 2] Let n is even. Then any function of the form*

$$f_{\mathbf{c}}(x) = \sum_{i=1}^{\frac{n-2}{2}} c_i Tr_1^n(x^{2^i+1}), \text{ where } \mathbf{c} = (c_1, \ldots, c_{\frac{n-2}{2}}) \in \mathbb{F}_2^{\frac{n-2}{2}}, x \in \mathbb{F}_{2^n} \tag{2}$$

is a semi-bent Boolean function if and only if the polynomial

$$Q_{\mathbf{c}}(x) = \sum_{i=1}^{\frac{n-2}{2}} c_i \left(x^{2^i} + x^{2^{n-i}}\right) \tag{3}$$

is such that $Q_{\mathbf{c}}(x) = 0$ implies $x \in \mathbb{F}_4$.

Proposition 4. *[5, Lemma 3] Suppose $n = 2t$ is even, and the function $f_{\mathbf{c}} \in \mathcal{B}_n$, $\mathbf{c} \neq 0$ given by (2). Then,*

(a) If $n = 4$, $f_{\mathbf{c}}$ is semi–bent;

(b) *Let $n = 2t$, $t > 2$, and consider the function $f_{\mathbf{c}}$ such that $c_i \neq c_{t-i}$ for some i, then $f_{\mathbf{c}}$ is semi–bent Boolean function for any such $\mathbf{c}$ if and only if t be an odd prime satisfying one of the following properties*

(i) $ord_t(2) = t - 1$;

(ii) $t = 2s + 1$, s *is odd, and* $ord_t(2) = s$.

The first ten primes satisfying either (i) or (ii) are

$$3, 5, 7, 11, 13, 19, 23, 29, 37, 41.$$

The similar result for the Sophie–Germain primes $t = 2s + 1$, where t, s are primes, is given in following

Proposition 5. *Let $m = 2t$, $t = 2s + 1$ where t, s are primes. Let $f_{\mathbf{c}}(x) = \sum_{i=1}^{t-1} c_i Tr_1^m(x^{2^i+1})$, for all $x \in \mathbb{F}_{2^m}$, where $\mathbf{c} = (c_1, \ldots, c_{t-1}) \in \mathbb{F}_2^{t-1}$. Then $f_{\mathbf{c}}$ is a semi-bent Boolean function in $\mathcal{B}_m$ if and only if $c_i \neq c_{t-i}$ for some i.*

The first ten Sophie–Germain primes are

$$5, 7, 11, 23, 47, 59, 83, 107, 167, 179.$$

A direct consequence of Propositions 4 is

Lemma 1. *Let $m = 2t$, t be an odd prime satisfying at least one of the conditions (i), (ii) of Proposition 4, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^{t-1}$ such that $\mathbf{c} = \mathbf{a} \oplus \mathbf{b}$, and let $f_{\mathbf{a}}, f_{\mathbf{b}} \in \mathcal{B}_m$ be Boolean functions of the form*

$$f_{\mathbf{a}}(x) = \sum_{i=1}^{t-1} a_i Tr_1^m(x^{2^i+1}), f_{\mathbf{a}}(x) = \sum_{i=1}^{t-1} a_i Tr_1^m(x^{2^i+1}), \tag{4}$$

where $\mathbf{a} = (a_1, \ldots, a_{t-1}) \in \mathbb{F}_2^{t-1}, x \in \mathbb{F}_{2^m}$. Then $f_{\mathbf{c}} = f_{\mathbf{a}} + f_{\mathbf{b}}$ is also semi-bent if and only if $c_i \neq c_{t-i}$ for some i. Moreover, the function $\sum_{i=1}^{t-1} Tr_1^m(x^{2^i+1})$ is not a semi-bent Boolean function.

The following lemma proved by Charpin, Pasalić and Tavernier [5] provides a construction of cubic semi-bent functions by concatenating semi-bent functions.

