Projected Subcodes of the Second Order Binary Reed-Muller Code

Matthieu Legeay
Université de Rennes 1
IRMAR
Rennes, France
Email: matthieu.legeay@univ-rennes1.fr

Pierre Loidreau
DGA MI and Université de Rennes 1
IRMAR
Rennes, France
Email: pierre.loidreau@univ-rennes1.fr

***Abstract*—In this paper we construct new subcodes of the second-order binary Reed-Muller code by using the permutation group and by projecting the code onto codes with smaller parameters. The permutation group of Reed-Muller codes is the general affine group and can be decomposed into the semi-direct product of the translation group and the general linear group. The action of the translation group projects the second order Reed-Muller code onto copies of the first order Reed-Muller code. The general linear group projects the code onto codes for which we can control the useful length and the dimension. These parameters depend on the dimension of the eigenspace of the chosen element of the general linear group for the eigenvalue 1.**

I. Introduction

Binary Reed-Muller codes are an ancient family of codes. Since their invention in 1954, many articles were dedicated to the study of their properties. They have especially efficient decoding algorithms. The most efficient in complexity (linear or quasi-linear) are the so-called recursive, or GMC (Generalized Multiple Concatenation) decoding algorithms,[1], [2], [3]. Although extremely fast, no algorithm of this type and none of their variants reaches the lower bound on the minimum distance decoding capability given for the BSC channel in [4] Corollary 2.

There exists another class of algorithms using algebraic properties of Reed-Muller codes, attempting to improve their decoding capacity, [4]. Although for second order Reed-Muller code, the best variants of the original algorithm practically correct more errors than the recursive decoding algorithms, the complexity of the decoder is quadratic in the code length rather than quasi-linear [7], [8]. The very interesting idea in the original paper is the algebraic approach that the authors use: they explicitly use a subgroup of the permutation group of Reed-Muller codes and project the r-order Reed-Muller code onto many copies of the $r-1$-order Reed-Muller code. They chain this projection until first order Reed-Muller code is reached. Then they decode in the many copies of the first order Reed-Muller code with a minimum distance decoder. To do this projection, they define an action of the group of translations on Reed-Muller codes and use it to construct the projection. Although this algebraic approach is seducing the number of different copies of the code that they obtain by projection is not sufficient enough to improve on the asymptotic performances of recursive decoding.

In this paper, we aim at studying the projection of second order Reed-Muller codes by using elements of the permuations group of the code. It not only contains the group of translations, but also the general linear group. We show that it is possible to project the second order Reed-Muller code onto many codes with smaller parameters - typically of the order of the parameters of the first order Reed-Muller code. This many codes could then be used in the design of algebraic decoding algorithms with better performances. The reason why we chose to focus on the second order Reed-Muller code is that it is the simplest non-trivial code of the Reed-Muller codes family, that its structure is perfectly known, and also that it is an optimal code in the sense of minimum distance decoding, [6].

In section II, we introduce binary Reed-Muller codes as evaluation codes of boolean functions of a fixed degree. We also recall some well known properties, in particular that their permutation group is exactly the general affine group, which is the semi-direct product of the group of translations and the general linear group. In section III, we describe the properties of the codes obtained by the projection of the second order Reed-Muller code using elements of the permutation group. In the case of a translation, we always obtain a first order Reed-Muller code. In the case where the permutation is an invertible linear permutation, the code that we obtain depends on the dimension of the eigenspace associated to the eigenvalue 1. We then derive bounds on the so-called projected subcodes. In Section IV we illustrate our approach with different examples.

II. Preliminaries

Binary Reed-Muller codes are among the oldest and best understood codes. They are relatively easy to decode but, except for the first order Reed-Muller code, they are not very good codes in terms of the number of errors that it is possible to practically correct over a BSC channel. In this section, we introduce the codes as evaluation codes of boolean functions.

A. Binary Reed-Muller Codes

There are many ways to introduce binary Reed-Muller codes. One of them consists in using properties of boolean functions.

