COVERING RADIUS OF $RM(4,8)$

VALÉRIE GILLOT AND PHILIPPE LANGEVIN

Abstract. We propose an effective version of the lift by derivation, an invariant that allows us to provide the classification of $B(5,6,8) = RM(6,8)/RM(4,8)$. The main consequence is to establish that the covering radius of the Reed-Muller $RM(4,8)$ is equal to 26. .

1. Boolean functions and classification

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 :

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

The degree of f is the maximal cardinality of S with $a_S = 1$ in the algebraic form. The valuation of $f \neq 0$, denoted by $\mathrm{val}(f)$, is the minimal cardinality of S for which $a_S = 1$. 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. Note that $B(s,t,m) = \{0\}$ whenever $s > t$. 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. Reducing modulo the space of functions of degree less than s, this group also acts on $B(s,t,m)$. The classification of $B(s,t,m)$ is a prerequisite for our approach. We denote by $\widetilde{B}(s,t,m)$ a classification of $B(s,t,m)$, that is a set of orbit representatives. The number of classes of $B(s,t,m)$ is denoted by $\mathrm{n}(s,t,m)$.

2. Covering radius of Reed-Muller codes

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 the space :

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

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 $f \in B(m)$. Classical parameters (length, dimension and minimum distance) of Reed-Muller codes are easy to determine and they all share $\mathrm{AGL}(m,2)$ as group of automorphisms. The classical results on covering radii of Reed-Muller codes are given in [8, p. 800]. Let us recall the simple however essential Lemma :

Date: April 2023.

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

Lemma 1.

(i) $2\rho(k,m-1) \leq \rho(k,m)$
(ii) $\rho(k-1,m-1) \leq \rho(k,m)$
(iii) $\rho(k,m) \leq \rho(k,m-1) + \rho(k-1,m-1)$

However, most of covering radii are still unknown. Recent results are obtained in [4, 9] in the case $m = 7$. Therefore, all the covering radii are known for $m \leq 7$. For $m = 8$, most the covering radii are unknown. Table 1 is an update of Table [8, p. 802] with the latest results corresponding to cases $m = 7, 8$.

TABLE 1. Updated Table of Handbook of coding theory.

k	1	2	3	4	5	6	7	8
$\rho(k,8)$	120	$88^a - 96$	$50^b - 67^f$	$\mathbf{26}^c$	10	2	1	0
$\rho(k,7)$	56	40^d	20^e	8	2	1	0	

(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) Obtained in this paper as a consequence of a lower bound found in [2];
(d) See the result in [9, Theorem 11] ;
(e) See the result in [4, Theorem 1] ;
(f) Consequence of Lemma 1-(iii).

We also consider $\rho_t(k,m)$ the relative covering radius of $RM(k,m)$ into $RM(t,m)$,

$$\rho_t(k,m) = \max_{f \in RM(t,m)} \mathrm{NL}_k(f) = \max_{f \in B(k+1,t,m)} \mathrm{NL}_k(f) \tag{1}$$

In the paper [2], the authors present methods for computing the distance from a Boolean function in $B(m)$ of degree $m-3$ to the Reed-Muller space $RM(m-4,m)$. It is useful to determine the relative covering radius $\rho_{m-3}(m-4,m)$. In particular, their result $\rho_5(4,8) = 26$ is a milestone for our purpose : computation of $\rho(4,8)$. It is necessary to determine $\rho_6(4,8)$, but considering the formula (1) the cardinality of $B(5,6,8) = 2^{84}$ is too large, using a set of representatives of $B(5,6,8)$

$$\rho_6(4,8) = \max_{f \in \widetilde{B}(5,6,8)} \mathrm{NL}_4(f).$$

Hence, the search space is reduced to the 20748 Boolean functions.

Our strategy for determining the covering radius $\rho(4,8)$ is described in figure 1. It consists in two parts. A first part dedicated to the tools which allow to obtain the classification of $B(5,6,8)$: cover set, invariant and equivalence. A second part is dedicated to the estimation of the 4th order nonlinearity of element in $\widetilde{B}(5,6,8)$.

