

The Generalized Reed-Muller codes and the radical powers of a modular algebra

Harinaivo Andriatahiny*

Mention: Mathematics and Computer Science, Domain: Sciences and Technologies, P.O.B. 906,
University of Antananarivo, 101 Antananarivo, Madagascar

**Original Research
Article**

Abstract

S.D. Berman and P. Charpin characterized the Reed-Muller codes over the binary field or over an arbitrary prime field as the powers of the radical in a modular group algebra. We present a new proof of this famous theorem. Furthermore, the same method is used for the study of the Generalized Reed-Muller codes over a non prime field.

Keywords: Generalized Reed-Muller codes; modular algebra; nilpotent radical; interpolation function.
2010 Mathematics Subject Classification: 16N40; 94B05; 12E05

1 Introduction

S.D. Berman [4] showed that the binary Reed-Muller codes may be identified with the powers of the radical in the group algebra over the two elements field $\mathbb{F}_2$ of an elementary abelian 2-group.

P. Charpin [6] gave a generalization of Berman's result for Reed-Muller codes over a prime field.

Many authors explored Berman's idea and gave another proofs of Berman's theorem (see [2],[9]).

Recently, I.N. Tumaikin [11][12] studied the connections between Basic Reed-Muller codes and the radical powers of the modular group algebra $\mathbb{F}_q[H]$ where H is a multiplicative group isomorphic to the additive group of the field $\mathbb{F}_q$ of order $q = p^r$ where p is a prime number and r is an integer. The index of nilpotency of the radical of $\mathbb{F}_q[H]$ is $r(p-1) + 1$.

This paper presents an elementary proof of Berman and Charpin's characterization of the Reed-Muller codes by using a polynomial approach.

The quotient ring $\mathbb{F}_p[X_1, \dots, X_m] / (X_1^p - 1, \dots, X_m^p - 1)$ where $m \geq 1$ is an integer is used to represent the ambient space of the codes. It is isomorphic to the group algebra $\mathbb{F}_p[\mathbb{F}_{p^m}]$ used by P. Charpin. We utilize some properties of a linear basis of the ambient space.

We study also the case of the Generalized Reed-Muller (GRM) codes over a non prime field $\mathbb{F}_q$ (with $r > 1$). We consider the quotient ring

$$A = \mathbb{F}_q[X_1, \dots, X_m] / (X_1^q - 1, \dots, X_m^q - 1).$$

*Corresponding author: E-mail: harinaivo.andriatahiny@univ-antananarivo.mg

A is a modular algebra and the index of nilpotency of the radical M of A is $m(q-1)+1$. Thus there are $m(q-1)+1$ non-zero powers of M (with $M^0 = A$). It is well-known that there are also $m(q-1)+1$ non-zero Reed-Muller codes of length q^m over $\mathbb{F}_q$. The main result is Theorem 3.6 which gives the GRM codes over a non prime field $\mathbb{F}_q$ which are radical powers of A . We show that except for M^0 , M and $M^{m(q-1)}$, none of the radical powers of A is a GRM code over the non prime field $\mathbb{F}_q$.

2 Definitions and Basic Properties

2.1 Definitions

Let $q = p^r$ with p a prime number and $r \geq 1$ an integer. We consider the finite field $\mathbb{F}_q$ of order q . Let $P(m, q)$ be the vector space of the reduced polynomials in m variables over $\mathbb{F}_q$:

$$P(m, q) := \left\{ P(Y_1, \dots, Y_m) = \sum_{i_1=0}^{q-1} \cdots \sum_{i_m=0}^{q-1} u_{i_1 \dots i_m} Y_1^{i_1} \cdots Y_m^{i_m} \mid u_{i_1 \dots i_m} \in \mathbb{F}_q \right\}. \quad (2.1)$$

The polynomial functions from $(\mathbb{F}_q)^m$ to $\mathbb{F}_q$ are given by the polynomials of $P(m, q)$.

Let ν be an integer such that $0 \leq \nu \leq m(q-1)$. Consider the subspace of $P(m, q)$ defined by

$$P_\nu(m, q) := \{P(Y_1, \dots, Y_m) \in P(m, q) \mid \deg(P(Y_1, \dots, Y_m)) \leq \nu\}$$

where $\deg(P(Y_1, \dots, Y_m))$ is the total degree of $P(Y_1, \dots, Y_m)$.

Consider the ideal $I = (X_1^q - 1, \dots, X_m^q - 1)$ of the ring $\mathbb{F}_q[X_1, \dots, X_m]$.

Set $x_1 = X_1 + I, \dots, x_m = X_m + I$. Then

$$A = \left\{ \sum_{i_1=0}^{q-1} \cdots \sum_{i_m=0}^{q-1} a_{i_1 \dots i_m} x_1^{i_1} \cdots x_m^{i_m} \mid a_{i_1 \dots i_m} \in \mathbb{F}_q \right\}. \quad (2.2)$$

Let us fix an order on the set of monomials

$$\{x_1^{i_1} \cdots x_m^{i_m} \mid 0 \leq i_1, \dots, i_m \leq q-1\}.$$

Then we have the following important remark:

Remark 2.1. Each element $\sum_{i_1=0}^{q-1} \cdots \sum_{i_m=0}^{q-1} a_{i_1 \dots i_m} x_1^{i_1} \cdots x_m^{i_m}$ of A can be identified with the vector $(a_{i_1 \dots i_m})_{0 \leq i_1, \dots, i_m \leq q-1}$ of $(\mathbb{F}_q)^{q^m}$ and vice-versa. Hence the modular algebra A is identified with $(\mathbb{F}_q)^{q^m}$.

Let α be a primitive element of the finite field $\mathbb{F}_q$. It is clear that $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$. Set

$$\beta_0 = 0 \quad \text{and} \quad \beta_i = \alpha^{i-1} \quad \text{for} \quad 1 \leq i \leq q-1. \quad (2.3)$$

When considering $P(m, q)$ and A as vector spaces over $\mathbb{F}_q$, we have the following isomorphism:

$$\begin{aligned} \phi: P(m, q) &\longrightarrow A \\ P(Y_1, \dots, Y_m) &\longmapsto \sum_{i_1=0}^{q-1} \cdots \sum_{i_m=0}^{q-1} P(\beta_{i_1}, \dots, \beta_{i_m}) x_1^{i_1} \cdots x_m^{i_m} \end{aligned} \quad (2.4)$$

We give the definition of the Generalized Reed-Muller codes as formulated in [5].