Lemma 2. *[5, Theorem 12] Let $n = 2t$. Let $f_{\mathbf{a}}$ and $f_{\mathbf{b}}$ defined by (2), be two semi–bent Boolean functions on $\mathbb{F}_{2^n}$. Let us define the Boolean function $f : \mathbb{F}_{2^n} \times \mathbb{F}_2 \to \mathbb{F}_2$ as*

$$f(x, y) = (f_{\mathbf{a}} + \phi_u)(x)y + f_{\mathbf{b}}(x)(1 + y),$$

where $u \in \mathbb{F}_{2^n}$ and $\phi_u(x) = Tr_1^n(ux)$ a linear function. Set $I_e(\mathbf{a}) = \{i : a_i \neq 0$ and i is even $\}$, and $I_e(\mathbf{b}) = \{i : b_i \neq 0$ and i is even $\}$. Then

(i) Assume t is even or $\{|I_e(\mathbf{a})|$ and $|I_e(\mathbf{b})|$ are even $\}$. Then for any $u \notin \mathbb{F}_4^{\perp}$, the function f is semi–bent Boolean function in $\mathcal{B}_{n+1}$. Moreover, $f + \phi_a + \epsilon y$ is balanced if and only if $u + a \notin \mathbb{F}_4^{\perp}$,

(ii) Assume that t is odd, $|I_e(\mathbf{a})|$ is odd and $|I_e(\mathbf{b})|$ is even, and $u = 0$. Then f which equal to $f_{\mathbf{a}}||f_{\mathbf{b}}$, is semi–bent Boolean function in $\mathcal{B}_{n+1}$.

2.3 Recursive lower bounds of higher-order nonlinearities

Carlet [3] developed a technique of obtaining lower bounds of higher-order nonlinearities of Boolean functions recursively.

Proposition 6. *[3, Proposition 2] Let $f \in \mathcal{B}_n$ and r be a positive integer smaller than n, then*

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

In particular, for $r = 2$,

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

Proposition 7. *[3, Proposition 3] Let $f \in \mathcal{B}_n$ and r be a positive integer such that $r < n$, then*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_2^n} nl_{r-1}(D_a f)}.$$

Carlet remarked that in general, the lower bounds obtained by the Proposition 7 is potentially stronger than those obtained by using Proposition 6. The following result known as McEliece Theorem is useful for improving the bounds of the rth-order nonlinearities.

Proposition 8. *[11, Chaper 15, Corollary 13] The rth-order nonlinearities of a Boolean function $f \in \mathcal{B}_n$ with algebraic degree d, is divisible by $2^{\lceil \frac{n}{d} \rceil - 1}$.*

The following result is due to Kurosawa et al. [10] useful for improving the bounds of the rth-order nonlinearities for $t-$resilient Boolean functions.

Proposition 9. *[10, Theorem 6.2] Let $1 \leq r \leq n-2$ and $0 \leq t \leq n-r-2$. If $f \in \mathcal{R}_{t,n}$, then*

$$d(f, RM(2,n)) \equiv 0 \mod 2^{\lfloor \frac{t}{r} \rfloor + 1}.$$

3 Known results on second-order nonlinearities of cubic bent functions constructed by concatenating semi-bent functions as given in [5]

Singh and Gangopadhyay [12] provided the following

Proposition 10. *[12, Theorem 1] Let $n = t+1$, where t is an odd prime satisfying at least one of the following conditions*

(i) $ord_t(2) = t-1$;

(ii) $t = 2s+1$, s is odd, and $ord_t(2) = s$.

Let $f : \mathbb{F}_{2^t} \times \mathbb{F}_2 \to \mathbb{F}_2$ be defined as $f(x,y) = f_{\mathbf{a}}(x)y + f_{\mathbf{b}}(x)(1+y)$, where

$$f_{\mathbf{a}}(x) = \sum_{i=1}^{\frac{t-1}{2}} a_i Tr_1^t(x^{2^i+1}), f_{\mathbf{b}}(x) = \sum_{i=1}^{\frac{t-1}{2}} b_i Tr_1^t(x^{2^i+1}), \tag{5}$$

Table 2: Improved bounds of Theorem 10 by using McEliece's Theorem

n	6	8	12	14	20
bounds obtained in Theorem 10 and 1	18	92	1744	7328	504832
Max known Hamming distance	18 (*exact*)	84	1760	–	–

where $\mathbf{a} = (a_1, \ldots, a_{\frac{t-1}{2}}), \mathbf{b} = (b_1, \ldots, b_{\frac{t-1}{2}}) \in \mathbb{F}_2^{\frac{t-1}{2}}$, $x \in \mathbb{F}_{2^t}$, *such that* $w_H(\mathbf{a})$ *is even and* $w_H(\mathbf{b})$ *is odd. Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n+1}{2}} + 2^{n+1} + 2^{\frac{n+4}{2}} - 2^{\frac{n+5}{2}}}. \tag{6}$$

The following theorem is the generalization of Theorem 10.

