

CLASSIFICATION OF SOME COSETS OF THE REED-MULLER CODE

Valérie Gillot, Philippe Langevin

▶ **To cite this version:**

Valérie Gillot, Philippe Langevin. CLASSIFICATION OF SOME COSETS OF THE REED-MULLER CODE. 2022. hal-03834481

HAL Id: hal-03834481

https://univ-tln.hal.science/hal-03834481

Preprint submitted on 30 Oct 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CLASSIFICATION OF SOME COSETS OF THE REED-MULLER CODE

VALÉRIE GILLOT AND PHILIPPE LANGEVIN

ABSTRACT. This paper presents a descending method to classify Boolean functions in 7 variables under the action of the affine general linear group. The classification determines the number of classes, a set of orbits representatives and a generator set of the stabilizer of each representative. The method consists in the iteration of the classification process of $RM(k,m)/RM(r-1,m)$ from that of $RM(k,m)/RM(r,m)$. We namely obtain the classifications of $RM(4,7)/RM(2,7)$ and of $RM(7,7)/RM(3,7)$, from which we deduce some consequences on the covering radius of $RM(3,7)$ and the classification of near bent functions.

1. INTRODUCTION

Let $\mathbb{F}_2$ be the finite field of order 2. Let m be a positive integer. A mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2$ is called a Boolean function. Every Boolean function has a unique algebraic reduced representation :

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

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 space $B(0,t,m)$ identifies with the Reed-Muller code $RM(t,m)$ and $B(s,t,m)$ is the representation of the quotient space $RM(t,m)/RM(s-1,m)$. The affine general linear group of $\mathbb{F}_2^m$, denoted by $\mathrm{AGL}(m,2)$, acts naturally over all these spaces. The number of classes of $B(s,t,m)$, denoted by $\mathrm{n}(s,t,m)$, satisfies a nice duality relation :

$$\mathrm{n}(s,t,m)=\mathrm{n}(m-t,m-s,m). \tag{1}$$

X.-D. Hou gives a proof of the above relation in [4]. In the proof of Lemma 1, we propose an alternative demonstration.

For the dimensions that we want to consider, all class numbers are very easy to determine using Burnside's Lemma and the theory of conjugacy classes of $\mathrm{AGL}(m,2)$, see e.g. [5].

In general, such a class number is huge, but, when it is reasonably small, one may consider to determine an orbit representative set that is a list of $\mathrm{n}(s,t,m)$ Boolean functions, of degree less than or equal to t, and pairwise non affine equivalent

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

modulo $RM(s-1,m)$. As an example, the class number $\mathrm{n}(2,6,6)$ is 150357 and J. Maiorana in [6] describes a recursive algorithm to find the 150357 equivalence classes.

More generally, the classification data of the space $B(s,t,m)$ plays an important role both in coding theory and cryptography. The covering radii of Reed-Muller codes are not generally known and the classification of $B(s,t,m)$ can be used to bound the covering radius of $RM(s-1,m)$ in $RM(t,m)$ as in the paper [9]. These classifications are also used to study the cryptographic parameters of Boolean functions.

This paper presents a procedure to provide classifications of Boolean functions spaces for $m=7$. Precisely, we compute orbit representative sets of $B(s,t,7)$, for all parameters $s \leq t \leq 7$ such that $\mathrm{n}(s,t,7)$ is less than 10^6.

Our approach gives *complete* classifications : not only sets of orbit representatives, but also for each representative, a generator set of stabilizer group. The most interesting cases are the classifications of $B(3,4,7)$ and of $B(4,7,7)$. From the first one, we determine the classification of near bent functions. From the second, we refind, with an alternative method, the covering radius of $RM(3,7)$ obtained in [2].

All computed data are available on the project page [3].

2. Boolean functions

A Boolean function f is a member of $B(s,t,m)$ if and only if $s \leq \mathrm{val}(f)$ and $\deg(f) \leq t$. Denoting $\bar{S}$ the complement set of $S \subseteq \{1,2,\ldots,m\}$, the complementary transform $\sum_S X_S \mapsto \sum_S X_{\bar{S}}$ maps $B(s,t,m)$ onto $B(m-t,m-s,m)$, in particular, these spaces have the same dimension. A Reed-Muller code of order k in m variables is the space of Boolean functions of degree less or equal to k :

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

Note that Reed-Muller spaces are nested :

$$\underbrace{RM(-1,m)}_{(0)} \subset RM(0,m) \subset RM(1,m) \subset \cdots \subset RM(m-1,m) \subset \underbrace{RM(m,m)}_{B(m)}.$$