Definition 2.1. The Generalized Reed-Muller code of length q^m and of order ν ($0 \leq \nu \leq m(q-1)$) over $\mathbb{F}_q$ is defined by

$$C_\nu(m, q) := \{(P(\beta_{i_1}, \dots, \beta_{i_m}))_{0 \leq i_1, \dots, i_m \leq q-1} \mid P(Y_1, \dots, Y_m) \in P_\nu(m, q)\}. \quad (2.5)$$

It is a subspace of $(\mathbb{F}_q)^{q^m}$ and we have the following ascending sequence:

$$\{0\} \subset C_0(m, q) \subset C_1(m, q) \subset \cdots \subset C_{m(q-1)-1}(m, q) \subset C_{m(q-1)}(m, q) = (\mathbb{F}_q)^{q^m} \quad (2.6)$$

2.2 Some properties of the ambient space

The ambient space A is a local ring with maximal ideal M which is the radical of A , i.e. $M = \text{Rad}(A)$. Let d be an integer such that $0 \leq d \leq m(q-1)$. Consider the powers M^d of M . A linear basis of M^d over $\mathbb{F}_q$ is

$$B_d := \left\{ (x_1 - 1)^{i_1} \dots (x_m - 1)^{i_m} \mid 0 \leq i_1, \dots, i_m \leq q-1, i_1 + \dots + i_m \geq d \right\} \quad (2.7)$$

We have the following ascending sequence of ideals:

$$\{0\} = M^{m(q-1)+1} \subset M^{m(q-1)} \subset \dots \subset M^2 \subset M \subset A \quad (2.8)$$

We need the following notation:

Notation 2.1. Set $[0, q-1] = \{0, 1, 2, \dots, q-1\}$,
 $\underline{i} := (i_1, \dots, i_m) \in ([0, q-1])^m$,
 $|\underline{i}| := i_1 + \dots + i_m$,
 $\underline{j} \leq \underline{i}$ if $j_l \leq i_l$ for all $l = 1, 2, \dots, m$ where $\underline{j} := (j_1, \dots, j_m) \in ([0, q-1])^m$,
 $\underline{x} := (x_1, \dots, x_m)$,
 $\underline{x}^{\underline{i}} := x_1^{i_1} \dots x_m^{i_m}$.

Consider the polynomial

$$B_{\underline{i}}(\underline{x}) := (x_1 - 1)^{i_1} \dots (x_m - 1)^{i_m}. \quad (2.9)$$

Proposition 2.1. Considering the sequences (2.6) and (2.8), we have

$$\dim_{\mathbb{F}_q}(M^d) = \dim_{\mathbb{F}_q}(C_{m(q-1)-d}(m, q))$$

for $0 \leq d \leq m(q-1)$ where $\dim_{\mathbb{F}_q}(M^d)$ is the dimension of the vector space M^d over $\mathbb{F}_q$.

Proof. Consider the set $E := \{\underline{i} \in ([0, q-1])^m \mid |\underline{i}| \geq d\}$.

Since $B_d = \{B_{\underline{i}}(\underline{x}) \mid |\underline{i}| \geq d\}$ is a basis of M^d , then $\dim_{\mathbb{F}_q}(M^d) = \text{Card}(E)$ where $\text{Card}(E)$ denotes the number of elements in the set E .

Consider the set $F := \{\underline{i} \in ([0, q-1])^m \mid |\underline{i}| \leq m(q-1) - d\}$.

We have $\dim_{\mathbb{F}_q}(C_{m(q-1)-d}(m, q)) = \dim_{\mathbb{F}_q}(P_{m(q-1)-d}(m, q)) = \text{Card}(F)$.

The mapping

$$\begin{aligned} \theta : ([0, q-1])^m &\longrightarrow ([0, q-1])^m \\ (i_1, \dots, i_m) &\longmapsto (q-1-i_1, \dots, q-1-i_m) \end{aligned}$$

is a bijection and the inverse mapping is $\theta^{-1} = \theta$.

Let $\underline{i} \in E$. Then $|\underline{i}| \geq d$, and $|\theta(\underline{i})| = m(q-1) - |\underline{i}| \leq m(q-1) - d$. Hence $\theta(\underline{i}) \in F$. And it follows that $\theta(E) \subseteq F$.

Conversely, let $\underline{i} \in F$. Then $|\underline{i}| \leq m(q-1) - d$, and $|\theta(\underline{i})| = m(q-1) - |\underline{i}| \geq d$. So $\theta(\underline{i}) \in E$. Note that $\theta(\theta(\underline{i})) = \underline{i}$. Thus $F \subseteq \theta(E)$.

Therefore, $F = \theta(E)$ and $\text{Card}(E) = \text{Card}(F)$. $\square$

It is clear that

$$(x_l - 1)^{i_l} = \sum_{j=0}^{i_l} (-1)^{i_l-j} \binom{i_l}{j} x_l^j \quad (2.10)$$

for all $l = 1, 2, \dots, m$.

Let $\beta_k \in \mathbb{F}_q$ as in (2.3). Consider the indicator function

$$F_{\beta_k}(Y_l) = 1 - (Y_l - \beta_k)^{q-1} \quad (2.11)$$

with $1 \leq l \leq m$.

