Classification of Boolean cubic forms of nine variables

Eric Brier
Gemplus Card International,
Card Security Group,
Parc d'Activités de Gémenos,
B.P. 100, 13881 Gémenos,
France, eric.brier@gemplus.com

Philippe Langevin
Université de Toulon et du Var,
Groupe de Recherche en Informatique
et Mathématiques,
BP 132, 83957 La Garde Cedex,
France. langevin@univ-tln.fr

Abstract — **We describe a new invariant that we have used to obtain the complete classification of the cubic forms of nine variables. In particular, we compute the covering radius of** $\mathrm{RM}(2,9)$ **into** $\mathrm{RM}(3,9)$**.**

I. Reed-Muller codes

Let m be a positive integer. A Boolean function is a mapping from $\mathbf{F}_2^m$ into $\mathbf{F}_2$. The *weight* of a Boolean function f, denoted by $\mathrm{wt}(f)$, is equal to the cardinality of its support,

$$\mathrm{wt}(f) = \sharp\{x \in \mathbf{F}_2^m \mid f(x) = 1\}.$$

The set of Boolean functions equipped of the distance $(f,g) \mapsto \mathrm{wt}(f+g)$ is an Hamming space. The $\mathbf{F}_2$-algebra of Boolean functions is isomorphic to the quotient ring $\mathbf{F}_2[X_1, X_2, \ldots, X_m]/I$ where I is the ideal generated by the polynomials $X_i^2 - X_i$, $i \in \{1, 2, \ldots, m\}$. In particular, for all Booolean function f, there exists one and only one polynomial π of partial degree less or equal than one in each variable (reduced polynomial) such that $\forall x \in \mathbf{F}_2^m$, $f(x) = \pi(x)$. By definition, the degree of π is the degree of f, denoted by $\deg(f)$, with the usual convention of $\deg(0) = -1$. In others words, f has a *polynomial representation*

$$f(x) = \sum_{S \subseteq \{1,2,\ldots,m\}} a_S X_S$$

with $a_S \in \mathbf{F}_2$ and where X_S is the monomial $\prod_{s\in S} X_s$. If $|S| \neq r$ implies $a_S = 0$ then f is a *polynomial form* of degree r. The *complementary map* transforms f in

$$f^{\mathrm{c}}(x) = \sum_{S \subseteq \{1,2,\ldots,m\}} a_S X_{\{1,2,\ldots,m\}\setminus S}.$$

In particular, if f is a form of degree r then f^{c} is the form of degree $m - r$. For any integer r, $0 \le r \le m$, the space of functions of degree r is called the *Reed-Muller code of order r of m variables*. The Reed-Muller codes are nested,

$$\mathrm{RM}(1,m) \subset \mathrm{RM}(2,m) \subset \cdots \subset \mathrm{RM}(m-2,m)$$

and they satisfy $\mathrm{RM}(r,m)^{\perp} = \mathrm{RM}(m-1-r,m)$ for duality by the usual dot product. The code $\mathrm{RM}(r,m)$ is a linear code of length 2^m, of dimension $\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$ and minimal distance 2^{m-r}. There exists formulas for the weight distribution of $\mathrm{RM}(r,m)$ for $r \in \{0,1,2\}$. Using the relation of duality, one can apply MacWilliams transformation of the weight enumerators to get the weight distribution of the Reed-Muller codes of order $m-1$, $m-2$ and $m-3$. The weight enumerator of the third order Reed-Muller codes and the covering radius of the second order Reed-Muller codes are not known in general. The main consequences of our numerical results are the determination of $\mathrm{RM}(3,10)$ (forthcoming paper), the determination of the covering radius of $\mathrm{RM}(3,9)$ into $\mathrm{RM}(2,9)$ and an improvement of the bounds concerning the covering radius of $\mathrm{RM}(2,9)$.

