British Journal of Mathematics & Computer Science
X(X): XX-XX, 20XX

SCIENCEDOMAIN *international*
www.sciencedomain.org

The Generalized Reed-Muller codes in a modular group algebra

Harinaivo Andriatahiny[*1] **and Vololona Harinoro Rakotomalala**[2]

[1] *Mention: Mathematics and Computer Science, Domain: Sciences and Technologies, University of Antananarivo, Madagascar.*

[2] *Mention: Meteorology, Domain: Sciences of the engineer, Higher Polytechnic School of Antananarivo (ESPA), University of Antananarivo, Madagascar.*

Original Research Article

Received: XX December 20XX
Accepted: XX December 20XX
Online Ready: XX December 20XX

Abstract

We study some properties of the modular group algebra of the additive group of a Galois ring over a finite field. A description of the Generalized Reed-Muller codes in this group algebra is presented.

Keywords: Generalized Reed-Muller codes; group algebra; Galois ring; Jennings basis
2010 Mathematics Subject Classification: 94B05; 94B15; 20C05; 16N40; 12E05

1 Introduction

It is well known that the Reed-Muller codes of length p^m over the prime field $\mathbb{F}_p$ are the radical powers of the modular group algebra $\mathbb{F}_p[\mathbb{F}_{p^m}]$ ([3],[4]).
In general, this property is no longer true for the Generalized Reed-Muller (GRM) codes over a non prime field $\mathbb{F}_{p^r}(r > 1)$. Let M be the radical of the modular group algebra $\mathbb{F}_{p^r}[G]$ where G is the additive group of the Galois ring $GR(p^r, m)$ of characteristic p^r and of rank m. Since $\mathbb{F}_{p^r}[G]$ is isomorphic to $\mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]/(X_0^{p^r} - 1, \ldots, X_{m-1}^{p^r} - 1)$ (see Proposition 3.7), then as shown in [1], except for M^0, M and $M^{m(p^r-1)}$, none of the radical powers of $\mathbb{F}_{p^r}[G]$ is a GRM code over the non prime field $\mathbb{F}_{p^r}$.
Many authors have described the GRM codes in group algebras, especially in the group algebra $\mathbb{F}_{p^r}[H]$ where H is an elementary abelian p-group or H is the additive group of an extension field of $\mathbb{F}_{p^r}$ ([4],[5],[9]).
We give a description of the GRM codes over an arbitrary finite field $\mathbb{F}_{p^r}$ in the group algebra $\mathbb{F}_{p^r}[G]$ where G is the additive group of the Galois ring $GR(p^r, m)$. The main theorem is Theorem 3.4.

**Corresponding author: E-mail: hariandriatahiny@gmail.com, harinaivo.andriatahiny@univ-antananarivo.mg*

2 Preliminaries

2.1 Galois ring

Let us start with some basic properties of Galois rings (see [10]).
Set $\mathbb{Z}_{p^r} := \mathbb{Z}/p^r\mathbb{Z}$ and let $h(X) \in \mathbb{Z}_{p^r}[X]$ be a monic basic irreducible polynomial of degree m. Such a polynomial always exists by Hensel's Lemma. The Galois ring of characteristic p^r and of rank m, denoted by $GR(p^r, m)$, is defined as the quotient ring

$$\mathbb{Z}_{p^r}[X]/(h(X)). \tag{2.1}$$

In particular, $GR(p^r, 1) = \mathbb{Z}_{p^r}$ and $GR(p^1, m) = \mathbb{F}_{p^m}$.
$GR(p^r, m)$ is a local ring with maximal ideal $pGR(p^r, m)$ and residue field

$$GR(p^r, m)/pGR(p^r, m) \cong \mathbb{F}_{p^m}.$$

The Galois ring $GR(p^r, m)$ is a finite chain ring; all the ideals of $GR(p^r, m)$ are ordered as follows:

$$\{0\} = p^r GR(p^r, m) \subset p^{r-1}GR(p^r, m) \subset \ldots \subset pGR(p^r, m) \subset GR(p^r, m).$$

Each element $v \in GR(p^r, m)$ can be expressed as $v = p^t u$ where u is an invertible element in $GR(p^r, m)$ and in this expression t is unique up to modulo p^{r-t}.
Finally, we recall that if m_1 is a positive integer such that $m_1 \mid m$, then $GR(p^r, m_1)$ is a subring of $GR(p^r, m)$. Conversely, any subring of $GR(p^r, m)$ is of the form $GR(p^r, m_1)$ for some $m_1 \mid m$.

