COVERING RADIUS OF $RM(4,8)$

VALÉRIE GILLOT AND PHILIPPE LANGEVIN

Abstract. We use our classification results in 7 variables to provide the classification of the $RM(6,8)/RM(4,8)$. The main consequence is determination of the covering radius of the Reed-Muller code $RM(4,8)$ into $RM(6,8)$ and new upper bound of the covering radius of $RM(4,8)$.

1. Introduction

Let $\mathbb{F}_2$ be the finite field of order 2. Let m be a positive integer. We denote $B(m)$ the set of Boolean functions $f\colon \mathbb{F}_2^m \to \mathbb{F}_2$. The Hamming weight of f is denoted by $\mathrm{wt}\,(f)$. Every Boolean function has a unique algebraic reduced representation :

$$f(x_1, x_2, \dots, x_m) = f(x) = \sum_{S\subseteq\{1,2,\dots,m\}} a_S X_S, \quad a_S \in \mathbb{F}_2,\ X_S(x) = \prod_{s\in S} x_s. \tag{1}$$

The degree of f is the maximal cardinality of S with $a_S = 1$ in the algebraic form. A Reed-Muller code of order k in m variables is a code of length 2^m, dimension $\sum_{i=0}^{k}\binom{m}{i}$ and minimal distance 2^{m-k}. The codewords correspond to the evaluation over $\mathbb{F}_2^m$ of Boolean functions of degree less or equal to k, we identify the code to :

$$RM(k,m) = \{f \in B(m) \mid \deg(f) \le k\}.$$

The covering radius $\rho(k,m)$ of $RM(k,m)$ is $\rho(k,m) = \max_{f\in B(m)} \mathrm{NL}_k(f)$, where $\mathrm{NL}_k(f) = \min_{g\in RM(k,m)} \mathrm{wt}\,(f+g)$ is the nonlinearity of order k of $f \in B(m)$. We also consider $\rho_t(k,m)$ the covering radius of $RM(k,m)$ into $RM(t,m)$. For $m \le 7$, all the covering radii are known. For $m = 8$, most the covering radii are unknown as summarized in Table 1.

Table 1. Bounds for covering radii of $RM(k,8)$

k	1	2	3	4	5	6	7	8
$\rho(k,8)$	120	$88^a - 96$	$50^b - 67$	$26^c - 28^d$	10	2	1	0

This table is an update of the one on page 802 of [8] :

(a) One can check the non-linearity of order 2 of $abd+bcf+bef+def+acg+deg+cdh+aeh+afh+bfh+efh+bgh+dgh$ is 88 ;
(b) The lower bound is a consequency of the classification of $B(4,4,8)$, see [3];
(c) The lower bound is found in [2];
(d) The present paper gives this upper bound.

Date: November 2022.

This work is partially supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012.

The paper [2] studies covering radii $\rho_{m-3}(m-4,m)$, in particular $\rho_5(4,8)=26$ is obtained. Here, the purpose is to determine $\rho_6(4,8)$, a milestone to obtain the value $\rho(4,8)$. Our approach consists to use our work [5] to determine the classification of $RM(6,8)/RM(4,8)$. The valuation of $f\neq 0$, denoted by $\mathrm{val}(f)$, is the minimal cardinality of S for which $a_S=1$ in the ANF of f (see 1). Conventionnally, $\mathrm{val}(0)$ is ∞. We denote by $B(s,t,m)$ the space of Boolean functions of valuation greater than or equal to s and of degree less than or equal to t.

The space $B(0,t,m)$ identifies with the Reed-Muller code $RM(t,m)$ and $B(s,t,m)$ with the quotient space $RM(t,m)/RM(s-1,m)$. It is important to note that calculations in $B(s,t,m)$ are done modulo $RM(s-1,m)$. The affine general linear group $\mathrm{AGL}(m,2)$ acts naturally on the right over Boolean functions. The action of $\mathfrak{s}\in\mathrm{AGL}(m,2)$ on a Boolean function f is $f\circ\mathfrak{s}$, the composition of applications. The Reed-Muller spaces are invariant under the action of $\mathrm{AGL}(m,2)$. The action of $\mathrm{AGL}(m,2)$ induces an action over $B(s,t,m)$ by reduction modulo $RM(s-1,m)$.

Given a set of orbit representatives $\widetilde{B}(s,t,m)$ of $B(s,t,m)$ under the action of $\mathrm{AGL}(m,2)$, we determine $\rho_t(s-1,m)$:

$$\rho_t(s-1,m)=\max_{\deg(f)\leq t}\mathrm{NL}_{s-1}(f)=\max_{f\in\widetilde{B}(s,t,m)}\mathrm{NL}_{s-1}(f).$$

In the article, we present a complete classification of the 20748 classes of $B(5,6,8)$, a set of orbits representatives and a generator set of the stabilizer of each representative in $\widetilde{B}(5,6,8)$. From this classification, we deduce the covering radius $\rho_6(4,8)$.