II. Action of the general linear group

The general linear group $\mathrm{GL}(m,\mathbf{F}_2)$ acts over the Reed-Muller codes whence over the quotient space $\mathrm{RM}^*(r,m) := \mathrm{RM}(r,m)/\mathrm{RM}(r-1,m)$ i.e. the space of forms of degree r. In [2], Hou uses Burnside's lemma to obtain the following formula on the number $n(r,m)$ of orbits of $\mathrm{RM}^*(r,m)$ under the action of $\mathrm{GL}(m,\mathbf{F}_2)$:

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

where A_i is a list of representatives of the conjugacy classes of $\mathrm{GL}(m,\mathbf{F}_2)$, $C_r(A)$ the rth compound matrix of A , I the $\binom{m}{r}\times\binom{m}{r}$-identity matrix and $\gamma(A)$ the order of the centralizer of A in $\mathrm{GL}(m,\mathbf{F}_2)$.

Table 1: Number of $\mathrm{GL}(m,\mathbf{F}_2)$-orbits in $\mathrm{RM}^*(r,m)$.

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

TABLE 1 reports the values of $n(r,m)$ for small r and m. In his article, Hou determines a list of 32 non equivalent cubics of 8 variables, this was used by Sugita, Kasami and Fujiwara [9] to compute simultaneously a complete classification of the Boolean cubic forms of 8 variables and the weight distribution of $\mathrm{RM}(3,9)$.

An *invariant of degree r of m variables*, in short (r,m)-invariant, is a map $\mathfrak{j}$ from $\mathrm{RM}^*(r,m)$ into a set X such that

$$\forall \omega_1, \omega_2 \in \mathrm{RM}^*(r,m), \quad \omega_1 \sim \omega_2 \Longrightarrow \mathfrak{j}(\omega_1) = \mathfrak{j}(\omega_2)$$

Of course, the map $\mathfrak{c}$ (resp. $\mathfrak{o}$) that sends $\omega \in \mathrm{RM}^*(r,m)$ to the orbit (resp. size of the orbit) of ω under the action of $\mathrm{GL}(m,\mathbf{F}_2)$ is an invariant. The object of a classification is construct $\mathfrak{c}$ effectively. The main goal of the present paper is to provide a complete classification of 349 Boolean cubics forms of 9 variables i.e. to construct $\mathfrak{c}$ and $\mathfrak{o}$ on $\mathrm{RM}^*(3,9)$.

In general, one invariant is not sufficient to determine all the classes. We say that $\mathfrak{j}$ is *discriminant* for $\mathrm{RM}^*(r,m)$ if it takes $n(r,m)$ distinct values, in that case

$$\forall \omega_1, \omega_2 \in \mathrm{RM}^*(r,m), \quad \omega_1 \sim \omega_2 \Longleftrightarrow \mathfrak{j}(\omega_1) = \mathfrak{j}(\omega_2)$$

Invariants can be combined in several ways to obtain new invariants. Numerical invariants can be combined by sum, product, etc... The direct product of two invariants is an invariant. If V is the image of an invariant $\mathfrak{j}$, the *development* of $\mathfrak{j}$ is the invariant of codomain $\{0,1\}^V$ defined by

$$\mathrm{dev}(\mathfrak{j})(\omega) = (b_v)_{v \in V}$$

where $b_v = 1$ if and only if $\mathfrak{j}(\omega) = v$.

Remark 1 (Hou, [2]) *If ω_1 and ω_2 are forms of the same degree then we have the equivalence $\omega_1 \sim \omega_2 \Longleftrightarrow \omega_1^{\mathrm{c}} \sim \omega_2^{\mathrm{c}}$. In particular, if $\mathfrak{j}$ is an invariant of degree r then $\omega \mapsto \mathfrak{j}(\omega^{\mathrm{c}})$ is an invariant of degree $m-r$, denoted by $\mathfrak{j}^{\mathrm{c}}$.*

It is well known that there are $n(2,m) = \lfloor \frac{m}{2} \rfloor + 1$ classes of quadratic forms. More precisely, the invariant of degree 2, say $\mathfrak{q}$, mapping a quadratic form to the rank of its bilinear symmetric form is discriminant, it splits completely the space $\mathrm{RM}^*(2,m)$.

