

The Parameters of Reed-Muller Projective $m\Theta$ Codes

Pemha Binyam Gabriel Cedric

University of Douala, Faculty of Science, Department of Mathematics and computer sciences, Douala Cameroon

***Corresponding author:** Pemha Binyam Gabriel Cedric, University of Douala, Faculty of Science, Department of Mathematics and computer sciences, Douala Cameroon.

Submitted: 15 February 2025 **Accepted:** 21 February 2025 **Published:** 26 February 2025

doi <https://doi.org/10.63620/MKWJAMS.2025.1001>

Citation: Pemha, B. G. C. (2025). The Parameters of Reed-Muller Projective $m\Theta$ Codes. *Wor Jour of Appl Math and Sta*, 1(1), 01-10.

Abstract

Reed-Muller codes were originally introduced by Muller in 1954, then Irving Reed gave a decoding method the same year. These codes, of lengths a power of 2, were the first family of codes for which it was possible to decode an infinite number of errors. The finite field underlying the Reed-Muller codes is $F_2 = \{0, 1\}$. By replacing this field with the $m\Theta$ finite field $F_{2Z} = \{0, 1, 12Z, 32Z\}$, the study of Reed-Muller codes on F_{2Z} becomes the $m\Theta$ Reed-Muller codes. The generalized Reed-Muller codes were introduced by Kasami, Lin and Peterson a Weldon. They showed that GRM codes are cyclic and thereby determined the minimum distance. The $m\Theta$ generalized Reed-Muller codes were developed by Pemha and Tsimi in 2022. Projective Reed-Muller codes are first introduced by Lachaud in 1988 and the dimensions and minimum distances of Projective Reed-Muller codes are determined by Sørensen in 1991. In this paper, we intend to define and to present a notion of Reed-Muller Projective $m\Theta$ Reed-Muller codes, in other words the Projective Reed-Muller codes on the $m\Theta$ field F_qZ , q prime or prime power. The nature of the number q will determine the type of Projective Reed-Muller codes. The exact parameters of the Reed-Muller Projective $m\Theta$ codes are derived and the dual are characterized. It is shown that the Reed-Muller Projective $m\Theta$ codes are an extension of Projective Reed-Muller codes such that the set of $m\Theta$ invariants C (Reed-Muller Projective $m\Theta$ codes) of the $m\Theta$ set Reed-Muller Projective $m\Theta$ codes is Projective Reed-Muller codes. The Reed-Muller Projective $m\Theta$ codes are $m\Theta$ cyclic and the generator polynomial is characterized.

Keywords: Chrysippian Modal Θ -Valent Logic, $m\Theta$ set, $m\Theta$ Generalized Reed-Muller Codes, $m\Theta$ Minimum Weight, Reed-Muller Projective $m\Theta$ Codes.

Introduction

Projective Reed-Muller codes are a class of linear error-correcting codes, constructed from Reed-Muller codes, and having interesting properties in terms of minimum distance and dimensionality relative to the code length [8, 10]. Classical Reed-Muller codes are defined over affine vector spaces, while the projectively normalized versions are defined over projective vector spaces [7, 9]. This projective normalization allows for some improved characteristics of the codes.

The main properties of projective Reed-Muller codes are: Better minimum distance than affine Reed-Muller codes of the same dimension and length; higher dimensionality than affine Reed-Muller codes of the same length and rich algebraic structure enabling in-depth mathematical analysis [11].

The purpose of the paper is to: provide an explicit construction of Reed-Muller projective $m\Theta$ codes and derive their fundamental parameters, such as their dimension and minimum distance; investigate the algebraic properties of these codes, including their automorphism group and compare the performance of these projective $m\Theta$ codes to classical Reed-Muller codes.

This paper recalls, in section II, the Generalized Reed-Muller Codes by its generator matrix over $GF(qm, r)$ and the canonical construction of modal Θ -valent fields, modal Θ -valent pseudo fields as defined in [1]. Section III gives exact definition of $m\Theta$ Generalized Reed-Muller Codes. The parameters of Reed-Muller Projective $m\Theta$ codes are characterized in section IV. It is shown that a subclass of Reed-Muller Projective $m\Theta$ codes is $m\Theta$ cyclic.

Definition 1. [2, 3] Let M be a non-empty set, I be a chain whose first and last elements are 0 and 1 respectively, $(F_\alpha)_{\alpha \in I_*}$ where $I_* = I \setminus \{0\}$ be a family of applications from E to E .

A $m\Theta$ set is the pair $(E, (F_\alpha)_{\alpha \in I_*})$ simply denoted by (E, F_α) satisfying the following four axioms :

- $\bigcap_{\alpha \in I_*} F_\alpha(E) = \bigcap_{\alpha \in I_*} \{F_\alpha(x) : x \in E\} \neq \emptyset$;
- $\forall \alpha, \beta \in I_*$, if $\alpha \neq \beta$ then $F_\alpha \neq F_\beta$;
- $\forall \alpha, \beta \in I_*$, $F_\alpha \circ F_\beta = F_\beta$;
- $\forall x, y \in E$, if $\forall \alpha \in I_*$, $F_\alpha(x) = F_\alpha(y)$ then $x = y$.

$m\Theta$ sets are considered to be non-classical sets which are compatible with a non-classical logic called the chrysippian $m\Theta$ logic.

Definition 0.2. [4] Let $C(E, F_\alpha) = \bigcap_{\alpha \in I_*} F_\alpha(E)$. We call $C(E, F_\alpha)$ the set of $m\Theta$ invariant elements of the $m\Theta$ set (E, F_α) .