3. Cover set and classification

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 $\rho_t(s-1,m)$:

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

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 will need a process to eliminate functions in same orbit. In the first instance, we construct a cover set with reasonable size in two reduction steps applied to $B(s,t,m)$. Any Boolean function $f \in B(m)$ can be written as $x_m g + h$ with $g, h \in B(m-1)$. In particular,

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

Lemma 2 (Initial cover set)**.** *The set*

$$B^{\dagger}(s,t,m) = \{x_m g + h \mid g \in \widetilde{B}(s-1,t-1,m-1), h \in B(s,t,m-1)\} \tag{3}$$

is a cover set of $B(s,t,m)$ *of size* $\sharp\widetilde{B}(s-1,t-1,m-1) \times \sharp B(s,t,m-1)$.

Proof. An element $\mathfrak{s} \in \mathrm{AGL}(m-1,2)$ acts on f by $x_m g \circ \mathfrak{s} + h \circ \mathfrak{s}$. □

Lemma 3 (Action of stabilizer)**.** *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* $x_m g + h$ *and* $x_m g + h \circ \mathfrak{s}$ *are in the same orbit.*
(2) For all $\alpha \in RM(1,m-1)$*, the functions* $x_m g + h$ *and* $x_m g + h + \alpha g$ *are in the same orbit.*

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

Lemma 4 (Second cover set)**.** *The set*

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

is a cover set of size $\sharp B^{\ddagger}(s,t,m) = \sum_{g\in\widetilde{B}(s-1,t-1,m-1)} \sharp\mathcal{R}(g)$. *Denoting by* $\mathcal{R}(g)$ *an orbit representatives set for the action over* $B(s,t,m-1)$ *of the group spaned by the transformations* $h \mapsto h\circ\mathfrak{s}$ *and* $h \mapsto h + \alpha g$.

Proof. For each $g \in \widetilde{B}(s-1,t-1,m-1)$ apply Lemma 3 to the cover set (3). □

In order to determine $\rho_6(4,8)$, the initial cover is $B^{\dagger}(5,6,8) = \widetilde{B}(4,5,7) \times B(5,6,7)$. The classification $\widetilde{B}(4,5,7)$ is obtained in [3], its cardinality is 179, whence $\sharp B^{\dagger}(5,6,8)$ is $179 \times 2^{28} \approx 2^{35.5}$.

Applying Lemma 4, 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 sections. Our approach is based on invariant tools and equivalence algorithm.

4. Invariant

From the result of the previous section in the case $B(5,6,8)$, we have to extract 20748 orbit representatives among 3828171 functions. 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 $f \sim^m_{s,t} f'$, 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 $f \sim^m_{s,t} f' \implies j(f) = j(f')$. If $j(f) = j(f')$ and $f \not\sim^m_{s,t} f'$, we say there is a collision.

Let us recall the derivative $\mathrm{d}_v f$ of a Boolean function f in the direction v is the application defined by $\mathbb{F}_2^m \ni x \mapsto \mathrm{d}_v f(x) = f(x+v) + f(x)$. In the specific case $f \in B(s,t,m)$, we define the derivative as

$$\mathrm{Der}_v f \equiv \mathrm{d}_v f \mod RM(s-2,m).$$

This derivative is an element of $B(s-1,t-1,m)$ and we consider the following map :

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

Lemma 5. *Let be $f \in B(m)$, $\mathfrak{s} \in \mathrm{AGL}(m,2)$. Considering the linear part $A \in \mathrm{GL}(m,2)$ and $a \in \mathbb{F}_2^m$ the affine part of $\mathfrak{s} = (A,a)$, $\mathfrak{s}(x) = A(x) + a$, we have $F(f \circ \mathfrak{s}) = F(f) \circ A$.*

