New bounds on the covering radius of the second order Reed-Muller code of length 128

Qichun Wang * Pantelimon Stănică †

Abstract

In 1981, Schatz proved that the covering radius of the binary Reed-Muller code $RM(2,6)$ is 18. It was previously shown that the covering radius of $RM(2,7)$ is between 40 and 44. In this paper, we prove that the covering radius of $RM(2,7)$ is at most 42. As a corollary, we also find new upper bounds for $RM(2,n)$, $n=8,9,10$. Moreover, we give a sufficient and necessary condition for the covering radius of $RM(2,7)$ to be equal to 42. Using this condition, we prove that the covering radius of $RM(2,7)$ in $RM(4,7)$ is exactly 40, and as a by-product, we conclude that the covering radius of $RM(2,7)$ in the set of 2-resilient Boolean functions is at most 40, which improves the bound given by Borissov et al. (IEEE Trans. Inf. Theory 51:1182-1189, 2005).

Keywords: Reed-Muller codes, covering radius, Boolean functions, second-order nonlinearity.

MSC 2010: 94B65.

1 Introduction

In [14], Schatz proved that the covering radius of the binary Reed-Muller code $RM(2,6)$ is 18. For $n \geq 7$, the exact covering radius of $RM(2,n)$ is still unknown, although, some bounds have been given [3, 4, 5]. For example, we know that the covering radius of the binary Reed-Muller code $RM(2,7)$ is between 40 and 44.

From a cryptographic viewpoint, Kurosawa et al. introduced the covering radius of the Reed-Muller code in the set of resilient Boolean functions

*School of Computer Science and Technology, Nanjing Normal University, Nanjing, P.R.China 210046. E-mail: qcwang@fudan.edu.cn.

†Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943, USA. Email: pstanica@nps.edu

[10]. In [1], the authors deduced some results on the covering radius of $RM(2,7)$ in the set of resilient Boolean functions and proved that the covering radius of $RM(2,7)$ in the set of 2-resilient Boolean functions is between 32 and 44.

In this paper, we prove that the covering radius of the binary Reed-Muller code $RM(2,7)$ is at most 42. We also find new upper bounds for $RM(2,n)$, $n = 8, 9, 10$. Moreover, we give a sufficient and necessary condition for the covering radius of $RM(2,7)$ to be equal to 42. Using this condition, we prove that the covering radius of $RM(2,7)$ in $RM(4,7)$ is 40. As a corollary, we conclude that the covering radius of $RM(2,7)$ in the set of 2-resilient Boolean functions is at most 40 which improves the bound given by Borissov et al.

The paper is organized as follows. In Section 2, the necessary background is established. In Section 3, we give some observations which will be used afterwards. We then deduce the new bound on the covering radius of $RM(2,7)$ in Section 4, and give a sufficient and necessary condition for the covering radius of $RM(2,7)$ to be equal to 42 in Section 5. In Section 6, we study the covering radius of $RM(2,7)$ in $RM(4,7)$. We end in Section 7 with conclusions.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. We denote by B_n the set of all n-variable Boolean functions, from $\mathbb{F}_2^n$ into $\mathbb{F}_2$.

Any Boolean function $f \in B_n$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \cdots, x_n]$, called *algebraic normal form* (ANF),

$$f(x_1, \ldots, x_n) = \sum_{K \subseteq \{1,2,\ldots,n\}} a_K \prod_{k \in K} x_k, \quad a_K \in \mathbb{F}_2.$$

The *algebraic degree* of f, denoted by $\deg(f)$, is the number of variables in the highest order term with nonzero coefficient. A Boolean function is *affine* if all its ANF terms have degree ≤ 1. The set of all affine functions is denoted by A_n. The *Hamming weight* of f is the cardinality of the set $\{x \in \mathbb{F}_2^n | f(x) = 1\}$. The *Hamming distance* between two functions f and g is the Hamming weight of $f + g$, and will be denoted by $d(f, g)$.

The *nonlinearity* of $f \in B_n$ is its distance from the set of all n-variable affine functions, that is,

$$nl(f) = \min_{g \in A_n} d(f, g).$$

The nonlinearity of an n-variable Boolean function is bounded above by $2^{n-1} - 2^{n/2-1}$ [2, 7, 13]. The *r-order nonlinearity* of a Boolean function f, denoted by $nl_r(f)$, is its distance from the set of all n-variable functions of algebraic degrees at most r.