Theorem 1. *Let* $n = t + 1$, t *is an odd integer. Consider a function* $f : \mathbb{F}_{2^t} \times \mathbb{F}_2 \to \mathbb{F}_2$ *as* $f(x, y) = f_{\mathbf{a}}(x)y + f_{\mathbf{b}}(x)(1 + y)$, *where* $f_{\mathbf{a}}$ *and* $f_{\mathbf{b}}$ *are two semi-bent Boolean functions on* $\mathbb{F}_{2^t}$ *defined as*

$$f_{\mathbf{a}}(x) = \sum_{i=1}^{\frac{t-1}{2}} a_i Tr_1^t(x^{2^i+1}), f_{\mathbf{b}}(x) = \sum_{i=1}^{\frac{t-1}{2}} b_i Tr_1^t(x^{2^i+1}), \tag{7}$$

such that $f_{\mathbf{a}} + f_{\mathbf{b}}$ *is also semi-bent. Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n+1}{2}} + 2^{n+1} + 2^{\frac{n+4}{2}} - 2^{\frac{n+5}{2}}}. \tag{8}$$

4 Main Results

In this section we prove that the covering radius, $\hat{\rho}(0, 2, n)$ of $RM(2, n)$ for some n in set $\mathcal{R}_{0,n}$ by computing the lower bound of second-order nonlinearities of the cubic semi-bent functions (see Lemma 2) constructed by Charpin, Pasalić and Tavernier [5].

Theorem 2. *Let* $n = m + 1$, *where* $m = 2t$, t *is an odd prime satisfying at least one of the following conditions*

(i) $ord_t(2) = t - 1$;

(ii) $t = 2s + 1$, s *is odd, and* $ord_t(2) = s$.

Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_2 \to \mathbb{F}_2$ *be defined as* $f(x, y) = (f_{\mathbf{a}} + \phi_u)(x)y + f_{\mathbf{b}}(x)(1 + y)$, *where*

$$f_{\mathbf{a}}(x) = \sum_{i=1}^{t-1} a_i Tr_1^m(x^{2^i+1}), f_{\mathbf{b}}(x) = \sum_{i=1}^{t-1} b_i Tr_1^m(x^{2^i+1}), \tag{9}$$

where $u, x \in \mathbb{F}_{2^m}$, $\phi_u(x) = Tr_1^m(ux)$ *a linear function, and* $\mathbf{a} = (a_1, \ldots, a_{t-1}), \mathbf{b} = (b_1, \ldots, b_{t-1}) \in \mathbb{F}_2^{t-1}$ *such that* $\mathbf{a} \oplus \mathbf{b} = \mathbf{k}$ *and* $k_i \neq k_{t-i}$ *for some* i. *Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n+2}{2}} + 2^{n+2} + 2^{\frac{n+7}{2}} - 2^{\frac{n+8}{2}}}. \tag{10}$$

Proof. Let $\mathbf{k} = \mathbf{a} \oplus \mathbf{b}$ with $k_i \neq k_{t-i}$ for some i, then f can be written as $f(x,y) = f_{\mathbf{k}}(x)y + \underbrace{f_{\mathbf{b}}(x) + y\phi_u(x)}$, where $f_{\mathbf{k}}$ is semi-bent by Lemma 1. Let $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_2$ such that $a \neq 0$. quadratic function

$$\begin{aligned}
D_{(a,b)}f(x,y) &= (y+b)f_{\mathbf{k}}(x+a) + yf_{\mathbf{k}}(x) + \ell(x,y) \\
&= y(f_{\mathbf{k}}(x+a) + f_{\mathbf{k}}(x)) + bf_{\mathbf{k}}(x+a) + \ell(x,y) \\
&= y\sum_{i=1}^{t-1} k_i Tr_1^m((x+a)^{2^i+1} + x^{2^i+1}) + b\sum_{i=1}^{t-1} k_i Tr_1^m((x+a)^{2^i+1}) + \ell(x,y) \\
&= y\sum_{i=1}^{t-1} k_i Tr_1^m(xa^{2^i} + x^{2^i}a) + b\sum_{i=1}^{t-1} k_i Tr_1^m(x^{2^i+1}) + \ell'(x,y) \\
&= y\sum_{i=1}^{t-1} k_i Tr_1^m((a^{2^i} + a^{2^{m-i}})x) + b\sum_{i=1}^{t-1} k_i Tr_1^m(x^{2^i+1}) + \ell'(x,y) \\
&= yTr_1^m\left(x\sum_{i=1}^{t-1} k_i(a^{2^i} + a^{2^{m-i}})\right) + b\sum_{i=1}^{t-1} k_i Tr_1^m(x^{2^i+1}) + \ell'(x,y) \\
&= yTr_1^m(xQ_{\mathbf{k}}(a)) + b\sum_{i=1}^{t-1} k_i Tr_1^m(x^{2^i+1}) + \ell'(x,y),
\end{aligned} \tag{11}$$