Proof. Note that $\mathfrak{s}(x+y) = A(x+y) + a = \mathfrak{s}(x) + A(y)$. For $x, v \in \mathbb{F}_2^m$, $f \in B(m)$

$$\begin{aligned} \mathrm{d}_v(f \circ \mathfrak{s})(x) &= f \circ \mathfrak{s}(x+v) + f \circ \mathfrak{s}(x) \\ &= f(\mathfrak{s}(x) + A(v)) + f \circ \mathfrak{s}(x) \\ &= (\mathrm{d}_{A(v)} f) \circ \mathfrak{s}(x) \end{aligned}$$

Reducing modulo $RM(s-2,m)$, we have $\mathrm{Der}_v(f \circ \mathfrak{s}) \equiv (\mathrm{Der}_{A(v)} f) \circ \mathfrak{s}$, therefore $\widetilde{\mathrm{Der}_v(f \circ \mathfrak{s})} = \widetilde{\mathrm{Der}_{A(v)} f}$, whence $F(f \circ \mathfrak{s}) = F(f) \circ A$. □

Lemma 6 (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.*

Proof. Let consider $f, f' \in B(s,t,m)$, $\mathfrak{s} \in \mathrm{AGL}(m,2)$, such that $f' \equiv f \circ \mathfrak{s} \mod RM(s-1,m)$ (i.e. $f \sim_{s,t}^m f'$). Applying Lemma 5, we obtain $F(f') = F(f) \circ A$. □

Let us observe the derivative of $f \in RM(t,m)$ in the direction e_m, using the decomposition of f as in (2), for $(y, y_m) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2$ and $e_m = (0,1) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2$, we obtain :

$$\begin{aligned} \mathrm{d}_{e_m} f(y, y_m) &= f((y, y_m) + (0,1)) + f(y, y_m) \\ &= x_m(y, y_m + 1) g(y) + x_m(y, y_m) g(y) + h(y) + h(y) \\ &= (y_m + 1) g(y) + y_m g(y) \\ &= g(y) \end{aligned}$$

It is nothing but the partial derivative with respect to x_m. Hence, g is a Boolean function in $m-1$ variables of degree less or equal to $t-1$. This fact holds in general for a derivation in any direction v. A Boolean function $f \in B(m)$ is v-periodic iff $f(x+v) = f(x), \forall x \in \mathbb{F}_2^m$. The v-perodic Boolean functions are invariant under the action of any transvection $T \in \mathrm{GL}(m,2)$ of type $T(x) = x + \theta(x)v$, where v is in the kernel of the linear form θ.

For any supplementary E_v of v, the restriction $f|_{E_v}$ of a v-periodic function $f \in B(m)$ is a function in $m-1$ variables. Note that for $f \in B(s,t,m)$, $\mathrm{Der}_v f$ is v-periodic whoose its restriction to E_v is a Boolean function in $m-1$ variables of degree less or equal to $t-1$.

Lemma 7. *Let be $f, g \in B(m)$ two v-perodic Boolean functions. If f is equivalent to g in $B(m)$ then $f|_{E_v}$ is equivalent to $g|_{E_v}$ in $B(m-1)$, for any supplementary E_v of v.*

Proof. If f and g are equivalent in $B(m)$, there exists $\mathfrak{s} = (A, a)$ such that $f \circ \mathfrak{s} = g$. The case of a translation is immediate. We may assume $a = 0$ that is the action of the linear part A, $f \circ A = g$. Since g is v-perodic, g is fixed by any transvection $T = x + \theta(x)v$ where v is in the kernel of the linear form θ :

$$\forall x \in \mathbb{F}_2^m, \quad g(T(x)) = g(x + \theta(x)v) = g(x)$$

We denote P the projection of $\mathbb{F}_2^m$ over E_v in the direction of v ($P(e + v) = e$),

$$\forall x \in \mathbb{F}_2^m, \quad g(x) = g(T(x)) = f(AT(x)) = f(PAT(x)).$$

Note that $AT(x) = A(x) + \theta(x)A(v)$. We are going to determine $\theta(A^{-1}(v))$ so that $\ker PAT \cap E_v = \{0\}$. That means for $x \in E_v \setminus \{0\}$, $AT(x) \notin \{0, v\}$. Let $x \in \mathbb{F}_2^m$ such that $AT(x) = \lambda v$ with $\lambda \in \mathbb{F}_2$.