Then $F_{\beta_k}(Y_l) \in P(m, q)$ and

$$F_{\beta_k}(\beta_j) = \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

Consider the interpolation function

$$H_{i_l}(Y_l) := \sum_{k=0}^{i_l} (-1)^{i_l-k} \binom{i_l}{k} F_{\beta_k}(Y_l). \quad (2.12)$$

We have $H_{i_l}(Y_l) \in P(m, q)$,

$$H_{i_l}(\beta_j) = \begin{cases} (-1)^{i_l-j} \binom{i_l}{j} & \text{if } 0 \leq j \leq i_l, \\ 0 & \text{if } i_l < j \leq q-1 \end{cases}$$

and

$$(x_l - 1)^{i_l} = \sum_{j=0}^{i_l} H_{i_l}(\beta_j) x_l^j. \quad (2.13)$$

Set

$$H_{\underline{i}}(\underline{Y}) := \prod_{l=1}^m H_{i_l}(Y_l). \quad (2.14)$$

Thus

$$\deg(H_{\underline{i}}(\underline{Y})) = \sum_{l=1}^m \deg(H_{i_l}(Y_l)). \quad (2.15)$$

Proposition 2.2. We have $H_{\underline{i}}(\underline{Y}) = \phi^{-1}(B_{\underline{i}}(\underline{x}))$, where ϕ is the isomorphism defined in (2.4), i.e.

$$B_{\underline{i}}(\underline{x}) = \sum_{\underline{j} \leq \underline{i}} H_{\underline{i}}(\beta_{j_1}, \dots, \beta_{j_m}) \underline{x}^{\underline{j}}$$

Proof.

$$\begin{aligned} B_{\underline{i}}(\underline{x}) &= \prod_{l=1}^m (x_l - 1)^{i_l} \\ &= \prod_{l=1}^m \left(\sum_{j_l=0}^{i_l} H_{i_l}(\beta_{j_l}) x_l^{j_l} \right) \\ &= \sum_{\underline{j} \leq \underline{i}} \left(\prod_{l=1}^m H_{i_l}(\beta_{j_l}) \right) \underline{x}^{\underline{j}} \\ &= \sum_{\underline{j} \leq \underline{i}} H_{\underline{i}}(\beta_{j_1}, \dots, \beta_{j_m}) \underline{x}^{\underline{j}}. \end{aligned}$$

□

3 Main Results

3.1 Generalized Reed-Muller codes over a prime field

Here, we give a new proof for the Berman and Charpin's result. We consider the case $r = 1$, i.e. $q = p$ a prime number and $\mathbb{F}_q = \mathbb{F}_p$ a prime field.

Let $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ and set $\beta_k = k$ for all $k = 0, 1, \dots, p-1$.

Let us study $(x-1)^i$ for $0 \leq i \leq p-1$ over $\mathbb{F}_p$.

We have

$$(x-1)^i = \sum_{j=0}^i (-1)^{i-j} \binom{i}{j} x^j.$$

For $k \in \mathbb{F}_p$, according to (2.1), we have

$$F_k(Y) = 1 - (Y-k)^{p-1} = - \prod_{j=0(j \neq k)}^{p-1} (Y-j) \in P(1, p)$$

and

$$F_k(j) = \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

Let us consider the interpolation function

$$H_i(Y) := \sum_{k=0}^i (-1)^{i-k} \binom{i}{k} F_k(Y) \quad (3.1)$$

which is in $P(1, p)$.

Thus, $H_i(j) = (-1)^{i-j} \binom{i}{j}$ for $0 \leq j \leq i$

and

$$(x-1)^i = \sum_{j=0}^i H_i(j) x^j.$$

Proposition 3.1. An explicit expression of $H_i(Y)$ is

$$H_i(Y) = \alpha_i \prod_{j=1}^{p-1-i} (Y+j),$$

where $\alpha_i = -i! \bmod p$.

Proof. As

$$(x-1)^i = \sum_{k=0}^i (-1)^{i-k} \binom{i}{k} x^k,$$

we have

$$H_i(k) = \begin{cases} (-1)^{i-k} \binom{i}{k} & \text{if } 0 \leq k \leq i. \\ 0 & \text{if } i+1 \leq k \leq p-1. \end{cases} \quad (3.2)$$

Therefore, $H_i(Y)$ may be written as

$$H_i(Y) = P_i(Y) \prod_{j=1}^{p-1-i} (Y+j), \quad (3.3)$$

where $P_i(Y)$ is a polynomial of degree less or equal to i .

For $Y = k$ in (3.3) with $0 \leq k \leq i$ and using (3.2), we get

$$\begin{aligned} (-1)^{i-k} \binom{i}{k} &= P_i(k)(k+1) \dots (k+p-1-i), \\ (-1)^{i-k} \frac{i!}{k!(i-k)!} &= P_i(k) \frac{(k+p-1-i)!}{k!}. \end{aligned}$$

As

$$(i - k)! = (-1)^{i-k} (p - 1) \dots (p - i + k) \bmod p,$$

we get

$$i! = P_i(k)(p - 1)!$$

and because $(p - 1)! = -1 \bmod p$ by the Wilson lemma, $P_i(k) = \alpha_i$ for $0 \leq k \leq i$. Therefore $P_i(Y)$ is a constant polynomial equal to α_i that achieves the proof. $\square$

Corollary 3.1.

$$\deg(H_i(Y)) = p - 1 - i.$$

Remark 3.1. Polynomials $H_i(Y)$, $0 \leq i \leq p - 1$, satisfy the backward recurrence relation

$$\begin{aligned} H_{p-1}(Y) &= 1, \\ H_i(Y) &= \frac{1}{i+1} (Y - i - 1) H_{i+1}(Y) \quad , \quad 0 \leq i \leq p - 2. \end{aligned}$$

It is clear that in this section, the Proposition 2.2 become

$$B_{\underline{i}}(\underline{x}) = \sum_{\underline{j} \leq \underline{i}} H_{\underline{i}}(\underline{j}) \underline{x}^{\underline{j}} \quad (3.4)$$

The following Theorem is well-known (see [4],[6]).