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

Definition 1: A Boolean function f in m variables $x_1, \ldots, x_m$ is a function f:

$$\begin{array}{rcl} \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2 \\ x_1, \ldots, x_m & \mapsto & f(x_1, \ldots, x_m) \end{array}$$

Definition 2: Let $0 \leq r \leq m$, $n = 2^m$ and let $(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^m$ be some ordering of the vector space $(\mathbb{F}_2^m)^n$. The r-th order binary Reed-Muller code $\mathcal{R}(r, m)$ is the set of all binary strings

$$(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_2^n,$$

where $f(x_1, \ldots, x_m)$ describes the set of binary multivariate polynomials of degree $\leq r$.

The code $\mathcal{R}(r, m)$ is a $[n = 2^m, k = \sum_{i=0}^{r} \binom{m}{i}, d = 2^{m-r}]$ binary linear code.

Example 1:

- $\mathcal{R}(0, m)$ is the repetition code.
- $\mathcal{R}(m, m)$ is all the ambient space $\mathbb{F}_2^n$, with $n = 2^m$.
- $\mathcal{R}(2, m)$ is the code of length $n = 2^m$ given by the Boolean functions of order ≤ 2, that is all quadratic forms

We now identify a codeword of $\mathcal{R}(r, m)$ and its associated Boolean function:

$$f \leftrightarrow \mathbf{c}_f = (f(\alpha_1), \ldots, f(\alpha_n)).$$

Since the second order Reed-Muller code $\mathcal{R}(2, m)$ is central in our study, we detail its structure. A codeword in $\mathcal{R}(2, m)$ is represented by the following function:

$$f(x) = \sum_{1 \leq i < j \leq m} f_{ij} x_i x_j + \sum_{1 \leq i \leq m} l_i x_i + a_f,$$

where $f_{ij},\ l_i,\ a_f \in \mathbb{F}_2$. Since $x_i^2 = x_i$ in characteristic 2, an equivalent form is:

$$f(x) = \sum_{1 \leq i \leq j \leq m} f_{ij} x_i x_j + a_f,$$

where $f_{ii} \stackrel{def}{=} l_i$ Therefore any codeword is uniquely represented by the following boolean function

$$f(x) = x^t F x + a_f, \tag{1}$$

where $F = (f_{i,j})_{i,j=1,..,m}$ is an upper triangular binary matrix (the diagonal forming the linear part) and a_f is a constant. The number of bits involved in F being $m(m+1)/2$, we have the correct dimension.

B. Permutation Group

Let $\mathcal{C}$ be a binary linear code of length n. Let $\sigma \in \mathfrak{S}_n$ be a permutation of the set $\{1, \ldots, n\}$. The permutation σ acts on vectors of $\mathbb{F}_2^n$ as follows: if $c = (c_i)_{i \in \{1,\ldots,n\}}$ is a vector of $\mathbb{F}_2^n$ then

$$\sigma(c) = (c_{\sigma^{-1}(i)})_{i \in \{1,\ldots,n\}}.$$

Definition 3: The permutation group of $\mathcal{C}$ is the set

$$Perm(\mathcal{C}) = \{\sigma \in \mathfrak{S}_n \mid \sigma(\mathcal{C}) = \mathcal{C}\},$$

where $\sigma(\mathcal{C}) = \{\sigma(c) \mid c \in \mathcal{C}\}$.

Generally speaking, the permutation group of a code without any particular structure is trivial. Instead, the permutation group of Reed-Muller codes is known and is far from being trivial, [5]. Namely, let A be the following transformation:

$$\begin{array}{rcl} A : \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2^m \\ x = (x_1, \ldots, x_m) & \mapsto & Gx^t + \alpha, \end{array}$$

where $G = (g_{i,j})_{i,j \in \{1,\ldots,m\}}$ is a non-singular $m \times m$ binary matrix and $\alpha = (\alpha^{(i)})_{i \in \{1,\ldots,m\}} \in \mathbb{F}_2^m$. We define the following action of A on the set of Boolean functions:

$$\begin{array}{rcl} (A \cdot f)(x_1, \ldots, x_m) & = & f(A \cdot (x_1, \ldots, x_m)) \\ & = & f\left(\sum_{j=1}^{m} g_{1,j} x_j + \alpha^{(1)}, \ldots, \sum_{j=1}^{m} g_{m,j} x_j + \alpha^{(m)} \right) \end{array}$$

This action does not increase the degree: if f is a Boolean function of degree r, $A \cdot f$ has degree $\leq r$. The set of all transformations A, with the composition operation forms the group $GA_m(\mathbb{F}_2)$. This groups is clearly a subgroup of the permutation group of $\mathcal{R}(r, m)$. The converse is trickier to show.