Remark 2 (Hou, [3]) *We can generalize the invariant $\mathfrak{q}$ to the functions of degree r in an invariant $\mathfrak{i}_{i,j}$ defined as follows. Let i, j, r positive integers such that $r = i + j$. Let $\sum_S a_S X_S$ the polynomial expression of a form ω of degree r. Let $M(\omega)$ be the $\binom{m}{i} \times \binom{m}{j}$ matrix whose the rows are indexed by the i-subsets of $\{1,2,\ldots,m\}$ and the columns by the j-subsets with the coefficients $m_{I,J} := a_{I \cup J}$. The mapping $\omega \mapsto \mathrm{rank}\big(M(\omega)\big)$ is an invariant of degree r. It generalizes the invariant $\mathfrak{q}$ in the sense that $\mathfrak{q} = \mathfrak{i}_{1,1}$.*

In order to classify $\mathrm{RM}^*(r,m)$ for the algorithmic point of view, we have to provide an effective construction of a invariant that splits a list of $n(r,m)$ Boolean forms of degree r. Here we will give a classification of $\mathrm{RM}^*(3,9)$ that depends on two important notions : derivation and restriction.

For a first approach of these notions, let us consider a Boolean function $F \in \mathrm{RM}(r,m)$. The polynomial representation of F decomposes as $F = f + gX_m$ with $f \in \mathrm{RM}(r,m-1)$ and $g \in \mathrm{RM}(r-1,m-1)$. The derivation of F in the direction of $(0,0,\ldots,1)$ is g i.e. the usual partial derivative $\frac{\partial F}{\partial X_m}$. The restriction of F at the hyperplane $X_m = 0$ corresponds to f. By this example, we guess a certain duality between restriction and derivation.

III. Derivation

The *derivation* of a Boolean function f in the direction of a vector $u \in \mathbf{F}_2^m$ is the Boolean function defined by $\mathrm{Der}_u(f)\colon x \mapsto f(x+u) + f(x)$. We denote by $\mathrm{Der}_{u,v}$ the composition $\mathrm{Der}_v \circ \mathrm{Der}_u$, note that is equal to $\mathrm{Der}_u \circ \mathrm{Der}_v$. The derivation of Boolean functions satisfy the following properties

D_0 if $f \neq 0$ then $\deg(\mathrm{Der}_u f) < \deg(f)$

D_1 $\mathrm{Der}_u(f+g) = \mathrm{Der}_u f + \mathrm{Der}_u g$

D_2 $\mathrm{Der}_u(f \circ A) = (\mathrm{Der}_{Au} f) \circ A$

D_3 $\mathrm{Der}_{u+v} f = \mathrm{Der}_u f + \mathrm{Der}_v f + \mathrm{Der}_{u,v} f$

Property (D_0) shows that the derivation is well defined over the space of forms. If ω is a form of degree r, the derivation of ω in the direction of u is defined by

$$\mathrm{Der}_u \omega := \mathrm{Der}_u f \pmod{\mathrm{RM}(r-2,m)}.$$

where f is any representative of ω. Properties (D_1) and (D_3) show that the derivation is bilinear over $\mathbf{F}_2^m \times \mathrm{RM}^*(r,m)$.