The quotient space $RM(k,m)/RM(k-1,m)$ is the space of homogeneous forms of degree k, identified with the space $B(k,k,m)$, its dimension is the value of the binomial coefficient $\binom{m}{k}$. The dimension of $B(s,t,m)$ is equal to the sum of binomial coefficients $\sum_{k=s}^{t}\binom{m}{k}$. It is easy to see that the weight of a Boolean function is even if and only if its degree is not maximal, consequently the orthogonal of $RM(k,m)$ is $RM(m-k-1,m)$, with respect to the scalar product $\langle f,g\rangle = \sum_{x\in\mathbb{F}_2^m} f(x)g(x)$.

Lemma 1 (duality)**.** *For all s,t such that $s \leq t \leq m$, $B(m-t,m-s,m)$ is a representation of $B(s,t,m)^*$, the dual space of $B(s,t,m)$. It means that for any form $\phi \in B(s,t,m)^*$ there exists one and only one $g \in B(m-t,m-s,m)$ such that $\phi(f) = \langle f,g\rangle$, for all $f \in B(s,t,m)$.*

Proof. Note that the dimension of $B(m-t,m-s,m)$ is precisely the dimension of $B(s,t,m)$. If $0 \neq g \in B(m-t,m-s,m)$ then $g \notin B(s,t,m)^{\perp}$. Indeed, consider a monomial term X_S of maximal degree in the algebraic representation of g :

$$m-t \leq \deg(g) = \deg(X_S) \leq m-s \quad \text{and} \quad s \leq \deg(X_{\bar{S}}) \leq t.$$

The product $X_{\bar{S}}g = X_{\bar{S}}X_S + \cdots$ has degree m whence $X_{\bar{S}}$ is member of $B(s,t,m)$ which is not orthogonal to g. In other words, the space $B(m-t,m-s,m)$ is a representation of $B(s,t,m)^*$. □

3. Action of the affine general linear group

First, let us recall some definitions. Let $(G,*)$ be a finite group and let U be a finite set, a right group action of G on U is a mapping from $U \times G$ to U denoted by $(u,g) \longmapsto u \circ g$ satisfying $u \circ e = u$ and $(u \circ g) \circ h = u \circ (g * h)$, for $u \in U$, $g,h \in G$ and e the identity of G. The orbit of an element u is the set of elements in U to which u can be moved by the elements of G, denoted by $\mathcal{O}_u = \{u \circ g \mid g \in G\}$. The stabilizer subgroup of G with respect to $u \in U$ is the set of elements in G that fixes u, denoted by $\textsc{stab}(u) = \{g \in G \mid u \circ g = u\}$.

The affine general linear group acts naturally on the right over Boolean functions. The action of $\mathfrak{s} \in \textsc{agl}(m,2)$ on a Boolean function f is $f \circ \mathfrak{s}$, the composition of applications. The order of $\textsc{agl}(m,2)$ is $2^m \prod_{i=0}^{m-1}(2^m - 2^i) \approx 0.29\ 2^{m^2+m}$. Note that the number of orbits of this group action has doubly exponential growth with the parameter m. For $m = 7$, it is already numerically impossible to list the $\approx 2^{74}$ classes of Boolean functions !

The Reed-Muller spaces are invariant under the action of $\textsc{agl}(m,2)$. Considering the action modulo $RM(r,m)$, the space of functions of degree less or equal than r, we introduce objects at level r. Two Boolean functions f and g in m variables are equivalent at level r, if there exists $\mathfrak{s} \in \textsc{agl}(m,2)$ such that $f \circ \mathfrak{s} \equiv g \mod RM(r,m)$. We introduce two notations $f \underset{r}{\sim} g$ for the equivalence at level r, and $\textsc{stab}_m^r(f)$, for the stabilizer of f at level r :

$$f \underset{r}{\sim} g \Longleftrightarrow \exists \mathfrak{s} \in \textsc{agl}(m,2),\ f \circ \mathfrak{s} \equiv g \mod RM(r,m). \tag{2}$$

$$\textsc{stab}_m^r(f) = \{\mathfrak{s} \in \textsc{agl}(m,2) \mid f \circ \mathfrak{s} \equiv f \mod RM(r,m)\}. \tag{3}$$

In this paper, we consider the action of $\textsc{agl}(m,2)$ over $B(s,t,m)$ as the composition of applications modulo $RM(s-1,m)$. Precisely, two elements $f,g \in B(s,t,m)$ are in the same orbit, under this action, if and only if they are equivalent at level $s-1$, that is $f \underset{s-1}{\sim} g$. In this context, the stabilizer of f is nothing but $\textsc{stab}_m^{s-1}(f)$ the stabilizer at level $s-1$.