The r-th order Reed-Muller code of length 2^n is denoted by $RM(r, n)$. Its codewords are the truth tables (output values) of the set of all n-variable Boolean functions of degree $\leq r$. The *covering radius* of $RM(r, n)$ is defined as

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

Two n-variable Boolean functions f_1 and f_2 are called affine equivalent modulo $RM(r, n)$ if there exist $A \in GL_n(\mathbb{F}_2)$ and $b \in \mathbb{F}_2^n$ such that $f_1(x) = f_2(xA + b)$ modulo $RM(r, n)$.

The *Walsh transform* of a given function $f \in B_n$ is the integer-valued function over $\mathbb{F}_2^n$ defined by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x},$$

where $\omega \in \mathbb{F}_2^n$ and $\omega \cdot x = \omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$.

An n-variable Boolean function $f(x)$ is called tth-order correlation-immune if $W_f(\omega) = 0$, for $1 \leq wt(\omega) \leq t$. Balanced tth-order correlation-immune functions are called t-resilient functions. It is known that the algebraic degree of a t-resilient function is at most $n - t - 1$ [2, 7].

We use $||$ to denote the concatenation, that is,

$$(f_1||f_2)(x_1, \ldots, x_n, x_{n+1}) = (x_{n+1} + 1)f_1(x_1, \ldots, x_n) + x_{n+1}f_2(x_1, \ldots, x_n),$$

where $f_1, f_2 \in B_n$. We let $|A|$ denote the cardinality of the set A.

3 Some computational observations on $RM(2, 6)$

For $n = 6$, the classification of Boolean functions under the affine group has been fully studied (see e.g. [11, 12]). It is known that there are exactly 205 affine equivalence classes modulo $RM(2, 6)$. In our study of these affine equivalence classes, we make the following observations. We let $fun_1(x_1, \ldots, x_6) = x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6$ and $fun_2(x_1, \ldots, x_6) = x_1x_2x_3x_4x_5x_6 + fun_1$.

Observation 1. *Let $f \in B_6$ with $f = fun_1 + g$, where g is any 6-variable Boolean function of* $\deg(g) \leq 2$. *Then $nl(f) \leq 22$.*

Observation 2. *Let $f \in B_6$. Then $nl_2(f) = 17$ if and only if there is a $g \in B_6$ with $\deg(g) \leq 2$ such that f is affine equivalent to $x_1x_2x_3x_4x_5x_6 + x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + g$.*

Observation 3. *Let $f \in B_6$. Then $nl_2(f) = 16$ if and only if there is a $g \in B_6$ with $\deg(g) \leq 2$ such that $f + g$ is affine equivalent to one of the following functions (they all depend upon $(x_1, \ldots, x_6)$):*

(1) $fun_3 = x_1x_2x_6 + x_1x_3x_5 + x_2x_3x_4$;
(2) $fun_4 = x_1x_2x_3x_4 + x_1x_2x_6 + x_1x_4x_5 + x_2x_3x_5$;
(3) $fun_5 = x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_4x_6 + x_2x_3x_5 + x_2x_3x_6 + x_2x_4x_5$;
(4) $fun_6 = x_1x_2x_3x_6 + x_1x_2x_4x_5 + x_1x_3x_5 + x_1x_4x_5 + x_1x_4x_6 + x_2x_3x_4$;
(5) $fun_7 = x_1x_2x_3x_4x_5 + x_1x_3x_5 + x_1x_4x_6 + x_2x_3x_5 + x_2x_3x_6 + x_2x_4x_5$.

Observation 4. *Let $f \in B_6$. Then $nl_2(f) = 15$ if and only if there is a $g \in B_6$ with $\deg(g) \leq 2$ such that $f + g$ is affine equivalent to one of the functions $x_1x_2x_3x_4x_5x_6 + fun_i$, where $3 \leq i \leq 7$.*

Definition 5. *Given $f \in B_n$, we denote by Fh_f the map from $\mathbb{Z}$ to the power set of B_n as follows:*

$$Fh_f(r) = \{g = \sum_{1 \leq i < j \leq n} a_{ij}x_ix_j \mid a_{ij} \in \mathbb{F}_2 \text{ and } nl(f + g) = r\}.$$

We let $NFh_f : \mathbb{Z} \to \mathbb{Z}$ be the function defined by $NFh_f(r) = |Fh_f(r)|$.