Proposition 1 *Let ω be a form of $\mathrm{RM}^*(r,m)$. The set $\Delta(\omega) := \{\mathrm{Der}_u \omega \mid u \in \mathbf{F}_2^m\}$ is a vector space. The map $\mathfrak{d}\colon \omega \mapsto \dim \Delta(\omega)$ is an invariant, $\mathfrak{d}(\omega)$ is the minimal number of variables that appear in the polynomial expression of a form equivalent to ω. Clearly, $\mathfrak{d} = \mathfrak{i}_{1,r-1}$.*

proof: It is a consequence of (D_3), see [3] for the last part. □

We want use property (D_2) to lift any invariant of degree $r-1$ to an invariant of degree r. For each $\omega \in \mathrm{RM}^*(r,m)$, we introduce the mapping

$$\begin{aligned} \delta_\omega \colon \mathbf{F}_2^m &\to \mathrm{RM}^*(r-1,m) \\ u &\mapsto \mathrm{Der}_u \omega \end{aligned}$$

Proposition 2 *Let $\mathfrak{j}$ be an invariant of degree $r-1$ of m variables. The distribution of the values of $\mathfrak{j} \circ \delta_\omega$ is an invariant of degree r of m variables.*

proof: Let $A \in \mathrm{GL}(m,\mathbf{F}_2)$ and let $\mathfrak{j}$ be a (r,m)-invariant. For all $\omega \in \mathrm{RM}^*(r,m)$, using property (D_2), we get

$$\mathfrak{j}(\mathrm{Der}_u(\omega \circ A)) = \mathfrak{j}((\mathrm{Der}_{Au}\omega) \circ A) = \mathfrak{j}(\mathrm{Der}_{Au}\omega)$$

whence the distribution of $\mathfrak{j}(\mathrm{Der}_u \omega)$ and $\mathfrak{j}(\mathrm{Der}_u \omega \circ A)$ are the same. □

This new invariant, denoted $\mathfrak{j}_d$, is *the lift of $\mathfrak{j}$ by derivation*. One can check by computer that the lift by derivation of $\mathfrak{q}$ discriminates the space $\mathrm{RM}(3,7)$ but it splits $\mathrm{RM}(3,8)$ in 29 classes, only. A slight modification of it by means of Fourier tool will be more powerful. The Fourier (or Walsh) transform of a vectorial complex function $F\colon \mathbf{F}_2^m \to \mathbf{C}^s$ is defined by

$$\hat{F}(v) = \sum_{x \in \mathbf{F}_2^m} (-1)^{xv} F(x)$$

Let $A \in \mathrm{GL}(m,\mathbf{F}_2)$, one can check that the Fourier transform of $F \circ A^{-1}$ is nothing but the composition $\hat{F} \circ A^*$ where A^* is the adjoint operator of A.

Proposition 3 *Let $\mathfrak{j}$ be an $(r-1,m)$-invariant. The distribution of the values of the Fourier transform of the mapping $u \mapsto \mathfrak{j} \circ \delta_\omega(u)$ is an invariant of degree r of m variables.*

proof: Clear. □

This new invariant, denoted $\widehat{\mathfrak{j}_d}$, is called the *Fourier lift of* $\mathfrak{j}$ *by derivation*. The Fourier lift of $\mathfrak{q}$ by derivation is discriminant over $\mathrm{RM}(3,8)$ but does not split completely $\mathrm{RM}(3,9)$. The direct product of the three invariants : $\hat{\mathfrak{q}}_d$, $\mathfrak{d}$ and $\mathfrak{i}^{\mathfrak{c}}_{3,3}$ splits the space $\mathrm{RM}(3,9)$ in 345 classes.

IV. The restriction

Let f be a Boolean function. Let H be linear hyperplane of $\mathbf{F}_2^m$, and let $\varphi\colon \mathbf{F}_2^{m-1} \to H$ a parametrization of H i.e. an isomorphism. The composition $f \circ \varphi$, denoted $\mathrm{Res}_\varphi f$ is *restriction* of f at the hyperplane H by mean of the parametrization φ. The main fact is that the class of $\mathrm{Res}_\varphi f$ does not depend on the parametrization φ but only of H whence we can define the symbol $\mathrm{Res}_H f$ up to to $\mathrm{GL}(m-1,\mathbf{F}_2)$ equivalence. Since the degree of $f\circ\varphi$ does not increase, the restriction is well define over the space of forms. As for derivation, we introduce a mapping

$$\begin{aligned}\rho_\omega\colon \mathbf{F}_2^m &\to \mathrm{RM}^*(r,m-1)\\ u &\mapsto \mathrm{Res}_{u^\perp}\omega\end{aligned}$$

the value of $\rho_\omega(0)$ is set to be zero. The symbol $\rho_\omega(u)$ is define up $\mathrm{GL}(m-1,\mathbf{F}_2)$ equivalence. Of course, for any $(r,m-1)$-invariant $\mathfrak{j}$ the value of $\mathfrak{j}\circ\rho_\omega(u)$ is well defined.