Theorem (Berman-Charpin) 3.2. Let $C_\nu(m, p)$ be the Reed-Muller code of length p^m and of order ν ($0 \leq \nu \leq m(p - 1)$) over the prime field $\mathbb{F}_p$ and M the radical of $\mathbb{F}_p[X_1, \dots, X_m] / (X_1^p - 1, \dots, X_m^p - 1)$. Then

$$C_\nu(m, p) = M^{m(p-1)-\nu}.$$

Proof. Set $d := m(p - 1) - \nu$. The set $B_d = \{B_{\underline{i}}(\underline{x}) \mid |\underline{i}| \geq d\}$ is a linear basis of M^d over $\mathbb{F}_p$. Consider $B_{\underline{i}}(\underline{x}) = \sum_{\underline{j} \leq \underline{i}} H_{\underline{i}}(\underline{j}) \underline{x}^{\underline{j}} \in M^d$. By (2.15) and Corollary 3.1, we have $\deg(H_{\underline{i}}(\underline{Y})) = \sum_{l=1}^m p - 1 - i_l = m(p - 1) - |\underline{i}| \leq m(p - 1) - d = \nu$. It follows from Remark 2.1 and (2.5) that $B_{\underline{i}}(\underline{x}) \in C_\nu(m, p)$. Thus $M^d \subseteq C_\nu(m, p)$. Moreover, if we take $r = 1$ in Proposition 2.1, we have $\dim_{\mathbb{F}_p}(M^d) = \dim_{\mathbb{F}_p}(C_\nu(m, p))$. $\square$

3.2 Binomial function over a finite field

In this subsection, we examine some properties of $(x - 1)^i$, $0 \leq i \leq q - 1$, over an arbitrary finite field $\mathbb{F}_q$ where $q = p^r$ with p a prime number and $r \geq 1$ an integer.

We have already seen from (2.13), (2.12) and (2.11) of Section 2 that

$$(x - 1)^i = \sum_{j=0}^i H_i(\beta_j) x^j \quad , \quad 0 \leq i \leq q - 1$$

where

$$H_i(Y) := \sum_{k=0}^i (-1)^{i-k} \binom{i}{k} F_{\beta_k}(Y) \quad , \quad 0 \leq i \leq q - 1 \quad (3.5)$$

and

$$F_{\beta_k}(Y) = 1 - (Y - \beta_k)^{q-1}.$$

Lemma 3.3.

$$\binom{p^r - 1}{d} = (-1)^d \bmod p$$

where p is a prime number, $r \geq 1$ an integer and $0 \leq d \leq p^r - 1$.

Proof. It can be proved easily by induction on d . □

The following proposition is fundamental.

Proposition 3.2. *The interpolation function (3.5) satisfies the relation*

$$H_i(Y) = \sum_{d=1}^{q-1} \alpha^{-d} \left[(-1)^i - (\alpha^d - 1)^i \right] Y^{q-1-d}$$

where α is a primitive element of $\mathbb{F}_q$ and $1 \leq i \leq q-1$.

Proof. We have

$$\begin{aligned} H_i(Y) &= \sum_{k=0}^i (-1)^{i-k} \binom{i}{k} F_{\beta_k}(Y) \\ &= \sum_{k=0}^i (-1)^{i-k} \binom{i}{k} [1 - (Y - \beta_k)^{q-1}] \\ &= (-1)^i (1 - Y^{q-1}) + \sum_{k=1}^i (-1)^{i-k} \binom{i}{k} [1 - (Y - \beta_k)^{q-1}] \\ &= (-1)^i (1 - Y^{q-1}) + \sum_{k=1}^i (-1)^{i-k} \binom{i}{k} - \sum_{k=1}^i (-1)^{i-k} \binom{i}{k} (Y - \beta_k)^{q-1}. \end{aligned}$$

Since

$$(Y - \beta_k)^{q-1} = \sum_{d=0}^{q-1} (-1)^d (\beta_k)^d \binom{q-1}{d} Y^{q-1-d}$$

and by Lemma 3.3, we have

$$(Y - \beta_k)^{q-1} = \sum_{d=0}^{q-1} (\beta_k)^d Y^{q-1-d}.$$

Thus, by (2.3),

$$\begin{aligned} H_i(Y) &= (-1)^i (1 - Y^{q-1}) + \sum_{k=1}^i (-1)^{i-k} \binom{i}{k} \\ &\quad - \sum_{k=1}^i (-1)^{i-k} \binom{i}{k} \left[\sum_{d=0}^{q-1} (\alpha^{k-1})^d Y^{q-1-d} \right] \\ &= (-1)^i (1 - Y^{q-1}) + \sum_{k=1}^i (-1)^{i-k} \binom{i}{k} \\ &\quad - \sum_{d=0}^{q-1} \left(\sum_{k=1}^i (-1)^{i-k} \binom{i}{k} (\alpha^{k-1})^d \right) Y^{q-1-d}. \end{aligned}$$

Since

$$\sum_{k=1}^i (-1)^{i-k} \binom{i}{k} = (-1)^{i+1}$$

then

$$\begin{aligned}
 H_i(Y) &= (-1)^i - (-1)^i Y^{q-1} - (-1)^i - \left(\sum_{k=1}^i (-1)^{i-k} \binom{i}{k} \right) Y^{q-1} \\
 &\quad - \sum_{d=1}^{q-1} \left(\sum_{k=1}^i (-1)^{i-k} \binom{i}{k} (\alpha^{k-1})^d \right) Y^{q-1-d} \\
 &= - \sum_{d=1}^{q-1} \left(\sum_{k=1}^i (-1)^{i-k} \binom{i}{k} (\alpha^{k-1})^d \right) Y^{q-1-d} \\
 &= - \sum_{d=1}^{q-1} \alpha^{-d} \left(\sum_{k=1}^i (-1)^{i-k} \binom{i}{k} (\alpha^k)^d \right) Y^{q-1-d} \\
 &= - \sum_{d=1}^{q-1} \alpha^{-d} \left[\sum_{k=0}^i (-1)^{i-k} \binom{i}{k} (\alpha^k)^d - (-1)^i \right] Y^{q-1-d} \\
 &= - \sum_{d=1}^{q-1} \alpha^{-d} \left[(\alpha^d - 1)^i - (-1)^i \right] Y^{q-1-d} \\
 &= \sum_{d=1}^{q-1} \alpha^{-d} \left[(-1)^i - (\alpha^d - 1)^i \right] Y^{q-1-d}.
 \end{aligned}$$

□

Corollary 3.4. 1. $H_1(Y) = - \sum_{d=0}^{q-2} Y^d$.