It is immediate that

$$\sum_{i=0}^{\infty} NFh_f(i) = 2^{n(n-1)/2}.$$

Moreover, if f_1 is affine equivalent to f_2, then $NFh_{f_1} = NFh_{f_2}$. We have computed and display in the next observation the values of $NFh_{fun_i}(r)$, $1 \leq i \leq 6$, for various inputs r.

Observation 6. *We have*

(1) $NFh_{fun_3}(16) = 448$, $NFh_{fun_3}(26) = 0$ *and* $NFh_{fun_3}(28) = 64$;

(2) $NFh_{fun_4}(16) = 384$, $NFh_{fun_4}(18) = 1024$, $NFh_{fun_4}(20) = 9216$, $NFh_{fun_4}(22) = 14336$, $NFh_{fun_4}(24) = 6784$, $NFh_{fun_4}(26) = 10244$ *and* $NFh_{fun_4}(28) = 0$;

(3) $NFh_{fun_5}(i) = 0$, *for* $i \geq 26$;

(4) $NFh_{fun_6}(16) = 224$, $NFh_{fun_6}(18) = 1792$, $NFh_{fun_6}(20) = 8640$, $NFh_{fun_6}(22) = 14080$, $NFh_{fun_6}(24) = 7520$, $NFh_{fun_6}(26) = 512$ *and* $NFh_{fun_6}(28) = 0$;

(5) $NFh_{fun_7}(i) = 0$, *for* $i \geq 26$.

Observation 7. *We have* $NFh_{x_1x_2x_3x_4x_5x_6+fun_i}(27) = 0$, *for* $4 \leq i \leq 7$. *Moreover,* $NFh_{fun_8}(15) = 112$ *and* $NFh_{fun_8}(27) = 64$, *where* $fun_8 = x_1x_2x_3x_4x_5x_6 + fun_3$.

Observation 8. *Let* $f \in B_6$ *and* $nl_2(f) = 14$. *Then* $NFh_f(r) = 0$, *for* $r > 26$. *Moreover, if* $NFh_f(26) > 0$, *then there is a* $g \in B_6$ *with* $\deg(g) \leq 2$ *such that* $f + g$ *is affine equivalent to one of the following functions:*

(1) $fun_9 = x_1x_2x_3x_4+x_1x_5x_6+x_2x_3x_6+x_2x_4x_5$; *moreover,* $NFh_{fun_9}(14) = 16$ *and* $NFh_{fun_9}(16) = 224$;

(2) $fun_{10} = x_1x_2x_3x_6 + x_1x_2x_4x_5 + x_1x_4x_5 + x_1x_5x_6 + x_2x_3x_5$; *moreover,* $NFh_{fun_{10}}(14) = 32$ *and* $NFh_{fun_{10}}(16) = 224$;

(3) $fun_{11} = x_1x_2x_3x_6 + x_1x_2x_4x_5 + x_1x_5x_6 + x_2x_4x_6 + x_3x_4x_5$; *moreover,* $NFh_{fun_{11}}(14) = 16$ *and* $NFh_{fun_{11}}(16) = 224$;

(4) $fun_{12} = x_1x_2x_5x_6+x_1x_3x_4x_6+x_2x_3x_4x_5+x_1x_2x_4+x_1x_3x_4+x_1x_3x_5+x_2x_3x_6$; *moreover,* $NFh_{fun_{12}}(14) = 8$ *and* $NFh_{fun_{12}}(16) = 224$;

(5) $fun_{13} = x_1x_2x_5x_6+x_1x_3x_4x_6+x_2x_3x_4x_5+x_1x_3x_4+x_1x_4x_5+x_2x_3x_6$; *moreover,* $NFh_{fun_{13}}(14) = 24$ *and* $NFh_{fun_{13}}(16) = 224$;

