

On a decoding algorithm of $m\Theta$ Reed-Muller codes

Tsimi Jean Armand *

Pemha Binyam Gabriel Cedric[†]

Department of Mathematics and Computer Science

University of Douala

Faculty of Sciences

P. O. Box 24157 Douala

Cameroon

Abstract

In this paper, we propose an algorithm for decoding for $m\Theta$ Reed-Muller codes. Thus, we present first the notion of $m\Theta$ spectrum of Reed-Muller codes as in [2]; and we define secondly the notion of $m\Theta$ extension of Reed-Muller codes.

Subject Classification: 94B60; 94B75.

Keywords: $m\Theta$ spectrum of Reed-Muller codes, $m\Theta$ extension of Reed-Muller codes, Pseudo $m\Theta$ extension of Reed-Muller codes, $m\Theta$ matrix, $m\Theta$ Reed-Muller decoding.

1. Introduction

Modal Θ -valent codes, modal Θ -valent linear codes and modal Θ -valent cyclic codes are defined in [6, 9, 11]. These codes are an enrichment of classical codes on a logical and set level. So error becomes a dynamic notion, so we speak of partial or complete errors.

The $m\Theta$ spectrum $RM_{\Theta}(r, m)$ of a classical Reed-Muller code $RM(r, m)$ is defined in [2]. If $RM(r, m)$ is a classical Reed-Muller code of length 2^m on the alphabet $\mathbb{F}_2$, then its $m\Theta$ spectrum $RM_{\Theta}(r, m)$ is a $m\Theta$ or a pseudo $m\Theta$ code of length 4^m on the $m\Theta$ alphabet $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$. When $RM_{\Theta}(r, m)$ is a $m\Theta$ code, its sub-set of invariant elements $C(RM_{\Theta}(r, m), F_{\alpha}^n) = RM(r, 2m)$ is the classical Reed-Muller code of length 2^{2m} .

*E-mail: tsimiye@yahoo.fr (Corresponding Author)

[†]E-mail: gpemha@yahoo.fr

However, The $m\Theta$ extension $(\mathcal{C}^\Theta, F_{\alpha|C^\Theta}^n)$ of the classical Reed-Muller code $RM(r, m)$ is a $m\Theta$ code of length 2^m whose the sub-set of invariant elements $C(\mathcal{C}^\Theta, F_{\alpha}^n) = RM(r, m)$. The pseudo $m\Theta$ extension $(\mathcal{C}_{ps}^\Theta, F_{\alpha|C_{ps}^\Theta}^n)$ of $RM(r, m)$ is a non linear $m\Theta$ codes of length 2^m such that its sub-set of invariant elements $C(\mathcal{C}_{ps}^\Theta, F_{\alpha}^n) = RM(r, m)$.

In this paper, we intend to present a decoding process of $m\Theta$ Reed-Muller codes.

Section 2 recalls the $m\Theta$ spectrum of Reed-Muller codes as defined in [2]. Section 3 presents the $m\Theta$ extensions of the classical Reed-Muller codes. Section 4 is devoted to a decoding process of $m\Theta$ or pseudo $m\Theta$ extensions of the classical Reed-Muller codes.

2. The $m\Theta$ spectrum of Reed-Muller codes [2]

2.1 The definition of a $m\Theta$ spectrum of a Reed-Muller code

The first notion we will need to define $m\Theta$ Reed-Muller codes is that of a $m\Theta$ Boolean function.

We fix $m \geq 1$.

Definition 1 : ($m\Theta$ spectra of a boolean function)

One $m\Theta$ extends a Boolean function $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$, to $f^\Theta : \mathbb{F}_{2\mathbb{Z}}^m \rightarrow \mathbb{F}_{2\mathbb{Z}}$ if $(\mathbb{F}_{2\mathbb{Z}}^m, F_{\alpha}^m)$ and $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$ are the $m\Theta$ set, such that $\forall \alpha \in I_*$, $f^\Theta \circ F_{\alpha}^m = F_{\alpha} \circ f^\Theta$. A $m\Theta$ Boolean function is a function $f^\Theta : \mathbb{F}_{2\mathbb{Z}}^m \rightarrow \mathbb{F}_{2\mathbb{Z}}$ such that the following diagram be commutative.

$$\begin{array}{ccc} \mathbb{F}_2^m & \xrightarrow{f} & \mathbb{F}_2 \\ \text{spec}_{2\mathbb{Z}} \downarrow & & \downarrow \text{spec}_{2\mathbb{Z}} \\ \mathbb{F}_{2\mathbb{Z}}^m & \xrightarrow{f^\Theta} & \mathbb{F}_{2\mathbb{Z}} \end{array}$$

Thus by definition, $\forall x \in \mathbb{F}_{2\mathbb{Z}}^m$

$$f^\Theta(x) = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_2^m \\ 1_{2\mathbb{Z}} f(s(x)) & \text{if not} \end{cases}$$

Where $\forall x \in \mathbb{F}_{2\mathbb{Z}}^m$, $x = \text{spec}_{2\mathbb{Z}}(s(x))$ and $s(x)$ is the support of x , the frame of x in $\mathbb{F}_2^m$.

We say that $\mathbb{F}_{2\mathbb{Z}}^m = \text{spec}_{2\mathbb{Z}} \mathbb{F}_2^m$ and $s(\mathbb{F}_{2\mathbb{Z}}^m) = \mathbb{F}_2^m$.

Remark 1 : The total number of all $m\Theta$ Boolean functions on $\mathbb{F}_{2\mathbb{Z}}^m$ is $|\mathbb{F}_{2\mathbb{Z}}^m|^{\mathbb{F}_{2\mathbb{Z}}^m} = 4^{4^m}$.

Because $m\Theta$ boolean functions take values in $\mathbb{F}_{2\mathbb{Z}} = \{0, 1, 1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}\}$ which is a $m\Theta$ field, $m\Theta$ Boolean functions can be added and multiplied point wise: if $f, g : \mathbb{F}_{2\mathbb{Z}}^m \rightarrow \mathbb{F}_{2\mathbb{Z}}$ are $m\Theta$ Boolean functions, then one has the $m\Theta$ functions

$$\begin{aligned} f +^\ominus g, f \cdot^\ominus g : \mathbb{F}_{2\mathbb{Z}}^m &\rightarrow \mathbb{F}_{2\mathbb{Z}}; \\ (f + g)^\ominus(x) &= \begin{cases} (f + g)(x) = f(x) + g(x) & \text{if } x \in \mathbb{F}_2^m \\ \text{spec}_{2\mathbb{Z}}((f + g)(s(x))) & \text{if not} \end{cases} \\ (f \cdot g)^\ominus(x) &= \begin{cases} (f \cdot g)(x) = f(x) \cdot g(x) & \text{if } x \in \mathbb{F}_2^m \\ \text{spec}_{2\mathbb{Z}}((f \cdot g)(s(x))) & \text{if not} \end{cases} \end{aligned}$$

Also, there are $m\Theta$ constant functions $3_{2\mathbb{Z}}$ and $1_{2\mathbb{Z}}$ and constant functions 0 and 1. The $m\Theta$ Boolean function $1_{2\mathbb{Z}}$ is called the $m\Theta$ tautological truth.