2. $H_2(Y) = - \sum_{k=0}^{q-2} (2 - \alpha^{-k}) Y^k$.

3. $H_{q-1}(Y) = 1$.

Remark 3.2. $H_0(Y) = F_{\beta_0}(Y) = F_0(Y) = 1 - Y^{q-1}$.

The next corollary is important to what follows.

Corollary 3.5. If $\mathbb{F}_q$ is a non prime field, then we have

$$\deg(H_{q-2}(Y)) = q - 2.$$

Proof. In Proposition 3.2, for $i = q - 2$, the coefficient of Y^{q-2} is $\alpha^{-1} [(-1)^{q-2} - (\alpha - 1)^{q-2}]$. If $(\alpha - 1)^{q-2} = (-1)^{q-2}$, then $(\alpha - 1)^{q-1} = (-1)^{q-2}(\alpha - 1)$. Since α is a primitive element of $\mathbb{F}_q$, then $\alpha \neq 1$ and $(\alpha - 1)^{q-1} = 1$. Thus $1 = (-1)^{q-2}\alpha + (-1)^{q-1}$, and $(-1)^{q-2}\alpha = 0$. hence, $\alpha = 0$. This is a contradiction. □

3.3 Main Theorem

Bearing in mind the Remark 2.1, we have our main theorem:

Theorem 3.6. Let $C_\nu(m, q)$ be the Generalized Reed-Muller code of length q^m ($m \geq 1$ an integer) and of order ν ($0 \leq \nu \leq m(q - 1)$) over a non prime field $\mathbb{F}_q$ and $M = \text{Rad}(A)$ where $A = \mathbb{F}_q[X_1, \dots, X_m] / (X_1^q - 1, \dots, X_m^q - 1)$. Then

- (i)- $M^{m(q-1)} = C_0(m, q)$, $M = C_{m(q-1)-1}(m, q)$ and $M^0 = C_{m(q-1)}(m, q)$
- (ii)- $M^i \neq C_{m(q-1)-i}(m, q)$ for all i such that $2 \leq i \leq m(q - 1) - 1$.

Proof. Since $\mathbb{F}_q$ is a non prime field then $q \geq 4$.

(i)-(a)- $M^{m(q-1)}$ is linearly generated over $\mathbb{F}_q$ by $B_{(q-1, \dots, q-1)}(\underline{x}) = \tilde{1}$ the “all one word”. By (2.15) and Corollary 3.4, we have $\deg(H_{(q-1, \dots, q-1)}(\underline{Y})) = 0$. It follows from Proposition 2.2, Remark 2.1 and (2.5) that $B_{(q-1, \dots, q-1)}(\underline{x}) \in C_0(m, q)$. Thus $M^{m(q-1)} \subseteq C_0(m, q)$. And by Proposition 2.1, we have

$$\dim_{\mathbb{F}_q}(M^{m(q-1)}) = \dim_{\mathbb{F}_q}(C_0(m, q)).$$

(b)- Consider $B_{\underline{i}}(\underline{x}) := (x_1 - 1)^{i_1} \dots (x_m - 1)^{i_m} \in M$. There is an integer l such that $1 \leq l \leq m$ and $i_l \geq 1$. By Proposition 3.2, $\deg(H_{i_l}(Y)) \leq q - 2$. And we have $\deg(H_i(Y)) \leq q - 1$ for all $i \neq i_l$. So $\deg(H_{\underline{i}}(\underline{Y})) \leq q - 2 + (m - 1)(q - 1) = m(q - 1) - 1$. Thus $B_{\underline{i}}(\underline{x}) \in C_{m(q-1)-1}$. This implies that $M \subseteq C_{m(q-1)-1}(m, q)$, and by Proposition 2.1, the equality holds.

(c)- It is obvious because $C_{m(q-1)}(m, q) \subseteq A = M^0$ and the Proposition 2.1 give the result.

(ii)- Consider the following sequence:

$$\begin{aligned} \{0\} &\subset M^{m(q-1)} \subset M^{m(q-1)-1} \subset \dots \subset M^{m(q-1)-(q-2)+1} \subset M^{m(q-1)-(q-2)} \\ &\subset \dots \subset M^{m(q-1)-2(q-2)+1} \subset \dots \subset M^{m(q-1)-(m-1)(q-2)} \subset \dots \\ &\subset M^{m(q-1)-m(q-2)+1} \subset M^m \subset M^{m-1} \subset M^{m-2} \subset \dots \subset M^2 \subset M \subset A. \end{aligned}$$

For simplicity, let us proceed step by step:

Step one:

- $M^{m(q-1)-1}$ is linearly generated over $\mathbb{F}_q$ by the $B_{\underline{i}}(\underline{x})$ such that $|\underline{i}| \geq m(q - 1) - 1$.

Consider $B_{(q-2, q-1, \dots, q-1)}(\underline{x})$ which is in $M^{m(q-1)-1}$. By Corollary 3.4, Corollary 3.5 and (2.15), we have $\deg(H_{(q-2, q-1, \dots, q-1)}(\underline{Y})) = q - 2 > 1$ (for $q \geq 4$).

Thus $B_{(q-2, q-1, \dots, q-1)}(\underline{x}) \notin C_1(m, q)$. It follows that $M^{m(q-1)-1} \neq C_1(m, q)$.

- Since $q \geq 4$, then $M^{m(q-1)-1} \subseteq M^{m(q-1)-(q-2)+1}$.

Therefore, $B_{(q-2, q-1, \dots, q-1)}(\underline{x}) \in M^{m(q-1)-(q-2)+1}$ (*).

And since $\deg(H_{(q-2, q-1, \dots, q-1)}(\underline{Y})) = q - 2 > q - 3$, then $B_{(q-2, q-1, \dots, q-1)}(\underline{x}) \notin C_{q-3}(m, q)$.

Hence $M^{m(q-1)-(q-2)+1} \neq C_{q-3}(m, q)$.