(6) $fun_{14} = x_1x_2x_3x_4x_5+x_1x_2x_6+x_1x_3x_5+x_2x_3x_4$; *moreover,* $NFh_{fun_{14}}(14) = 48$ *and* $NFh_{fun_{14}}(16) = 128$;

(7) $fun_{15} = x_1x_2x_3x_4x_5+x_1x_2x_5+x_1x_4x_6+x_2x_3x_6$; *moreover,* $NFh_{fun_{15}}(14) = 24$ *and* $NFh_{fun_{15}}(16) = 176$;

(8) $fun_{16} = x_1x_2x_3x_4x_5+x_1x_2x_3x_6+x_1x_2x_6+x_1x_3x_5+x_2x_3x_4$; *moreover,* $NFh_{fun_{16}}(14) = 64$ *and* $NFh_{fun_{16}}(16) = 160$;

(9) $fun_{17} = x_1x_2x_3x_4x_5+x_1x_2x_5x_6+x_1x_3x_4x_6+x_1x_2x_4+x_1x_3x_5+x_3x_4x_6$; *moreover,* $NFh_{fun_{17}}(14) = 20$ *and* $NFh_{fun_{17}}(16) = 224$;

(10) $fun_{18} = x_1x_2x_3x_4x_5 + x_1x_2x_5x_6 + x_1x_3x_4x_6 + x_1x_2x_4 + x_1x_3x_4 + x_1x_3x_5+x_2x_5x_6+x_3x_4x_6$; *moreover,* $NFh_{fun_{18}}(14) = 26$ *and* $NFh_{fun_{18}}(16) = 212$.

Remark 9. *From the above observations, it is easy to see that the maximum possible second-order nonlinearity of a 6-variable bent function is 16, and there is no 6-variable bent function with the second-order nonlinearity 14. Moreover, the function* $x_1x_3x_4 + x_1x_2x_5 + x_1x_6 + x_2x_4 + x_3x_4 + x_3x_5$ *is a bent function with the second-order nonlinearity 16.*

4 New upper bound on the covering radius of the binary Reed-Muller code $RM(2, 7)$

The known bounds for the covering radius of $RM(r, m)$, for example, $\rho(r, m) \leq 2^{m-1} - \frac{1}{(\sqrt{2}-1)^{r-1}} 2^{(m-2)/2} + \binom{m}{r}$ (which holds for $m \geq (\sqrt{2}+2)r$) will only give better results for m large enough (see [6]). That being said, we point out that for small m, none of the previous results was able to improve upon the known bounds for the covering radius of $RM(2, 7)$, that is, $40 \leq \rho(2, 7) \leq 44$. In this section, we will find a new upper bound, namely $\rho(2, 7) \leq 42$.

We start with a few preparatory results.

Lemma 10 ([1])**.** *Let* $f \in B_6$*. Then* $nl_2(f) = 18$ *if and only if there exists a* $g \in B_6$ *with* $\deg(g) \leq 2$ *such that* f *is affine equivalent to* $fun_1 + g$*.*

Proposition 11. *Let* $f \in B_7$ *and* $f = f_1||f_2$*. If* $nl_2(f) > 40$*, then* $nl_2(f_1) \leq 16$ *and* $nl_2(f_2) \leq 16$*.*

Proof. Let $nl_2(f) > 40$. We divide the proof into the following two cases.

Case 1: $nl_2(f_1) = 18$ or $nl_2(f_2) = 18$. Without loss of generality, we assume that $nl_2(f_1) = 18$. Then by Lemma 10, f_1 is affine equivalent to $fun_1 + g_0$, where $g_0 \in B_6$ and $\deg(g_0) \leq 2$. Therefore, by Observation 1, $nl(f_1 + g_1) \leq 22$ for any $g_1 \in B_6$ with $\deg(g_1) \leq 2$. Since $nl_2(f_2) \leq 18$, there exists a $g_2 \in B_6$ with $\deg(g_2) \leq 2$ such that $d(f_2, g_2) \leq 18$. Since $nl(f_1 + g_2) \leq 22$, there exists an $l \in B_6$ with $\deg(l) \leq 1$ such that $d(f_1, g_2 + l) \leq 22$. Let $g = (g_2 + l)||g_2$. Then $nl_2(f) \leq d(f, g) \leq 40$. Hence, $nl_2(f_1) \leq 17$ and $nl_2(f_2) \leq 17$.