We conclude that the set of $m\Theta$ Boolean functions denoted $(B(\mathbb{F}_{2\mathbb{Z}}^m, \mathbb{F}_{2\mathbb{Z}}), +^\ominus, \cdot^\ominus)$, is a $m\Theta$ commutative ring.

Definition 2 : The set of $m\Theta$ Boolean functions is called the $m\Theta$ Boolean algebra on $(\mathbb{F}_{2\mathbb{Z}}^m, F_\alpha)$.

Because the $m\Theta$ Boolean algebra on $\mathbb{F}_{2\mathbb{Z}}^m$ has 4^{4^m} elements, it is of $m\Theta$ dimension 4^m over $\mathbb{F}_{2\mathbb{Z}}$.

We will now introduce two special kinds of elements of the $m\Theta$ Boolean algebra: $m\Theta$ coordinate functions and, more generally, $m\Theta$ monomial functions.

Definition 3 : ($m\Theta$ coordinate function, $m\Theta$ monomial)

1. The $m\Theta$ Boolean function $f_i^\ominus : \mathbb{F}_{2\mathbb{Z}}^m \rightarrow \mathbb{F}_{2\mathbb{Z}}$ defined by $(f_i^\ominus(x_1, x_2, \dots, x_m) = x_i)$ is called the i th $m\Theta$ coordinate function.
2. To each subset $\{i_1, i_2, \dots, i_r\} \subset \{1, \dots, m\}$ there corresponds the $m\Theta$ monomial function $f_{i_1}^\ominus, f_{i_2}^\ominus, \dots, f_{i_r}^\ominus$, of degree r .

Where a $m\Theta$ monomial function is an element $f^\ominus \in \mathbb{F}_{2\mathbb{Z}}[X_0, X_1, \dots, X_{m-1}]$ of the form $f^\ominus = \gamma X_0^{r_0} X_1^{r_1} \dots X_{m-1}^{r_{m-1}}$, with $r_i \in \mathbb{N}$ and $\gamma \in \mathbb{F}_{2\mathbb{Z}}$.

Lemma 1 : $m\Theta$ monomials are a basis of the $m\Theta$ Boolean algebra.

Proof 1 : [2]

Definition 4 : ($m\Theta$ spectrum of a Reed-Muller code)

The r th order $m\Theta$ spectrum of a Reed-Muller code on $\mathbb{F}_{2\mathbb{Z}}^m$, denoted $RM_{\Theta}(r, m)$, is the subspace of the $m\Theta$ Boolean algebra on $\mathbb{F}_{2\mathbb{Z}}$ spanned by $m\Theta$ monomials of degree at most r .

(Here $0 \leq r \leq m$).

Generally, order all words of $\mathbb{F}_{2\mathbb{Z}}$ and of length m as $y_0, \dots, y_{4^m-1} \in \mathbb{F}_{2\mathbb{Z}}^m$.

Let $f^{\Theta} : \mathbb{F}_{2\mathbb{Z}}^m \rightarrow \mathbb{F}_{2\mathbb{Z}}$ be a $m\Theta$ Boolean function. To f^{Θ} we associate the value vector of f^{Θ} , which is $\underline{f}^{\Theta} = (f^{\Theta}(y_0), \dots, f^{\Theta}(y_{4^m-1}))$, of length 4^m .

We can say that $RM_{\Theta}(r, m)$ is spanned by the value vectors of all $m\Theta$ monomials of degree at most r in the $m\Theta$ Boolean algebra on $\mathbb{F}_{2\mathbb{Z}}^m$.

Thus

$$\mathbb{F}_{2\mathbb{Z}}[X_1, X_2, \dots, X_m] \simeq \mathbb{F}_{2\mathbb{Z}}^{4^m}.$$

Assume that we are given a $m\Theta$ vector space $(\mathbb{F}_{2\mathbb{Z}}^{4^m}, F_{\alpha}^{4^m})$. Then we consider the $m\Theta$ ring $\mathbb{F}_{2\mathbb{Z}}[X_1, X_2, \dots, X_m]$. We will see shortly that there exists a $m\Theta$ bijection ψ^{Θ} between elements of $\mathbb{F}_{2\mathbb{Z}}[X_1, X_2, \dots, X_m]$ and $\mathbb{F}_{2\mathbb{Z}}^{4^m}$.

Let ψ a bijection between $\mathbb{F}_2[X_1, X_2, \dots, X_m]$ and $\mathbb{F}_2^{2^m}$.

One $spec_{n\mathbb{Z}}$ $m\Theta$ extends $\psi : \mathbb{F}_2[X_1, X_2, \dots, X_m] \rightarrow \mathbb{F}_2^{2^m}$, to

$$\psi^{\Theta} : (\mathbb{F}_{2\mathbb{Z}}[X_1, X_2, \dots, X_m], F_{\alpha}^{4^m}) \rightarrow (\mathbb{F}_{2\mathbb{Z}}^{4^m}, F_{\alpha}^{4^m})$$

is such that

$$spec_{2\mathbb{Z}} \circ \psi = \psi^{\Theta} \circ spec_{2\mathbb{Z}}$$

Thus by definition, $\forall p \in \mathbb{F}_{2\mathbb{Z}}[X_1, X_2, \dots, X_m]$

$$\psi^{\Theta}(p) = \begin{cases} \psi(p) & \text{if } p \in \mathbb{F}_2[X_1, X_2, \dots, X_m] \\ spec_{2\mathbb{Z}}(\psi(s(p))) & \text{if not} \end{cases}$$

2.2 The parameters of $m\Theta$ spectrum of Reed-Muller codes

Lemma 2 : $RM_{\Theta}(r, m)$ has length 4^m , dimension $\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$.

Proof 2 : [2]

To find the $m\Theta$ minimum distance of $RM_{\Theta}(r, m)$, we need the following auxiliary construction.