- It is clear by (2.6) that $B_{(q-2, q-1, \dots, q-1)}(\underline{x}) \notin C_i(m, q)$ for $2 \leq i \leq q - 4$, then by (2.8) we have $M^{m(q-1)-i} \neq C_i(m, q)$ for $2 \leq i \leq q - 4$.

In particular, the statement is proved for the case $m = 1$.

Step two:

- $M^{m(q-1)-(q-2)}$ is linearly generated over $\mathbb{F}_q$ by the $B_{\underline{i}}(\underline{x})$ such that $|\underline{i}| \geq m(q - 1) - (q - 2)$.

Consider $B_{(q-2, q-2, q-1, \dots, q-1)}(\underline{x})$ which is in $M^{m(q-1)-(q-2)}$ by (*).

We have $\deg(H_{(q-2, q-2, q-1, \dots, q-1)}(\underline{Y})) = 2(q - 2) > q - 2$ (for $q \geq 4$).

Thus $B_{(q-2, q-2, q-1, \dots, q-1)}(\underline{x}) \notin C_{q-2}(m, q)$. So $M^{m(q-1)-(q-2)} \neq C_{q-2}(m, q)$.

- Since $q \geq 4$, then $M^{m(q-1)-(q-2)} \subseteq M^{m(q-1)-2(q-2)+1}$.

Therefore $B_{(q-2, q-2, q-1, \dots, q-1)}(\underline{x}) \in M^{m(q-1)-2(q-2)+1}$.

And since $\deg(H_{(q-2, q-2, q-1, \dots, q-1)}(\underline{Y})) = 2(q - 2) > 2(q - 2) - 1$, we have

$B_{(q-2, q-2, q-1, \dots, q-1)}(\underline{x}) \notin C_{2(q-2)-1}(m, q)$.

Hence $M^{m(q-1)-2(q-2)+1} \neq C_{2(q-2)-1}(m, q)$.

- For $q > 4$, since $B_{(q-2, q-2, q-1, \dots, q-1)}(\underline{x}) \notin C_i(m, q)$ where $q-1 \leq i \leq 2(q-2)-2$, then $M^{m(q-1)-i} \neq C_i(m, q)$ for $q-1 \leq i \leq 2(q-2)-2$.

Continuing in this way, we apply the same method for each step. Thus, for the m-th step, we have

Step m:

- $M^{m(q-1)-(m-1)(q-2)}$ is linearly generated over $\mathbb{F}_q$ by the $B_{\underline{i}}(\underline{x})$ such that $|\underline{i}| \geq m(q - 1) - (m - 1)(q - 2)$.

Consider $B_{(q-2, \dots, q-2)}(\underline{x})$ which is in $M^{m(q-1)-(m-1)(q-2)}$ (for $m \geq 2$). By Corollary 3.5 and (2.15), we have $\deg(H_{(q-2, \dots, q-2)}(\underline{Y})) = m(q - 2) > (m - 1)(q - 2)$ (for $q \geq 4$).

Thus $B_{(q-2, \dots, q-2)}(\underline{x}) \notin C_{(m-1)(q-2)}(m, q)$. Therefore

$M^{m(q-1)-(m-1)(q-2)} \neq C_{(m-1)(q-2)}(m, q)$.

- Since $q \geq 4$, then $M^{m(q-1)-(m-1)(q-2)} \subseteq M^{m(q-1)-m(q-2)+1}$.

Hence $B_{(q-2, \dots, q-2)}(\underline{x}) \in M^{m(q-1)-m(q-2)+1}$.

And since $\deg(H_{(q-2, \dots, q-2)}(\underline{Y})) = m(q-2) > m(q-2) - 1$,

then $B_{(q-2, \dots, q-2)}(\underline{x}) \notin C_{m(q-2)-1}(m, q)$.

Therefore $M^{m(q-1)-m(q-2)+1} \neq C_{m(q-2)-1}(m, q)$.

- For $q > 4$, since $B_{(q-2, \dots, q-2)}(\underline{x}) \notin C_i(m, q)$ where $(m-1)(q-2) + 1 \leq i \leq m(q-2) - 2$, we have $M^{m(q-1)-i} \neq C_i(m, q)$ for $(m-1)(q-2) + 1 \leq i \leq m(q-2) - 2$.

To end the proof, we consider the following final step:

- $M^{m(q-1)-m(q-2)} = M^m$ is linearly generated over $\mathbb{F}_q$ by the $B_{\underline{i}}(\underline{x})$ such that $|\underline{i}| \geq m$.

Consider $B_{(0, 2, 1, \dots, 1)}(\underline{x})$ which is in M^m . By Corollary 3.4, Remark 3.2 and (2.15) we have

$\deg(H_{(0, 2, 1, \dots, 1)}(\underline{Y})) = m(q-2) + 1 > m(q-2)$.

Thus $B_{(0, 2, 1, \dots, 1)}(\underline{x}) \notin C_{m(q-2)}(m, q)$. Hence $M^m \neq C_{m(q-2)}(m, q)$.

- M^{m-1} is linearly generated over $\mathbb{F}_q$ by the $B_{\underline{i}}(\underline{x})$ such that $|\underline{i}| \geq m-1$.

Consider $B_{(0, 0, 2, 1, \dots, 1)}(\underline{x})$ which is in M^{m-1} .

We have $\deg(H_{(0, 0, 2, 1, \dots, 1)}(\underline{Y})) = m(q-2) + 2 > m(q-2) + 1$.

Thus $B_{(0, 0, 2, 1, \dots, 1)}(\underline{x}) \notin C_{m(q-2)+1}(m, q)$. So $M^{m-1} \neq C_{m(q-2)+1}(m, q)$.

Similarly, we have finally:

- M^2 is linearly generated over $\mathbb{F}_q$ by the $B_{\underline{i}}(\underline{x})$ such that $|\underline{i}| \geq 2$.

Consider $B_{(0, \dots, 0, 2)}(\underline{x})$ which is in M^2 .

We have $\deg(H_{(0, \dots, 0, 2)}(\underline{Y})) = m(q-1) - 1 > m(q-1) - 2$.