Let $p \in \mathbb{N}$, a prime number. Let us recall that if $a \in \mathbb{F}_{p\mathbb{Z}}$.

$$\mathbb{F}_{p\mathbb{Z}} = \mathbb{F}_p \cup \{x_{p\mathbb{Z}} : \neg(x \equiv 0 \pmod{p})\}; \quad \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}.$$

2.2. Generalized Reed-Muller codes over $\mathbb{GF}(q^m, r)$ [5]

Let ξ be a primitive element of $\mathbb{GF}(q^m, r)$, then $\mathbb{GF}(q^m, r) = \{0, 1, \xi, \xi^2, \dots, \xi^{q^m-2}\}$. The field $\mathbb{GF}(q^m, r)$ can be viewed as an m -dimensional vector space over $\mathbb{GF}(q, r)$ with $1, \xi, \xi^2, \dots, \xi^{m-1}$ as basis elements, so,

$$\xi^j = \sum_{i=0}^{m-1} a_{ij} \xi^i \quad 0 \leq j \leq q^m - 2.$$

Where $a_{ij} \in \mathbb{GF}(q^m, r)$, $0 \leq i \leq m-1$, $0 \leq j \leq q^m - 2$, since $\mathbb{GF}(q^m, r)$ can be considered a vector space over the field $\mathbb{GF}(q, r)$, with $1, \xi, \xi^2, \dots, \xi^{m-1}$ as basis elements. The matrix $G_q(r, m)$ can then be rewritten as

$$G_q(r, m) = \begin{pmatrix} v_I \\ v_0 \\ v_1 \\ \vdots \\ v_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_{00} & a_{01} & a_{02} & \cdots & a_{0,n-1} \\ a_{10} & a_{11} & a_{12} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{m-1,0} & a_{m-1,1} & a_{m-1,2} & \cdots & a_{m-1,n-1} \end{pmatrix}$$

In other words, the elements of $\mathbb{GF}(q^m, r)$ can be written in the vector form as

$$\xi^j = \begin{pmatrix} a_{0j} \\ a_{1j} \\ \vdots \\ a_{m-1,j} \end{pmatrix}; \quad j = 0, 1, \dots, q^m - 2.$$

Let $n = q^m$. The vector space $\mathbb{GF}(q^m, r)$ has n elements which are often call points. Let

$$P_0 := (0, 0, \dots, 0), \quad P_j := (a_{0,j-1}, a_{1,j-1}, \dots, a_{m-1,j-1}); \quad j = 0, 1, \dots, n-1.$$

Then P_0, P_1, \dots, P_{n-1} is an enumeration of the points of $\mathbb{GF}(q^m, r)$. Under this enumeration, a q -ary Reed-Muller code $RM_q(r, m)$ of order r is defined as in [5]

$$RM_q(r, m) = \{(f(P_0), f(P_1), \dots, f(P_{n-1})), | f \in \mathbb{F}_q[X_1, \dots, X_m], \deg(f) \leq r\}.$$

2.3. Canonical construction of modal Θ -valent fields ($m\Theta f$) and modal Θ -valent pseudo fields ($m\Theta pf$). [6]

Let p be a prime number, $k \neq 0$ a positive integer, $q = p^k$ and \mathbb{F}_q a finite field with q elements.

Modal Θ -valent fields ($m\Theta f$)

Consider that $k = 1$, so $q = p$. $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ is the prime field of characteristic p and of p elements. The modal Θ -valent quotient ring ($m\Theta qr$) $\mathbb{F}_{p\mathbb{Z}}$ as the modal Θ -valent quotient $\frac{\mathbb{Z}_{p\mathbb{Z}}}{p\mathbb{Z}_{p\mathbb{Z}}}$.

Let $\mathbb{F}_{p\mathbb{Z}}^* = \mathbb{F}_{p\mathbb{Z}} - \{0\}$. $\forall x \in \mathbb{F}_{p\mathbb{Z}}^*, \exists x' \in \mathbb{F}_{p\mathbb{Z}}^* / x \cdot x' = \frac{1_{p\mathbb{Z}}}{p\mathbb{Z}_{p\mathbb{Z}}}$.

$\mathbb{F}_{p\mathbb{Z}}$ has p^2 elements but has no proper sub $m\Theta$ ring verifying the preceding property for $\mathbb{F}_{p\mathbb{Z}}^*$.

For which reason, $\mathbb{F}_{p\mathbb{Z}}$ is the prime $m\Theta f$ with p^2 elements. \mathbb{F}_p is the prime sub field of the $m\Theta$ invariants of $\mathbb{F}_{p\mathbb{Z}}$.

Modal Θ -valent pseudo fields ($m\Theta pf$)

Consider that $k \neq 1$, so $q = p^k$. Let then $\mathbb{F}(p^k\mathbb{Z}, 1)$ denote the quotient $m\Theta r$ $\mathbb{F}_{p^k\mathbb{Z}} = \frac{\mathbb{Z}_{p\mathbb{Z}}}{p^k\mathbb{Z}_{p\mathbb{Z}}}$ and let

$$O(p^k, 1) = O_{p^k} = \left\{ \frac{a}{p^k\mathbb{Z}_{p\mathbb{Z}}} : a \in \mathbb{Z}_{p\mathbb{Z}}, s(a)/p^k \right\} = \left\{ \frac{a}{p^k\mathbb{Z}} : a \in \mathbb{Z}, a/p^k \right\}.$$

Let $\mathbb{F}^*(p^k\mathbb{Z}, 1) = \mathbb{F}(p^k\mathbb{Z}, 1) - O(p^k, 1)$; $k \in \mathbb{N}^*$. Then $\forall x : x \in \mathbb{F}^*(p^k\mathbb{Z}, 1), \exists x' : x' \in \mathbb{F}^*(p^k\mathbb{Z}, 1) : x \cdot x' = \frac{1_{p\mathbb{Z}}}{p^k\mathbb{Z}_{p\mathbb{Z}}}$.