where $Q_{\mathbf{k}}(x) = \sum_{i=1}^{t-1} k_i \left(x^{2^i} + x^{2^{m-i}}\right)$, and $\ell(x,y)$ and $\ell'(x,y)$ are affine functions. If $D_{(a,b)}f$ is quadratic, then by Proposition 2,

$$\mathcal{E}_{D_{(a,b)}f} = \{(c,d) \in \mathbb{F}_{2^m} \times \mathbb{F}_2 : D_{(c,d)}D_{(a,b)}f(x,y) = \text{ constant}\}. \tag{12}$$

For $(a,b),(c,d) \in \mathbb{F}_{2^m} \times \mathbb{F}_2$ we obtain

$$\begin{aligned}
D_{(c,d)}D_{(a,b)}f(x,y) &= yTr_1^m(cQ_{\mathbf{k}}(a)) + dTr_1^m(xQ_{\mathbf{k}}(a)) + b\sum_{i=1}^{t-1} k_i Tr_1^m((c^{2^i} + c^{2^{m-i}})x) + \text{ constant} \\
&= yTr_1^m(cQ_{\mathbf{k}}(a)) + Tr_1^m(dxQ_{\mathbf{k}}(a)) \\
&\quad + Tr_1^m\left(bx\sum_{i=1}^{t-1} k_i(c^{2^i} + c^{2^{m-i}})\right) + \text{ constant} \\
&= yTr_1^m(cQ_{\mathbf{k}}(a)) + Tr_1^m(x(dQ_{\mathbf{k}}(a) + bQ_{\mathbf{k}}(c))) + \text{ constant} \\
&= yTr_1^m(aQ_{\mathbf{k}}(c)) + Tr_1^m(x(dQ_{\mathbf{k}}(a) + bQ_{\mathbf{k}}(c))) + \text{ constant},
\end{aligned} \tag{13}$$

where $Q_{\mathbf{k}}(x) = \sum_{i=1}^{t-1} k_i \left(x^{2^i} + x^{2^{m-i}}\right)$ and $b, d, k_i \in \mathbb{F}_2$. The last equality is due to the fact that $Tr_1^m(aQ_k(c)) = Tr_1^m(cQ_k(a))$. The second-derivative $D_{(c,d)}D_{(a,b)}f$ is constant if and only if one of the following is satisfied:

1. $aQ_k(c) = 0$ and $dQ_k(a) + bQ_k(c) = 0$;
2. $cQ_k(a) = 0$ and $dQ_k(a) + bQ_k(c) = 0$.

In order to determine the nonlinearities of $D_{(a,b)}f$ for all $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_2$ the following cases are considered.

Case 1. Let $a \in \mathbb{F}_4$, $b = 0$. From the conditions (1), (2) and Proposition 3 $D_{(a,b)}f$ is affine. Thus, there are 4 choices of $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_2$ for which the Walsh–Hadamard spectrum of $D_{(a,b)}f$ consists of all the values from the set $\{0, \pm 2^n\}$.

Case 2. Let $a \in \mathbb{F}_4$, $b = 1$. From the conditions (1), (2) and Proposition 3 it can be inferred that $D_{(c,d)}D_{(a,b)}f(x,y)$ is constant if and only if $c \in \mathbb{F}_4$ and $d \in \mathbb{F}_2$. Therefore by Proposition 2, the dimension, of $\mathcal{E}_{D_{(a,b)}f}$ is $k(a,b) = 3$. Thus, there are 4 choices of $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_2$ for which the Walsh–Hadamard spectrum of $D_{(a,b)}f$ consists of all the values from the set $\{0, \pm 2^{\frac{n+3}{2}}\}$.