Definition 5 :

1. A linear code of dimension k and of length n on $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ is a vector subspace of dimension k of $(\mathbb{F}_{2\mathbb{Z}}^n, F_\alpha^n)$.
2. A $m\Theta$ linear code of $m\Theta$ dimension k and of length n on $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ is a $m\Theta$ vector subspace of $m\Theta$ dimension k of $(\mathbb{F}_{2\mathbb{Z}}^n, F_\alpha^n)$.
3. A pseudo $m\Theta$ linear code of $m\Theta$ dimension k and of length n on $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ is a pseudo $m\Theta$ vector subspace of $m\Theta$ dimension k of $(\mathbb{F}_{2\mathbb{Z}}^n, F_\alpha^n)$.

Theorem 1 : The $m\Theta$ spectrum Reed-Muller code $RM_\Theta(r, m)$ is a $[4^m, k, \omega_{H_\Theta}]_{2\mathbb{Z}}$ - $m\Theta$ code, where

$$k = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r} \text{ and } \omega_{H_\Theta}(x) = d_{H_\Theta}(x, 0)$$

Where ω_{H_Θ} and d_{H_Θ} are respectively the $m\Theta$ weight and the $m\Theta$ Hamming distance.

Proof 3 : [2]

Example 1 : We know that:

- $\text{spec}_{2\mathbb{Z}}(RM(0, 0)) = RM_\Theta(0, 0) = \{0, 1, 1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}\} = \mathbb{F}_{2\mathbb{Z}}$.
- $\forall \alpha \in I_*, F_\alpha^4 RM_\Theta(0, 1) = RM(0, 2)$ and $\text{spec}_{2\mathbb{Z}}(RM(0, 1)) = RM_\Theta(0, 1) = \{(0, 0, 0, 0); (1, 1, 1, 1); (1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}); (3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}})\}$.
- $\forall \alpha \in I_*, F_\alpha^{16} RM_\Theta(0, 2) = RM(0, 4)$ and $\text{spec}_{2\mathbb{Z}}(RM(0, 2)) = RM_\Theta(0, 2) = \{(0, 0, 0, 0, 0, 0, 0, 0); (1, 1, 1, 1, 1, 1, 1, 1); (1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}); (3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}})\}$.
- In general, $\forall \alpha \in I_*, F_\alpha^{4^m} RM_\Theta(0, m) = RM(0, 2m)$. Thus $\text{spec}_{2\mathbb{Z}}(RM(0, m)) = RM_\Theta(0, 2m)$.

The first order $m\Theta$ Reed-Muller codes $RM_\Theta(1, m)$ are the subspace of the $m\Theta$ Boolean algebra on $\mathbb{F}_{2\mathbb{Z}}^m$ spanned by $m\Theta$ monomials of degree at most 1.

$$RM_\Theta(1, 1) = \{(0, 0, 0, 0), (0, 1, 1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}), (0, 1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}), (0, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}}, 3_{2\mathbb{Z}})\}.$$

Thus, $\text{spec}_{2\mathbb{Z}}(RM(1, 1)) = RM_\Theta(1, 1)$

For $m \geq 1$, $RM_\Theta(1, m+1) = \{(u, u, u+1_{2\mathbb{Z}}, u+1_{2\mathbb{Z}}) \mid u \in RM_\Theta(1, m)\}$ or $RM_\Theta(1, m+1) = \{(u, u, u+3_{2\mathbb{Z}}, u+3_{2\mathbb{Z}}) \mid u \in RM_\Theta(1, m)\}$.

Thus,

$$RM_{\Theta}(1,2) = \{(u, u, u+v, u+v) | u \in RM_{\Theta}(1,1); v \in RM_{\Theta}(0,1)\}$$

Generally, $RM_{\Theta}(r,m) = \text{spec}_{2\mathbb{Z}}(RM(r,m))$ is a pseudo $m\Theta$ set.

2.3 The $m\Theta$ matrix

Let $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$ be a $m\Theta$ field.

Definition 6 : Every matrix M with coefficients in $\mathbb{F}_{2\mathbb{Z}}$ is said a $m\Theta$ matrix.

Proposition 1 : Let $\mathcal{M}_{\Theta}$ be the set of $m\Theta$ matrixes of order $m \times n$ with coefficients in $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$.

$\forall \alpha \in I_*$, we define F'_{α} on $\mathcal{M}_{\Theta}$ as follows:

For every $M = [m_{ij}]_{1 \leq i \leq m \text{ et } 1 \leq j \leq n}$ element of $\mathcal{M}_{\Theta}$, we have:

$$F'_{\alpha} M = [F_{\alpha} m_{ij}]_{1 \leq i \leq m \text{ et } 1 \leq j \leq n}$$

Then $(\mathcal{M}_{\Theta}, F'_{\alpha})$ is a $m\Theta$ set.

Proof 4 : [9]

Definition 7 : Let $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$ be the $m\Theta$ field with 4 elements. A matrix $M = [m_{ij}]_{1 \leq i \leq m \text{ et } 1 \leq j \leq n}$ is said $m\Theta$ on $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$ when $\forall i, j: m_{ij} \in \mathbb{F}_{2\mathbb{Z}}$.

Remark 2 : The algebra of $m\Theta$ matrixes is defined the same way as the algebra of classical matrixes. But operations or laws on coefficients are $m\Theta$ laws of $\mathbb{F}_{2\mathbb{Z}}$.

Definition 8 : A $m\Theta$ generator matrix of a $m\Theta$ linear code (C, F_{α}) on $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$ is a $m\Theta$ matrix on $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$ whose lines form a $m\Theta$ basis of (C, F_{α}) .

Notation 1 : Let G_{Θ} be a $m\Theta$ generator matrix of the $m\Theta$ linear code C of $m\Theta$ dimension k and of length n on $(\mathbb{F}_{2\mathbb{Z}}, F_{\alpha})$.

Theorem 2 : The $m\Theta$ matrix $G_{\Theta}(r,m)$ has dimension $k \times n$ where:

$$k = \sum_{i=0}^r \binom{m}{i}$$

$$n = 4^m$$

The $m\Theta$ dimension of the $m\Theta$ code is hence k .

Proof 5 : The rows of the $m\Theta$ matrix may be partitioned by the degree of the $m\Theta$ monomial they represent; for the $m\Theta$ code $RM_\Theta(r, m)$, there are $\binom{m}{0}$ rows corresponding to $m\Theta$ monomials of degree 0 (0), $\binom{m}{1}$ rows corresponding to $m\Theta$ monomials of degree 1 ($X_0, X_1, \dots, X_{m-1}$), $\binom{m}{2}$ rows corresponding to $m\Theta$ monomials of degree 2, ($X_0X_1, X_0X_2, \dots, X_{m-2}X_{m-1}$), etc ...

Hence, there are:

$$\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r} = \sum_{i=0}^r \binom{m}{i}$$

Such rows, and thus, the $m\Theta$ dimension of the $m\Theta$ code is k .