So we call $\mathbb{F}_{p^k\mathbb{Z}}$ a $m\Theta$ pseudo field ($m\Theta pf$). $\mathbb{F}_{p^k\mathbb{Z}}$ has p^{k+1} elements and is of characteristic p^k . It has no proper sub $m\Theta pf$ with the same as the preceding properties for $\mathbb{F}^*(p^k\mathbb{Z}, 1)$. Finally, $\mathbb{F}(p^k\mathbb{Z}, 1)$ is the prime $m\Theta pf$ with p^{k+1} elements.

Nomenclature 0.1. We call:

- $\mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]$ $m\Theta$ Ring of polynomials in X_0, X_1, \dots, X_m with coefficients in $\mathbb{F}_{q\mathbb{Z}}$.
- $\mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]^\nu \cup \{0\}$ $m\Theta$ Vectorspace of polynomials in X_0, X_1, \dots, X_m with coefficients in $\mathbb{F}_{q\mathbb{Z}}$ and of degree ν .
- $\mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]_h \cup \{0\}$ $m\Theta$ Vectorspace of homogeneous polynomials in X_0, X_1, \dots, X_m with coefficients in $\mathbb{F}_{q\mathbb{Z}}$.
- $\mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]^\nu_h \cup \{0\}$ $m\Theta$ Vectorspace of homogeneous polynomials in X_0, X_1, \dots, X_m with coefficients in $\mathbb{F}_{q\mathbb{Z}}$ and of degree ν .
- $\mathbb{A}^m(\mathbb{F}_{q\mathbb{Z}})$ m -dimensional affine space over $\mathbb{F}_{q\mathbb{Z}}$.
- $\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$ m -dimensional projective space over $\mathbb{F}_{q\mathbb{Z}}$.

3. Reed-Muller projective $m\Theta$ Codes

3.1. Generalized $m\Theta$ Reed-Muller Codes [1]

If m is a positive integer, we denote by \mathbb{B}_m^Θ the $\mathbb{F}_{p\mathbb{Z}}$ -algebra of the $m\Theta$ functions from $\mathbb{F}_{p\mathbb{Z}}^m$ to $\mathbb{F}_{p\mathbb{Z}}$ and by $\mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m]$ the $\mathbb{F}_{p\mathbb{Z}}$ -algebra of $m\Theta$ polynomials over $\mathbb{F}_{p\mathbb{Z}}$ in m variables.

We consider the morphism of \mathbb{F}_p -algebras (from the \mathbb{F}_p -algebra of polynomials

mials over \mathbb{F}_p in m variables to the \mathbb{F}_p -algebra of the functions from \mathbb{F}_p^m to \mathbb{F}_p)

$$\varphi : \mathbb{F}_p[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m.$$

Definition 0.3. One $m\Theta$ extends $\varphi : \mathbb{F}_p[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m$, a morphism of \mathbb{F}_p -algebras, to $\varphi^\Theta : \mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m^\Theta$ if $(\mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m], F_\alpha)$ and $(\mathbb{B}_m^\Theta, F'_\alpha)$ are the $m\Theta$ set, such that $\forall \alpha \in I_*$, $\varphi \circ F_\alpha = F'_\alpha \circ \varphi$. A $m\Theta$ morphism of \mathbb{F}_p -algebras is a morphism

$$\varphi^\Theta : \mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m^\Theta$$

such that the following diagram be commutative:

$$\begin{array}{ccc} \mathbb{F}_p[X_1, \dots, X_m] & \xrightarrow{\varphi} & \mathbb{B}_m \\ \text{spec}_{p\mathbb{Z}} \downarrow & & \downarrow \text{spec}_{p\mathbb{Z}} \\ \mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m] & \xrightarrow{\varphi^\Theta} & \mathbb{B}_m^\Theta \end{array}$$

Thus by definition, $\forall P \in \mathbb{A}^m(\mathbb{F}_{p\mathbb{Z}})$

$$\varphi^\Theta(P) = \begin{cases} \varphi(P) & \text{if } P \in \mathbb{A}^m(\mathbb{F}_p) \\ 1_{p\mathbb{Z}}\varphi(s(P)) & \text{if not} \end{cases}$$

We consider now the $m\Theta$ -morphism of $\mathbb{F}_{p\mathbb{Z}}$ -algebras $\varphi^\Theta : \mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m^\Theta$ which associates to $P \in \mathbb{A}^m(\mathbb{F}_{p\mathbb{Z}})$ the $m\Theta$ function $f^\Theta \in \mathbb{B}_m^\Theta$ such that:

$$\forall X = (X_1, \dots, X_m) \in \mathbb{F}_{p\mathbb{Z}}^m, \quad f^\Theta(X) = P(X_1, \dots, X_m)$$

The $m\Theta$ morphism φ^Θ is onto and its kernel is the ideal generated by the polynomials $X_1^{p^2} - X_1, \dots, X_m^{p^2} - X_m$.

So, for each $f \in \mathbb{B}_m^\Theta$, there exists a unique $m\Theta$ polynomial $P \in \mathbb{A}^m(\mathbb{F}_{p\mathbb{Z}})$ such that the degree of P in each variable is at most $p^2 - 1$ and $\varphi^\Theta(P) = f^\Theta$.

