CLASSIFICATION OF BOOLEAN QUARTIC FORMS IN EIGHT VARIABLES

PHILIPPE LANGEVIN AND GREGOR LEANDER

Abstract. We present the strategy that we recently used to compute the complete classification of Boolean quartic forms in eight variables. Furthermore, we outline some applications of this result.

1. Introduction

Let m be a positive integer. By a *Boolean function* we understand a mapping f from $\mathbb{F}_2^m$ in $\mathbb{F}_2$. The Boolean functions form a $\mathbb{F}_2$-space of dimension 2^m. The system of monomial functions $X_S\colon x \mapsto \prod_{i\in S} x_i$ where S ranges the subsets of $\{1, 2, \ldots, m\}$ is the standard basis of this space. The decomposition of f in the standard basis

$$f = \sum_{S\subset\{1,2,\ldots,m\}} a_S X_S, \quad a_s \in \mathbb{F}_2.$$

if often called the algebraic normal form of f. The set of Boolean functions of degree less or equal to k forms a subspace of dimension $\sum_{i=0}^{k} \binom{m}{i}$. From the coding theory point of view [4], it corresponds to the Reed-Muller code of order k of length 2^m, and we use the notation $\mathrm{RM}(k, m)$. The Reed-Muller code are nested, an element of the quotient space

$$\mathrm{RM}^*(k, m) = \mathrm{RM}(k, m)/\mathrm{RM}(k - 1, m).$$

is called a *Boolean form* of degree k. From the algebraic point of view, the space $\mathrm{RM}^*(k, m)$ is nothing but the r-th alternate product of $\mathbb{F}_2^m$, its dimension over $\mathbb{F}_2$ is $\binom{m}{k}$. A Boolean form ω of degree k has one and only one homogeneous representative.

$$\sum_{|S|=k} a_S X_S \in \omega$$

In this paper, the symbol ω will be interpreted in two ways : as a form or as a function. In the later case, it will be the homogeneous representative of ω. The general linear group acts naturally over the set of Boolean functions in leaving the spaces $\mathrm{RM}(k, m)$ invariant. In particular, it acts on $\mathrm{RM}^*(k, m)$. Given a $\omega \in \mathrm{RM}^*(k, m)$, the action of $A \in \mathrm{GL}(2, m)$ on ω, denoted by ω^A, is the reduction modulo $\mathrm{RM}(k-1, m)$ of the function $\omega \circ A$. Conversely, we say that ω' is equivalent to ω ($\omega' \overset{k}{\sim} \omega$), if there exists $A \in \mathrm{GL}(2, m)$ such that $\omega' = \omega^A$. The determination of a system of represensatives $\mathrm{cl}(k, m)$ is an important step for the study of parameters of $\mathrm{RM}(k, m)$. In this paper, we describe (sections 3, 4, 5) the strategy that we used to compute a *complete classification* of $\mathrm{RM}^*(4, 8)$ under the action of $\mathrm{GL}(2, 8)$

Algorithm C. (Classification). The number of orbits N is assumed to be known.

C1 [initialize] Construct a preclassification (P, π).
C2 [select] choose $x \neq y$ randomly in P such that $\mathfrak{j}(x) = \mathfrak{j}(y)$.
C3 [sample] $l_x \leftarrow \texttt{suborbit}(x, K)$ $l_y \leftarrow \texttt{suborbit}(y, K)$
C5 [test] if $l_x \cap l_y = \emptyset$ go to L2.
C6 [update] $\pi(x) \leftarrow \pi(x) \cup \pi(y)$. Delete entry y in P.
C7 if $\sharp P \neq N$ then go to L2.
C8 return P.

FIGURE 1. The strategy to reduce a preclassification to a classification by means of the invariant $\mathfrak{j}$. The procedure `suborbit`(x,K) selects K elements at random in the reduced part of orb (x).

finalizing the work presented in [11], continuing the works [**?**, 10, 2, **?**, **?**, 9]. The method is discussed in general in section 2, some interesting numerical results are outlined in the last section.