It is simple to see that the number of columns is 4^m .

3. The $m\Theta$ extensions of Classical Reed-Muller codes

Let $\mathbb{F}_2$ be a finite field and $RM(r, m)$ a Reed-Muller code of alphabet $\mathbb{F}_2$, of length n , of dimension k and of encoder f . Let $G(r, m)$ be a generator matrix of $RM(r, m)$. Let $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ be the finite $m\Theta$ field such that $C(\mathbb{F}_{2\mathbb{Z}}, F_\alpha) = \mathbb{F}_2$.

Proposition 2 : Let $RM(r, m)$ be a classical Reed-Muller code of alphabet $\mathbb{F}_2$, of length n , of dimension k and $G(r, m)$ its generator matrix.

Let f be an encoder of $RM(r, m)$. Let $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ be the finite $m\Theta$ set such that $C(\mathbb{F}_{2\mathbb{Z}}, F_\alpha) = \mathbb{F}_2$. Let

$$f^\Theta : \mathbb{F}_{2\mathbb{Z}}^k \rightarrow \mathbb{F}_{2\mathbb{Z}}^n \quad x \mapsto xG(r, m)$$

1. f^Θ is $m\Theta$ If only if $r = 0$.
2. If f^Θ is $m\Theta$ then, f^Θ is an injective and linear map.

Proof 6 :

1. Let suppose that $r = 0$ and let show that f^Θ is $m\Theta$ i.e $\forall \alpha \in I_*, F_\alpha^n \circ f^\Theta = f^\Theta \circ F_\alpha$.

$$\text{Let } \alpha \in I_* \text{ and } x \in \mathbb{F}_{2\mathbb{Z}}$$

$$\begin{aligned}
F_\alpha^n \circ f^\Theta(x) &= F_\alpha^n(xG(0,m)) \\
&= F_\alpha^n \begin{pmatrix} x & x & \cdots & x \end{pmatrix} \\
&= \begin{pmatrix} F_\alpha(x) & F_\alpha(x) & \cdots & F_\alpha(x) \end{pmatrix} \\
&= F_\alpha(x) \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \\
&= F_\alpha(x)(G(0,m)) \\
&= f^\Theta(F_\alpha(x))
\end{aligned}$$

Conversely, let suppose that $r \neq 0$ and let show that $\exists \alpha_0 \in I_*$ such that $F_{\alpha_0}^n \circ f^\Theta \neq f^\Theta \circ F_{\alpha_0}^k$

Let $x = (1_{2\mathbb{Z}}, 0, 0, \dots, 1) \in \mathbb{F}_{2\mathbb{Z}}^k$

Firstly,

$$\begin{aligned}
F_2^n \circ f^\Theta(x) &= F_2^n(xG(r,m)) \\
&= F_2^n(1_{2\mathbb{Z}}, 0, 0, \dots, 1_{2\mathbb{Z}} + 1) \\
&= (F_2(1_{2\mathbb{Z}}), F_2(0), F_2(0), \dots, F_2(1_{2\mathbb{Z}} + 1)) \\
&= (0, 0, 0, \dots, 0)
\end{aligned}$$

On the other hand

$$\begin{aligned}
f^\Theta \circ F_2^k(1_{2\mathbb{Z}}, 0, 0, \dots, 1) &= f^\Theta(F_2(1_{2\mathbb{Z}}), F_2(0), F_2(0), \dots, F_2(1)) \\
&= f^\Theta(0, 0, 0, \dots, 1) \\
&= (0, 0, 0, \dots, 1)G(r, m) \\
&= (0, 0, 0, \dots, 1)
\end{aligned}$$

As $(0, 0, 0, \dots, 0) \neq (0, 0, 0, \dots, 1)$, thus $F_{\alpha_0}^n \circ f^\Theta \neq f^\Theta \circ F_{\alpha_0}^k$.

2. • Let us show that f^Θ is a map. Let $x, y \in \mathbb{F}_{2\mathbb{Z}}^k$ and $\alpha \in I_*$

Let us suppose that $x = y$ and let us show that $f^\Theta(x) = f^\Theta(y)$

$$\begin{aligned}
x = y &\Rightarrow \forall \alpha \in I_*, F_\alpha^k(x) = F_\alpha^k(y) \\
&\Rightarrow \forall \alpha \in I_*, f^\Theta(F_\alpha^k(x)) = f^\Theta(F_\alpha^k(y)) \quad (f_{\|\mathbb{F}_2^k}^\Theta = f) \\
&\Rightarrow \forall \alpha \in I_*, F_\alpha^n(f^\Theta(x)) = F_\alpha^n(f^\Theta(y)) \quad \text{because } f^\Theta \text{ is } m\Theta \\
&\Rightarrow f^\Theta(x) = f^\Theta(y)
\end{aligned}$$

- Let us show that f^Θ is injective. Let $x, y \in \mathbb{F}_{2\mathbb{Z}}^k$ such that $f^\Theta(x) = f^\Theta(y)$.

$$\begin{aligned}
 f^\Theta(x) = f^\Theta(y) &\Rightarrow \forall \alpha \in I_*, F_\alpha^n(f^\Theta(x)) = F_\alpha^n(f^\Theta(y)) \\
 &\Rightarrow \forall \alpha \in I_*, f^\Theta(F_\alpha^k(x)) = f^\Theta(F_\alpha^k(y)) \\
 &\Rightarrow \forall \alpha \in I_*, F_\alpha^k(x) = F_\alpha^k(y) \text{ because } f|_{\mathbb{F}_2^k} = f \\
 &\Rightarrow x = y
 \end{aligned}$$

- Let us show that f^Θ is linear. Let $x, y \in \mathbb{F}_{2\mathbb{Z}}^k$ and $\gamma \in \mathbb{F}_{2\mathbb{Z}}$.

$$\begin{aligned}
 \text{We have } f^\Theta(x + \gamma y) &= (x + \gamma y)G(0, m) = xG(0, m) + \gamma yG(0, m) = \\
 &= f^\Theta(x) + \gamma f^\Theta(y)
 \end{aligned}$$

Proposition 3 : Let $f^\Theta : \mathbb{F}_{2\mathbb{Z}} \rightarrow \mathbb{F}_{2\mathbb{Z}}^n ; x \mapsto xG(0, m)$

Let us set $\mathcal{C}^\Theta = \text{Im}(f^\Theta)$.

$(\mathcal{C}^\Theta, F_{\alpha|\mathcal{C}^\Theta}^n)$ is a $m\Theta$ code of alphabet $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ such that $C(\mathcal{C}^\Theta, F_{\alpha|\mathcal{C}^\Theta}^n) = RM(0, m)$.