The support of f^Θ is the set $\{X \in \mathbb{F}_{p\mathbb{Z}}^m : f^\Theta(X) \neq 0\}$ and we denote by $|f^\Theta|$ the cardinal of its support, and is the $m\Theta$ Hamming weight of f^Θ .

Definition 0.4. (*$m\Theta$ Generalized Reed-Muller codes*)

For $0 \leq r \leq m(p^2 - 1)$, the r th order $m\Theta$ generalized Reed-Muller code of length p^{2m} is:

$$RM_p^\Theta(r, m) := \{(f^\Theta(P_0), \dots, f^\Theta(P_{n-1})) / f^\Theta \in \mathbb{F}_{p\mathbb{Z}}[X_1, X_2, \dots, X_m], \deg(f^\Theta) \leq r\}$$

Observation:

$\mathbb{F}_{p\mathbb{Z}}$ is a $m\Theta$ field. Let p^k be a power of a prime number p . We saw in section 2 that $\mathbb{F}_{p^k\mathbb{Z}}$ is not a $m\Theta$ field. Now, we want to define a generalized Reed-Muller codes on $\mathbb{F}_{p^k\mathbb{Z}}$.

Let p be a prime number, k a positive integer and $\mathbb{F}_{p^k\mathbb{Z}}$ a pseudo $m\Theta$ field ($m\Theta pf$). $\mathbb{F}_{p^k\mathbb{Z}}$ has p^{k+1} elements and is of characteristic p^k .

In this case, $\mathbb{B}_m^{ps\Theta}$ is the pseudo $m\Theta$ $\mathbb{F}_{p^k\mathbb{Z}}$ -algebra of the $m\Theta$ functions from $\mathbb{F}_{p^k\mathbb{Z}}^m$ to $\mathbb{F}_{p^k\mathbb{Z}}$ and by $\mathbb{F}_{p^k\mathbb{Z}}[X_1, \dots, X_m]$ the pseudo $m\Theta$ $\mathbb{F}_{p^k\mathbb{Z}}$ -algebra of $m\Theta$ polynomials over $\mathbb{F}_{p^k\mathbb{Z}}$ in m variables.

We consider the $m\Theta$ morphism $\mathbb{F}_{p^k\mathbb{Z}}$ -algebras $\varphi^\Theta : \mathbb{F}_{p^k\mathbb{Z}}[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m^{ps\Theta}$ which associates to $P \in \mathbb{A}^m(\mathbb{F}_{p^k\mathbb{Z}})$ the $m\Theta$ function $f^\Theta \in \mathbb{B}_m^{ps\Theta}$ such that:

$$\forall X = (X_1, \dots, X_m) \in \mathbb{F}_{p^k\mathbb{Z}}^m, \quad f^\Theta(X) = P(X_1, \dots, X_m)$$

So, for each $f \in \mathbb{B}_m^{ps\Theta}$, there exists a unique $m\Theta$ polynomial $P \in \mathbb{A}^m(\mathbb{F}_{p^k\mathbb{Z}})$ such that the degree of P in each variable is at most $p^{k+1} - 1$ and $\varphi^\Theta(P) = f^\Theta$.

Definition 0.5. (*pseudo $m\Theta$ Generalized Reed-Muller codes*)

For $0 \leq r \leq m(p^{k+1} - 1)$, the r th order pseudo $m\Theta$ generalized Reed-Muller code of length $p^{m(k+1)}$ is:

$$RM_{p^k}^\Theta(r, m) := \{(f^\Theta(P_0), \dots, f^\Theta(P_{n-1})) / f^\Theta \in \mathbb{F}_{p^k\mathbb{Z}}[X_1, X_2, \dots, X_m], \deg(f^\Theta) \leq r\}$$

Thus by definition, $\forall P \in \mathbb{A}^m(\mathbb{F}_{p\mathbb{Z}})$

$$\varphi^\Theta(P) = \begin{cases} \varphi(P) & \text{if } P \in \mathbb{A}^m(\mathbb{F}_p) \\ 1_{p\mathbb{Z}}\varphi(s(P)) & \text{if not} \end{cases}$$

We consider now the $m\Theta$ -morphism of $\mathbb{F}_{p\mathbb{Z}}$ -algebras $\varphi^\Theta : \mathbb{F}_{p\mathbb{Z}}[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m^\Theta$ which associates to $P \in \mathbb{A}^m(\mathbb{F}_{p\mathbb{Z}})$ the $m\Theta$ function $f^\Theta \in \mathbb{B}_m^\Theta$ such that:

$$\forall X = (X_1, \dots, X_m) \in \mathbb{F}_{p\mathbb{Z}}^m, \quad f^\Theta(X) = P(X_1, \dots, X_m)$$

The $m\Theta$ morphism φ^Θ is onto and its kernel is the ideal generated by the polynomials $X_1^{p^2} - X_1, \dots, X_m^{p^2} - X_m$.

So, for each $f \in \mathbb{B}_m^\Theta$, there exists a unique $m\Theta$ polynomial $P \in \mathbb{A}^m(\mathbb{F}_{p\mathbb{Z}})$ such that the degree of P in each variable is at most $p^2 - 1$ and $\varphi^\Theta(P) = f^\Theta$.

The support of f^Θ is the set $\{X \in \mathbb{F}_{p\mathbb{Z}}^m : f^\Theta(X) \neq 0\}$ and we denote by $|f^\Theta|$ the cardinal of its support, and is the $m\Theta$ Hamming weight of f^Θ .