Thus, the affine general linear group acts over the $B(s,t,m)$, the corresponding class number $\mathrm{n}(s,t,m)$ is given by Burnside's formula :

$$|\textsc{agl}(m,2)| \times \mathrm{n}(s,t,m) = \sum_{\mathfrak{s} \in \textsc{agl}(m,2)} \sharp \mathrm{fix}_m^{s,t}(\mathfrak{s}) = \sum_{\mathfrak{s} \in \Gamma} R(\mathfrak{s})\, \sharp \mathrm{fix}_m^{s,t}(\mathfrak{s}). \tag{4}$$

where $\mathrm{fix}_m^{s,t}(\mathfrak{s})$ is the set $\{f \in B(s,t,m) \mid f \circ \mathfrak{s} \equiv f \mod RM(s-1,m)\}$, i.e. the kernel of the endomorphism of $B(s,t,m)$ defined by $f \mapsto f \circ \mathfrak{s}$. In practice, we reduce the sum to the Γ, a set of representatives of conjugacy classes of $\textsc{agl}(m,2)$, and $R(\mathfrak{s})$ the size of the conjugacy class of $\mathfrak{s}$, see book [5] for the finite fields combinatoric details.

Lemma 2 (formula)**.** *For all s,t such that $s \leq t \leq m$,*

$$\mathrm{n}(s,t,m) = \mathrm{n}(m-t,m-s,m)$$

Proof. Let us recall that the rank of a subgroup of the general linear group over a finite space is the same that the dual group. For $\mathfrak{s} \in \mathrm{AGL}(m,2)$, the adjoint of the automorphism $f \mapsto f \circ \mathfrak{s}$ corresponds to the inverse of $\mathfrak{s}$, because

$$\langle f \circ \mathfrak{s}, g \rangle = \sum_{x \in \mathbb{F}_2^m} f \circ \mathfrak{s}(x) g(x) = \sum_{x \in \mathbb{F}_2^m} f(x) g \circ \mathfrak{s}^{-1}(x) = \langle f, g \circ \mathfrak{s}^{-1} \rangle.$$

The result follows using Burnside's formula by observing

$$\sum_{\substack{f \in B(s,t,m) \\ g \in B(s,t,m)^*}} (-1)^{\langle f \circ \mathfrak{s} + f, g \rangle} = \sum_{\substack{f \in B(s,t,m) \\ g \in B(s,t,m)^*}} (-1)^{\langle f, g \circ \mathfrak{s}^{-1} + g \rangle}$$

$$\sharp B(s,t,m)^* \times \sharp \mathrm{fix}_m^{s,t}(\mathfrak{s}) = \sharp B(s,t,m) \times \sharp \mathrm{fix}_m^{m-t,m-s}(\mathfrak{s}^{-1})$$

□

In this paper, by a classification at level r of degree k in m variables, we mean a classification of $B(r+1,k,m)$, that is a set of orbit representatives at level r under the right action of $\mathrm{AGL}(m,2)$, and for each orbit representative f, a generator set of $\mathrm{STAB}_m^r(f)$, the stabilizer of f at level r. It is important to note that at level r, we calculate modulo $RM(r,m)$, and we consider polynomials whose valuations are strictly greater than r.

Recall that $\mathrm{AGL}(m,2)$ can be generated by three following transformations : the shift operator $S\colon v \mapsto (v_{m-1}, \ldots, v_1, v_m)$, the transvection $T\colon v \mapsto (v_m, \ldots, v_2, v_1 + v_2)$ and the translation $U\colon v \mapsto v + (0, \ldots, 0, 1)$.

In next section, we detail the procedure that we used to build a classification at level $r-1$ from a classification at level r. Starting at level k, there is only one orbit $\{0\} = B(k+1,k,m)$ stabilized by full group $\mathrm{AGL}(m,2) = \langle S, T, U \rangle$. One can start from this classification at level k to determine the classifications at level $k-1$, level $k-2$, etc. The process can be stopped at any level or be continued until level -1 to reach the classfication of $B(0,k,m) = RM(k,m)$. In the same way, we classify $B(s,t,m)$ in $t-s+1$ iterations starting from the classification of $B(t+1,t,m) = \{0\}$.