Proposition 4 *Let* $\mathfrak{j}$ *be an invariant of degree* r *of* $m-1$ *variables. The distribution of the values* $\mathfrak{j}\circ\rho_\omega$ *is a* (r,m)*-invariant.*

proof: Let $A \in \mathrm{GL}(m,\mathbf{F}_2)$ and $0 \neq u \in \mathbf{F}_2^m$. We have the equalities :

$$\mathrm{Res}_{u^\perp}(\omega\circ A^{-1}) = \mathrm{Res}_{A^{-1}(u^\perp)}(\omega) = \mathrm{Res}_{(A^*u)^\perp}(\omega)$$

□

This new invariant, say $\mathfrak{j}_r$, is called the *lift of* $\mathfrak{j}$ *by restriction*. The sketch of the above proof, shows we can also define a Fourier version of it.

Proposition 5 *Let* $\mathfrak{j}$ *be a* $(r,m-1)$*-invariant. The distribution of the Fourier transform of* $u \mapsto \mathfrak{j}(\mathrm{Res}_{u^\perp}\omega)$ *is a invariant of degree* r *of* m *variables.*

proof: It is clear. □

In section (III) we have obtained a discriminant invariant, say $\mathfrak{k}$, to classify $\mathrm{RM}^*(3,8)$. On the other hand, we have an invariant $\mathfrak{q}$ that discriminates the quadratic form of 9 variables. Unfortunately, the direct product of Fourier lifts : $\widehat{\mathrm{dev}(\mathfrak{k})} \times \widehat{\mathrm{dev}(\mathfrak{q})}$ does not splits the space of cubic forms of 9 variables in 349 classes.

Let $\mathfrak{a}$ be an $(r,m-1)$-invariant, and let $\mathfrak{b}$ be an $(r-1,m)$-invariant. The relation of duality between the restriction and derivation shows the invariance of the distributions of the mapping :

$$\begin{aligned}u &\mapsto (\mathfrak{a}\circ\rho_\omega(u), \widehat{\mathfrak{b}\circ\delta_\omega}(u))\\ u &\mapsto (\widehat{\mathfrak{a}\circ\rho_\omega}(u), \mathfrak{b}\circ\delta_\omega(u))\end{aligned}$$

That leads to the construction of two (r,m)-invariants and the main fact is that the direct product of these new invariants, where $\mathfrak{a}$ is the development of $\mathfrak{k}$ and $\mathfrak{b}$ those of $\mathfrak{q}$, discriminates $\mathrm{RM}^*(3,9)$.

V. Classification

Let ω be a cubic form of 9 variables. Let $\mathcal{R}$ be a set of 32 representatives of the orbits of $\mathrm{RM}(3,8)$ under the action of $\mathrm{GL}(8,\mathbf{F}_2)$. There is one and only one $f\in\mathcal{R}$ such that

$$\omega \sim f + gX_9$$

with $g \in \mathrm{RM}^*(2,8)$.