Case 2: $nl_2(f_1) = 17$ or $nl_2(f_2) = 17$. Without loss of generality, we assume that $nl_2(f_1) = 17$. Then by Observation 2, f_1 is affine equivalent to $fun_2 + g_0$, where $g_0 \in B_6$ and $\deg(g_0) \leq 2$. By Observation 1 and $d(fun_2, fun_1) = 1$, we have $nl(f_1 + g_1) \leq 23$ for any $g_1 \in B_6$ with $\deg(g_1) \leq 2$. Since $nl_2(f_2) \leq 17$, there exists a $g_2 \in B_6$ with $\deg(g_2) \leq 2$ such that $d(f_2, g_2) \leq 17$. Since $nl(f_1 + g_2) \leq 23$, there exists an $l \in B_6$ with $\deg(l) \leq 1$ such that $d(f_1, g_2 + l) \leq 23$. Let $g = (g_2 + l)||g_2$. Then $nl_2(f) \leq d(f, g) \leq 40$, and the result follows. □

Lemma 12. *Let $f \in B_n$ and $f = f_1||f_2$. If*

$$NFh_{f_i}(n_2) > \sum_{k \geq n_1} NFh_{f_j}(k),$$

where $\{i, j\} = \{1, 2\}$, then $nl_2(f) < n_1 + n_2$.

Proof. Without loss of generality, we assume that $i = 2$ and $j = 1$ in the assumption of our lemma. Since $NFh_{f_2}(n_2) > \sum_{k \geq n_1} NFh_{f_1}(k)$, there exists a homogeneous polynomial $g_0 \in B_{n-1}$ of degree 2 or 0 such that $nl(f_2 + g_0) = n_2$ and $nl(f_1 + g_0) < n_1$. That is, there exist $l_1, l_2 \in B_{n-1}$ with $\deg(l_1) \leq 1$ and $\deg(l_2) \leq 1$ such that $d(f_1 + g_0 + l_1) < n_1$ and $d(f_2 + g_0 + l_2) = n_2$. Let $g = (g_0 + l_1)||(g_0 + l_2)$. Then $d(f, g) < n_1 + n_2$. □

Proposition 13. *Let $f \in B_7$ and $f = f_1||f_2$. Let $nl_2(f_1) = nl_2(f_2) = 16$. Then $nl_2(f) \leq 42$.*

Proof. By Observation 3, there exist $g_1, g_2 \in B_6$ with $\deg(g_1) \leq 2$ and $\deg(g_2) \leq 2$ such that f_1 is affine equivalent to $fun_i + g_1$ and f_2 is affine equivalent to $fun_j + g_2$, where $3 \leq i, j \leq 7$. By Observation 5,

$$NFh_{fun_j + g_2}(16) > NFh_{fun_i + g_1}(28).$$

Therefore, by Lemma 12 and $nl_2(f)$ is even, we have $nl_2(f) \leq 42$. □

Proposition 14. *Let $f \in B_7$ and $f = f_1||f_2$. If $nl_2(f_1) \leq 16$ and $nl_2(f_2) \leq 15$, then $nl_2(f) < 42$.*

Proof. We divide the proof into the following four cases.

Case 1: $nl_2(f_1) = 16$ and $nl_2(f_2) = 15$. Suppose $nl_2(f) \geq 42$. Then by Observations 3–6, there exist $g_1, g_2 \in B_6$ with $\deg(g_1) \leq 2$ and $\deg(g_2) \leq 2$ such that f_1 is affine equivalent to $fun_3 + g_1$ and f_2 is affine equivalent to $fun_8 + g_2$ (since $16 + 25 = 15 + 26 < 42$). Since

$$NFh_{fun_8}(15) > NFh_{fun_3}(28)$$

and $nl_2(f)$ is odd, then by Lemma 12, $nl_2(f) \leq 41$.