4. Descending procedure

In order to deduce a classification at level $r-1$ from a classification a level r, we have to consider some "boundary actions" on $B(r,r,m)$ the space of homogeneous forms of degree r.

An element $\mathfrak{s}$ of the stabilizer of f at level r induces an action on homogeneous forms of degree r defined for $u \in B(r,r,m)$ by

$$u \mapsto u \circ \mathfrak{s} + f \circ \mathfrak{s} + f \mod RM(r-1,m)$$

Lemma 3 (boundary)**.** *Let $\mathcal{R}$ be a set of orbit representatives of degree k at level r. For each $f \in \mathcal{R}$, $\mathcal{U}(f)$ denotes a set of orbit representatives of $B(r,r,m)$ under the boundary action of $\mathrm{STAB}_m^r(f)$. We obtain that $\{f + u \mid f \in \mathcal{R}, u \in \mathcal{U}(f)\}$ is a set of orbit representatives with same degree at level $r-1$.*

Proof. We start by showing the elements of this set are not equivalent at level $r-1$. Indeed, let f' and f be in $\mathcal{R}$, and two forms $u' \in \mathcal{U}(f')$ and $u \in \mathcal{U}(f)$ such that $f + u \underset{r-1}{\sim} f' + u'$. There exists $\mathfrak{s} \in \mathrm{AGL}(m,2)$ such that $f' + u' \equiv (f+u) \circ \mathfrak{s}$

mod $RM(r-1,m)$. Reducing more, we obtain $f' \equiv f \circ \mathfrak{s} \mod RM(r,m)$; so that f' and f are equivalent at level r, thus $f' = f$. The boundary action of $\mathfrak{s} \in \text{STAB}_m^r(f)$ sends u to u' and finally $u' = u$. Now, we prove that the set represents all polynomials at level $r-1$. Indeed, let $g \in B(r-1,k,m)$ there exists a pair $(\mathfrak{t}, f) \in \text{AGL}(m,2) \times \mathcal{R}$ such that $g \circ \mathfrak{t} \equiv f \mod RM(r,m)$ whence $g \circ \mathfrak{t} \equiv f + v \mod RM(r-1,m)$ where v is a form of degree r, and there is a boundary action $\mathfrak{s} \in \text{STAB}_m^r(f)$ that sends v to some $u \in \mathcal{U}(f)$ whence $g \circ \mathfrak{t}\mathfrak{s} \equiv (f+v) \circ \mathfrak{s} \equiv f + u \mod RM(r-1,m)$. □

Considering the right action of a group G over a set U, we denote by $u \circ s$ the action of $s \in G$ on $u \in U$, $\mathcal{O}_u$ the orbit of u, S_u the stabilizer of u and s_u the order of S_u.

Lemma 4 (class formula)**.** *If G is a finite group acting on a finite set U then the size of the orbit of an element $u \in U$ is equal to $|G|/s_u$ where s_u is the order of the stabilizer S_u of u.*

Proof. There is a bijection from G/S_u onto $\mathcal{O}_u$ the orbit of u. □

Lemma 5 (Schreier)**.** *Let L be a set of generators of a finite group G right acting on a finite set U. Let $\mathcal{O}_u$ be the orbit of some element $u \in U$. If $R\colon \mathcal{O}_u \to G$ is a map such that $u \circ R(x) = x$ for all $x \in \mathcal{O}_u$ then $\{R(x)\lambda R(x \circ \lambda)^{-1} \mid \lambda \in L, x \in \mathcal{O}_u\}$ spans the stabilizer S_u of u.*

Proof. See [8]. □

Knowing the value s_u, one can build a generator set of its stablizer S_u applying Schreier's Lemma. We implement this idea in the algorithm `generatorSet` where $*$ denotes the law group and $\circ$ denotes the action of the group.

Now, we describe our descending procedure based on Lemma 3 and Lemma 5 to construct a set of orbit representatives at level $r-1$ from level r. In view of dimension of forms space $B(r,r,m)$ and to save memory space, we proceed in two phases :

(1) For each representative f at level r, we use a classical algorithm to enumerate an orbit representatives set of $B(r,r,m)$ under the action of $\text{STAB}_m^r(f)$. For each representative u, we obtain the orbit $\mathcal{O}_u$, and by Lemma 4, the order s_u of $\text{STAB}_m^{r-1}(f+u)$ is equal to $\sharp\text{STAB}_m^r(f)/\sharp\mathcal{O}_u$.
(2) For each representative f at level r, let L be a generator set of $\text{STAB}_m^r(f)$. For each pair (u, s_u), obtained in (1), we apply `generatorSet(`u`, `L`, `s_u`)` to construct a set of generators of $\text{STAB}_m^{r-1}(f+u)$.