2. Classification: terminology and algorithm

In this section, we consider a finite group G acting over a finite set X. The action of $A \in G$ on $x \in X$ is denoted by x^A. Two elements x and y are said equivalent ($x \sim y$) if there exists $A \in G$ such that $y = x^A$. The class or orbit of x is the set $\operatorname{orb}(x) = \{y \in X \mid y \sim x\}$. The number of orbits is often call the rank of the action of G over X. It is given by the Bursnside's Lemma

$$n(X, G) = \frac{1}{\sharp G} \sum_{A \in G} F(A, X), \quad F(A, X) = \sharp\{x \in X \mid x^A = x\}$$

The subgroup $\operatorname{fix}(x) = \{A \in G \mid x^A = x\}$ is called the fixator of x.

By a *complete classification* of X under G, we understand the determination of the class number $n(X, G)$, a set of representatives, the size of the orbits and a system of generators for all the fixators.

- A *preclassification* consists in pair (P, π) where $P \subset X$ and π maps P into $\mathcal{P}(X)$ such that $\{\pi(p) \mid p \in P\}$ is a partition of X compatible with the action of G that is
$$\forall p \in P, \quad \forall x, y \in \pi(p), \quad x \sim y.$$
- A *invariant* is a mapping $\mathfrak{j}$ from X into a set of values V such that
$$\forall x, y \in X, \quad x \sim y \Longrightarrow \mathfrak{j}(x) = \mathfrak{j}(y).$$
If there exists $x \not\sim y$ such that $\mathfrak{j}(x) = \mathfrak{j}(y) = v \in V$, we say that v is a collision value, of order k when $\mathfrak{j}^{-1}(v)$ is the union of k equivalent classes.
- A K-*sampler* is a mapping red from X into X such that
$$\forall x \in X, \operatorname{red}(x) \in \operatorname{orb}(x), \quad \text{and} \quad \sharp\operatorname{red}(\operatorname{orb}(x)) \leq K^2$$

The algorithm FIG. 1 is based on the birthday paradox to determine the classification of X assuming the number of equivalent classes is known. The success of the method depends on several parameters : the size of the preclassification, the number of collision values and on the capacity of the routine `suborbit` to provide *samples* of size K.

3. The Number of equivalent classes

The action of $A \in \mathrm{GL}(2,m)$ on the monomial X_S is given by

$$\begin{aligned} {X_S}^A(x) &= \prod_{i\in S}(\sum_{j=1}^{m} a_{ij}x_j) \\ &= \sum_{\sharp T=k}\sum_{j:\ S\to T}\prod_{i\in S} a_{ij(i)}X_T \end{aligned}$$

(j one to one)

$$= \sum_T \det A_{S,T}X_T$$

where $A_{S,T}$ is the square matrix of order k obtained by keeping the columns of index $i \in S$ and the lines of index $j \in T$. The matrix of $\omega \mapsto \omega^A$ in the standard basis $\mathrm{RM}^*(k,m)$, denoted by $C^k(A)$, is known as the k-th *compound matrix* of A,

$$C^k(A) = \big(\det(A_{S,T})\big), \quad \sharp S = \sharp T = k.$$

Note that when $k = 1$, we recover the known action on linear forms since $C^1(A)$ equals the transpose of A. By mean of Burnside's Lemma, the rank of the action of $\mathrm{GL}(2,m)$ over $\mathrm{RM}^*(k,m)$ satisfies

$$n(k,m) \times |\mathrm{GL}(2,m)| = \sum_{A\in \mathrm{GL}(2,m)} F(A) \tag{1}$$

where for simplicity we denote by $n(k,m)$ the number $n(\mathrm{RM}^*(k,m),\mathrm{GL}(2,m))$ and $F(A)$ is the number of forms fixed by A. By replacing $F(A)$ this formula can be rewritten as