2.2 Group algebra of an elementary abelian p-group

We recall in this subsection some properties of the group algebra $\mathbb{F}_{p^r}[\mathbb{F}_{p^m}]$ treated in [2]. Let $F := \mathbb{F}_{p^r}$ be any subfield of $\mathbb{F}_{p^m}$. Set G equal to the additive group of the finite field $\mathbb{F}_{p^m}$. Thus G can be viewed as an elementary abelian p-group of order p^m, i.e. G is an abelian group such that $pg = 0$ for every $g \in G$. Set

$$R = F[G] \tag{2.2}$$

the group algebra of G over the field F. Using polynomial notation, an element of R, which is a function from G to F, is a formal sum $\sum_{g\in G} a_g X^g$ where the coefficient a_g is simply the value of the function at the group element g.
The operations in the group algebra R are defined as follows:

$$\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g = \sum_{g\in G}(a_g + b_g)X^g;$$

$$(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g) = \sum_{g,h\in G} a_g b_h X^{g+h} = \sum_{k\in G}(\sum_{h\in G} a_{k-h} b_h)X^k;$$

and, for $c \in F$,

$$c(\sum_{g\in G} a_g X^g) = \sum_{g\in G}(ca_g)X^g.$$

X^0 is the multiplicative identity of the group algebra R; i.e $X^0 a = a$ for every $a \in R$. We will simply denote it by 1.
The augmentation map

$$\begin{aligned} \phi : \quad R &\longrightarrow F \\ \sum_{g\in G} a_g X^g &\longmapsto \sum_{g\in G} a_g \end{aligned} \tag{2.3}$$

is an algebra homomorphism.
The kernel of ϕ is denoted by

$$M = \left\{ \sum_{g \in G} a_g X^g \in R \mid \sum_{g \in G} a_g = 0 \right\}. \tag{2.4}$$

Thus, M is an ideal of R.
Since G is an elementary abelian p-group and the coefficients are in a field of characteristic p, then we have

$$(\sum_{g \in G} a_g X^g)^p = \sum_{g \in G} (a_g)^p X^{pg} = \sum_{g \in G} (a_g)^p X^0 = (\sum_{g \in G} a_g)^p X^0. \tag{2.5}$$

Proposition 2.1. *R is a local group algebra with unique maximal ideal*

$$M = \mathrm{Rad}(R) = \{a \in R \mid a^p = 0\}$$

where $\mathrm{Rad}(R)$ is the radical of R.

Remark 2.1. Let p be a prime number. Then

1. $(-1)^{p-1} = 1$ mod p.
2. $\binom{p-1}{i} = (-1)^i$ mod p for all $i = 0, 1, \ldots, p-1$.

Proposition 2.2. *Provided $g \neq 0$, we have*

$$(X^g - 1)^{p-1} = \sum_{i=0}^{p-1} X^{ig}$$

Remark 2.2. Let U be a non-empty subset of G. Then

$$\prod_{g \in U} (X^g - 1)^{p-1} = \begin{cases} \sum_{g \in \langle U \rangle} X^g & \text{if } U \text{ is a linearly independent set} \\ 0 & \text{otherwise} \end{cases}$$

where $\langle U \rangle$ is the subspace spanned by U.