5. RESULTS AND APPLICATIONS

Our implementation in C language of the descending procedure, without any parallelization, builds the full classification of $B(2,6,6)$ in 15 secondes. It classifies $B(3,4,7)$ in three days by requiring about 50GB of memory.

The values of $\mathrm{n}(s,t,7)$ for $0 \le s \le t \le 7$ are listed in Table 1. For all parameters $0 \le s \le t \le 7$ such that $\mathrm{n}(s,t,7) < 10^6$, the descending procedure classifies $B(s,t,7)$, it computes for each orbit, a representative and also a generator sets of the corresponding stabilizer. All the numerical data are available in project page [3].

LISTING 1. Construction of a generator set of S_u.

```
1  Algorithm generatorSet( u , L, s_u )
2  {   // return a generator set of the stabilizer of u
3      // under the action of the group generated by L
4      // knowing its order s_u
5      S ←∅
6      push( u )
7      R [ u ] ← id
8      Y ← { u }
9      while ( order( <S> ) < s_u) {
10         pop( x )
11         for λ ∈ L {
12             y ← x ∘ λ
13             if y ∉ Y {
14                 push(y)
15                 R[ y ] ←R[ x ] ∗ λ
16                 Y← Y ∪ {y}
17             } else {
18               s ← R[x] ∗ λ ∗ inverse ( R[ y ] )
19               if ( s not in <S> )
20                  S ←S ∪ { s }
21             }
22         }
23     return S;
24 }
```

TABLE 1. Class numbers $\mathrm{n}(s,t,7)$.

$s\backslash t$	1	2	3	4	5	6	7
0	3	12	3486	$10^{13.5}$	$10^{19.8}$	$10^{21.9}$	$10^{22.2}$
1	2	8	1890	$10^{13.1}$	$10^{19.5}$	$10^{21.6}$	$10^{21.9}$
2		4	179	$10^{11.0}$	$10^{17.3}$	$10^{19.5}$	$10^{19.8}$
3			12	68443	$10^{11.0}$	$10^{13.1}$	$10^{13.5}$
4				12	179	1890	3486
5					4	8	12
6						2	3
7							2

In the next subsections, we focus on applications of the classifications of $B(3,4,7)$ and $B(4,7,7)$.

5.1. **Using invariant.** An alternative way to build a list of orbit representatives consists to use invariants. Success for invariant based approach is not guaranteed for two reasons : small orbits are hidden and difficult to detect, and the invariants used may not be discriminating enough ! Moreover, invariant approach does not give orbit sizes and even less the generator set of stabilizers. The invariant approach proposed in [7] failed to find a list of representatives of $B(3,4,7)$. In that case, the

number of orbits is $\mathrm{n}(2,4,7) = 68433$ and using invariants, the authors got 68095 classes whence missing 338 orbits.

5.2. **Counting near bent functions.** Let us recall that a 7-bit Boolean function is near bent when its Walsh spectrum takes three values 0, ± 16. A such function has degree less or equal to 4. The set of near bent functions is invariant under the action of affine general linear group. From the classification of $B(3,4,7)$, it is possible to count the number of near bent functions. For each $f \in B(3,4,7)$, we determine the number $N(f)$ of quadratic forms $q \in B(2,2,7)$ such that $f+q$ is near bent. By this naive approach, one find the total number of near-bent functions in seven variables:

$$\sum_{f \in B(3,4,7)/\underset{2}{\sim}} N(f) \times \frac{\sharp \mathrm{AGL}(m,2)}{\sharp \mathrm{STAB}_7^2(f)} = 88624918554694407235840 \approx 2^{76.3}$$

In Table 2, we can read the number of classes of $B(s,t,m)$ whose the stabilizer has a small order. For example, there is 50308 classes of $B(3,4,7)$ with a stabilizer of order 1 that represents 74% of classes. Since, it is not reasonnable to store the full

TABLE 2. Multiplicities of small order stablizers.