$$n(k,m) = \sum_{i=1}^{t} \frac{2^{\binom{m}{k}-\mathrm{rank}\,\left(C^k(A_i)-I\right)}}{\gamma(A_i)}, \tag{2}$$

where A_i is a list of representatives of the conjugacy classes of $\mathrm{GL}(2,m)$, I the $\binom{m}{k} \times \binom{m}{k}$-identity matrix and $\gamma(A)$ the order of the centralizer of A in $\mathrm{GL}(2,m)$. The enumeration of all the irreducible polynomials of degree less or equal to m allows the construction of all the possible invariant factors using the notion of *companion matrices*.

In [2], Hou proposed to go farther in the analysis of the formula (2) using elementary factors. It is not really necessary for the present purpose. Indeed, the number of orbits $n(k,m)$ for the small values of k and m indicated by Tab. 1 can be computed in a few seconds.

$k\backslash m$	6	7	8	9	10
3	6	12	32	349	3691561
4	3	12	999	$\sim 10^{15}$	$\sim 10^{34}$

Table 1. Number of $\mathrm{GL}(2,m)$-orbits in $\mathrm{RM}^*(k,m)$.

The *complementary map* is the linear operator from $\mathrm{RM}^*(k,m)$ to $\mathrm{RM}^*(m-k,m)$ such that $X_S \to X_{\bar S}$, where $\bar S$ is the complement of the set S in $\{1,2,\dots,m\}$.

Thanks to the commutativity of the following diagram, see [2],

$$
\begin{tikzcd}
\mathrm{RM}^*(k,m) \arrow[r, "\mathrm{comp}"] \arrow[d, "A"'] & \mathrm{RM}^*(m-k,m) \arrow[d, "A^{-1*}"] \\
\mathrm{RM}^*(k,m) \arrow[r, "\mathrm{comp}"] & \mathrm{RM}^*(m-k,m)
\end{tikzcd}
\tag{3}
$$

we have

$$\omega' \overset{k}{\sim} \omega \Longleftrightarrow \mathrm{comp}\,(\omega') \overset{m-k}{\sim} \mathrm{comp}\,(\omega),$$

whence $n(k,m) = n(m-k,m)$.

4. Sampler

Since the size of an orbit can be equal to the order of $\mathrm{GL}(2,m) \approx 0.272^{m^2}$ we can not use just the identity as sampler. In this section, we construct a sampler that was good enough to obtain the classification of $\mathrm{RM}^*(4,8)$. It is based on the notions of derivation and transvection.

The *derivation* of f at $u \in \mathbb{F}_2^m$ is the Boolean function $\mathrm{Der}_u f(x) = f(x+u)+f(x)$. The derivation operator satisfies the following properties, see [10]:

(1) if $f \neq 0$ then $\deg(\mathrm{Der}_u f) < \deg(f)$
(2) $\mathrm{Der}_u(f+g) = \mathrm{Der}_u f + \mathrm{Der}_u g$
(3) $\mathrm{Der}_u(f \circ A) = (\mathrm{Der}_{uA} f) \circ A$
(4) $\mathrm{Der}_{u+v} f = \mathrm{Der}_u f + \mathrm{Der}_v f + \mathrm{Der}_v \circ \mathrm{Der}_u f$

Note that property (4) means the mapping $(u,\omega) \mapsto \mathrm{Der}_u(\omega)$ on $\mathbb{F}_2^m \times \mathrm{RM}^*(k,m)$ is a bilinear map. In particular,

$$\Delta(\omega) = \{\mathrm{Der}_u(\omega) \mid u \in \mathbb{F}_2^m\}$$

is a linear space having dimension m in general, see next section.