Case 2: $nl_2(f_1) = 16$ and $nl_2(f_2) = 14$. Suppose $nl_2(f) \geq 42$. Then by Observations 3 and 5, there exists a $g_1 \in B_6$ with $\deg(g_1) \leq 2$, such that f_1 is affine equivalent to $fun_3 + g_1$ (since $14 + 26 < 42$). Moreover, we have $NFh_{f_2}(26) > 0$ (since $16 + 24 < 42$). Therefore, by Observations 7, there is

a $g_2 \in B_6$ with $\deg(g_2) \leq 2$, such that $f_2 + g_2$ is affine equivalent to one of fun_i, where $9 \leq i \leq 18$. By Observations 5 and 7, it is easy to check that

$$NFh_{fun_i}(16) > NFh_{fun_3}(26) + NFh_{fun_3}(28),$$

for $9 \leq i \leq 18$. Hence, by Lemma 12, $nl_2(f) < 42$.

Case 3: $nl_2(f_1) = 15$ and $nl_2(f_2) = 15$. By Observations 4 and 6, we have $nl_2(f) \leq 15+27 = 42$. Moreover, if $nl_2(f) = 42$, then there exist $h_1, h_2 \in B_6$ with $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 2$, such that $f_1 + h_1$ and $f_2 + h_2$ are affine equivalent to fun_8. Since

$$NFh_{fun_8}(27) < NFh_{fun_8}(15),$$

then by Lemma 12, $nl_2(f) < 42$.

Case 4: $nl_2(f_1) < 15$ and $nl_2(f_2) < 15$. If $nl_2(f_1) \leq 13$ or $nl_2(f_2) \leq 13$, then $nl_2(f) \leq 13 + 28 = 41$. If $nl_2(f_1) = nl_2(f_2) = 14$, then by Observation 7, we have $nl_2(f) \leq 14 + 26 = 40$. □

Remark 15. *Since $f_1||f_2$ is affine equivalent to $f_2||f_1$, if $nl_2(f_1) \leq 15$ and $nl_2(f_2) \leq 16$, we also have $nl_2(f_1||f_2) < 42$.*

Putting together the previous results we obtain the following theorem.

Theorem 16. *If $f \in B_7$, then $nl_2(f) \leq 42$. That is, the covering radius of the binary Reed-Muller code $RM(2, 7)$ is at most* 42.

Corollary 17. *The covering radius of $RM(2, n)$ is at most* $98, 218, 462$*, for $n = 8, 9, 10$ respectively.*

Proof. Let $f \in B_8$. Then f can be written as $f_1||f_2$, where $f_1, f_2 \in B_7$. Since $nl_2(f_1) \leq 42$, there exists a $g_1 \in B_7$ with $\deg(g_1) \leq 2$ such that $d(f_1, g_1) \leq 42$. Since $nl(f_2+g_1) \leq 56$, there exists an affine function $g_2 \in B_7$ such that $d(f_2 + g_1, g_2) \leq 56$. Let $g = g_1||(g_1 + g_2)$. Then $\deg(g) \leq 2$ and $d(f, g) \leq 98$. Therefore, the covering radius of $RM(2, 8)$ is at most 98. Similarly, one can show that the covering radius of $RM(2, n)$ is at most 218, 462 for $n = 9, 10$ respectively. □

In Table 1, we summarize the best known bounds on the covering radius of $RM(2, n)$ [3, 4, 5, 8] for $7 \leq n \leq 12$, showing in boldface the contributions of this paper.

Table 1: The best known bounds on the covering radius of $RM(2,n)$

n	7	8	9	10	11	12
lower bound	40	84	196	400	848	1760
upper bound	**42**	**98**	**218**	**462**	956	1946

5 A sufficient and necessary condition on the covering radius of the Reed-Muller code $RM(2,7)$

Theorem 18. *Let $f \in B_7$ and $f = f_1||f_2$. Then $nl_2(f) = 42$ if and only if the following conditions hold:*

(1) *f is affine equivalent to $fun_{i_1}||(fun_{i_2}(Ax+b)+g)$ modulo $RM(2,7)$, where $i_1, i_2 \in \{4,6\}$, $A \in GL_n(\mathbb{F}_2)$, $b \in \mathbb{F}_2^n$ and $g \in B_6$ is of degree at most 2.*