Theorem 1 ([5]):

$$Perm(\mathcal{R}(r, m)) = GA_m(\mathbb{F}_2).$$

A transformation A in $GA_m(\mathbb{F}_2)$ can be decomposed into two parts:

- First, $x = (x_1, \ldots, x_m)$ is mapped to $x' = Gx^t$.
- Second, $x' = (x'_1, \ldots, x'_m)$ is mapped to $x' + \alpha = (x'_1 + \alpha^{(1)}, \ldots, x'_m + \alpha^{(m)})$.

Therefore $GA_m(\mathbb{F}_2)$ can be decomposed into the semi-direct product $\mathcal{T} \rtimes GL_m(\mathbb{F}_2)$, where

- $\mathcal{T}$ is the group of all translations

$$\begin{array}{rcl} T_\alpha : \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2^m \\ x & \mapsto & x + \alpha, \end{array}$$

  where $\alpha \in \mathbb{F}_2^m$. The cardinality of $\mathcal{T}$ is $n = 2^m$.
- $GL_m(\mathbb{F}_2)$ is the group of all non-singular binary matrices of size $m \times m$ with coefficients in $\mathbb{F}_2$. The cardinality of $GL_m(\mathbb{F}_2)$ is equal to $\prod_{i=0}^{m-1} (2^m - 2^i) = O(2^{m^2})$.

The group operation $\circ$ is defined by: let $(\alpha, G), (\alpha', G') \in T \rtimes GL_m(\mathbb{F}_2)$, then

$$(\alpha', G') \circ (\alpha, G) = (G'\alpha^t + \alpha', G'G).$$

The permutation group of Reed-Muller codes has therefore cardinality $n \prod_{i=0}^{m-1} (2^m - 2^i)$.

III. Actions of the permutation group on $\mathcal{R}(2, m)$

As shown in previous section, the permutation group of the second order Reed-Muller code $\mathcal{R}(2, m)$ is $GA_m(\mathbb{F}_2) = \mathcal{T} \rtimes GL_m(\mathbb{F}_2)$, where $\mathcal{T}$ is the group of all translations T_α of the element $\alpha \in \mathbb{F}_2^m$, and where and $GL_m(\mathbb{F}_2)$ is the group of all invertible matrices of size $m \times m$ with coefficients in $\mathbb{F}_2$.

The action of the group $\mathcal{T}$ is clearly described in [4]. In the first part we recall its main properties and in the second part forming the heart of the paper we describe how the action of $GL_m(\mathbb{F}_2)$ the second order Reed-Muller code can produce subcodes with smaller parameters.

A. The action of $\mathcal{T}$

Every element T_α of $\mathcal{T}$ is a permutation of order 2, with orbits of size 2. We show how to use this group to project $\mathcal{R}(2,m)$, on a subcode which is in fact isomorphic to $\mathcal{R}(1,m-1)$.

Recall from previous section that for $\alpha \in \mathbb{F}_2^m$, the action of T_α on a codeword f is given by

$$T_\alpha \cdot f\ (x) = f(T_\alpha(x)) = f(x+\alpha).$$

Given $\alpha \in \mathbb{F}_2^m$, we write

$$(Id + T_\alpha) \cdot \mathcal{R}(2,m) \stackrel{def}{=} \{f + T_\alpha \cdot f | f \in \mathcal{R}(2,m).\}$$

Hence, we have

Proposition 1: The set $(Id+T_\alpha)\cdot\mathcal{R}(2,m)$ is a subcode of $\mathcal{R}(2,m)$ and is isomorphic to $\mathcal{R}(1,m-1)$.