$$\begin{aligned}
&A(x) + \theta(x)A(v) = \lambda v \\
&x + \theta(x)v = \lambda A^{-1}(v) \\
&\theta(x) + \theta(x)\theta(v) = \lambda\theta(A^{-1}(v)) \quad \theta(x) = \lambda\theta(A^{-1}(v)) \\
&x = \lambda(A^{-1}(v) + \theta(A^{-1}(v))v)
\end{aligned}$$

There are two cases to be considered :

- $v \in A(E_v)$: $A^{-1}(v) \neq v$, we can fix $\theta(A^{-1}(v)) = 1$. Thus, $x = \lambda(A^{-1}(v) + v)$.
$$x = \lambda(A^{-1}(v) + v) \quad \lambda = \begin{cases} 0,\ x = 0 \\ 1,\ x \notin E_v \end{cases}$$
- $v \notin A(E_v)$: $A^{-1}(v) \notin E_v$, we can fix $\theta(A^{-1}(v)) = 0$. Thus $x = \lambda A^{-1}(v)$, we obtain $x = 0$ for $\lambda = 0$ and $x \notin E_v$ for $\lambda = 1$
$$x = \lambda A^{-1}(v) \quad \lambda = \begin{cases} 0,\ x = 0 \\ 1,\ x \notin E_v \end{cases}$$

In these two cases, we obtain $x = 0$ for $\lambda = 0$ and $x \notin E_v$ for $\lambda = 1$. Hence, the restriction of PAT to E_v is an automorphism, thus, $f|_{E_v}$ is equivalent to $g|_{E_v}$ in $B(m-1)$. □

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 and $\widehat{J}$ were introduced in [1]. In our context the invariant $\widehat{J}$ is more discriminating than J. The application of Lemma 7 allows us to consider the derivatives functions in $B(s-1, t-1, m-1)$ instead of $B(s-1, t-1, m)$.

Remark 1. *To make the algorithm* `Invariant`*, we need to optimise the class determination of an element of $B(4, 5, 7)$. There is only 4 classes in $\widetilde{B}(5, 5, 7)$. We precompute the complete classification of $B(5, 5, 7)$ by determining a representatives*

set $\{r_1, r_2, r_3, r_4\}$ *of* $\widetilde{B}(5,5,7)$*, stabilizers* $\{S_1, S_2, S_3, S_4\}$ *of each representative and a transversale. For each stabilizer, we keep in memory a description of the orbits of* $B(4,4,7)$ *under the stabilizer* S_i*. The class of an element* $h \in B(4,5,7)$ *is obtained from a representative* $r_i \sim^7_{5,5} h$ *and a transversale element* $\mathfrak{s} \in \mathrm{AGL}(7)$ *such that* $h \circ \mathfrak{s} \equiv r_i \mod RM(4,7)$ *using a lookup table for the key* $h \circ \mathfrak{s} + r_i$*.*
There is 179 *classes dans* $\widetilde{B}(4,5,7)$*. The amount of memory to store this data is about 32 GB.*

Listing 1. Invariant

```
Algorithm Invariant( f, s, t, m )
{   // f element of B(s,t,m)
    for each v in F_2^m
        g← d_v f
        h ←g|_{E_v}
        F[v] ←Class( h, s−1, t−1, m−1 )
    return FourierTransform( F )
}
```

Applying the invariant J to the 3828171 Boolean functions of the cover set $B^{\ddagger}(5,6,8)$, one finds 20694 distributions that means there are 54 collisions. On the same set, the invariant $\widehat{J}$ takes 20742 values : there are only 6 collisions. In the next section, we describe an equivalence algorithm to detect and solve theses collisions.