Definition 0.4. (*$m\Theta$ Generalized Reed-Muller codes*)

For $0 \leq r \leq m(p^2 - 1)$, the r th order $m\Theta$ generalized Reed-Muller code of length p^{2m} is:

$$RM_p^\Theta(r, m) := \{(f^\Theta(P_0), \dots, f^\Theta(P_{n-1})) / f^\Theta \in \mathbb{F}_{p\mathbb{Z}}[X_1, X_2, \dots, X_m], \deg(f^\Theta) \leq r\}$$

Observation:

$\mathbb{F}_{p\mathbb{Z}}$ is a $m\Theta$ field. Let p^k be a power of a prime number p . We saw in section 2 that $\mathbb{F}_{p^k\mathbb{Z}}$ is not a $m\Theta$ field. Now, we want to define a generalized Reed-Muller codes on $\mathbb{F}_{p^k\mathbb{Z}}$.

Let p be a prime number, k a positive integer and $\mathbb{F}_{p^k\mathbb{Z}}$ a pseudo $m\Theta$ field ($m\Theta pf$). $\mathbb{F}_{p^k\mathbb{Z}}$ has p^{k+1} elements and is of characteristic p^k .

In this case, $\mathbb{B}_m^{ps\Theta}$ is the pseudo $m\Theta$ $\mathbb{F}_{p^k\mathbb{Z}}$ -algebra of the $m\Theta$ functions from $\mathbb{F}_{p^k\mathbb{Z}}^m$ to $\mathbb{F}_{p^k\mathbb{Z}}$ and by $\mathbb{F}_{p^k\mathbb{Z}}[X_1, \dots, X_m]$ the pseudo $m\Theta$ $\mathbb{F}_{p^k\mathbb{Z}}$ -algebra of $m\Theta$ polynomials over $\mathbb{F}_{p^k\mathbb{Z}}$ in m variables.

We consider the $m\Theta$ morphism $\mathbb{F}_{p^k\mathbb{Z}}$ -algebras $\varphi^\Theta : \mathbb{F}_{p^k\mathbb{Z}}[X_1, \dots, X_m] \longrightarrow \mathbb{B}_m^{ps\Theta}$ which associates to $P \in \mathbb{A}^m(\mathbb{F}_{p^k\mathbb{Z}})$ the $m\Theta$ function $f^\Theta \in \mathbb{B}_m^{ps\Theta}$ such that:

$$\forall X = (X_1, \dots, X_m) \in \mathbb{F}_{p^k\mathbb{Z}}^m, \quad f^\Theta(X) = P(X_1, \dots, X_m)$$

So, for each $f \in \mathbb{B}_m^{ps\Theta}$, there exists a unique $m\Theta$ polynomial $P \in \mathbb{A}^m(\mathbb{F}_{p^k\mathbb{Z}})$ such that the degree of P in each variable is at most $p^{k+1} - 1$ and $\varphi^\Theta(P) = f^\Theta$.

Definition 0.5. (*pseudo $m\Theta$ Generalized Reed-Muller codes*)

For $0 \leq r \leq m(p^{k+1} - 1)$, the r th order pseudo $m\Theta$ generalized Reed-Muller code of length $p^{m(k+1)}$ is:

$$RM_{p^k}^\Theta(r, m) := \{(f^\Theta(P_0), \dots, f^\Theta(P_{n-1})) / f^\Theta \in \mathbb{F}_{p^k\mathbb{Z}}[X_1, X_2, \dots, X_m], \deg(f^\Theta) \leq r\}$$

choose P and $P' \in \mathbb{A}^n(\mathbb{F}_{q\mathbb{Z}} \setminus \{0\})$ such that $Q = p^\Theta(P)$ and $Q' = p^\Theta(P')$. Then,

$$\begin{aligned} g^\Theta(Q) = g^\Theta(Q') &\iff g^\Theta \circ p^\Theta(P) = g^\Theta \circ p^\Theta(P') \\ &\iff \pi^\Theta \circ h^\Theta(P) = \pi^\Theta \circ h^\Theta(P') \end{aligned}$$

$\exists \lambda \in \mathbb{F}_p \setminus \{0\}$ such that $h^\Theta(P) = \lambda h^\Theta(P') = h^\Theta(\lambda P') \implies P = \lambda P'$. Hence $p^\Theta(P) = p^\Theta(\lambda P') = p^\Theta(P') \implies Q = Q'$.

Finally, for all $m\Theta$ injective linear map $h^\Theta : \mathbb{A}^n(\mathbb{F}_{q\mathbb{Z}} \setminus \{0\}) \longrightarrow \mathbb{A}^m(\mathbb{F}_{q\mathbb{Z}} \setminus \{0\})$ induces a $m\Theta$ projective map $g^\Theta : \mathbb{P}(\mathbb{F}_{q\mathbb{Z}}^n) \longrightarrow \mathbb{P}(\mathbb{F}_{q\mathbb{Z}}^m)$.

4. The properties of Reed-Muller Projective $m\Theta$ Codes

The most difficult parameter to calculate is the minimum distance. The

natural idea is to use the knowledge from the affine situation of the minimum distance of $RM_p^\Theta(r, m)$ codes. We start with some necessary notation and some lemmas.

Notation 0.1. If $F(X) = \sum c_{i_0 i_1 \dots i_m} X_0^{i_0} X_1^{i_1} \dots X_m^{i_m}$ is a polynomial in $\mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]$, denoted by $\bar{F}(X)$ the reduced form of $F(X)$, so the polynomial we get by in any term replacing any factor $X_j^{t_j}$, where $t_j = a(q-1) + b$, $0 < b \leq q-1$, with X_j^b .