Proof: Let f be a codeword under the form (1). We have

$$\begin{array}{rcl}(f+T_\alpha\cdot f)\ (x) & = & x^tFx + a_f + (x+\alpha)^tF(x+\alpha) + a_f \\ & = & x^tFx + x^tFx + x^tF\alpha + \alpha^tFx + \alpha^tF\alpha \\ & = & x^tF\alpha + \alpha^tFx + \alpha^tF\alpha \\ & = & \alpha^t(F+F^t)x + \alpha^tF\alpha \\ & = & \sum\limits_{1\le i\le m} \lambda_i x_i + a_{f+T_\alpha\cdot f}\end{array}$$

Thus the function characterizing the codeword $f + T_\alpha \cdot f$ is an affine function. Moreover, the obtained codeword is formed by two copies of the same codeword of length 2^{m-1}. Namely,

$$\begin{array}{rcl}(f+T_\alpha\cdot f)\ (x+\alpha) & = & \alpha^t(F+F^t)(x+\alpha) + \alpha^tF\alpha \\ & = & \alpha^t(F+F^t)x + \alpha^tF\alpha + \alpha^tF^t\alpha \\ & & +\alpha^tF\alpha \\ & = & \alpha^t(F+F^t)x + \alpha^tF^t\alpha \\ & = & \alpha^t(F+F^t)x + \alpha^tF\alpha \\ & = & (f+T_\alpha\cdot f)\ (x)\end{array}$$

This means that $f + T_\alpha \cdot f$ takes always the same values on the positions x and $x+\alpha$. Therefore we can divide the set of positions by two without loosing information. It is the reason why we conclude that $(Id + T_\alpha) \cdot \mathcal{R}(2,m)$ is isomorphic to $\mathcal{R}(1,m-1)$. ∎

This is also the reason why we say that we *project* the second-order Reed-Muller code on copies of the first order Reed-Muller codes. All these copies are isomorphic. We now explicit the isomorphism: suppose that a codeword of length n is written under the form

$$\mathbf{c}_f = (f(\alpha_1), \ldots, f(\alpha_n)),$$

where α_i runs through $\mathbb{F}_2^m$ for $i = 1, \ldots, n$. The codeword $(Id + T_\alpha) \cdot f$ corresponds to:

$$\mathbf{c}_{f+T_\alpha\cdot f} = (f(\alpha_1) + f(\alpha_1+\alpha), \ldots, f(\alpha_n) + f(\alpha_n+\alpha)).$$

Since any position in the codeword is symmetric in α if we keep only one element per orbit in $\mathbb{F}_2^m/(\alpha)$, we get a codeword of $\mathcal{R}(1,m-1)$.

As we now understand perfectly how the group of translations $\mathcal{T}$ can project second order Reed-Muller codes, we show in next section how to copy the previous construction by using elements of $GL_m(\mathbb{F}_2)$ rather than translations.

B. The action of $GL_m(\mathbb{F}_2)$

We show that if the permutations are carefully chosen, we obtain new codes of smaller parameters by projection. As usual, the action of an element $G \in GL_m(\mathbb{F}_2)$ on a codeword is defined by

$$G \cdot f\ (x) = f(G \cdot x).$$

Given $G \in GL_m(\mathbb{F}_2)$, we write

$$(Id + G) \cdot \mathcal{R}(2,m) \stackrel{def}{=} \{f + G \cdot f | f \in \mathcal{R}(2,m)\}$$

Proposition 2: Given $G \in GL_m(\mathbb{F}_2)$, the set $(Id + G) \cdot \mathcal{R}(2,m)$ is a subcode of $\mathcal{R}(2,m)$.

Proof: Since $\forall f \in \mathcal{R}(2,m)$ we have $G \cdot f \in \mathcal{R}(2,m)$ this implies

$$(Id + G) \cdot \mathcal{R}(2,m) \subset \mathcal{R}(2,m).$$

Second, let $f_1, f_2 \in \mathcal{R}(2,m)$. It is straightforward to verify that

$$(f_1 + G \cdot f_1) + (f_2 + G \cdot f_2) \in (Id + G) \cdot \mathcal{R}(2,m).$$

∎

From now on, our motivations are to study properties of this subcode. They clearly depend on the choice of the element G in the permutation group. From the definition of the second order Reed-Muller code and from the representation (1) we can explicit the structure of the codewords of $(Id+G)\cdot\mathcal{R}(2,m)$:

$$\begin{array}{rcl}(f+G\cdot f)(x) & = & x^tFx + a_f + (Gx)^tF(Gx) + a_f \\ & = & x^tFx + x^tG^tFGx \\ & = & x^t(F+G^tFG)x\end{array}$$