5. Equivalence

In this section, we work exclusively in the space $B(t-1,t,m)$, i.e. in the particular case $s = t-1$. Considering $\widehat{J}$, the invariant corresponding to the values distribution of $\widehat{F}(f)$. Two functions $f, f' \in B(t-1,t,m)$ that do not have the same values distribution are not equivalent. In the case $f \sim^m_{t-1,t} f'$, the distributions are identical and there exists $A \in \mathrm{GL}(m,2)$ such that

$$F(f') = F(f) \circ A \quad \text{and} \quad \widehat{F}(f') \circ A^* = \widehat{F}(f). \tag{5}$$

The existence of A does not guarantee the equivalence of the functions. Such an A is said a candidate which must be completed by an affine part $a \in \mathbb{F}_2^m$ to be able to conclude equivalence. For $f \in RM(t,m)$ and $x \in \mathbb{F}_2^m$,

$$\begin{aligned}
\mathrm{d}_{u,v} f(x) &= \mathrm{d}_v(\mathrm{d}_u f)(x) \\
&= \mathrm{d}_u(f(x+v) + f(x)) \\
&= f(x+u+v) + f(x+u) + f(x+v) + f(x) \\
&= f(x+u+v) + f(x) + f(x+u) + f(x) + f(x+v) + f(x) \\
&= \mathrm{d}_{u+v} f(x) + \mathrm{d}_u f(x) + \mathrm{d}_v f(x)
\end{aligned}$$

The degree of $\mathrm{d}_{u,v} f$ is less or equal $t-2$, reducing modulo $RM(t-2,m)$, we obtain

$$\mathrm{d}_{u+v} f(x) + \mathrm{d}_u f(x) + \mathrm{d}_v f(x) \equiv 0.$$

The set $\Delta(f) = \{\mathrm{d}_v f \mod RM(t-2,m) \mid v \in \mathbb{F}_2^m\}$ is a subspace of $B(t-1,t-1,m)$.

Lemma 8 (Candidate checking)**.** *Let f, f' be in $B(t-1,t,m)$. Let us consider a candidate $A \in \mathrm{GL}\,(m)$. 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 $f' \circ A^{-1} + f \in \Delta(f)$.*

Proof. If $f' \equiv f \circ (A,a) \mod RM(t-2,m)$, there exists $r \in RM(t-2,m)$ such that for all $x \in \mathbb{F}_2^m$

$$\begin{aligned} f'(x) &= f \circ (A,a)(x) + r(x) = f(A(x)+a) + r(x) \\ f' \circ A^{-1}(x) &= f(x+a) + r(x) \\ f' \circ A^{-1}(x) + f(x) &= f(x+a) + f(x) + r(x) \\ (f' \circ A^{-1} + f)(x) &= \mathrm{d}_a f(x) + r(x) \end{aligned}$$

Thus $f' \circ A^{-1} + f \in \Delta(f)$. Conversely, for $f' \circ A^{-1} + f \in \Delta(f)$, there exists $a \in \mathbb{F}_2^m$ such that $f' \circ A^{-1} + f \equiv \mathrm{d}_a f \mod RM(t-2,m)$. There exists $r \in RM(t-2,m)$ such that for all $x \in \mathbb{F}_2^m$, $(f' \circ A^{-1} + f)(x) = \mathrm{d}_a f(x) + r(x)$. By repeating the calculations in reverse order, we have $f' \equiv f \circ (A,a) \mod RM(t-2,m)$. ☐

From Lemma 8, one deduces an algorithm `CandidateChecking(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 $\widehat{J}(f) = \widehat{J}(f')$, 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 `CandidateChecking(A,f,f')`.

The algorithm ends with one of following three values :

$$\texttt{Equivalent}(f,f',\texttt{iter}) = \begin{cases} \texttt{NotEquiv}, & \text{all potential } A \text{ were tested, so } f \not\sim^m_{t-1,t} f'; \\ \texttt{Equiv}, & \text{there exists a } (A,a) \text{ to prove } f \sim^m_{t-1,t} f'; \\ \texttt{Undefined}, & \texttt{iter} \text{ is too small to conclude.} \end{cases}$$

Listing 2. 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
}
```

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

Listing 3. Search

```
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 CandidateChecking(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)
```

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.

6. Determination of $\rho(4, 8)$

The different steps of our strategy to determine $\rho(4, 8)$ are sumarised in 1.