2. Cover set and classification

In general, the determination of a $\widetilde{B}(s,t,m)$ is hard computational task. So, we introduce an intermediate concept, a cover set of $B(s,t,m)$ is a set containing $\widetilde{B}(s,t,m)$ and eventually other functions of $B(s,t,m)$. In order to obtain a classification from a cover set, we need a process to eliminate functions in same orbit. Any Boolean function $f\in B(m)$ can be written as x_mg+h with $g,h\in B(m-1)$. In particular,

$$B(s,t,m)=\big\{x_mg+h\mid g\in B(s-1,t-1,m-1),\ h\in B(s,t,m-1)\big\}. \tag{2}$$

An element $\mathfrak{s}\in\mathrm{AGL}(m-1,2)$ acts on f by $x_mg\circ\mathfrak{s}+h\circ\mathfrak{s}$. Hence, we can consider the initial cover set of $B(s,t,m)$

$$\{x_mg+h\mid g\in\widetilde{B}(s-1,t-1,m-1),h\in B(s,t,m-1)\}. \tag{3}$$

Lemma 1 (Cover set)**.** *Let us fix $g\in\widetilde{B}(s-1,t-1,m-1)$.*

1. *For all $\mathfrak{s}\in\mathrm{AGL}(m-1,2)$ in the stabilizer of g, the functions x_mg+h and $x_mg+h\circ\mathfrak{s}$ are in the same orbit.*
2. *For all $\alpha\in RM(1,m-1)$, the functions x_mg+h and $x_mg+h+\alpha g$ are in the same orbit.*

where orbits correspond to the action of $\mathrm{AGL}(m,2)$ on $B(s,t,m)$.

For each $g\in\widetilde{B}(s-1,t-1,m-1)$, we consider the action over $B(s,t,m-1)$ of the group spaned by the transformations $h\mapsto h\circ\mathfrak{s}$ and $h\mapsto h+\alpha g$. Denoting by $\mathcal{R}(g)$ an orbit representatives set for this action and applying this lemma to the cover set (3), we obtain a new cover set with a smaller size :

$$\bigsqcup_{g\in \widetilde{B}(s-1,t-1,m-1)} \{\ x_m g + h \mid h \in \mathcal{R}(g)\ \}. \tag{4}$$

In the case of $B(5,6,8)$, the initial cover is $\widetilde{B}(4,5,7)\times B(5,6,7)$, whose cardinality is $179\times 2^{28} \approx 2^{35.5}$. Reducing with Lemma 1, we obtain a cover set of size $3828171 \approx 2^{21.9}$. It is already known that $\sharp\widetilde{B}(5,6,8) = 20748$, the determination of an orbit representatives set is the subject of the next section.

3. Invariant and equivalence

From the result of the previous section in the case $B(5,6,8)$, we have to extract 20748 orbit representatives among 3828171 functions. Our approach is based on invariant tools and equivalence algorithm. Two elements $f, f' \in B(s,t,m)$ in the same orbit under the action of $\mathrm{AGL}(m,2)$ are said equivalent, we denote $f \sim f'$, that means that there exists $\mathfrak{s} \in \mathrm{AGL}(m,2)$ such that $f' \equiv f\circ\mathfrak{s} \mod RM(s-1,m)$. An invariant $j : B(s,t,m) \to X$, for an arbitrary set X, satisfies $f \sim f' \Longrightarrow j(f) = j(f')$. If $j(f) = j(f')$ and $f \not\sim f'$, we say there is a collision.

Let us recall the derivative $\mathrm{Der}_v(f)$ of a Boolean function f in the direction v is the application defined by $\mathbb{F}_2^m \ni x \mapsto \mathrm{Der}_v(f)(x) = f(x+v) + f(x)$. Note that if $f \in B(s,t,m)$ then $\mathrm{Der}_v(f) \in B(s-1,t-1,m)$. In fact we can also see this derivative in $B(s-1,t-1,m-1)$. Indeed, let us consider $f \in B(s,t,m)$ decomposed as in 2, applying the derivative of f in the direction e_m, for $t = \sum_{i=1}^m t_i e_i \in \mathbb{F}_2^m$, we obtain :

$$\begin{aligned}
\mathrm{Der}_{e_m}(f)(t) &= f(t+e_m) + f(t)\\
&= x_m(t+e_m)g(t+e_m) + x_m(t)g(t) + h(t+e_m) + h(t)\\
&= (t_m+1)g(t) + t_m g(t) + h(t) + h(t)\\
&= g(t)
\end{aligned}$$