A *transvection* $T \in \mathrm{GL}(2,m)$ is defined by a pair $(\phi, u) \in \mathrm{RM}^*(1,m) \times \mathbb{F}_2^m$ such that $\phi(u) = 0$:

$$T(x) = x + \phi(x)u$$

The action of T over a Boolean function f is

$$
\begin{aligned}
f^T(x) &= f(x+\phi(x)u) = f(x).(1+\phi(x)) + f(x+u).\phi(x) \\
&= \mathrm{Der}_u f(x).\phi(x) + f(x)
\end{aligned}
$$

Let us consider the form $\omega \in \mathrm{RM}^*(k,m)$. Using the tranvection T defined by the pair (X_m, u) where $u = (v,0)$ with $v \in \mathbb{F}_2^{m-1}$, we get :

$$\omega^T(x) = \mathrm{Der}_u \omega(x).X_m + \omega(x)$$

In particular, writing $\omega = \omega_1 + X_m\omega_2$ where ω_1 and ω_2 are respectively forms of degree k and $k-1$ in $m-1$ variables.

$$\omega^T = (\mathrm{Der}_u \omega_1 + \omega_2).X_m + \omega_1$$

We define the reduction of ω as $\mathrm{red}\,(\omega) = \omega_1 + X_m\omega'$ where ω' is a representative of the affine space $\omega_2 + \Delta(\omega_1)$. We will see in the next section that the set $\mathrm{red}\,(\omega)$ is in general 2^m smaller than $\sharp\mathrm{orb}\,(\omega)$.

5. Invariant

Sometimes, it will be necessary to precise the parameters in our notations: $\mathrm{orb}^k_m(\omega)$ the orbit of ω, and $\mathrm{fix}^k_m(\omega)$ the fixator. An *invariant of degree* k in m variables is a mapping $\mathfrak{j}$ such that

$$\omega' \overset{k}{\sim} \omega \Longrightarrow \mathfrak{j}(\omega') = \mathfrak{j}(\omega)$$

As it is pointed by Dillon in his thesis, finding invariants that are efficiently computable is a fundamental question in the theory of Boolean functions or Boolean forms. Note that given an invariant $\mathfrak{j}$ of degree k in m variables, one obtains an invariant of degree $m-k$ using the operator comp defined at the end of the third section.

The most basic invariant is certainly those that map $\omega \in \mathrm{RM}^*(k,m)$ to the minimal number of variables needed to express the degree k part of an element in the class ω. It is denoted by $\mathrm{var}(\omega)$. It is directly connected to the notion of derivation

$$\mathrm{var}(\omega) = \dim_{\mathbb{F}_2} \Delta(\omega). \tag{4}$$

Similarly, there exists an invariant $\mathfrak{T}$ connected to the notion of transvection. Indeed, the set of transvections is invariant by conjugation in $\mathrm{GL}(2,m)$ thus the mapping $\omega \mapsto \mathfrak{T}(\omega) = \sharp\{T \mid \omega^T = \omega\}$ in an invariant. Denoting by $\Psi_u \colon \phi \mapsto (\phi.\mathrm{Der}_u h, \phi(u))$, it is easy to compute since it is equal to

$$\mathfrak{T}(\omega) = \sum_{u \in \mathbb{F}_2^m} \dim_{\mathbb{F}_2} \ker \Psi_u, \tag{5}$$

For all i, $0 \le i \le m-k$, we can construct a *multiplicative invariant* $\mathfrak{R}_{i,k}$ in considering the dimension of the kernel of the multiplication by ω over the forms of degree i. Denoting by $\omega_i^\times \colon f \in \mathrm{RM}(i,m) \mapsto f\omega \in \mathrm{RM}^*(k+i,m)$,

$$\mathfrak{R}_{i,k}(\omega) = \dim_{\mathbb{F}_2} \ker \omega_i^\times \tag{6}$$