Proposition 6 *Let* $\omega = f + gX_m$ *be a form of degree* r *in* m *variables,* $f \in \mathrm{RM}^*(r,m-1)$ *and* $g\in\mathrm{RM}^*(r-1,m-1)$. *For all* $u \in \mathbf{F}_2^{m-1}$*, we have the equivalence of forms*

$$f + gX_m \sim f + gX_m + X_m\mathrm{Der}_u f$$

proof: We identify an element $x\in\mathbf{F}_2^m$ with an ordered pair $(y,z)\in\mathbf{F}_2^{m-1}\times\mathbf{F}_2$. Let $v=(u,0)$ and let us consider the action of the linear transvection $\theta(x) = x + X_m(x)v$ over ω.

$$\begin{aligned}[f+gX_m]\circ\theta(x) &= f(y+zu) + g(y+zu)z\\ &= f(y+u)z + f(y)\bar{z} + g(y+u)z\\ (\bar{z} = z+1) &\\ &= z\mathrm{Der}_u f(y) + f(y) + g(y+u)z\\ &= [f + (g + \mathrm{Der}_u g + \mathrm{Der}_u f)X_m](x)\end{aligned}$$

and the result follows since $\deg(\mathrm{Der}_u g) < r-1$. □

The above proposition shows that we can find all the classes of cubic forms of 9 variables enumerating the homogeneous Boolean functions of the form :

$$f + gX_m, \quad f\in\mathcal{R}, \quad g\in\mathrm{RM}^*(2,9)/\Delta(f).$$

Using the invariants described at the end of the section (IV), we have an algorithm of work factor

$$52\times 2^{20}\times 2^9\times 2^8\times 2^6 < 2^{49}$$

to obtain the complete classification of the cubic forms of 9 variables.

VI. Covering radius

The covering radius of the Reed-Muller code of order two are unknown in general. The table below, see [1], indicates the values of the covering radii of the small Reed-Muller codes.

Table 2: Covering radii of Reed-Muller codes

$r\backslash m$	2	3	4	5	6	7	8	9
1	1	2	6	12	28	56	120	240-244
2	0	1	2	6	18	40–44	81–100	171–220
3		0	1	2	8	20–23	43–67	111–167
4			0	1	2	8	22–31	58-98

The classification of the cubic forms allows us to improve the entries corresponding to covering radii of the codes $\mathrm{RM}(2,8)$ and $\mathrm{RM}(2,9)$. By example, see [2], the "less quadratic function" among the cubic forms of 8 variables is at distance 88 of $\mathrm{RM}(2,8)$. One of such a cubic form is

$$X_{1,2,3}+X_{1,4,7}+X_{1,6,8}+X_{1,7,8} + X_{2,4,8}+X_{2,5,7}+X_{3,5,8}+X_{4,5,6}$$

Let us denote by $W^F_{r-1,m}(X,Y)$ the weight enumerator of the translate $F+\mathrm{RM}(r-1,m)$. If F is a form of degree r, then $F = f + gX_m$ where $f \in \mathrm{RM}^*(r,m-1)$ and $g \in \mathrm{RM}^*(r-1,m-1)$. From the $(u \mid u+v)$ structure of the Reed-Muller codes,

$$W^{f+gX_m}_{r-1,m}(X,Y) = \sum_{\kappa} W^{f+g+\kappa}_{r-2,m-1}(X,Y) W^{f+\kappa}_{r-2,m-1}(X,Y)$$

where κ ranges the space $\mathrm{RM}^*(r-1,m-1)$.

Proposition 7 *Let $F = f + gX_m$ be a Boolean function of degree r. For all $u \in \mathbf{F}_2^m$, the weight enumerators of $F + \mathrm{RM}(r-1,m)$ and $F + \mathrm{Der}_u f X_m + \mathrm{RM}(r-1,m)$ are equal.*

proof: It is a second important consequence of Proposition 6. □

Hence,

$$W^{f+gX_m}_{r-1,m}(X,Y) = 2^{\mathfrak{d}(f)} \times \sum_{\kappa} W^{f+g+\kappa}_{r-2,m-1}(X,Y) W^{f+\kappa}_{r-2,m-1}(X,Y)$$

where κ ranges in the quotient space $\mathrm{RM}^*(r-1,m-1)/\Delta(f)$.