Let us consider

$$\begin{aligned}
F\colon B(s,t,m) &\longrightarrow \widetilde{B}(s-1,t-1,m)^{\mathbb{F}_2^m}\\
f &\longmapsto \widetilde{\mathrm{Der}_{.}}(f),
\end{aligned}$$

Lemma 2 (Invariant)**.** *The application J mapping $f \in B(s,t,m)$ to the distribution of the values of $F(f)(v)$, for all $v \in \mathbb{F}_2^m$, is an invariant. More precisely, when $f \sim f'$, there exists $\mathfrak{s} \in \mathrm{AGL}(m,2)$ such that $f' \equiv f\circ\mathfrak{s} \mod RM(s-1,m)$. Considering the linear part $A \in \mathrm{GL}\,(m)$ of $\mathfrak{s} = (A,a)$, $\mathfrak{s}(x) = A(x)+a$, we have $F(f') = F(f)\circ A$.*

By numbering the elements of $\widetilde{B}(s-1,t-1,m)$, $F(f)$ takes its values in $\mathbb{N}$. We can consider its Fourier transform $\widehat{F}(f)(b) = \sum_{v\in\mathbb{F}_2^m} F(f)(v)(-1)^{b.v}$. For $A \in \mathrm{GL}\,(m)$, the relation $F(f') = F(f)\circ A$ becomes $\widehat{F}(f')\circ A^* = \widehat{F}(f)$, A^* is the adjoint of A. We denote by J the invariant corresponding to the values distribution of $F(f)$ and $\widehat{J}$ the invariant corresponding the values distribution of $\widehat{F}(f)$. These invariants J

Listing 1. Equivalence in $B(t-1,t,m)$ under the action of $\mathrm{AGL}(m,2)$

```
Algorithm Equivalent(f,f', iter)
{   // f,f' given elements of B(t−1,t,m)
    // satisfying  Ĵ(f') = Ĵ(f)
    // return Equiv or NotEquiv or Undefined
    s  ← random element of AGL(m)
    f  ← f ∘ s
    basis ←(b_1, ..., b_n)a basis of F_2^m
    flag ←NotEquiv
    // determine A*in GL(m)
    A*(0) ←0
    Search(1,basis)
    return flag
}
```

and $\widehat{J}$ were introduced in [1]. In our context the invariant $\widehat{J}$ is more discriminating than J.

From now and on, we only consider the particular case $s = t-1$ in $B(s,t,m)$.

Lemma 3 (Affine equivalence)**.** *Let f, f' be in $B(t-1,t,m)$. Let us consider $A \in \mathrm{GL}\,(m)$ and $\Delta(f) = \{\mathrm{Der}_v(f) \mid v \in \mathbb{F}_2^m\}$a subspace of $B(t-2,t-1,m)$. There exists $a \in \mathbb{F}_2^m$ such that $f' \equiv f \circ (A,a) \mod RM(t-2,m)$ if and only if $f' \circ A^{-1} + f \in \Delta(f)$.*

From Lemma 3, one deduces an algorithm `AffineTest(A,f,f')` returning `true` if there exists an element $a \in \mathbb{F}_2^m$ such that $f' \equiv f \circ (A,a) \mod RM(t-2,m)$, `false` otherwise. Given $f, f' \in B(t-1,t,m)$ satisfying $\widehat{J}(f) = \widehat{J}(f')$ with $\widehat{J}$ the invariant defined below Lemma 2, the algorithm `Equivalent(f,f',iter)`[1] tests in two phases if f and f' are equivalent under the action of $\mathrm{AGL}(m,2)$ modulo $RM(t-2,m)$:

(1) determine at most `iter` candidates $A^* \in \mathrm{GL}\,(m)$ such that $\widehat{F}(f') \circ A^* = \widehat{F}(f)$
(2) For each candidate A^*, call `AffineTest(A,f,f')`.

The algorithm ends with one of following three values :

$$\mathtt{Equivalent}(f\mathtt{,}f'\mathtt{,iter}) = \begin{cases} \mathtt{NotEquiv}, & \text{all potential } A \text{ were tested, so } f \not\sim f'; \\ \mathtt{Equiv}, & \text{there exists a } (A,a) \text{ to prove } f \sim f'; \\ \mathtt{Undefined}, & \mathtt{iter} \text{ is too small to conclude.} \end{cases}$$

The algorithm `Admissible(y,i)` checks the possible continuation of the construction of A^* over $\langle b_1, \ldots, b_{i-1}, b_i\rangle$, setting $A^*(x + b_i) := A^*(x) + y$ for all $x \in \langle b_1, \ldots, b_{i-1}\rangle$. Then, the function returns `true` if $\forall x \in \langle b_1, \ldots, b_{i-1}, b_i\rangle$, $\widehat{F}(f') \circ A^*(x) = \widehat{F}(f)(x)$, and `false` otherwise.