Let S be a subset of $R = F[G]$. The annihilator of S is defined by

$$\mathrm{Ann}(S) := \{a \in R \mid as = 0 \text{ for all } s \in S\}. \tag{2.6}$$

Theorem 2.1. *Let G be an elementary abelian p-group of order p^m, F a field of characteristic p and $R = F[G]$.*

1. *For any basis $\{g_0, \ldots, g_{m-1}\}$ of G, the p^m elements $\prod_{\nu=0}^{m-1} (X^{g_\nu} - 1)^{e_\nu}$ where $0 \leq e_\nu < p$ form a linear basis for R.*
2. *Moreover, $\{\prod_{\nu=0}^{m-1} (X^{g_\nu} - 1)^{e_\nu} \mid \sum_{\nu=0}^{m-1} e_\nu \geq t, 0 \leq e_\nu < p\}$ forms a linear basis of M^t, where M is the radical of R.*
3. $\mathrm{Ann}(M^t) = m^{m(p-1)+1-t}$.

Definition 2.1. The basis for $F[G]$ given in theorem 2.1. is called a Jennings basis of the group algebra.

3 Main Results

3.1 Group algebra of the additive group of a Galois ring

In this subsection, we give some natural generalizations of the properties of the group algebra $\mathbb{F}_{p^r}[\mathbb{F}_{p^m}]$ formulated in subsection 2.2.
Let F be the field $\mathbb{F}_{p^r}$ of p^r elements where p is a prime number and $r \geq 1$ is an integer. Set G equal to the additive group of the Galois ring $GR(p^r, m)$. Set

$$R = F[G] = \left\{ \sum_{g \in G} a_g X^g \mid a_g \in F \right\} \tag{3.1}$$

the group algebra of G over the field F. The operations in R are defined as in subsection 2.2.
We consider the ideal $M := \left\{ \sum_{g \in G} a_g X^g \in R \mid \sum_{g \in G} a_g = 0 \right\}$ of R.
Since G is of characteristic p^r and the coefficients are in the field of p^r elements, we have by the Freshmen identity

$$(\sum_{g \in G} a_g X^g)^{p^r} = \sum_{g \in G} (a_g)^{p^r} X^{p^r g} = \sum_{g \in G} a_g X^0 = (\sum_{g \in G} a_g) X^0. \tag{3.2}$$

Proposition 3.1. *R is a local group algebra with unique maximal ideal*

$$M = \mathrm{Rad}(R) = \left\{ a \in R \mid a^{p^r} = 0 \right\}.$$

Proof. The relation (3.2) shows that $(\sum_{g \in G} a_g X^g)^{p^r}$ is zero if and only if $\sum_{g \in G} a_g = 0$. Thus, M is the radical of R.
Moreover, it shows also that every element of R that is not in M is a unit of R and it follows that M is the unique maximal ideal of R. □

Remark 3.1. The set $\{X^g \mid g \in G\}$ is a linear basis of R considered as a vector space over F.

Proposition 3.2. *The ideal M is generated linearly over the field F by the elements $X^g - 1$ where $g \in G - \{0\}$.*

Proof. Each element $X^g - 1$ is in M. Conversely, let $\sum_{g \in G} a_g X^g \in M$, i.e $\sum_{g \in G} a_g = 0$. We have

$$\begin{aligned}
\sum_{g \in G} a_g X^g &= \sum_{g \in G} a_g \left[(X^g - 1) + 1 \right] \\
&= \sum_{g \in G} \left[a_g (X^g - 1) + a_g 1 \right] = \sum_{g \in G} a_g (X^g - 1) + \sum_{g \in G} a_g 1 \\
&= \sum_{g \in G} a_g (X^g - 1) + (\sum_{g \in G} a_g) 1 = \sum_{g \in G} a_g (X^g - 1) \\
&= \sum_{g \in G - \{0\}} a_g (X^g - 1).
\end{aligned}$$

□

Lemma 3.1. *Let p be a prime number and $r \geq 1$ an integer. Then*

1. $(-1)^{p^r - 1} = 1$ *mod* p.
2. $\binom{p^r - 1}{i} = (-1)^i$ *mod* p *for all* $i = 0, 1, \ldots, p^r - 1$.