If $M \subset \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]$ is any set of polynomials denote by \bar{M} the corresponding set of reduced polynomials. So, $\overline{\mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]}$ denotes the set of all reduced polynomials over \mathbb{F}_{q^Z} in the variables X_0, \dots, X_m . For F homogeneous, we denote by $Z(F)_{\mathbb{F}_{q^Z}}$, when \mathbb{F}_{q^Z} is clear from the context, the algebraic set of zeros of F in $\mathbb{P}^m(\mathbb{F}_{q^Z})$. The degree of $X = Z(F)_{\mathbb{F}_{q^Z}}$ is $\deg(X) = \deg(F)$.

Lemma 0.1. If $F(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]$ and $G(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h$ then

1. $F(P) = \bar{F}(P)$, for any $P \in \mathbb{A}^{m+1}(\mathbb{F}_{p^Z})$;
2. $G(P) = \bar{G}(P)$, for any $P \in \mathbb{P}^m(\mathbb{F}_{p^Z})$;
3. if $F(P) = 0$, for any $P \in \mathbb{A}^{m+1}(\mathbb{F}_{p^Z})$, then $\bar{F}(X) = 0$;
4. if $G(P) = 0$, for any $P \in \mathbb{P}^{m+1}(\mathbb{F}_{p^Z})$, then $\bar{G}(X) = 0$.

Proof 0.2. [6, 7]

Lemma 0.2. Let $F(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^r$ and $H(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^l$. Assume $F(P) = 0$, for all $P \in Z(H)_{\mathbb{F}_{q^Z}}$. Then there exists $\tilde{F}(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^r$ and $G(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^{r-1}$ such that

$$Z(F)_{\mathbb{F}_{q^Z}} = Z(\tilde{F})_{\mathbb{F}_{q^Z}} \quad \text{and} \quad \tilde{F} = HG.$$

Proof 0.3. Assume that $H(X) = X_0$. Let $F(X) = X_0 F_1(X) + F_2(X)$, where $F_2(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^r$ and $F_1(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^{r-1}$. We get that $\bar{F}_2(X) = 0$, such that $\bar{F}(X) = X_0 \bar{F}_1(X)$. Then $\tilde{F}(X) = X_0 F_1(X)$ has the desired properties.

If $H(X) \neq X_0$, then consider a \mathbb{F}_{q^Z} -linear bijective transformation ϕ that maps $H(X)$ into X_0 . Then write

$$\phi(\tilde{F}) = X_0 F_3(X),$$

$F_3(X) \in \mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^{r-1}$ and let $\tilde{F} = \phi^{-1}(\phi(\tilde{F})) = H\phi^{-1}(F_3)$.

Lemma 0.3. Let $P = (0, 0, \dots, 1, \omega_{j+1}, \dots, \omega_m) \in \mathbb{P}^m(\mathbb{F}_{q^Z})$, $0 \leq j \leq m$. For any s , $0 < s \leq q-1$, the polynomial

$$F_P^s(X) = X_j^s \prod_{i=0}^{j-1} (X_j^{q-1} - X_i^{q-1}) \cdot \prod_{i=j+1}^m (X_j^{q-1} - (X_i - \omega_i X_j)^{q-1})$$

is indicator function for P and of degree $d = s \bmod q - 1$.

The $(q^{m+1}-1)/(q-1)$ polynomials $\bar{F}_P^s(X)$ are a basis for $\overline{\mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^d}$, the set of homogeneous polynomials of degree d in reduced form, and any $H \in \overline{\mathbb{F}_{q^Z}[X_0, X_1, \dots, X_m]_h^d}$ is uniquely written as

$$H(X) = \sum_{P \in \mathbb{P}^m(\mathbb{F}_{q^Z})} H(P) \bar{F}_P^s(X). \quad (3)$$

Proof 0.4. $\bar{F}_P^s(Q) = 1$, if $Q = P$ and $\bar{F}_P^s(Q) = 0$, if $Q \neq P$, so $\bar{F}_P^s(X)$ is indicator function for P and $\bar{F}_P^s(X)$ is homogeneous of degree $m(q-1) + s = s \bmod (q-1)$. These functions are linearly independent and any $H \in \mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]_h^d$ can be written as (3).

Remark 0.2. Only PRM $m\Theta$ codes of degree $0 < r \leq m(q-1)$ are of any interest, since RM Projective $m\Theta$ codes of order $r \geq m(q-1)+1$ are trivial. Let $c = (c_1, c_2, \dots, c_m)$ be any word. Choose $F(X) \in \mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]_h^r$ such that

$$\bar{F}(X) = \sum_{P_i \in \mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})} c_i \bar{F}_{P_i}^s(X), \quad s = r \bmod (q-1).$$

Then $c_i = F(P_i)$, so c is a $m\Theta$ codeword and the $m\Theta$ code is trivial.

Lemma 0.4. Let $\mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]$ and $Q \in \mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$. Assume $\bar{F}(X)$ has degree $d \leq m(q-1)$ and $F(P) = 0$ for all $P \in \mathbb{P}^m \setminus Q$. Then $F(Q) = 0$.

Proof 0.5. Assume $F(Q) \neq 0$. Then $\lambda \bar{F}$ will be an indicator function for Q , $\lambda = F(Q)^{-1}$, and by previous lemma $\lambda \bar{F} = \bar{F}_P^s(X)$ for some s , $0 < s \leq q-1$. Now $\deg(\bar{F}_P^s(X)) > m(q-1)$ and we have a contradiction.

Now we are able to state and prove the main theorem.