[1] the parameter `iter` ranges from 1024 to 2^{23} depending on the situation

```
Algorithm Search(i, basis)
{   // basis =(b_1, ..., b_n) a basis of F_2^m
    // i index of basis elements in {1,2,..., m}
    if (i >m)
        // A* in GL(m) is fully constructed
        // check the existence of a in F_2^m
        if AffineTest(A,f,f')
            flag ←Equiv
            return
        iter ←iter − 1
        if (iter < 0)
            flag ←Undefined
            return
    else
        // ∀x ∈ ⟨b_1, ..., b_{i−1}⟩, F̂(f') ∘ A*(x) = F̂(f)(x)
        // continue construction of A*
        for each y in F_2^m
            if Admissible(y,i) and ( flag = NotEquiv )
                Search(i+1,basis)
```

4. Numerical results

The classification of $B(5,6,8)$ is obtained after the following steps :

(1) We start from the cover set $\widetilde{B}(4,5,7)\times B(5,6,7)$ defined in 3 size is 179×2^{28}. The classification of $B(4,5,7)$ was computed in [5]

(2) Applying Lemma 1, we reduce to the cover set $\bigsqcup_{g\in\widetilde{B}(4,5,7)} \left\{\ x_m g + h \mid h \in \mathcal{R}(g)\ \right\}$, see 4, where $\mathcal{R}(g)$ is a orbit representative set of $B(5,6,7)$ under the action of the group described after Lemma 1. The cardinality of this cover set is 3828171.

(3) We iterate the algorithm `Equivalence` to the cover set obtained previously to eliminate redundancy of equivalent elements. We obtain the 20748 orbit representatives of $B(5,6,8)$. This step requieres about 40 GB of memory and several weeks of computation.

Note that, the invariant $\widehat{J}$ takes 20742 values whose 6 collisions solved by the algorithm **`AffineTest`**, whereas the invariant J taking 20695 values is less useful.

The covering radius $\rho_5(4,8) = 26$ was established in [2]. To verify that $\rho_6(4,8) = 26$, it is enough to prove $\mathrm{NL}_4(f) < 27$ for all $f \in \widetilde{B}(5,6,8)$. The algorithm **`distance`**, presented in [5], checks this point in two days on a 24 cores computer. All the computed dats are available at the webpage [7].

5. Conclusion

In this paper, we successfully classify $B(5,6,8)$. We also obtain $\rho_6(4,8) = 26$ and deduce $\rho(4,8) \leq \rho_6(4,8) + \rho(6,8) = 28$. An important step to determine the covering radius $\rho(4,8)$, our computation is still in progress.

References

[1] Éric Brier and Philippe Langevin. Classification of Boolean cubic forms of 9 variables. *ITW 2003*, 179–182, 2003.

[2] Randall Dougherty, R. Daniel Mauldin, and Mark Tiefenbruck. The covering radius of the Reed-Muller code $RM(m-4,m)$ in $RM(m-3,m)$. *IEEE Trans. Inform. Theory*, 68(1):560–571, 2022.

[3] Classification of Boolean Quartic Forms in Eight Variables Philippe Langevin, Gregor Leander. NATO Science for Peace and Security Series - D: Information and Communication Security *Boolean Functions in Cryptology and Information Security* (18) 139 – 147, 2005.

[4] J. Gao, H. Kan, Y. Li, and Q. Wang. The covering radius of the third-order reed-muller codes $\mathrm{rm}(3,7)$ is 20. *submitted to IEEE IT*, 2023.

[5] Valérie Gillot and Philippe Langevin. Classification of some cosets of the Reed-Muller code. `https://hal-univ-tln.archives-ouvertes.fr/hal-03834481`, 2022.

[6] Valérie Gillot and Philippe Langevin. Classification of $B(s,t,7)$. `http://langevin.univ-tln.fr/project/agl7/aglclass.html`, 2022.

[7] Valérie Gillot and Philippe Langevin. The covering radius of $RM(4,8)$. `http://langevin.univ-tln.fr/project/agl8`, 2022.

[8] Pless, V. S. and Huffman, W. C. and Brualdi, R. A. Handbook of coding theory. Vol. I, II, North-Holland, Amsterdam, 1998

[9] Qichun Wang. The covering radius of the Reed-Muller code $RM(2,7)$ is 40. *Discrete Math.*, 342(12):111625, 7, 2019.

Email address: `valerie.gillot@univ-tln.fr`

Email address: `philippe.langevin@univ-tln.fr`

Imath, université de Toulon