Proof7: f^Θ is $m\Theta$ because $r = 0$, thus f^Θ is injective and linear (according **Proposition 1**). So $(\mathcal{C}^\Theta, F_{\alpha|\mathcal{C}^\Theta}^n)$ is a $m\Theta$ code.

As $\text{Im}(f|_{\mathbb{F}_2}) = \text{Im}(f)$ where f is the encoder of $RM(0, m)$. Then $C(\mathcal{C}^\Theta, F_{\alpha|\mathcal{C}^\Theta}^n) = RM(0, m)$.

Definition 9 : $(\mathcal{C}^\Theta, F_{\alpha|\mathcal{C}^\Theta}^n)$ is called a $m\Theta$ extension of $RM(0, m)$.

Example 2 : Let $G(0, 1)$ a generator matrix of $RM(0, 1) = \{00; 11\}$.

$G(0, 1) = [11]$ and f^Θ the $m\Theta$ encoder defined by:

$$f^\Theta : \mathbb{F}_{2\mathbb{Z}} \rightarrow \mathbb{F}_{2\mathbb{Z}}^2 \quad x \mapsto xG(0, 1)$$

f^Θ is a $m\Theta$ linear map from $(\mathbb{F}_{2\mathbb{Z}}, F_\beta)$ into $((\mathbb{F}_{2\mathbb{Z}})^2, F_\beta^2)$:

Indeed, let $\beta \in I_*$ and $a \in \mathbb{F}_{2\mathbb{Z}}$,

$$\begin{aligned}
 f^\Theta \circ F_\beta(a) &= F_\beta(a)G(0, 1) \\
 &= (F_\beta(a)F_\beta(a)) \\
 &= F_\beta^2(a) \\
 &= F_\beta^2 \circ f^\Theta(a)
 \end{aligned}$$

Then, according to the proposition 2., f^Θ is injective and linear.

Thus, $\mathcal{C}^\Theta = \text{Im}(f^\Theta) = \{00; 11; 1_{2\mathbb{Z}}1_{2\mathbb{Z}}; 3_{2\mathbb{Z}}3_{2\mathbb{Z}}\}$ and $C(\mathcal{C}^\Theta, F_\beta^2) = RM(0, 1)$.

Observation

If $r \neq 0$, then $f^\ominus : \mathbb{F}_{2\mathbb{Z}}^k \rightarrow \mathbb{F}_{2\mathbb{Z}}^n ; x \mapsto xG(0, m)$ is not a $m\Theta$ map, thus $\text{Im}(f^\ominus)$ is not a $m\Theta$ set. So the classical Reed-Muller code $RM(r, m)$ can not be $m\Theta$ extensible as above, but can be pseudo $m\Theta$ extensible as follows:

Proposition 4 : Let $r \neq 0$, the encoder $g^\ominus$ is defined such that:

$$g^\ominus : \mathbb{F}_{2\mathbb{Z}}^k \rightarrow \mathbb{F}_{2\mathbb{Z}}^n \quad x \mapsto (F_\alpha^k(x)G(r, m))_{\alpha \in I_*}$$

is an injective $m\Theta$ map that is not linear.

Proof 8 : Let $x, y \in \mathbb{F}_{2\mathbb{Z}}^k$ such that $x = y$.

$$\begin{aligned} x = y &\Rightarrow \forall \alpha \in I_*, F_\alpha^k(x) = F_\alpha^k(y) \\ &\Rightarrow \forall \alpha \in I_*, F_\alpha^k(x)G = F_\alpha^k(y)G \\ &\Rightarrow g^\ominus(x) = g^\ominus(y) \end{aligned}$$

Let us show that $g^\ominus$ is injective.

Let $x, y \in \mathbb{F}_{2\mathbb{Z}}^k$ such that $g^\ominus(x) = g^\ominus(y)$.

$$\begin{aligned} g^\ominus(x) = g^\ominus(y) &\Rightarrow \forall \alpha \in I_*, F_\alpha^k(x)G = F_\alpha^k(y)G \\ &\Rightarrow \forall \alpha \in I_*, f(F_\alpha^k(x)) = f(F_\alpha^k(y)) \text{ because } F_\alpha^k(x), F_\alpha^k(y) \in \mathbb{F}_2^k \\ &\Rightarrow \forall \alpha \in I_*, F_\alpha^k(x) = F_\alpha^k(y) \text{ because } f \text{ is injective} \\ &\Rightarrow x = y \end{aligned}$$

Let us show that $g^\ominus$ is not linear.

Let $RM(1, 1)$ a Reed-Muller code whose the generator matrix

$$G(1, 1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

$$g^\ominus((10) + (13_{2\mathbb{Z}})) = g^\ominus(03_{2\mathbb{Z}}) = ((00)G(1, 1); (01)G(1, 1)) = ((00); (01)) = (03_{2\mathbb{Z}})$$

$$\begin{aligned} g^\ominus(10) &= ((10)G(1, 1); (10)G(1, 1)) = ((11); (11)) = (11) \quad \text{and} \quad g^\ominus(13_{2\mathbb{Z}}) = \\ &= ((10)G(1, 1); (11)G(1, 1)) = ((11); (10)) = (11_{2\mathbb{Z}}). \end{aligned}$$

Thus,

$$g^\ominus(10) + g^\ominus(13_{2\mathbb{Z}}) = (00) \neq g^\ominus((10) + (13_{2\mathbb{Z}})) = (03_{2\mathbb{Z}})$$

Finally, let us show that $g^\ominus$ is a $m\Theta$ map. Let $\alpha \in I_*$;

$$\begin{aligned}
 F_\alpha^n \circ g^\Theta(x) &= F_\alpha^n \circ (F_\alpha^k(x)G(r,m))_{\alpha \in I_*} \\
 &= (F_\alpha^n \circ F_\alpha^k(x)G(r,m))_{\alpha \in I_*} \\
 &= (F_\alpha^k(x)G(r,m))_{\alpha \in I_*} \\
 &= g^\Theta(F_\alpha^k(x)) = g^\Theta \circ F_\alpha^k(x)
 \end{aligned}$$

Proposition 5 : Let g^Θ defined as above. Let us set $\mathcal{C}_{ps}^\Theta = Im(g^\Theta)$. $(\mathcal{C}_{ps}^\Theta, F_{\alpha|\mathcal{C}_{ps}^\Theta}^n)$ is a $m\Theta$ code on $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ that is not linear such that $C(\mathcal{C}_{ps}^\Theta, F_{\alpha|\mathcal{C}_{ps}^\Theta}^n) = RM(r, m)$.