Theorem 0.1. The Reed-Muller projective $m\Theta$ Reed-Muller code $PC_r(m, q\mathbb{Z})$, $1 \leq r \leq m(q-1)$, is an $[n, k, d]_{q\mathbb{Z}}$ code with

$$n = \frac{q^{m+1} - 1}{q - 1}, \quad k = \sum_{t=r \bmod q-1; 0 \leq t \leq r} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right);$$

$$d = (q-s)q^{m-r-1}.$$

where $r-1 = u(q-1) + s$, $0 \leq s < q-1$.

Proof 0.6. The length n is $(q^{m+1} - 1)/(q - 1)$ by definition.

To find the minimum distance we consider a $m\Theta$ codeword $c = (F(P_1), \dots, F(P_n))$ and $F(X) \in \mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]_h^r$ where $r-1 = u(q-1) + s$; $0 \leq s < q-1$, $r \leq m(q-1) + 1$.

We want to estimate the weight of c , i.e., the number of zeros of F , when F is evaluated in all points of the $m\Theta$ -dimensional projective space. If $|Z(F)_{\mathbb{F}_{q\mathbb{Z}}}|$ denotes the number of zeros of F in $\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$, the claim is

$$|Z(F)_{\mathbb{F}_{q\mathbb{Z}}}| = \frac{q^{m+1} - 1}{q - 1} \quad \text{or} \quad |Z(F)_{\mathbb{F}_{q\mathbb{Z}}}| \leq \frac{q^{m+1} - 1}{q - 1} - (q-s)q^{m-u-1}. \quad (4)$$

We will prove (4) by induction on m .

If $m = 1$ then $\deg(F) = s + 1$, $0 \leq s < q-1$, and on the projective line $\mathbb{P}^1(\mathbb{F}_{q\mathbb{Z}})$, F has at most $s+1$ zeros: If $P_\infty = (0, 1)$ is zero of F , then $F(1, X_1)$ has degree (in X_1) less than or equal to s .

Assume that (4) is correct for $m-1$ and consider now the case m : Consider $X = Z(F)_{\mathbb{F}_{q\mathbb{Z}}} \subseteq \mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$, the algebraic set of zeros of F , and let F be of degree r , where $r-1 \leq m(q-1)$, $r-1 = u(q-1) + s$, $0 \leq s < q-1$.

1. If $r - 1 = (m - 1)(q - 1) + s$, $0 \leq s < q - 1$ we would like to prove

$$|Z(F)_{\mathbb{F}_{q\mathbb{Z}}}| = \frac{q^{m+1} - 1}{q - 1} \text{ or } |Z(F)_{\mathbb{F}_{q\mathbb{Z}}}| \leq \frac{q^{m+1} - 1}{q - 1} - (q - s). \quad (5)$$

Assume that (5) is false, i.e., that $0 < |\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}}) \setminus X| = t < q - s$, and let $\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}}) \setminus X = \{P_1, P_2, \dots, P_t\}$. Let $G_i(X)$, $i = 1, \dots, t - 1$ be

linear polynomials defining $t - 1$ hyperplanes such that $G_i(P_j) = \delta_{ij}$, $i = 1, \dots, t - 1$; $j = 1, \dots, t$.

Then the polynomial $H(X) = F(X) \prod_{i=1}^{t-1} G_i(X)$ has degree $(m - 1)(q - 1) + s + t \leq m(q - 1)$ and $Z(H)_{\mathbb{F}_{q\mathbb{Z}}} = \mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}}) \setminus \{P_t\}$.

This contradicts Lemma 0.4.

2. If $r \leq (m - 1)(q - 1)$ consider the following two cases.

- Assume X does not contain (as a set of points) any hyperplane in $\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$. For any hyperplane π we can consider $Y = X \cap \pi$ as an algebraic set in $\mathbb{P}^{m-1}(\mathbb{F}_{q\mathbb{Z}})$ with $\deg(Y) = \deg(X)$. We observe that $\deg(Y) = \deg(X) = r \leq (m - 1)(q - 1)$, so by the induction hypothesis we have for all $\mathbb{F}_{q\mathbb{Z}}$ -hyperplanes π that

$$|X \cap \pi| \leq \frac{q^{m+1} - 1}{q - 1} - (q - s)q^{m-r-2}.$$

By counting pairs (P, π) , $P \in (\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}}) \setminus X) \cap \pi$, π a $\mathbb{F}_{q\mathbb{Z}}$ -hyperplane, in two different ways, we have

$$|\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}}) \setminus X| \cdot \frac{q^{m+1} - 1}{q - 1} \geq \frac{q^{m+1} - 1}{q - 1} (q - s)q^{m-r-2}; \quad (6)$$

since $(q^{m+1} - 1)/(q - 1)$ is the number of $\mathbb{F}_{q\mathbb{Z}}$ -hyperplanes in $\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$ through a fixed point and $(q^{m+1} - 1)/(q - 1)$ is the number of $\mathbb{F}_{q\mathbb{Z}}$ -hyperplanes in $\mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}})$.

Equation (6) gives $|\mathbb{P}^m \setminus X| \geq (q - s)q^{m-r-1}$; and we are done.