If we fix $G \in GL_m(\mathbb{F}_2)$, and if $\mathcal{M}_m(\mathbb{F}_2)$ denotes the vector space of $m \times m$ binary matrices then the mapping

$$\begin{array}{rcl}\mathcal{P}_G : \mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & F + G^tFG\end{array}$$

is linear. However studying its properties in the general case is difficult. Namely, a codeword f corresponds a unique uppertriangular matrix F. However the transformation $\mathcal{P}_G$ does not keep upper-triangularity. An upper-triangular matrix is transformed into a matrix which is not necessarily upper-triangular. However the size of $\mathcal{P}_G(\mathcal{M}_m(\mathbb{F}_2))$ is an upper bound on the size of $(Id+G)\cdot\mathcal{R}(2,m)$. Since under this form obtaining a bound on the size of $\mathcal{P}_G(\mathcal{M}_m(\mathbb{F}_2))$ is difficult, we chose to rewrite the matrix G under the particular form $G = Id + E$. Now we have:

$$\begin{array}{rcl}(f+G\cdot f)(x) & = & x^t(F + (Id+E)^tF(Id+E))x \\ & = & x^t(E^tF + FE + E^tFE)x\end{array}$$

The idea is now to study, for a fixed $E \in \mathcal{M}_m(\mathbb{F}_2)$, the mapping

$$\begin{array}{rcl}\mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & E^tF + FE + E^tFE\end{array}$$

Let r be the rank of E. We have the following upper bound on the dimension of $(Id+G)\cdot\mathcal{R}(2,m)$:

Proposition 3: The dimension k' of the subcode $(Id+G)\cdot\mathcal{R}(2,m)$ satisfies

$$k' \leq 4r(m-r)+1 \tag{2}$$

Moreover $(Id+G)\cdot\mathcal{R}(2,m)$ is isomorphic to a code of length $n-2^{m-r}$

Proof: By using the fact that

$$Rk(AB) \leq \min(Rk(A), Rk(B)),$$

we get

$$Rk(E^tF+FE+E^tFE) = Rk(E^tF+(F+E^tF)E) \leq 2r.$$

By construction, the number of codewords in $(Id+G)\cdot\mathcal{R}(2,m)$ is upper bounded by the number of $m\times m$ binary matrices of the form $E^tF+FE+E^tFE$. This quantity is itself upper-bounded by the number of matrices of rank $\leq 2r$. Therefore, the size of $(Id+G)\cdot\mathcal{R}(2,m)$ is upper-bounded by the number of binary matrices of size $m\times m$ and of rank $\leq 2r$.

From [9] for instance, it is well known that the number of binary matrices of size $m\times n$ and of rank r is equal to

$$\sum_{j=0}^{r}\prod_{i=0}^{j-1}\frac{(2^m-2^i)(2^n-2^i)}{2^j-2^i}.$$

This quantity is upper bounded by $2^{(m+n-r)r+1}$. Therefore,

$$2^{k'} \leq 2^{4r(m-r)+1},$$

which gives the bound on the dimension of the code.

Now, we show that there are coordinates in the code which are always equal to 0. Let $\alpha\in\mathbb{F}_2^m$, be such that $G\alpha=\alpha$, that is α is a fixed point of G or equivalently α is in the kernel of E. In this case $(f+G\cdot f)(\alpha)=0$, for all f. The number of coordinates on which every codeword is equal zero is at least equal to the size of the kernel of E, that is 2^{m-r}. We can remove all these positions equal to 0 and obtain an isomorphic subcode of dimension k' and of length $n'=n-2^{m-r}$. ∎

The bounds for $r=1$ and $r=2$ give:

- If $r=1$, then $k'\leq 4(m-1)+1$, for a length of 2^{m-1}.
- If $r=2$, then $k'\leq 8(m-2)+1$, for a length of 2^m-2^{m-2}.

The bound show that if one fixes the rank of E, then the dimension of the projected subcodes cannot grow faster than linearly in the number of variables. Therefore we come close to construct codes which are *similar* to first order Reed-Muller code, and which could be minimum distance decoded in linear time.

The bound remains interesting if it does not exceed the dimension of the second order Reed-Muller code, that is if

$$4r(m-r)+1 \leq \frac{m(m+1)}{2}+1.$$

By solving this equation, we find that the bound gives a smaller dimension than the dimension of $\mathcal{RM}(2,m)$ if:

$$r \leq m\left(\frac{2-\sqrt{2}}{4}\right) \simeq 0.15m.$$

Definition 4: Let $G = Id+E \in GL_m(\mathbb{F}_2)$, and let $r=Rk(E)$. The subcode of length $n-2^r$ obtained from $(Id+G)\cdot\mathcal{R}(2,m)$ by removing the 2^r positions equal to 0 corresponding to the kernel of E is called *G-projected subcode* of $\mathcal{R}(2,m)$.