Proof 9 : g^Θ is a $m\Theta$ map that is not linear, then $(\mathcal{C}_{ps}^\Theta, F_{\alpha|\mathcal{C}_{ps}^\Theta}^n)$ is a $m\Theta$ s and therefore a non linear $m\Theta$ code. Let f be an encoder of $RM(r, m)$, we have $g_{|\mathbb{F}_2^k}^\Theta = f$, so $Im(f) = Im g_{|\mathbb{F}_2^k}^\Theta$ and therefore $RM(r, m) = C(\mathcal{C}_{ps}^\Theta, F_{\alpha|\mathcal{C}_{ps}^\Theta}^n)$.

Definition 10 : $(\mathcal{C}_{ps}^\Theta, F_{\alpha|\mathcal{C}_{ps}^\Theta}^n)$ is called a pseudo $m\Theta$ extension of $RM(r, m)$.

Example Let us build a pseudo $m\Theta$ extension of $RM(1, 1)$.

A generator matrix $G(1, 1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and the $m\Theta$ encoder g^Θ is defined by:

$$g^\Theta : \mathbb{F}_{2\mathbb{Z}}^2 \rightarrow \mathbb{F}_{2\mathbb{Z}}^2 \quad x \mapsto (F_\alpha^2(x)G(1, 1))_{\alpha \in I_*}$$

Let $x = (1_{2\mathbb{Z}} \ 3_{2\mathbb{Z}})$ be an information to transmit. When we code this word by the encoder g^Θ , we obtain the codeword: $g^\Theta(x) = (F_1^2(x)G(1, 1); F_2^2(x)G(1, 1))$ and $F_1^2(x)G(1, 1) = (11); \quad F_2^2(x)G(1, 1) = (01)$.

So,

$$g^\Theta(1_{2\mathbb{Z}} \ 3_{2\mathbb{Z}}) = (F_1^2(1_{2\mathbb{Z}} \ 3_{2\mathbb{Z}})G(1, 1), F_2^2(1_{2\mathbb{Z}} \ 3_{2\mathbb{Z}})G(1, 1)) = (1_{2\mathbb{Z}} \ 1)$$

$$\begin{aligned}
 \mathcal{C}_{ps}^\Theta = Im(g^\Theta) &= \{(00); (01); (01_{2\mathbb{Z}}); (11); (03_{2\mathbb{Z}}); (10); (13_{2\mathbb{Z}}); (11_{2\mathbb{Z}}); \\
 &\quad (1_{2\mathbb{Z}} \ 1_{2\mathbb{Z}}); (1_{2\mathbb{Z}} \ 1); (3_{2\mathbb{Z}} \ 3_{2\mathbb{Z}}); (3_{2\mathbb{Z}} \ 1_{2\mathbb{Z}}); (3_{2\mathbb{Z}} \ 1); (3_{2\mathbb{Z}} \ 0)\}
 \end{aligned}$$

$$C(\mathcal{C}_{ps}^\Theta, F_\alpha^2) = \{(00); (01); (10); (11)\} = RM(1, 1).$$

4. A decoding process of $m\Theta$ Reed-Muller codes

In section 2, we presented the $m\Theta$ spectrum of Reed-Muller codes and recalled its parameters. In section 3, we saw that $\mathcal{C}^\Theta$ is an $m\Theta$ extension of classical Reed-Muller codes $RM(0, m)$.

It appears that if $r = 0$, C^Θ is a $m\Theta$ code and if $r \neq 0$, C_{ps}^Θ is a non linear $m\Theta$ code. An algorithm of decoding of $m\Theta$ Reed-Muller codes will distinguish two cases.

4.1 A decoding process of a $m\Theta$ extension of classical Reed-Muller codes

Let $RM(0, m)$ be a Reed-Muller code of alphabet $\mathbb{F}_2$, of length n , of dimension k and of encoder f . Let $G(0, m)$ (respectively H) be a generator matrix (respectively a control matrix) of $RM(0, m)$. Let $(C^\Theta, F_{\alpha|C^\Theta}^n)$ be the $m\Theta$ canonical extension of $RM(0, m)$.

Let c be a transmitted $m\Theta$ codeword ($c \in C^\Theta$) and y a received $m\Theta$ word. Let $s(y)$ be the syndrome of y .

- If $s(y) = 0_{\mathbb{F}_2^{n-k}}$, and $\forall \alpha \in I_*, s(F_\alpha^n(y)) = 0_{\mathbb{F}_2^{n-k}}$ then y is correct
- If not, y is not correct. To correct y , we have to correct the α -modalities $F_\alpha^n(y)$ of y .

Let recall that $y = (F_\alpha^n(y))_{\alpha \in I_*}$ and $\forall \alpha \in I_*, F_\alpha^n(y) \in C(C^\Theta, F_{\alpha|C^\Theta}^n) = RM(0, m)$. Thus, to correct y , we proceed as follows:

1. $\forall \alpha \in I_*$, determine $F_\alpha^n(y)$.
2. For $\alpha \in I_*$, if $s(F_\alpha^n(y)) = 0$, then the α -modality $F_\alpha^n(y)$ of y is correct.
3. For $\alpha \in I_*$, if $s(F_\alpha^n(y)) \neq 0$, then the α -modality $F_\alpha^n(y)$ is not correct: to correct it, we use the majority logic decoding.
4. y is finally corrected when all the damaged α -modalities $F_\alpha^n(y)$ of y are corrected.

Example 4 : We consider a $m\Theta$ extension of Reed-Muller code $RM(0, 2)$ over $\mathbb{F}_2$, of length $n = 4$ and of dimension $k = 1$.

Let $f^\Theta : \mathbb{F}_{2\mathbb{Z}} \rightarrow \mathbb{F}_{2\mathbb{Z}}^4$ $x \mapsto xG(0, 2)$. Let recall that $C^\Theta = \text{Im}(f^\Theta) = \{0000; 1111; 1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}; 3_{2\mathbb{Z}}3_{2\mathbb{Z}}3_{2\mathbb{Z}}3_{2\mathbb{Z}}\}$ the $m\Theta$ extension of $RM(0, 2)$, of $m\Theta$ minimal distance $d_\Theta(C^\Theta) = 4$.

Let suppose that the $m\Theta$ codeword $c = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}$ is received as $y = 01_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}$. The $m\Theta$ code C^Θ corrects at most 1 errors, and can detects 3 errors. c is partially damaged because $1_{2\mathbb{Z}} = (1, 0)$ becomes $0 = (0, 0)$.