Proof. The first assertion is trivial. The second can be proved by induction on i. □

Proposition 3.3. *Provided $g \neq 0$, we have*

$$(X^g - 1)^{p^r - 1} = \sum_{i=0}^{p^r-1} X^{ig}$$

Proof.

$$\begin{aligned}(X^g - 1)^{p^r-1} &= \sum_{i=0}^{p^r-1} \binom{p^r - 1}{i} (-1)^{p^r-1-i} X^{ig} \\ &= \sum_{i=0}^{p^r-1} \binom{p^r - 1}{i} (-1)^{p^r-1}(-1)^{-i} X^{ig} = \sum_{i=0}^{p^r-1} X^{ig}\end{aligned}$$

by Lemma 3.1. □

From (2.1), notice that

$$\begin{aligned}GR(p^r, m) &= \mathbb{Z}_{p^r}[X]/(h(X)) \\ &= \left\{i_0 + i_1\alpha + \ldots + i_{m-1}\alpha^{m-1} \mid i_l \in \mathbb{Z}_{p^r}, 0 \leq l \leq m-1\right\}\end{aligned} \tag{3.3}$$

where $\alpha := X + (h(X))$.

Proposition 3.4. *We have*

$$(X^1 - 1)^{p^r-1}(X^\alpha - 1)^{p^r-1} \ldots (X^{\alpha^{m-1}} - 1)^{p^r-1} = \sum_{g \in G} X^g$$

Proof. By Proposition 3.3, we have

$$\begin{aligned}&(X^1 - 1)^{p^r-1}(X^\alpha - 1)^{p^r-1} \ldots (X^{\alpha^{m-1}} - 1)^{p^r-1} \\ &= (\sum_{i_0=0}^{p^r-1} X^{i_0 1})(\sum_{i_1=0}^{p^r-1} X^{i_1\alpha}) \ldots (\sum_{i_{m-1}=0}^{p^r-1} X^{i_{m-1}\alpha^{m-1}}) \\ &= \sum_{0 \leq i_l \leq p^r-1, 0 \leq l \leq m-1} X^{i_0 1} X^{i_1\alpha} \ldots X^{i_{m-1}\alpha^{m-1}} \\ &= \sum_{0 \leq i_l \leq p^r-1, 0 \leq l \leq m-1} X^{i_0 1 + i_1\alpha + \ldots + i_{m-1}\alpha^{m-1}} = \sum_{g \in G} X^g\end{aligned}$$

□

Set

$$E := [0, p^{rm} - 1] = \{0, 1, \ldots, p^{rm} - 1\} \tag{3.4}$$

the set of integers between 0 and $p^{mr} - 1$. Let i be an element of E and

$$i = i_0 + i_1 p^r + i_2 p^{2r} + \ldots + i_{m-1} p^{(m-1)r} \tag{3.5}$$

where $0 \leq i_l \leq p^r - 1$ for all $l = 0, 1, \ldots, m-1$ its p^r-adic expansion.
The p^r-weight of i is defined by

$$\omega_{p^r}(i) := \sum_{l=0}^{m-1} i_l. \tag{3.6}$$

Then, set

$$V_i := (X^1 - 1)^{i_0}(X^\alpha - 1)^{i_1} \ldots (X^{\alpha^{m-1}} - 1)^{i_{m-1}} \tag{3.7}$$

and

$$B_t := \{V_i \mid i \in E, \omega_{p^r}(i) \geq t\} \tag{3.8}$$

for all t such that $0 \leq t \leq m(p^r - 1)$.

Proposition 3.5. *B_0 is a linear basis of R over F.*

Proof. We have $\mathrm{card}(B_0) = p^{rm} = \dim_F(R)$ where $\mathrm{card}(B_0)$ is the number of elements in B_0 and $\dim_F(R)$ is the dimension of R over F.
Let us prove that B_0 is a linearly independant set over F. Consider the linear combination

$$\sum_{\omega_{p^r}(i) \geq 0} \lambda_i V_i = 0$$

where $\lambda_i \in F$ for all $i \in E$. We have

$$\lambda_0 V_0 + \sum_{\omega_{p^r}(i) \geq 1} \lambda_i V_i = 0$$

where $V_0 = 1$ is the identity element of R. Multiplying by $V_{p^{rm}-1}$, we get

$$\lambda_0 V_{p^{rm}-1} + \sum_{\omega_{p^r}(i) \geq 1} \lambda_i V_i V_{p^{rm}-1} = 0.$$