Thus $B_{(0, \dots, 0, 2)}(\underline{x}) \notin C_{m(q-1)-2}(m, q)$. Hence $M^2 \neq C_{m(q-1)-2}(m, q)$. $\square$

3.4 An example with two variables over $\mathbb{F}_4$

In this section, we consider the case $m = 2$, $q = 4$ and $n = 4^2 = 16$.

Let $\alpha \in \mathbb{F}_4$ be a root of the irreducible polynomial $1 + Z + Z^2$ over $\mathbb{F}_2$. It is clear that $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$.

Set

$$\beta_0 = 0, \quad \beta_1 = 1, \quad \beta_2 = \alpha \quad \text{and} \quad \beta_3 = \alpha^2.$$

Consider the modular algebra

$$A = \mathbb{F}_4[X_1, X_2] / (X_1^4 - 1, X_2^4 - 1) = \left\{ \sum_{j=0}^3 \sum_{l=0}^3 a_{jl} x_1^j x_2^l \mid a_{jl} \in \mathbb{F}_4 \right\}$$

with $x_1 = X_1 + I$, $x_2 = X_2 + I$ and $I = (X_1^4 - 1, X_2^4 - 1)$.

Set $[0, 3] := \{0, 1, 2, 3\}$,

$\underline{i} := (i_1, i_2) \in ([0, 3])^2$,

and $\underline{x} := (x_1, x_2)$.

Let us fix an order on the set of monomials

$$\{x_1^j x_2^l \mid 0 \leq j, l \leq 3\}. \quad (3.6)$$

Consider the polynomial

$$B_{(i_1, i_2)}(\underline{x}) := (x_1 - 1)^{i_1} (x_2 - 1)^{i_2} = \sum_{j=0}^{i_1} \sum_{l=0}^{i_2} H_{(i_1, i_2)}(\beta_j, \beta_l) x_1^j x_2^l$$

with $H_{(i_1, i_2)}(Y_1, Y_2) = H_{i_1}(Y_1) H_{i_2}(Y_2)$.

From Proposition 3.2, we have $H_1(Y) = 1 + Y + Y^2$, $H_2(Y) = 1 + \alpha^2 Y + \alpha Y^2$ and $H_3(Y) = 1$.

And by (2.12) and (2.11), we have $H_0(Y) = F_0(Y) = 1 + Y^3$.

We have the sequence of ideals

$\{0\} \subset M^6 \subset M^5 \subset M^4 \subset M^3 \subset M^2 \subset M \subset A$ where $M = \text{Rad}(A)$.

The ideal M^d ($0 \leq d \leq 6$) is linearly generated over $\mathbb{F}_4$ by

$$B_d := \{B_{(i_1, i_2)}(\underline{x}) \mid 0 \leq i_1, i_2 \leq 3, i_1 + i_2 \geq d\}$$

Let ν be an integer such that $0 \leq \nu \leq 6$. Consider the GRM codes $C_\nu(2, 4)$ of length 16 and of order ν over $\mathbb{F}_4$:

$$C_\nu(2, 4) := \{(P(\beta_j, \beta_l))_{0 \leq j, l \leq 3} \mid P(Y_1, Y_2) \in P_\nu(2, 4)\}.$$

where

$$P_\nu(2, 4) := \left\{ P(Y_1, Y_2) = \sum_{j=0}^3 \sum_{l=0}^3 u_{jl} Y_1^j Y_2^l \mid u_{jl} \in \mathbb{F}_4, \deg(P(Y_1, Y_2)) \leq \nu \right\}$$

and $\{(\beta_j, \beta_l) \mid 0 \leq j, l \leq 3\}$ is ordered as in (3.6).

We have the ascending sequence:

$$\{0\} \subset C_0(2, 4) \subset C_1(2, 4) \subset C_2(2, 4) \subset C_3(2, 4) \subset C_4(2, 4) \subset C_5(2, 4) \subset C_6(2, 4) = (\mathbb{F}_4)^{16}.$$

In virtue of the isomorphism (2.4) and the Remark 2.1, we have the following results:

- M^6 and $C_0(2, 4)$ are linearly generated by $B_{(3,3)}(\underline{x}) = \bar{1}$ (the “all one word”), and we have $M^6 = C_0(2, 4)$.

-Since $B_{(2,3)}(\underline{x}) = \sum_{j=0}^2 \sum_{l=0}^3 H_{(2,3)}(\beta_j, \beta_l) x_1^j x_2^l \in M^5$ and $\deg(H_{(2,3)}(Y_1, Y_2)) = 2 > 1$, then $B_{(2,3)}(\underline{x}) \notin C_1(2, 4)$. Thus, $M^5 \neq C_1(2, 4)$.

-Since $B_{(2,2)}(\underline{x}) = \sum_{j=0}^2 \sum_{l=0}^2 H_{(2,2)}(\beta_j, \beta_l) x_1^j x_2^l \in M^4$ and $\deg(H_{(2,2)}(Y_1, Y_2)) = 4 > 2$, then $B_{(2,2)}(\underline{x}) \notin C_2(2, 4)$. Therefore, $M^4 \neq C_2(2, 4)$.

Since $B_{(2,2)}(\underline{x}) = \sum_{j=0}^2 \sum_{l=0}^2 H_{(2,2)}(\beta_j, \beta_l) x_1^j x_2^l \in M^3$ and $\deg(H_{(2,2)}(Y_1, Y_2)) = 4 > 3$, then $B_{(2,2)}(\underline{x}) \notin C_3(2, 4)$, and we have $M^3 \neq C_3(2, 4)$.

-Since $B_{(0,2)}(\underline{x}) = \sum_{j=0}^0 \sum_{l=0}^2 H_{(0,2)}(\beta_j, \beta_l) x_1^j x_2^l \in M^2$ and $\deg(H_{(0,2)}(Y_1, Y_2)) = 5 > 4$, then $B_{(0,2)}(\underline{x}) \notin C_4(2, 4)$. This implies $M^2 \neq C_4(2, 4)$.

It is clear by the proof of the Theorem 3.6. that $M = C_5(2, 4)$.