Case 3. Let $a \in \mathbb{F}_{2^m} \setminus \mathbb{F}_4$ and $b \in \mathbb{F}_2$. From the conditions (1), (2) and Proposition 3 it can be inferred that $D_{(c,d)}D_{(a,b)}f(x,y)$ is constant if and only if $c \in \mathbb{F}_4$ and $d = 0$. Therefore by Proposition 2, the dimension, of $\mathcal{E}_{D_{(a,b)}f}$ is $k(a,b) = 2$. Thus, there are $2(2^m - 4) = 2^n - 8$ choices of $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_2$ for which the Walsh–Hadamard spectrum of $D_{(a,b)}f$ consists of all the values from the set $\{0, \pm 2^{\frac{n+2}{2}}\}$.
The maximum value in the Walsh–Hadamard spectrum of $D_{(a,b)}f$ is

$$\max_{(\alpha,\ \beta)\in\mathbb{F}_{2^m}\times\mathbb{F}_2} |W_{D_{(a,b)}f}(\alpha,\beta)| = 2^{\frac{n+k(a,b)}{2}} = \begin{cases} 2^n & \text{if } a \in \mathbb{F}_4, b = 0; \\ 2^{\frac{n+3}{2}}, & \text{if } a \in \mathbb{F}_4, b = 1; \\ 2^{\frac{n+2}{2}}, & \text{if } a \in \mathbb{F}_{2^m} \setminus \mathbb{F}_4, b \in \mathbb{F}_2. \end{cases}$$

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

$$nl(D_{(a,b)}f) = \begin{cases} 0 & \text{if } a \in \mathbb{F}_4, b = 0; \\ 2^{n-1} - 2^{\frac{n+1}{2}} & \text{if } a \in \mathbb{F}_4, b = 1; \\ 2^{n-1} - 2^{\frac{n}{2}} & \text{if } a \in \mathbb{F}_{2^m} \setminus \mathbb{F}_4, b \in \mathbb{F}_2. \end{cases} \tag{14}$$

Using Proposition 6, we have

$$nl_2(f) \geq 2^{n-2} - 2^{\frac{n-2}{2}}. \tag{15}$$

Using (14), we have

$$\begin{aligned} \sum_{a\in\mathbb{F}_{2^m}, b\in\mathbb{F}_2} nl(D_{(a,b)}f) &= \sum_{a\in\mathbb{F}_4} nl(D_{(a,0)}f) + \sum_{a\in\mathbb{F}_4} nl(D_{(a,1)}f) + \sum_{a\in\mathbb{F}_{2^m}\setminus\mathbb{F}_4, b\in\mathbb{F}_2} nl(D_{(a,b)}f) \\ &= 4(2^{n-1} - 2^{\frac{n+1}{2}}) + (2^n - 8)(2^{n-1} - 2^{\frac{n}{2}}) \\ &= 2^{2n-1} - 2^{\frac{3n}{2}} - 2^{n+1} - 2^{\frac{n+5}{2}} + 2^{\frac{n+6}{2}}. \end{aligned} \tag{16}$$

Using Proposition 7 and (16) we have,

$$\begin{aligned} nl_2(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2(2^{2n-1} - 2^{\frac{3n}{2}} - 2^{n+1} - 2^{\frac{n+5}{2}} + 2^{\frac{n+6}{2}})} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n+2}{2}} + 2^{n+2} + 2^{\frac{n+7}{2}} - 2^{\frac{n+8}{2}}}. \end{aligned} \tag{17}$$

□

Table 3: Comparison of $nl_2(f)$ obtained in Theorem 3 with maximum Hamming distance to $RM(2,n)$

n	7	11	15	23
bounds obtained in Theorem 3	36	805	14653	4174607
Max known Hamming distance	$40-44$	848	–	–

Table 4: Improved bounds of Theorem 3 by using Proposition 9

n	7	11	15	23
bounds obtained in Theorem 3	36	806	14654	4174608
Max known Hamming distance	$40-44$	848	–	–