(2) *Moreover, for $\{i,j\} = \{1,2\}$, we have $Fh_{f_i}(16) \subseteq Fh_{f_j}(26)$, $Fh_{f_i}(18) \subseteq Fh_{f_j}(24) \cup Fh_{f_j}(26)$ and $Fh_{f_i}(20) \subseteq Fh_{f_j}(22) \cup Fh_{f_j}(24) \cup Fh_{f_j}(26)$.*

Proof. By Propositions 11, 13, 14, we have $nl_2(f) \leq 42$. Moreover, if $nl_2(f) = 42$, then $nl_2(f_1) = nl_2(f_2) = 16$. By Observation 3, f_i ($i = 1$ or 2) is affine equivalent to $fun_j + g_j$ ($3 \leq j \leq 7$), where $g_j \in B_6$ is of degree at most 2. Clearly, f_i ($i = 1$ or 2) cannot be affine equivalent to $fun_j + g$ ($j = 5$ or 7) for any $g \in B_6$ of degree at most 2 (otherwise, by Observation 5, $nl_2(f) \leq 24 + 16 = 40$). Since

$$NFh_{fun_3}(26) + NFh_{fun_3}(28) < NFh_{fun_j}(16),$$

for $j \in \{3,4,6\}$, by Lemma 12, f_i ($i = 1$ or 2) cannot be affine equivalent to $fun_3 + g$ for any $g \in B_6$ of degree at most 2. Therefore, there exist $h_1, h_2 \in B_6$ with $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 2$ such that

$$f = (fun_{i_1}(A_1x + b_1) + h_1)||(fun_{i_2}(A_2x + b_2) + h_2),$$

where $i_1, i_2 \in \{4,6\}$, $A_i \in GL_n(\mathbb{F}_2)$ and $b_i \in \mathbb{F}_2^n$, for $i = 1,2$. Clearly, f is affine equivalent to $fun_{i_1}||(fun_{i_2}(Ax+b)+g)$ modulo $RM(2,7)$, where $A = A_2A_1^{-1}$, $b = A_2A_1^{-1}b_1 + b_2$ and $g = (h_1 + h_2)(A_1^{-1}x + A_1^{-1}b_1)$.
For $\{i,j\} = \{1,2\}$, let us suppose that there is a function $g_1 \in Fh_{f_i}(16) - Fh_{f_j}(26)$. Then $nl(f_i + g_1) = 16$ and $nl(f_j + g_1) \leq 24$. Hence, there exist affine functions l_1 and l_2 such that $d(f_i + g_1, l_1) = 16$ and $d(f_j +$

$g_1, l_2) \leq 24$. Therefore, $nl_2(f) \leq 40$, which is a contradiction. Hence, $Fh_{f_i}(16) \subseteq Fh_{f_j}(26)$. Similarly, we have $Fh_{f_i}(18) \subseteq Fh_{f_j}(24) \cup Fh_{f_j}(26)$ and $Fh_{f_i}(20) \subseteq Fh_{f_j}(22) \cup Fh_{f_j}(24) \cup Fh_{f_j}(26)$.
Let $q \in B_7$ be of degree at most 2. Then it can be written as $q_1||q_2$, where $q_1, q_2 \in B_6$ have the same terms of degree 2. If the two conditions hold, then it is easy to check that $d(f, q) \geq 42$, and the result follows. □

Corollary 19. *Let $f \in B_7$ and $f = f_1||f_2$. If $nl_2(f) = 42$, then* $\deg(f) = 5$.

Proof. By Theorem 18, f is affine equivalent to $fun_{i_1}||(fun_{i_2}(Ax + b) + g)$ modulo $RM(2, 7)$, where $i_1, i_2 \in \{4, 6\}$, $A \in GL_n(\mathbb{F}_2)$, $b \in \mathbb{F}_2^n$ and $g \in B_6$ is of degree at most 2. Clearly, $\deg(fun_{i_1}) = \deg(fun_{i_2}(Ax + b) + g) = 4$. Since fun_4 and fun_6 are not affine equivalent modulo $RM(3, 6)$, we have $\deg(fun_{i_1} + fun_{i_2}(Ax + b)) = 4$ and $\deg(fun_{i_1}||(fun_{i_2}(Ax + b) + g)) = 5$. Therefore, $\deg(f) = 5$. □

6 The covering radius of $RM(2, 7)$ in $RM(4, 7)$

We now deduce the exact value of the covering radius of $RM(2, 7)$ in $RM(4, 7)$ (see also [9] where he showed that the covering radius of $RM(2, 7)$ in $RM(3, 7)$ is 40).