There is a *fundamental invariant* of degree 2 arising from the quadratic form theory. Let us recall that the radical of a quadratic form $\omega \in \mathrm{RM}^*(2,m)$ is the subspace $\mathrm{rad}(\omega) = \{y \in \mathbb{F}_2^m \mid \forall x, \quad \omega(x+y)+\omega(x)+\omega(y) = 0\}$. The fundamental invariant $\mathfrak{q}$ is

$$\mathfrak{q}(\omega) = \dim_{\mathbb{F}_2} \mathrm{rad}(\omega).$$

On an other side, when $m = 2t$, it is possible to define a *quadratic invariant* $\mathfrak{Q}$ of degree t that take only two values. However, it will be particulary useful. It maps $\omega = \sum_S a_S X_S \in \mathrm{RM}^*(t,m)$, to

$$\mathfrak{Q}(\omega) = \sum_S^{\star} a_S a_{\bar{S}}, \tag{7}$$

where the sum runs over the subset of cardinality t up to complementary in $\{1,2,\ldots,m\}$.

It is connected to the well known [4] notion of *bent function* in the sense that the existence of a Boolean function $f \in \mathrm{RM}(t-1,m)$ such that $\omega + f$ is bent implies that $\mathfrak{Q}(\omega) = 0$.

Given an invariant $\mathfrak{j}$ of degree $k-1$ in m variables, it is possible to construct an invariant of degree k. Indeed using the property (3) of the derivation in $\mathrm{RM}^*(k,m)$,

TABLE 2. The lift by derivation of $\mathfrak{q}$ discriminates the 12 class of $\mathrm{RM}^*(3,7)$.

orb. size	fix. size	cubic
1	163849992929280	0
11811	13872660480	123
1763776	92897280	137+237+147+247+157+267+467
2314956	70778880	145+123
45354240	3612672	123+456
59527440	2752512	123+245+346
21165312	7741440	123+145+246+356+456
238109760	688128	124+235+346+457+561+267+137
444471552	368640	712+724+134+234+135+745+146
2222357760	73728	127+123+147+245+167
13545799680	12096	127+123+234+345+456+567+617
17777862080	9216	127+234+125+457+245+167+126

the distribution of the values of the mapping $F_\omega\colon u \mapsto \mathfrak{j}(\mathrm{Der}_u\omega)$, is invariant. We denote this distribution by $\mathfrak{j}'(\omega)$. We refer it as the *lift by derivation* of $\mathfrak{j}$.

The distribution of the values of the Fourier coefficients of the F_ω is also invariant. It is denoted by $\widehat{\mathfrak{j}}(\omega)$. In practice, $\widehat{\mathfrak{j}}$ is often more discriminant than $\mathfrak{j}'$, we call it the *Fourier lift* of $\mathfrak{j}$.

In the case that concerns us, the Fourier lift of $\mathfrak{q}'$ (a double lift), say $\mathfrak{L}$, takes 952 values. The combinaison of this invariant with $\mathfrak{Q}$, $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{L}$ takes 966 values. That is the maximal value we actually get using fast computable invariants.

6. Preclassification of $\mathrm{RM}^*(4,8)$

The work factor for the computation of the combination of the invariants presented in the above section is about 2^{20}. Thus, we have to reduce drastically the space of quartics constructing a preclassification. We achieved this in three steps.

6.1. **First step.** Let $\omega \in \mathrm{RM}^*(4,8)$, we decompose

$$\omega = \omega_1 + X_8\omega_2, \quad \omega_1 \in \mathrm{RM}^*(4,7), \quad \omega_2 \in \mathrm{RM}^*(3,7)$$

The group $\mathrm{GL}(2,7)$ acts naturally over $\mathrm{RM}^*(4,8)$,

$$B \in \mathrm{GL}(2,7), \quad \omega \overset{4}{\sim} \omega_1^B + X_8\omega_2^B = \omega^A, \quad A = \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix}.$$

Using the classification TAB. 2, the set of pairs $(\omega_1, \omega_2) \in \mathrm{cl}(4,7) \times \mathrm{RM}^*(3,7)$ provides a preclassification of $\mathrm{RM}^*(4,8)$ of size

$$12 \times 2^{\binom{7}{3}} = 12 \times 2^{35} = 412316860416$$

each pair (ω_1, ω_2) represents $\sharp\mathrm{orb}_7^4(\omega_1)$ elements.