- Assume that X contains the set of points of a hyperplane $\pi = Z(H)$, $H(X) \in \mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]_h^1$. Then by lemma 0.2, we can assume that $X = Z(HF_1)$, $F_1(X) \in \mathbb{F}_{q\mathbb{Z}}[X_0, X_1, \dots, X_m]_h^{r-1}$. Let $X' = Z(F_1)$ and observe

$$|X| = |X' \setminus (X' \cap \pi)| + |\pi|. \quad (7)$$

Since $X' \setminus (X' \cap \pi) \subseteq \mathbb{P}^m(\mathbb{F}_{q\mathbb{Z}}) \setminus \pi \simeq \mathbb{A}^m(\mathbb{F}_{q\mathbb{Z}})$, $X' \setminus (X' \cap \pi)$ is an affine algebraic set, the zero set for some polynomial of degree $r - 1 = u(q - 1) + s$, then, if $\pi = Z(X_0)$, the polynomial defining $X' \setminus (X' \cap \pi)$ is $F_1(1, X_1, \dots, X_n)$ and $\deg(F_1) = r - 1$. Using a $\mathbb{F}_{q\mathbb{Z}}$ -linear coordinate transformation taking $H(X)$ to X_0 , the gen-

eral situation is reduced to this case.

We have seen that $X' \setminus (X' \cap \pi)$ corresponds to zeros of some polynomial of degree $r - 1 = u(q - 1) + s$. Using (2) we get

$$|X' \setminus (X' \cap \pi)| \leq q^m - (q - s)q^{m-r-1}. \quad (8)$$

Adding $|\pi|$ to (8) yields $|X| \leq \frac{q^{m+1}-1}{q-1} - (q - s)q^{m-r-1}$. This completes the proof of (4) and gives a lower bound $d \geq (q - s)q^{m-r-1}$. Equality follows since the polynomial

$$F(X) = X_r \prod_{i=0}^{r-1} (X_i^{q-1} - X_r^{q-1}) \prod_{j=1}^s (\lambda_j X_r - X_{r+1}),$$

where $\lambda_i \neq \lambda_j$ for $i \neq j$ and $\lambda_i \in \mathbb{F}_{q\mathbb{Z}}^*$, has zeros at all points except those of the form $(0, 0, \dots, 1, a_{r+1}, \dots, a_m)$, where $a_{r+1} \neq \lambda_j$, $j = 1, \dots, s$ and $a_t \in \mathbb{F}_{q\mathbb{Z}}$ for $t = r + 2, \dots, m$.

We see that there is exactly $(q - s)q^{m-r-1}$ such points, so F corresponds to a codeword of minimum distance d .

The dimension k of $PC_r(m, q)$ is found by combinatorial reasoning: It follows from Lemma 5 that

$$N(t, m + 1, q - 1) = \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t - jq + m}{t - jq}$$

is the number of distinct monomials in X_0, X_1, \dots, X_m of degree t , such that no reduction is possible.

Lemma 0.5. *The number of ways one can place t objects in m cells such that no cell contains more than s objects is*

$$N(t, m, s) = \sum_{j=0}^m (-1)^j \binom{m}{j} \binom{t - j(s+1) + m - 1}{t - j(s+1)}$$

Proof 0.7. $\binom{t+m-1}{t}$ is the number of ways one can place t objects in m cells without restrictions.

$\binom{t-j(s+1)+m-1}{t-j(s+1)}$ is the number of ways one can place t objects in m cells such that j cells contain at least $s + 1$ objects. The principle of exclusion and inclusion now gives the result.

Conclusion

In this paper, we have presented a modal Θ -valent approach of the Reed-Muller Projective $m\Theta$ codes. The construction of the parameters of these codes requires the notion of a $m\Theta$ Generalized Reed-Muller Codes, chrysippian $m\Theta$ representation of $GF(p\mathbb{Z}, r)$, the classical theory of Projective Reed-

Muller codes. The length of Reed-Muller projective $m\Theta$ codes grows exponentially with the code order m , allowing for the construction of very large codes; this makes them interesting candidates for applications requiring high storage or transmission capacity. The high minimum weight of Reed-Muller projective $m\Theta$ codes gives them good error detection and correction capabilities; This makes them robust to perturbations and suitable for applications sensitive to errors.

While their parameters are attractive, Reed-Muller projective $m\Theta$ codes do not always achieve the best coding performance compared to other code families; a tradeoff may sometimes need to be made between performance and complexity.

References

1. Tsimi, J. A., & Pemha, G. (2021). On the generalized modal Θ -valent Reed-Muller codes. *Journal of Information and Optimization Sciences*, 42(8), 1885-1906.
2. Ayissi Eteme, F. (1984). Anneau chrysippien Θ -valent. *Comptes Rendus de l'Académie des Sciences, Paris*, 298(1), 1-4.
3. Ayissi Eteme, F. (2009). Logique et algèbre de structure mathématiques modales Θ -valentes chrysippiennes. *Hermann*.

4. Eteme, F. A., & Tsimi, J. A. (2011). A modal Θ -valent approach of the notion of code. *Journal of Discrete Mathematical Sciences and Cryptography*, 14, 445-473.
5. Ayissi Eteme, F. (2015). *Chrm Θ introducing pure and applied mathematics*. Lambert Academic Publishing.
6. Lang, S. (1965). *Algebra*. Addison-Wesley
7. Weldon, E. J. (1968). New generalizations of the Reed-Muller codes—Part II: Nonprimitive codes. *IEEE Transactions on Information Theory*, 14(2).
8. Tsimi, J. A., & Youdom, R. (2021). The modal Θ -valent extensions of BCH codes. *Journal of Information and Optimization Sciences*.
9. Kasami, T., Lin, S., & Peterson, W. W. (1968). New generalizations of the Reed-Muller codes. Part I: Primitive codes. *IEEE Transactions on Information Theory*, 14(2), 189-199.
10. Lachaud, G. (1990). The parameters of projective Reed-Muller codes. *Luminy Case* 916, 217-221.
11. Pellikaan, R., & Wu, X.-W. (2004). List decoding of q -ary Reed-Muller codes. *Chinese Academy of Sciences*, 679-682.