Let $i \in E$ such that $\omega_{p^r}(i) \geq 1$. Then, there is an integer l $(0 \leq l \leq m-1)$ such that $i_l \geq 1$. Thus, $i_l + p^r - 1 \geq p^r$. Since $(X^g - 1)^{p^r} = 0$ for any g, we have

$$V_i V_{p^{rm}-1} = (X^1 - 1)^{i_0 + p^r - 1} \dots (X^{\alpha^l} - 1)^{i_l + p^r - 1} \dots (X^{\alpha^{m-1}} - 1)^{i_{m-1} + p^r - 1} = 0.$$

Then

$$0 = \lambda_0 V_{p^{rm}-1} = \lambda_0 \sum_{g \in G} X^g$$

by Proposition 3.4. Hence, $\lambda_0 = 0$.
Thus, we have

$$\sum_{\omega_{p^r}(i) \geq 1} \lambda_i V_i = 0.$$

Let $i \in E$ such that $\omega_{p^r}(i) = 1$. We have

$$\lambda_i V_i + \sum_{\omega_{p^r}(j) \geq 1, j \neq i} \lambda_j V_j = 0.$$

Multiplying by $V_{p^{rm}-1-i}$, we have

$$\lambda_i V_i V_{p^{rm}-1-i} + \sum_{\omega_{p^r}(j) \geq 1, j \neq i} \lambda_j V_j V_{p^{rm}-1-i} = 0.$$

Let $j = \sum_{l=0}^{m-1} j_l p^{lr} \neq i = \sum_{l=0}^{m-1} i_l p^{lr}$ be two elements of E such that $\omega_{p^r}(j) \geq 1 = \omega_{p^r}(i)$. Then, there is an integer l $(0 \leq l \leq m-1)$ such that $j_l > i_l$, and hence $j_l \geq i_l + 1$ and $j_l + p^r - 1 - i_l \geq (i_l + 1) + p^r - 1 - i_l = p^r$. Since $(X^g - 1)^{p^r} = 0$ for any $g \in G$, we have

$$V_j V_{p^{rm}-1-i} = (X^1 - 1)^{j_0 + p^r - 1 - i_0} \dots (X^{\alpha^l} - 1)^{j_l + p^r - 1 - i_l} \dots (X^{\alpha^{m-1}} - 1)^{j_{m-1} + p^r - 1 - i_{m-1}} = 0.$$

Consequently,

$$0 = \lambda_i V_i V_{p^{rm}-1-i} = \lambda_i \sum_{g \in G} X^g.$$

Hence $\lambda_i = 0$.
Continuing in this way, we have
$\lambda_i = 0$ for all $i \in E$ such that $\omega_{p^r}(i) = 1$, and $\lambda_i = 0$ for all $i \in E$ such that $\omega_{p^r}(i) = 2, 3, \ldots, m(p^r - 1)$. □

Corollary 3.2. *B_1 is a linear basis of M over F.*

Proof. Since $B_1 \subset B_0$, then B_1 is a linearly independant set of R over F. And since $V_i \in M$ for all i such that $\omega_{p^r}(i) \geq 1$, $B_1 \subseteq M$. Moreover, we have $\dim_F(M) = p^{rm} - 1 = \mathrm{card}(B_1)$. □

Corollary 3.3. *B_t is a linear basis of M^t over F where $1 \leq t \leq m(p^r - 1)$.*