6.2. **Second step.** As we saw in section 4, for any vector $v \in \mathbb{F}_2^{m-1}$:

$$\omega = \omega_1 + X_8\omega_2 \overset{4}{\sim} \omega_1 + X_8\omega_2 + X_8\mathrm{Der}_v\omega_1.$$

The set of pairs $(\omega_1, \omega_2) \in \mathrm{cl}(4,7) \times \mathrm{RM}^*(3,7)/\Delta(\omega_1)$ give a new reduction. Every pair represents $\sharp\mathrm{orb}_7^4(\omega_1) \times 2^{\mathrm{var}(\omega_1)}$, the size of this preclassification is equal to 6442450944.

6.3. **Third step.** The group $\mathrm{fix}_7^4(\omega_1)$ acts over $\mathrm{RM}^*(3,7)/\Delta(\omega_1)$ since the space $\Delta(\omega_1)$ is invariant. Starting from a complete classification of $\mathrm{RM}^*(4,7)$, for all $\omega_1 \in \mathrm{cl}(4,7)$, we determine a set of representatives of $\mathrm{RM}^*(3,7)/\Delta(\omega_1)$ under the action of $\mathrm{fix}_7^4(\omega_1)$.

The set

$$\omega_1 + X_8\omega_2, \quad \omega_1 \in \mathrm{cl}(4,7), \omega_2 \in \mathrm{RM}^*(3,7)/\Delta(\omega_1)/\mathrm{fix}_7^4(\omega_1)$$

provides a preclassification $\mathrm{RM}^*(4,8)$ of size 68647 this is very small. Each pair (ω_1, ω_2) represents

$$\sharp\mathrm{orb}_7^4(\omega_1) \times 2^{\mathrm{var}(\omega_1)} \times \sharp\mathrm{orb}(\omega_2/\mathrm{fix}_7^4(\omega_1))$$

7. Numerical results

Applying all the notions presented in the preceding sections, we get an invariant say $\mathfrak{J}$ representing the combination of the three invariants $\mathfrak{Q}$, $\mathfrak{R}$, and $\mathfrak{L}$. The algorithm of section two achieves the classification of $\mathrm{RM}^*(4,8)$. The details concerning the output of the numerical experiment are available on the projects web site of the first author [10].

- *Collisions.* There are exactly 30 collisions, 27 collisions of order 2, and 3 collisions of order 3. The number of classes is effectively

$$966 + 27 + 6 = 999$$

- *Equivalence.* To test the equivalence between ω and ω', we compute $\mathfrak{J}(\omega)$ and $\mathfrak{J}(\omega')$ and if the values are distinct then clearly the forms are not equivalent. If not, we use backtracking to construct (or to prove the nonexistence of) $A \in \mathrm{GL}(2,m)$ such that $F_{\omega'} = F_\omega \circ A$.
- *Classification up to complementary.*

  Using the previous point, it is possible to determine equivalence up to complementary, we obtain the following repartition.

	self comp.	not self comp.
$\mathfrak{Q}=1$	294	168
$\mathfrak{Q}=0$	300	236

  In particular, there are 418 class of homogeneous forms h, up to complementary, with $\mathfrak{Q}(h) = 0$ that can provide bent functions.
- *Fixator.*

  The determination of the fixators is strongly ease by the knowledge of the size of the orbits using the Schreier basis method. We have to generate random element in $\mathrm{fix}(\omega)$ up to we find a group of expected order.
- *Covering radius of RM-code.*

  The covering radius of Reed-Muller codes are not known in general. The handbook of coding theory [1] says the covering radius of $\mathrm{RM}(3,8)$ satisfies $44 \le \rho(3,8) \le 67$. Let $\omega \in \mathrm{RM}^*(k,m)$, and let $g \in \mathrm{RM}(k-1,m)$:

$$\mathrm{wt}(\omega+g) = 2^{m-1} - \frac{1}{2}S(\omega+g), \quad \text{where} \quad S(f) = \sum_{x\in\mathbb{F}_2^m} (-1)^f(x).$$