3.5 An example with one variable over $\mathbb{F}_4$

In this section, we consider the case $m = 1$, $q = 4$ and $n = 4$.

Let $\alpha \in \mathbb{F}_4$ be a root of the irreducible polynomial $1 + Z + Z^2$ over $\mathbb{F}_2$. We have $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$.

Set

$$\beta_0 = 0, \quad \beta_1 = 1, \quad \beta_2 = \alpha \quad \text{and} \quad \beta_3 = \alpha^2,$$

Consider the modular algebra

$$A = \mathbb{F}_4[X] / (X^4 - 1) = \left\{ \sum_{j=0}^3 a_j x^j \mid a_j \in \mathbb{F}_4 \right\}$$

with $x = X + I$ and $I = (X^4 - 1)$.

Let us consider the following order on the set of monomials

$$\{x^j \mid 0 \leq j \leq 3\} :$$

$$1 < x < x^2 < x^3.$$

For $0 \leq i \leq 3$, consider the polynomial

$$B_i(x) := (x - 1)^i = \sum_{j=0}^i H_i(\beta_j) x^j$$

From Proposition 3.2, we have $H_1(Y) = 1 + Y + Y^2$, $H_2(Y) = 1 + \alpha^2 Y + \alpha Y^2$ and $H_3(Y) = 1$.

And from (2.12) and (2.11), we have $H_0(Y) = F_0(Y) = 1 + Y^3$.

We have the sequence of ideals

$$\{0\} \subset M^3 \subset M^2 \subset M \subset A \quad \text{where} \quad M = \text{Rad}(A).$$

The ideal M^d ($0 \leq d \leq 3$) is linearly generated over $\mathbb{F}_4$ by

$$B_d := \{B_i(x) \mid d \leq i \leq 3\}$$

Let ν be an integer such that $0 \leq \nu \leq 3$. Consider the GRM codes $C_\nu(1, 4)$ of length 4 and of order ν over $\mathbb{F}_4$:

$$C_\nu(1, 4) := \{(P(\beta_0), P(\beta_1), P(\beta_2), P(\beta_3)) \mid P(Y) \in P_\nu(1, 4)\}.$$

where

$$P_\nu(1, 4) := \left\{ P(Y) = \sum_{j=0}^3 u_j Y^j \mid u_j \in \mathbb{F}_4, \deg(P(Y)) \leq \nu \right\}.$$

We have the ascending sequence:

$$\{0\} \subset C_0(1, 4) \subset C_1(1, 4) \subset C_2(1, 4) \subset C_3(1, 4) = (\mathbb{F}_4)^4.$$

By the isomorphism (2.4) and the Remark 2.1, we have the following results:

- M^3 and $C_0(1, 4)$ are linearly generated by $B_3(x) = \bar{1}$ (the “all one word”), and we have $M^3 = C_0(1, 4)$.

-Since $B_2(x) = \sum_{j=0}^2 H_2(\beta_j)x^j \in M^2$ and $\deg(H_2(Y)) = 2 > 1$, then

$B_2(x) \notin C_1(1, 4)$. Thus, $M^2 \neq C_1(1, 4)$.

It follows that M^2 is not a Reed-Solomon code of length 4 over $\mathbb{F}_4$.

It is clear by the proof of the Theorem 3.6. that $M = C_2(1, 4)$.

4 Conclusions

- a In the section 2, we have given the definition of the GRM codes of length q^m over a finite field $\mathbb{F}_q$ and some general properties of the residue class ring A .
- b In the subsection 3.1, we have given a new proof of the theorem of Berman and Charpin about the Reed-Muller codes over a prime field.
- c In the subsection 3.2, we have studied the coefficients of the binomial function over a finite field.
- d In the subsection 3.3, we have studied the relations between the Generalized Reed-Muller codes over a non prime field and the radical powers of A .
- e In the subsection 3.4 and 3.5, we give some examples.

A possible future work is to describe the Generalized Reed-Muller codes over a non prime field in the ambient space A .

Competing Interests

The author declare that no competing interests exist.

References

- [1] Andriatahiny H., Anneaux de Galois et Codes polynomiaux, Thèse de Doctorat de Troisième Cycle, Université d'Antananarivo, 2002.
- [2] Assmus EF., On Berman's characterization of the Reed-Muller codes, Journal of Statistical planning and Inference, 56 (1994), pp.17-21.
- [3] Assmus EF. and Key JD., Polynomial codes and finite geometries, Handbook of Coding Theory, 1994.
- [4] Berman SD., On the theory of group codes, Kibernetika 3(1) (1967), pp.31-39.
- [5] Blake IF. and Mullin RC., The mathematical theory of coding, Academic Press, 1975.

-
- [6] Charpin P., Une généralisation de la construction de Berman des codes de Reed et Muller p-aires, *Communications in algebra* 16 (1988), pp.2231-2246.
 - [7] Couselo E., Gonzalez S., Markov VT., Martinez C., Nechaev AA., Ideal representation of Reed-Solomon and Reed-Muller codes, *Algebra and Logic*, vol.51, no.3 (2012).
 - [8] Kasami T., Lin S. and Peterson WW., New generalizations of the Reed-Muller codes, *IEEE Transactions on Information Theory* 14 (1968), no.2, pp.189-205.
 - [9] Landrock P. and Manz O., Classical Codes as Ideals in Group Algebras, *Designs, Codes and Cryptography*, 2 (1992), pp.273-285.
 - [10] Poli A., Codes stables sous le groupe des automorphismes isométriques de $A = \mathbb{F}_p[X_1, \dots, X_n]/(X_1^p - 1, \dots, X_m^p - 1)$, *C.R. Acad. Sc. Paris*, t.290 (1980), pp.1029-1032.
 - [11] Tumaikin IN., Basic Reed-Muller codes and their connections with powers of radical of group algebra over a non-prime field, *Moscow University Bulletin*, 2013, vol.68, no.6, pp.295-298.
 - [12] Tumaikin IN., Basic Reed-Muller codes as group codes, *Journal of Mathematical Sciences*, May 2015, vol.206, Issue 6, pp.699-710.