```
Algorithm NonLinearity(k,m,f,iter,limit)
{
    G ←generator matrix of RM(k,m)
    while ( iter > 0 )
        for( i = 0 ; i < k; i++ )
        do {
            p = random( n )
        } while ( not G[i][ p] )
        for( j = i+1 ; j < k; j++ )
            if ( G[j][ p] )
            G[j] ←G[j] xor G[i]
        if ( f[ p ] )
            f ←f xor G[i]
        w = weight( f )
        if ( w <= limit )
            return true
    iter ←iter − 1
    return false
}
```

This algorithm proceeds ramdom Gaussian eliminations to generate small weight codewords in a translate of $RM(k,m)$. To dertermine the covering radii $\rho_6(4,8)$ and $\rho(6,8)$, we have to estimate the nonlinearity of order 4 of some functions in $B(8)$. We use the probabilistic algorithm `NonLinearity` three times :

(1) to check the non-existence of function in $\widetilde{B}(5,6,8)$ of nonlinearity of order 4 greater or equal to 28 ;
(2) to extract the set of two functions $\{f,g\}$ in $\widetilde{B}(5,6,8)$ with nonlinearity of order 4 greater or equal to 26 ;
(3) to prove the nonlinearity of order 4 of the functions $\{f+\delta_a, g+\delta_a\}$ is not greater or equal to 27.

6.1. **Compute** $\rho_6(4,8)$**.** Recall that

$$\rho_6(4,8) = \max_{f\in\widetilde{B}(5,6,8)} \mathrm{NL}_4(f) = \max_{f\in\widetilde{B}(5,6,8)} \min_{g\in RM(4,8)} \mathrm{wt}\,(f+g).$$

We apply the algorithm `NonLinearity` to $\widetilde{B}(5,6,8)$ to confirm that all these functions have a nonlinearity of order 4 less or equal to 26. Using the result $\rho_5(4,8)=26$ of [2], we obtain $\rho_6(4,8)=26$.

6.2. **Compute** $\rho(4,8)$**.** Knowing that $\rho(6,8)=2$ and from the previous result of $\rho_6(4,8)=26$, we have

$$\rho(4,8) \le \rho_6(4,8) + \rho(6,8) = 28.$$

A second application of the algorithm `NonLinearity` eliminates from $\widetilde{B}(5,6,8)$ 20746 functions of nonlinearity of order 4 less than 26. After this process, there are two remaining functions :

$$\begin{aligned} f = abcef + acdef + abcdg + abdeg + abcfg + acdeh + abcfh \\ + bdefh + bcdgh + abegh + adfgh + cefgh \end{aligned}$$

and

$$g = abcdeh + abcdf + abcef + abdeg + bcefh + adefh + bcdgh + acegh + abfgh$$