$G(0,2)=[1111]$ a generator matrix of $RM(0,2)$ and $H=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ its control matrix. We have:

$$s(y) = (01_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}) \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}) \neq 0_{\mathbb{F}_2^3}.$$

So there is an error. Thus $\exists \alpha_0 \in I_*$ such that $s(F_{\alpha_0}^4(y)) \neq 0_{\mathbb{F}_2^3}$.

$$F_1^4(y) = F_1^4(01_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}) = (F_1(0)F_1(1_{2\mathbb{Z}})F_1(1_{2\mathbb{Z}})F_1(1_{2\mathbb{Z}})) = (0111)$$

$$F_2^4(y) = F_2^4(01_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}) = (F_2(0)F_2(1_{2\mathbb{Z}})F_2(1_{2\mathbb{Z}})F_2(1_{2\mathbb{Z}})) = (0000).$$

$$\text{Thus, } s(F_1^4(y)) = (0111) \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (111) \neq 0_{\mathbb{F}_2^3} \text{ and}$$

$$s(F_2^4(y)) = (0000) \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (000) = 0_{\mathbb{F}_2^3}.$$

Since $s(F_2^4(y)) = 0_{\mathbb{F}_2^3}$, $F_2^4(y)$ is correct and $F_2^4(y) = F_2^4(c)$. $F_1^4(y)$ is not correct, we correct this by majority decoding.

We have $G(0,2)=[1111]$. Any vector v of the code is such that $v = av_0 = a(1111) = (aaaa)$ where $a \in \mathbb{F}_2$.

Otherwise, $F_1^4(y) = (0111) = av_0 \Rightarrow a = 0 = 1 = 1 = 1$; so $a = 1$. Thus, $F_1^4(c) = (1111)$.

We have $F_1^4(c) = (1111)$ and $F_2^4(c) = (0000)$.

Since $c = (F_1^4(c), F_2^4(c)) = (1111; 0000)$, in conclusion we obtain

$$c = (1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}}1_{2\mathbb{Z}})$$

4.2 A decoding process of a pseudo $m\Theta$ extension of classical Reed-Muller codes

Let recall that the pseudo $m\Theta$ extension $\mathcal{C}_{ps}^\Theta$ is a non linear $m\Theta$ code and $\forall \alpha \in I_*, \forall c \in \mathcal{C}_{ps}^\Theta, F_\alpha^n(c) \in RM(r, m)$ which is a classical linear code. Thus if y is a received word, then:

1. If $\forall \alpha \in I_*, s(F_\alpha^n(y)) = 0$, then y is correct.
2. If not, $\exists \alpha \in I_*$ such that $s(F_\alpha^n(y)) \neq 0$, then y is not correct.
3. To correct y , we have to correct by the majority logic all the α -modality $F_\alpha^n(y)$ of y such that $s(F_\alpha^n(y)) \neq 0$.

Let $RM(r, m)$, $r \neq 0$ be a Reed-Muller code of alphabet $\mathbb{F}_2$, of length n , of dimension k and $G(r, m)$ its generator matrix.

The rows of $G(r, m)$ are basis vectors for the code; label them $v_0, v_1, \dots, v_{k-1}$. Any vector c of $\mathcal{C}_{ps}^\Theta$ is linear combination of these. So, $\forall \alpha \in I_*, F_\alpha^n(c) = a_0 v_0 + a_1 v_1 + \dots + a_{k-1} v_{k-1}$ $a_i \in \mathbb{F}_2, \forall i \in \{0, 1, \dots, k-1\}$.

If no error occur, a received vector y is such that $F_\alpha^n(y) = (y_0, y_1, \dots, y_{n-1})$ can be used to solve for the a_i other than a_0 in several ways (k ways for each).

If p errors has occurred in y , $p \leq \lfloor \frac{d_\Theta - 1}{2} \rfloor$ where d_Θ is minimal $m\Theta$ distance, then when all the calculations above are made ($k-p$) of the k values will agree for each a_i , so the correct value will be obtained by majority decoding.

Finally, a_0 can be determined as the majority of the components of $F_\alpha^n(y) + a_1 v_1 + a_2 v_2 + \dots + a_{k-1} v_{k-1}$.

Example 5 : We consider a $m\Theta$ pseudo extension $\mathcal{C}_{ps}^\Theta$ of Reed-Muller code $RM(1, 3)$ over $\mathbb{F}_2$, of length $n = 8$ and of dimension $k = 4$.

$$G(1, 3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Here, $v_0 = (11111111); \quad v_1 = (01010101); \quad v_2 = (00110011);$
 $v_3 = (00001111).$

Let $g^\Theta : \mathbb{F}_{2\mathbb{Z}}^4 \rightarrow \mathbb{F}_{2\mathbb{Z}}^8; x \mapsto (F_\alpha^4(x)G(1, 3))_{\alpha \in I_*}$ a non linear, $m\Theta$ injective map. $(\text{Img}^\Theta, F_\alpha^8|_{\text{Img}^\Theta})$ is a pseudo $m\Theta$ extension of $RM(1, 3)$. Otherwise, $(\text{Img}^\Theta, F_\alpha^8|_{\text{Img}^\Theta})$ is a $m\Theta$ non linear code.

Let $x = (11_{2\mathbb{Z}} 03_{2\mathbb{Z}}) \in \mathbb{F}_{2\mathbb{Z}}^4$; $F_1^4(x) = (1100)$ and $F_2^4(x) = (1001)$.

$$F_1^4(x)G(1,3) = (1100) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (10101010)$$

$$F_2^4(x)G(1,3) = (1001) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (11110000)$$

$$g^\Theta(11_{2\mathbb{Z}} 03_{2\mathbb{Z}}) = (F_1^4(x)G(1,3), F_2^4(x)G(1,3)) = (10101010, 11110000) = 13_{2\mathbb{Z}} 13_{2\mathbb{Z}} 1_{2\mathbb{Z}} 01_{2\mathbb{Z}} 0.$$

Suppose that $c = 13_{2\mathbb{Z}} 13_{2\mathbb{Z}} 1_{2\mathbb{Z}} 01_{2\mathbb{Z}} 0$ is a transmitted $m\Theta$ codeword, received as $y = 13_{2\mathbb{Z}} 11_{2\mathbb{Z}} 1_{2\mathbb{Z}} 01_{2\mathbb{Z}} 0$. Thus, $3_{2\mathbb{Z}} = (0,1)$ becomes $1_{2\mathbb{Z}} = (1,0)$ i.e all the modalities of $3_{2\mathbb{Z}}$ have been damaged.

So $\forall \alpha \in I_*$, $F_\alpha^8(c) = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3$, where $a_i \in \mathbb{F}_2$.