Proof. Since $B_t \subset B_0$, B_t is a linearly independant set of R over F. M^t is generated as ideal by the set $\{a_1 a_2 \ldots a_t \mid a_i \in M, 1 \leq i \leq t\}$. Consider a product $a_1 a_2 \ldots a_t$ where $a_i \in M$ for all i $(1 \leq i \leq t)$. Since M is linearly generated by B_1 over F, then we have

$$a_i = \sum_{j=1}^{p^{rm}-1} \lambda_{i_j} V_j$$

where $\lambda_{i_j} \in F$ for all i and j. Therefore,

$$a_1 a_2 \ldots a_t = \prod_{i=1}^{t} \Big(\sum_{j=1}^{p^{rm}-1} \lambda_{i_j} V_j \Big) = \sum_{\omega_{p^r}(j) \geq t} \beta_j V_j \in B_t$$

where $\beta_j \in F$. And it is clear that a finite sum of such products is a linear combination of the elements of B_t with coefficients in F. Thus, M^t is generated by B_t over F. □

Remark 3.2. The index of nilpotency of the radical M is $1 + m(p^r - 1)$. And we have the following sequence of ideals:

$$\{0\} = M^{1+m(p^r-1)} \subset M^{m(p^r-1)} \subset \ldots \subset M^2 \subset M \subset R.$$

Proposition 3.6. $\mathrm{Ann}(M^t) = M^{1+m(p^r-1)-t}$ *where* $1 \leq t \leq m(p^r - 1)$.

Proof. Let t be an integer such that $1 \leq t \leq m(p^r - 1)$. By Corollary 3.3, (3.8), (3.7) and (3.3),

$$B_t := \{V_i \mid i \in E, \omega_{p^r}(i) \geq t\}$$

is a linear basis of M^t over F where

$$V_i := (X^1 - 1)^{i_0} (X^\alpha - 1)^{i_1} \ldots (X^{\alpha^{m-1}} - 1)^{i_{m-1}}$$

and $i = i_0 + i_1 p^r + \ldots + i_{m-1} p^{(m-1)r}$ $(0 \leq i_l \leq p^r - 1, \forall l)$ by (3.5).
By definition, $\mathrm{Ann}(M^t) := \{a \in R \mid as = 0 \text{ for all } s \in M^t\}$.
Since the index of nilpotency of M is $1 + m(p^r - 1)$, then we have $\mathrm{Ann}(M^t) \supseteq M^{1+m(p^r-1)-t}$.
Let $a \in \mathrm{Ann}(M^t)$. Since $a \in R$, we have

$$a = \sum_{\omega_{p^r}(i) \geq 0} \lambda_i V_i$$

where $\lambda_i \in F$ for all $i \in E$.
Let $i \in E$ such that $\omega_{p^r}(i) = m(p^r - 1)$. Thus, $i = p^{rm} - 1$.
Since $V_{p^{rm}-1} \in M^{m(p^r-1)} \subseteq M^t$, then

$$aV_{p^{rm}-1} = \lambda_0 V_{p^{rm}-1} = \lambda_0 \sum_{g \in G} X^g = 0.$$

Hence, $\lambda_0 = 0$.
Let $i \in E$ such that $\omega_{p^r}(i) = m(p^r - 1) - 1$.
Since $V_i \in M^{m(p^r-1)-1} \subseteq M^t$, then

$$aV_i = \lambda_{\bar{i}} \sum_{g \in G} X^g = 0$$

where $\bar{i} = (p^r - 1 - i_0) + (p^r - 1 - i_1)p^r + \ldots + (p^r - 1 - i_{m-1})p^{(m-1)r}$. Hence $\lambda_{\bar{i}} = 0$. We have $\omega_{p^r}(\bar{i}) = m(p^r - 1) - \omega_{p^r}(i) = 1$. Therefore, $\lambda_{\bar{i}} = 0$ for all $i \in E$ such that $\omega_{p^r}(i) = m(p^r - 1) - 1$.
Let $i \in E$ such that $\omega_{p^r}(i) = m(p^r - 1) - 2$.
Since $V_i \in M^{m(p^r-1)-2} \subseteq M^t$, then