We now improve the bound (2) by constructing explicitly matrices E. We choose to consider E under the under triangular form with zero diagonal:

$$E(\mathbf{e}_1,\ldots,\mathbf{e}_{m-1}) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \mathbf{e}_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{e}_{m-1} & & & 0 \end{pmatrix}$$

where $\mathbf{e}_i$ is a binary vector of length i. This construction implies in particular that $G=Id+E((\mathbf{e}_1,\ldots,\mathbf{e}_{m-1})$ is non-singular. Written under this form, the matricial product

$$E^tF+FE+E^tFE$$

depends on at most $\sum_{i=0}^{r-1}(m-i)$ bits where r is the rank of E. Our improvement on bound (2) is:

$$k' \leq \sum_{i=0}^{r-1}(m-i) = rm-\frac{r(r-1)}{2}$$

This bound is always less than the dimension of $\mathcal{RM}(2,m)$.

To illustrate this property, suppose that we take $E(0,\ldots,0,\mathbf{e}_m)$, where $\mathbf{e}_m=(e_{m,j})_{j=1}^{m-1}\neq 0$. Then E has rank 1 and if we define $F=(f_{i,j})$ upper triangular, and if we define $e_{m,m}=0$, we have

$$(FE+E^tF+E^tFE)_{i,j} = e_{m,j}(f_{i,m}+e_{m,i}f_{m,m}), \tag{3}$$

$\forall i,j\in[1,\ldots,m]$. This quantity depends on the m bits $(f_{1,m},\ldots,f_{m,m})$. Hence the dimension $k'\leq m$. Moreover, since the eigenspace with eigenvalue 1 has dimension $m-1$, the corresponding G-projected subcode has length 2^{m-1} and dimension $\leq m$.

We made some simulations in the Magma language. These simulations are presented in the next section. In practice the bound is never reached. For the case where $E(0,\ldots,0,\mathbf{e}_m)$, where $\mathbf{e}_m=(0,\ldots,0,1)$, we have

$$(f+G\cdot f)(x) = x_1\left(\sum_{i=2}^{m-1}(x_if_{i,m})+(f_{1,m}+f_{m,m})\right).$$

This means that on the positions where $x_1=0$, the subcode is equal to 0 and on the positions where $x_1=1$, the subcode corresponds to the first-order Reed-Muller code $\mathcal{R}(1,m-2)$ (doubled because it is the same for $x_m=0$ and $x_m=1$). Therefore its dimension $k'=m-1$. If we do the same

for every matrix $E(\mathbf{e}_1, \ldots, \mathbf{e}_{m-1})$ of rank 1, we see that the corresponding projected subcdoes are always isomorphic to $\mathcal{R}(1, m-2)$.

For ranks higher than 1, it is difficult to find a general structure in the matrix which would allow to prove that the dimension does not reach the bound.

The final parameter of the G-projected codes that we would like to study are their minimal distance. Since they are isomorphic to subcodes of $\mathcal{RM}(2, m)$ we have a lower bound which is 2^{m-2}. In our simulations, we always found $d' = d = 2^{m-2}$ but so far we have been unable to proove it.

IV. Examples

To illustrate our results we made some simulations in the Magma language whose results are presented below.

A. Example for the translation group

Let $\alpha = (1, 0, 1, 0, 1)$. Then $(Id + T_\alpha) \cdot \mathcal{R}(2, 5)$ is a $[32, 5, 16]$ subcode. However, on the first 16 coordinates of its generator matrix, we have the submatrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

which is exactly a generator matrix of the first-order Reed-Muller code $\mathcal{R}(1, 4)$;
on the last 16 coordinates, we have the submatrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

which is the same matrix as above but permuted with $(1, 6)(2, 5)(3, 8)(4, 7)(9, 14)(10, 13)(11, 16)(12, 15)$.
Thus the permutation of the global matrix is
$\sigma = (1, 22)(6, 17)(2, 21)(5, 18)(3, 24)(8, 19)(4, 23)(7, 20)(9, 30)$
$(14, 25)(10, 29)(13, 26)(11, 32)(16, 27)(12, 31)(15, 28)$