In the case where $r=3$, we can use Fourier algorithm to compute the translates of $\mathrm{RM}(1,m)$, and the divisibility by 4 of the weight of cubics, to compute the weight distribution of the translate $F + \mathrm{RM}(2,9)$ by work factor $2^{40-\Delta(f)}$, in particular it is not hard to compute the distance of a cubic form of rank 9. After a 2 days of running times, we have obtained the weight enumerators of the translates of the 348 nonzero classes of cubic forms. It appears that the covering radius of $\mathrm{RM}(2,9)$ into $\mathrm{RM}(3,9)$ is 196 whence the covering radius of $\mathrm{RM}(2,8)$ is greater or equal to 196 improving the known result presented by TABLE 2. More precisely, there are four type of cosets of weight 196 and the reader can recover the complete weight distribution using TABLE 3. Note that the multiplicities are given up to the factor 256, and recall that the enumerator of a translate of $\mathrm{RM}(2,9)$ is symmetric since the all 1's vector lies in $\mathrm{RM}(2,9)$.

$$X_{1,2,3}+X_{4,5,6}+X_{1,4,7}+X_{2,5,7} +X_{3,4,8}+X_{2,6,8}+X_{2,7,8}+X_{3,5,9} + X_{1,6,9}+X_{5,6,9}+X_{7,8,9}$$

The weight of the polynomial representation, the size of the orbit and the factorization of the order of the group of symmetry corresponding to the four cubic forms are

weight	size	symmetry
24	130136218384151347200	$2^8 \cdot 3 \cdot 7$
22	86757478922767564800	$2^7 \cdot 3^2 \cdot 7$
44	1032827130032947200	$2^9 \cdot 3^3 \cdot 7^2$
11	14148316849766400	$2^9 \cdot 3^3 \cdot 7^2 \cdot 73$

In particular, the probability to find one these cubics by a random search is $\sim 2.10^{-4}$.

Table 3: Weight distribution of the 4 maximal cosets of $\mathrm{RM}(3,9)$ into $\mathrm{RM}(2,9)$ up to the factor 256

wt				×256
196	49664	24576	3584	112128
204	1844736	1771520	1645056	1831424
212	39549440	39782400	40330752	40029696
220	487456256	488599552	488624640	481815040
228	3623950848	3620843520	3620345344	3637992960
236	16266890752	16265410560	16259830272	16257550848
244	44206772736	44217169920	44231667200	44198278656
252	72812439040	72805351424	72796506624	72821342720

The reader will find the complete classification size of orbits, representatives and weight distribution of translates on the web page [10].

VII. *

References

[1] Richard Brualdi, Simon Litsyn & Vera Pless *Covering Radius* Handbook of coding theory, chap. 8, North Holland, 1998.

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

[3] Xiang-dong Hou. *Cubic bent functions*, Discrete Mathematics, vol. 189, pp 149-161, 1998.

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

[5] T. Kasami, N. Tokura & S. Azumi. *On the Weight Enumeration of Weight Less than 2.5d of Reed-Muller Codes*, Information and Control, vol. 30, no. 4, pp 380-395, Apr. 1976.

[6] M. Sugino, Y. Ienaga, N. Tokura & T. Kasami. *Weight Distribution of (128,64) Reed-Muller Code*, IEEE Trans. Inform. Theory, vol. IT-17, no. 5, pp 627-628, Sept. 1971.

[7] T. Kasami, T. Fujiwara & Y. Desaki. *The Weight Distribution of cosets of the second-order Reed-Muller Code of length 128 in third-order Reed-Muller code of length 128*, IEICE Technical Report, IT95-27, July 1995.

[8] T. Kasami, T. Fujiwara, Y. Desaki & R. Morelos-Zaragoza *New method for computing the weight distribution of a linear block code based on its treillis structure*, Proc. Int. Symp. on Information Theory Applications, pp 25-28, Nov. 1994.

[9] 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.

[10] E. Brier & P. Langevin. *Classification of the cubic forms of nine variables*, (numerical results) www.univ-tln.fr/langevin/cubics/index.html