Remark 1. *Let $t=3$. By Theorem 2, we have $\mathbf{a},\mathbf{b}\in\mathbb{F}_2^2$, take $\mathbf{a}=(1,0)$, $\mathbf{b}=(1,1)$ which implies $\mathbf{k}(0,1)$. Thus $f_{\mathbf{k}}=Tr_1^6(x^5)$ is semi-bent Boolean function. Therefore from (17) we have $nl_2(f)\geq 36$. Moreover, $f_{\mathbf{b}}=Tr_1^6(x^3+x^5)$ is not semi-bent Boolean function while $f_{\mathbf{b}}=Tr_1^6(x^3)$ is semi-bent (see Lemma 1). Moreover, it can be be compute easily that $nl(f_{\mathbf{b}})=16$ and therefore $nl(f)\geq 40$ (since $nl(f)\geq nl(f_{\mathbf{a}})+nl(f_{\mathbf{b}})$).*

Theorem 3. *Let f be a semi-bent Boolean function as defined in part (ii) of Lemma 2 with an extra property that $k_i\neq k_{p-i}$ for some i, where $\mathbf{k}=\mathbf{a}\oplus\mathbf{b}$ and $f_{\mathbf{a}}+f_{\mathbf{b}}=f_{\mathbf{k}}$. Let t is an odd prime satisfying at least one of the following conditions*

(i) $ord_t(2)=t-1$;

(ii) $t=2s+1$, s is odd, and $ord_t(2)=s$.

Then

$$nl_2(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{\frac{3n+2}{2}}+2^{n+2}+2^{\frac{n+7}{2}}-2^{\frac{n+8}{2}}}. \tag{18}$$

Remark 2. *A semi-bent bent Boolean function is either balanced or can be change into a balanced semi-bent functions by adding some linear functions ($W_f(\alpha_0)=0 \implies W_{f+\phi_{\alpha_0}}(0)=0$).*

Theorem 4. *Let $n=2t+1$, t is an odd prime satisfying at least one of the following conditions*

(i) $ord_t(2)=t-1$;

(ii) $t=2s+1$, s is odd, and $ord_t(2)=s$.

Then the covering radius of Reed-Muller code $RM(2,n)$ in $\mathcal{R}_{0,n}$ is

$$\hat{\rho}(0,2,n)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{\frac{3n+2}{2}}+2^{n+2}+2^{\frac{n+7}{2}}-2^{\frac{n+8}{2}}}.$$

The following corollary is due to Theorem 4.

Corollary 1. *The covering radius of Reed-Muller code $RM(2,15)$ in $\mathcal{R}_{0,11}$ is at least* 806 *i.e.,* $\hat{\rho}(0,2,11)\geq 806$.

Acknowledgment
Brajesh Kumar Singh thanks the CSIR for supporting his research.

References

[1] Y. Borissov, A. Braeken, S. Nikova, and B Preneel, "On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions," *Cryptography and Coding 2003*, LNCS, vol. 2898, pp. 8292, 2003.

[2] A. Canteaut, P. Charpin and G. M. Kyureghyan, "A new class of monomial bent functions," *Finite Fields and their Applications*, vol. 14, pp. 221–241, 2008.

[3] C. Carlet, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 1262–1272, 2008.

[4] C. Carlet, "Boolean functions for cryptography and error correcting codes," Chapter of the monograph, "*Boolean Models and Methods in Mathematics, Computer Science and Engineering*," Cambridge Univ. Press, Y. Crama, P. Hammer (eds.), pp. 257–397, 2010.

[5] P. Charpin, E. Pasalic and C. Tavernier, "On bent and semi–bent quadratic Boolean functions," *IEEE Transactions of Information Theory*, vol. 51, no. 12, pp. 4286–4298, 2005.

[6] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North–Holland, 1997.

[7] R. Fourquet and C. Tavernier, "An improved list decoding algorithm for the second-order Reed Muller codes and its applications," *Designs Codes and Cryptography*, vol. 49, pp. 323-340, 2008.

[8] X.-d. Hou, "Some results on the covering radii of Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 366–378, 2008.

[9] K. Kurosawa, T. Iwata, T. Yoshiwara, "New covering radius of Reed-Muller codes for t-resilient functions," in *SAC01* , LNCS, vol. 2259, pp. 7586, 2001.

[10] K. Kurosawa, T. Iwata, T. Yoshiwara, "New covering radius of Reed-Muller codes for t-resilient functions," IEEE Trans. Inform. Theory, vol. 50, no. 3, pp. 468-475, 2004.

[11] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, North-Holland, Amsterdam, 1977.

[12] B. K. Singh and S. Gangopadhyay, *On the Covering Radius of* $RM(2, 8)$, preprint.