We retrieve the cocubic function f, mentioned in [2], its degree is 5 and its nonlinearity of order 4 is 26. The other function g has degree 6 and its nonlinearity is probabily 26 and certainly less or equal to 26. Now, we are going to prove that there is no Boolean function in $B(8)$ with a nonlinearity of order 4 equal to 28. For this purpose, it is sufficient to check the non-existence of a function h satisfying $\mathrm{NL}_4(h)=27$, such a h has an odd weight and therefore its degree is 8. For $a\in\mathbb{F}_2^m$, we denote by δ_a the Dirac function, $\delta_a(x)=1$ iff $x=a$. Every Boolean function can be expressed by a sum of Dirac $f(x)=\sum_{\{a|f(a)=1\}}\delta_a(x)$. The polynomial form of δ_a is :

$$\delta_a(X_1,X_2,\ldots,X_m) = (X_1+\bar{a}_1)(X_2+\bar{a}_2)\cdots(X_m+\bar{a}_m) \tag{6}$$

where $\bar{a}_i = a_i+1$.

Lemma 9. *An odd weight function is at distance one from $RM(m-2,m)$.*

Proof. We denote $\widetilde{X_i}$ the monomial term of degree $m-1$ with all variables except X_i. Let us consider an odd weight function $h\in B(m)$, its degree is m, so

$$h(X_1,X_2,\ldots,X_m) = X_1X_2\ldots X_m + \bar{a}_1\widetilde{X_1} + \cdots + \bar{a}_m\widetilde{X_m} + r(x)$$

where $\deg(r) \leq m-2$. From (6), we also have

$$\delta_a(X_1, X_2, \ldots, X_m) = X_1X_2\ldots X_m + \bar{a}_1\widetilde{X_1} + \cdots + \bar{a}_m\widetilde{X_m} + r'(x)$$

with $\deg(r') \leq m-2$. We obtain $h \equiv \delta_a \mod RM(m-2,m)$. The Dirac function has weight 1, so the distance of h to $RM(m-2,m)$ is 1. $\square$

A third application of the algorithm `NonLinearity` to the set $\{f,g\}$ translated by the 256 Dirac functions give the non-existence of odd weight functions of nonlinearity of order 4 greater or equal to 27. That means there is no function in $B(8)$, with nonlinearity of order 4 greater or equal to 27 and we obtain $\rho(6,8) = 26$. The second and third applications of the algorithm `NonLinearity` need 569713 iterations.

Remark 2. *The extraction of 20748 classes of $\widetilde{B}(5,6,8)$ with invariant approach and* `equivalent` *algorithm needs several weeks of computation (equivalence test)*

Remark 3. *The number of iterations to estimate the 4th order nonlinearity of Boolean functions 565252 in average. The total running time to check the nonlinearity is about one day using 48 processors.*

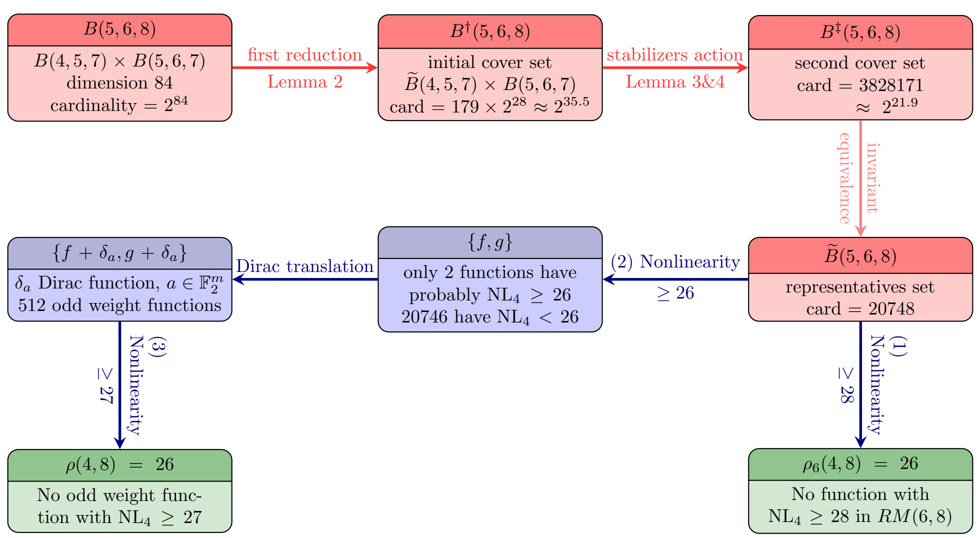

FIGURE 1. Strategy to compute $\rho(4,8)$

7. CONCLUSION

We have determine the covering radius of $RM(4,8)$ from the classification of $B(5,6,8)$. It is not obvious how to apply our method to obtain the covering radii of the second and third order Reed-Muller in 8 variables. However, we believe that our approach can help to improve lower bounds in these open cases.

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 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