Thus,

$$F_\alpha^8(c) = (a_0, a_0 + a_1, a_0 + a_2, a_0 + a_1 + a_2, a_0 + a_3, a_0 + a_1 + a_3, a_0 + a_2 + a_3, a_0 + a_1 + a_2 + a_3).$$

Let's find and correct an error.

A received vector $F_\alpha^8(y) = (y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7)$, $\forall \alpha \in I_*$, can be used to solve for the a_i other than a_0 in several ways. $\forall \alpha \in I_*$, $F_\alpha^8(c) = F_\alpha^8(y)$, we have:

$$\begin{cases} a_0 = y_0 \\ a_0 + a_1 = y_1 \\ a_0 + a_2 = y_2 \\ a_0 + a_1 + a_2 = y_3 \\ a_0 + a_3 = y_4 \\ a_0 + a_1 + a_3 = y_5 \\ a_0 + a_2 + a_3 = y_6 \\ a_0 + a_1 + a_2 + a_3 = y_7 \end{cases} \Rightarrow \begin{cases} a_1 = y_0 + y_1 = y_2 + y_3 = y_4 + y_5 = y_6 + y_7 \\ a_2 = y_0 + y_2 = y_1 + y_3 = y_4 + y_6 = y_5 + y_7 \\ a_3 = y_0 + y_4 = y_1 + y_5 = y_2 + y_6 = y_3 + y_7 \end{cases}$$

The α -modality of y are:

$$F_1^8(y) = (10111010) \text{ and } F_2^8(y) = (11100000).$$

1. First decode $F_1^8(y)$ by majority logic.

$$F_1^8(y) = (10111010). \text{ Using, } \begin{cases} a_1 = y_0 + y_1 = y_2 + y_3 = y_4 + y_5 = y_6 + y_7 \\ a_2 = y_0 + y_2 = y_1 + y_3 = y_4 + y_6 = y_5 + y_7 \\ a_3 = y_0 + y_4 = y_1 + y_5 = y_2 + y_6 = y_3 + y_7 \end{cases}$$

We calculate:

$$a_1 = 1 = 0 = 1 = 1 \Rightarrow a_1 = 1$$

$$a_2 = 0 = 1 = 0 = 0 \Rightarrow a_2 = 0$$

$$a_3 = 0 = 0 = 0 = 1 \Rightarrow a_3 = 0$$

There is one error that has occurred in $F_1^8(y)$ because all the calculations above are made, 3 of the 4 values will agree for each a_i , so the correct value will be obtained by majority decoding. $a_0 = 1$ since $(10111010) + (01010101) = (11101111)$.

So, $F_1^8(c) = (11111111) + (01010101) = (10101010)$.

2. Secondly decode $F_2^8(y)$ by majority logic. $F_2^8(y) = (11100000)$.

Similarly we have:

$$a_1 = 0 = 1 = 0 = 0 \Rightarrow a_1 = 0$$

$$a_2 = 0 = 1 = 0 = 0 \Rightarrow a_2 = 0$$

$$a_3 = 1 = 1 = 1 = 0 \Rightarrow a_3 = 1.$$

$a_0 = 1$ since $(11100000) + (00001111) = (11101111)$.

So, $F_2^8(c) = (11111111) + (00001111) = (11110000)$.

Since $c = (F_{\alpha|Im(g^\odot)}^8(c))_{\alpha \in I_*} = (10101010; 11110000)$, we obtain:

$$c = 13_{2\mathbb{Z}} 13_{2\mathbb{Z}} 1_{2\mathbb{Z}} 01_{2\mathbb{Z}} 0$$

As $3_{2\mathbb{Z}} = (0,1)$ becomes $1_{2\mathbb{Z}} = (1,0)$, then we can conclude that the information is completely damaged.

5. Conclusion

In this paper, we have presented a decoding process of $m\Theta$ Reed-Muller codes. This process of decoding is based on the α -modalities of the received $m\Theta$ words, and from the majority logic decoding. Thus we have first brought to define the $m\Theta$ and the pseudo $m\Theta$ extension of classical Reed-Muller codes.

We have also recalled the definition of the $m\Theta$ spectrum of a classical Reed-Muller code as presented in [2].

References

- [1] F. Ayissi Eteme, Logique et Algèbre de structures mathématiques modales Θ -valentes chrysippiennes. Edition Hermann, Paris, 2009.
- [2] J. A. Tsimi and G. Pemha, A $m\Theta$ spectrum of Reed-Muller codes, *Journal of Discrete Mathematical Sciences and Cryptography* vol. 24, 2021, pp. 1 – 17.
- [3] F. Ayissi Eteme, Anneau chrysipien Θ -valent, CRAS, Paris 298, série 1, 1984, pp. 1 – 4.
- [4] F. Ayissi Eteme, Complétion chrysippienne d'une algèbre de Lukasiewicz Θ -valent, CRAS, Paris, 299, Série 1(3), 1984, pp. 69 – 72.
- [5] F. Ayissi Eteme, Complétion chrysippienne d'une algèbre de Lukasiewicz Θ -valent, CRAS, Paris, 299, Série 1, 1984, pp. 1-4.
- [6] F.A. Eteme and J.A. Tsimi, A modal Θ -valent approach of the notion of code, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 14, October 2011, pp. 445-473.
- [7] F. Ayissi Eteme, Spectre Θ -valent d'un $\text{ach}\Theta$ et représentation intrinsèque d' $\text{ach}\Theta$, *Revue Romaine de Mathématiques Pures et Appliquées*, Bucarest, Roumanie, 1992.
- [8] Papini O. and Wolfmann J., Algèbre discrete et codes correcteurs, Springer-Verlag, *Mathématiques et Application*, No. 20, 1995.
- [9] F.A. Eteme and J.A. Tsimi, A $m\Theta$ approach of the algebraic theory of linear codes, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 14 (2011), No. 6, pp. 559-581
- [10] F. Ayissi Eteme, Chrysippian $m\Theta$ valent introducing pure and applied mathematics, LAP Lambert Academic Publishing, 2015, Deutschland, Germany.

- [11] F. Ayissi Eteme and J.A.Tsimi, The $m\Theta$ cyclic codes on a $m\Theta$ field, 2016, pp 313 – 344, Volume 25 Issue3 (*International Journal of Mathematics, Game theory and algebra*).
- [12] Mercier D.J., L'algèbre dans la correction des erreurs, A.P.M.E.P., Bulletin n°415, 1998, pp. 173-191
- [13] R.E. Blahut, Theory and Practice of error control codes Addison-Wesley, 1983.
- [14] S. Lin and D.J. Costello Jr., Error control coding Fundamentals and Applications. Prentice Hall, 1983.

Received Septebmer, 2020

Revised January, 2021