order	1	2	3	4	6	7	8	12	14	16
$B(3,4,7)$	50308	9591	134	3059	235	12	1877	163	15	895
$B(4,7,7)$	389	571	7	444	48	3	384	68	7	236

classfication of $B(2,4,7)$ simply because the number of classes is huge : $\mathrm{n}(2,4,7) = 118140881980$. However, we can adapt the descending method to classify the set of near bent functions $f+q$ where $\sharp \mathrm{STAB}_7^2(f) > 1$. Finally, we obtain 4243482 classes of near bent functions in $B(2,4,7)$. Note that 99.2% of classes have a trivial stabilizer. The classification of the near bent function of $B(2,4,7)$ is availble on the website of the project. We hope that all the data presented here can be used to answer the following open problems :

Open problem 1. *It is well known that the restriction to any hyperplane of a bent function is nearbent. Are all the near bent function a restriction of a bent function ?*

Open problem 2. *As suggested in note* [7]*, is it feasible to count/classify the 8-bit bent function from the classification 7-bit near bent ?*

5.3. **Covering radius of RM(3,7).** In 2019, Wang [9] proved that the covering radius of $RM(2,7)$ is equal to 40. A part of that proof, is based on the classification of $B(2,6,6)$. The covering radius of $RM(3,7)$ into $RM(4,7)$ is known to be 20 see [1]. In the recent preprint [2], Gao, Kan, Li and Wang showed the covering radius of $RM(3,7)$ is less or equal to 20 using the classification of $B(4,6,6)$. All these methods use more or less computer assistance. Here, we point out how to use directely the classification of $B(4,7,7)$ to obtain that the covering radius of $RM(3,7)$ is less or equal to 20. The key point is to use a variation of Leon's algorithm to exibit small weight codewords in the translate of a code.

Given the generator matrix G of an $[n,k]$- Reed-Muller code C, the algorithm `distance(f, G, T)` applies a random procedure to check the existence of a Boolean

LISTING 2. Counting trials to find a small cosetword.

```
maxIter = 2048
Algorithm distance( f, G, T )
{
// G generator matrix of a [n,k]−Reed−Muller code
    score  = n
    trials  = 0
    while ( score > T ) and ( trails  < maxIter) {
        g ←action( f )
        pivoting( G )
        reduce( g, G )
        w ←weight( g )
        if ( w < score )
            score ←w
        trials  = trials  + 1
    }
    return trials;
}
```

function of weight less or equal to T in the translate code $f + C$. This algorithm uses three components :

- `action(f)` returns a random action of AGL$(m, 2)$ on `f`
- `pivoting(G)` applies Gauss elimination algorithm to the generator matrix `G` choosing a random pivot on each of its line. Each line of the matrix obtained has weight less or equal to $n - k + 1$
- `reduce(g,G)` transforms `g` adding to it the lines of `G` corresponding of the pivot position. More precisely, for each line L_i of `G`, let us denote p_i the position of the pivot on this line, `reduce` adds to `g` the line L_i when $\mathtt{g}(p_i) = 1$. Again, `g` has weight less or equal to $n - k + 1$

The algorithm finishes when it finds a Boolean function `g` in the translate code of weight less or equal to `T` or when the number of trials exceeds an arbitrary limit `maxIter`.

We apply `distance(f, G, T)` to each representative of $B(4, 4, 7)$ to prove the non-existence of Boolean functions at distance greater than 20 from $RM(3, 7)$. This work requires an average of 538.6 trials with standard deviation 806.17.

Open problem 3. *In* [1]*, the covering radius of* $RM(4, 8)$ *in* $RM(5, 8)$ *is shown to be 26. Is it possible to build a classification of* $B(5, 6, 8)$ *and to apply similar methods in order to determine the covering radius of* $RM(4, 8)$ *or at least in* $RM(6, 8)$ *?*

6. CONCLUSION

We present an efficient descending method to classify the cosets of Reed-Muller codes. This procedure allow us to obtain the classification of two important cosets of length 128 : $RM(4, 7)/RM(2, 7)$ and $RM(7, 7)/RM(3, 7)$. The first one provides the classification of near bent functions in seven variable. From the the second, we explain how we refind the value of the covering radius of $RM(3, 7)$.

References

[1] 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.

[2] 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.

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

[4] Xiang-Dong Hou. $\mathrm{AGL}(m,2)$ acting on $R(r,m)/R(s,m)$. *J. Algebra*, 171(3):921–938, 1995.

[5] Xiang-Dong Hou. *Lectures on finite fields*, volume 190 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.

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

[7] Meng Qingshu, Zhang Huanguo, Cui Jingsong, and Yang Min. Almost enumeration of eight-variable bent functions. *iacr preprint*, 2005.

[8] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[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