Theorem 20. *The covering radius of $RM(2, 7)$ in $RM(4, 7)$ is* 40.

Proof. Let $f \in B_7$ and $\deg(f) \leq 4$. By Theorem 16, $nl_2(f) \leq 42$. Then by Corollary 19, we have $nl_2(f) < 42$. Since the Hamming weight of a 7-variable Boolean function with degree 4 is an even number, we have $nl_2(f) \leq 40$. Let

$$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6x_7.$$

It is easy to check that $nl_2(f) = 40$, and the result follows. □

In [1], the authors proved that the covering radius of $RM(2, 7)$ in the set of 2-resilient Boolean functions is between 32 and 44. Since the degree of a 7-variable 2-resilient Boolean function is at most 4, by Theorem 20, we have the following corollary.

Corollary 21. *The covering radius of $RM(2, 7)$ in the set of 2-resilient Boolean functions is at most* 40.

7 Conclusion

In this paper, we prove that the covering radius of the binary Reed-Muller code $RM(2,7)$ is at most 42. We also find new upper bounds for $RM(2,n)$, $n = 8, 9, 10$. Moreover, we give a sufficient and necessary condition for the covering radius of $RM(2,7)$ to be equal to 42. Using this condition, we prove that the covering radius of $RM(2,7)$ in $RM(4,7)$ is 40. As a corollary, we conclude that the covering radius of $RM(2,7)$ in the set of 2-resilient Boolean functions is at most 40 which improves the bound given by Borissov et al. [1].

Acknowledgment

The first author would like to thank the financial support from the National Natural Science Foundation of China (Grants 61572189 and 61202463).

References

[1] Y. Borissov, A. Braeken, S. Nikova and B. Preneel, "On the Covering Radii of Binary Reed-Muller Codes in the Set of Resilient Boolean Functions," *IEEE Trans. Inf. Theory* 51:3 (2005), 1182–1189.

[2] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, pp. 257–397, 2010. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

[3] C. Carlet, "The complexity of Boolean functions from cryptographic viewpoint," 2006. Available: http://dblp.uni-trier.de/db/conf/dagstuhl/P6111.html

[4] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary Reed–Muller codes," *IEEE Trans. Inf. Theory* 53:1 (2007), 162–173.

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

[6] G. Cohen, S. Litsyn, "On the covering radius of Reed-Muller codes", *Disc. Math.* 106–107 (1992), 147–155.

[7] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications* (2nd ed.), Elsevier–Academic Press, 2017.

[8] R. Fourquet and C. Tavernier, "An improved list decoding algorithm for the second order Reed–Muller codes and its applications," *Des. Codes Cryptogr.* 49 (2008), 323–340.

[9] X. D. Hou, "$GL(m, 2)$ acting on $RM(r, m)/RM(r-1, m)$", *Discr. Math.* 149 (1996), 99–122.

[10] K. Kurosawa, T. Iwata and T. Yoshiwara, "New covering radius of Reed–Muller codes for t-resilient functions," *Selected Areas in Cryptography – SAC* 2001, LNCS 2259, Springer–Verlag, 2001, pp. 75–86.

[11] P. Langevin, "Classification of Boolean functions under the affine group", Online: http://langevin.univ-tln.fr/project/agl/agl.html.

[12] J. A. Maiorana, "A classification of the cosets of the Reed–Muller code R(1,6)," *Math. Comp.* 57:195 (1991), 403–414.

[13] O. S. Rothaus, "On bent functions," *J. Comb. Theory – Ser. A* 20:3 (1976), 300–305.

[14] J. Schatz, "The second order Reed-Muller code of length 64 has covering radius 18," *IEEE Trans. Inf. Theory* 27:4 (1981), 529–530.