As explained in section III.A,

- $\alpha_1 = (1, 0, 0, 0, 0) \leftrightarrow \sigma_1 = (1, 2)(3, 4) \ldots (31, 32)$
- $\alpha_3 = (0, 0, 1, 0, 0) \leftrightarrow \sigma_3 = (1, 5)(2, 6) \ldots (28, 32)$
- $\alpha_5 = (0, 0, 0, 0, 1) \leftrightarrow \sigma_5 = (1, 17)(2, 18) \ldots (16, 32)$

It is easy to verify that $\alpha = \alpha_1 + \alpha_3 + \alpha_5$ and so that $\sigma = \sigma_1 \circ \sigma_3 \circ \sigma_5$.

B. Example for the general linear group

Let

$$G = Id + E = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ g_1 & 1 & 0 & 0 & 0 \\ 0 & g_2 & 1 & 0 & 0 \\ 0 & 0 & g_3 & 1 & 0 \\ 0 & 0 & 0 & g_4 & 1 \end{pmatrix}$$

and let the successive matrices be

- G_1 is the matrix G with $g_1 = 1$ and $g_2 = g_3 = g_4 = 0$. Then $(Id + G_1) \cdot \mathcal{R}(2, 5)$ is a $[32, 4, 8]$ subcode, isomorphic to the first-order Reed-Muller code $\mathcal{R}(1, 3)$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

  by deleting the columns as said in the previous section. In this case, the subcode became a [8,4,4] code.
- G_2 is the matrix G with $g_1 = g_2 = 1$ and $g_3 = g_4 = 0$. Then $(Id + G_2) \cdot \mathcal{R}(2, 5)$ is a $[32, 8, 8]$ subcode. We have $k' = 2m - 2 \leq 2m - 1$.
- G_1 is the matrix G with $g_1 = g_2 = g_3 = 1$ and $g_4 = 0$. Then $(Id + G_3) \cdot \mathcal{R}(2, 5)$ is a $[32, 10, 8]$ subcode. We have $k' = 3m - 5 \leq 3m - 3$.
- G_1 is the matrix G with $g_1 = g_2 = g_3 = g_4 = 1$. Then $(Id + G_4) \cdot \mathcal{R}(2, 5)$ is a $[32, 12, 8]$ subcode. We have $k' = 4m - 8 \leq 4m - 6$.

V. Conclusion

We have constructed numerous codes from the second order Reed-Muller code by projecting the code under the action of an element of the general linear group. We have obtained a bound on the dimension of the projected codes, and in some cases we were able to tighten it.

References

[1] G. Schnabl and M. Bossert, Soft Decision Decoding of Reed-Muller Codes as Generalized Multiple Concatenated Codes, *IEEE Transactions on Information Theory*, 41(1):304-308, 1995.

[2] I. Dumer, Recursive Decoding and its performance for low-rate Reed-Muller codes, *IEEE Transactions on Information Theory*, 50(5):811-822, 2004.

[3] I. Dumer and K. Shabunov, Recursive error construction for general Reed-Muller codes, *Discrete Applied Mathematics*, 154:253-269, 2006.

[4] V. M. Sidel'nikov and A. S. Pershakov, Decoding Reed-Muller codes with a large number of errors, *Problems of Information Transmission*, 28(3):80-94, 1992.

[5] F. J. MacWilliams and N. J. Sloane, *The theory of error-correcting codes*, 3nd edition Amsterdam, The Nederlands : North-Holland, 2009.

[6] T. Helleseth, T. Klove and V. I. Levenshtein, Error-Correction Capability of Binary Linear Codes, *IEEE Transactions on Information Theory*, 51(4):1408-1423, 2005.

[7] P. Loidreau and B. Sakkour, Modified version of the Sidel'nikov-Pershakov decoding algorithm for binary second order Reed-Muller codes, *Algebraic and Combinatorial Theory - ACCT-9*, pp 266-271, Kranevo, June 2004.

[8] B. Sakkour, Decoding of Second Order Reed-Muller Codes with a Large Number of Errors, *In ITW 2005*,pp 176-179, Rotoua, New Zealand, 2005.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 2nd edition, 1997.