  Adapting a recent trick of Claude Carlet [**?**],

$$S(\omega+g)^2 = 2^{2m} - 2\sum_{u\in\mathbb{F}_2^m} \mathrm{wt}\,(\mathrm{Der}_u\omega + \mathrm{Der}_u g)$$
$$\leq 2^{2m} - 2\sum_{u\in\mathbb{F}_2^m} D(u)$$

where $D(u)$ is the distance of $\mathrm{Der}_u\omega$ to the code $\mathrm{Der}_u\mathrm{RM}(3,8)$. Using this result one can verify that the distance (non-linearity of order 3) from

Q=2345+1246+1356+2467+3467+2567+1348+1258+1358+2478+3578+1678

to the set $\mathrm{RM}(3,8)$ satisfies

$$44 < 50 \leq \mathrm{nl}_{3,8}(Q)$$

improving seriously the above estimation. Moreover, we solicited Ilya Dumer to run his decoding algorithm for us in order to decode Q. The computation shows that $\mathrm{nl}_{3,8}(Q) \leq 52$.

- *Number of bent functions.*

  Let $\omega \in \mathrm{RM}^*(4,8)$ and let $\mathrm{nbf}\,(\omega)$ be the number of bent functions of the form $\omega + g$ where $g \in \mathrm{RM}(3,8)/\mathrm{RM}(1,8)$. For a given ω, it is possible to compute $\mathrm{nbf}\,(\omega)$ in less than 18 days on a single computer. It appears that the total number of bent functions satisfies

$$\sum_{\omega\in \mathrm{cl}(4,8)} \mathrm{nbf}\,(\omega) \times \sharp\mathrm{orb}\,(\omega) \approx 2^{97.3}.$$

The method used to obtain this last numerical result is based on the knowledge of the fixator groups (complete classification). It will the subject of a forthcoming paper.

References

[1] E.R. Berlekamp, L. R. Welch, *Distributions of the cosets of the* $(32,6)$ *Reed-Muller code* IEEE Trans. IT-13, 1, pp 203–207 (1972).

[2] R. Brualdi, S. Litsyn, V. Pless *Covering Radius* Handbook of coding theory, chap. 8, North Holland, 1998.

[3] C. Carlet *Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications* Cryptology ePrint Archive, Report 2006/459 (2006) `http://eprint.iacr.org/`,

[4] X.-D. Hou. *Gl(m,2) acting on R(r,m)/R(r-1,m)*, Discrete Mathematics, vol. 149, pp 99-122, 1996.

[5] F. J. MacWilliams, N. J. A. Sloane. *The Theory of Error Correcting Codes*, North Holland Mathematical Library, 1977.

[6] J. A. Maiorana. *A classification of the cosets of the Reed-Muller code* $R(1,6)$, Mathematics of Computation, vol. 57, 195, pp 403–414 (1991).

[7] T. Sugita, T. Kasami, T. Fujiwara. *Weight distributions of the third and fifth order Reed-Muller codes of length 512*, Nara Inst. Sci. Tech. Report, Feb. 1996.

[8] E. Brier, P. Langevin. *Classification of the cubic forms of nine variables*, IEEE Information Theory Workshop La Sorbonne, Paris, France (2003)

[9] P. Langevin. *Classification of the quartic forms of eight variables*, Output of the numerical experiment `www.univ-tln.fr/langevin/projects/quartics.html`

[10] P. Langevin, P. Rabizzoni, P. Véron and J.-P.Zanotti *On the number of bent functions with 8 variables* , BFCA'06, pp 125–135 (2006)

[11] O. S. Rothaus. *On Bent Functions*, Journal of Combinatorial Theory (A) 20, pp 300–305, (1976).