$$aV_i = \lambda_{\bar{i}} \sum_{g \in G} X^g = 0.$$

Hence $\lambda_{\bar{i}} = 0$. It follows that $\lambda_{\bar{i}} = 0$ for all $i \in E$ such that $\omega_{p^r}(i) = m(p^r - 1) - 2$, i.e $\omega_{p^r}(\bar{i}) = 2$.
Continuing in this way, finally let $i \in E$ such that $\omega_{p^r}(i) = t$.
Since $V_i \in M^t$, then

$$aV_i = \lambda_{\bar{i}} \sum_{g \in G} X^g = 0.$$

Hence $\lambda_{\bar{i}} = 0$ with $\omega_{p^r}(\bar{i}) = m(p^r - 1) - t$.
It follows that $\lambda_{\bar{i}} = 0$ for all $i \in E$ such that $\omega_{p^r}(i) = t$, i.e $\omega_{p^r}(\bar{i}) = m(p^r - 1) - t$.
Then $a \in M^{m(p^r-1)-t+1}$. □

3.2 Isomorphism

We give here an isomorphism between $\mathbb{F}_{p^r}[G]$ and $\mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]/(X_0^{p^r} - 1, \ldots, X_{m-1}^{p^r} - 1)$ where G is the additive group of the Galois ring $GR(p^r, m)$.
Recall that $\mathbb{F}_{p^r}[G] = \left\{ \sum_{g \in G} a_g X^g \mid a_g \in \mathbb{F}_{p^r} \right\}$.

Proposition 3.7. *The group algebra $\mathbb{F}_{p^r}[G]$ is isomorphic to the quotient ring*

$$\mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]/(X_0^{p^r} - 1, \ldots, X_{m-1}^{p^r} - 1).$$

Proof. Consider the mapping

$$\begin{aligned} \psi : \quad \mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}] &\longrightarrow \mathbb{F}_{p^r}[G] \\ X_i &\longmapsto X^{\alpha^i} \end{aligned} \tag{3.9}$$

where α is defined in (3.3).
It is clear that the ideal $\left\langle X_i^{p^r} - 1 \mid 0 \leq i \leq m-1 \right\rangle \subseteq \ker \psi$.
Conversely, let $a(X_0, \ldots, X_{m-1}) \in \ker \psi$. By using the division algorithm in $\mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]$

(see [6]) with the lexicographic order such that $X_0 > X_1 > \ldots > X_{m-1}$, let us divide $a(X_0, \ldots, X_{m-1})$ by $\left\{X_0^{p^r} - 1, \ldots, X_{m-1}^{p^r} - 1\right\}$. We have

$$a(X_0, \ldots, X_{m-1}) = b_0(X_0^{p^r} - 1) + \ldots + b_{m-1}(X_{m-1}^{p^r} - 1) + g(X_0, \ldots, X_{m-1})$$

where $b_i \in \mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]$ for all i and

$$g(X_0, \ldots, X_{m-1}) = \sum_{0 \le i_k \le p^r - 1} g_{i_0, \ldots, i_{m-1}} X_0^{i_0} \ldots X_{m-1}^{i_{m-1}}$$

with $g_{i_0, \ldots, i_{m-1}} \in \mathbb{F}_{p^r}$.
Then

$$\begin{aligned} \psi(a(X_0, \ldots, X_{m-1})) &= \psi(g(X_0, \ldots, X_{m-1})) \\ &= \sum_{0 \le i_k \le p^r - 1} g_{i_0, \ldots, i_{m-1}} X^{i_0 + i_1 \alpha + \ldots + i_{m-1} \alpha^{m-1}} = 0. \end{aligned}$$

By Remark 3.1, $g_{i_0, \ldots, i_{m-1}} = 0$ for all i_k such that $0 \le i_k \le p^r - 1$ $(0 \le k \le m-1)$. This implies that $g(X_0, \ldots, X_{m-1}) = 0$ and thus $a(X_0, \ldots, X_{m-1}) \in \left\langle X_i^{p^r} - 1 \mid 0 \le i \le m-1 \right\rangle$. □

By the isomorphism induced by (3.9), the group algebra $\mathbb{F}_{p^r}[G]$ and the quotient ring $B = \mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]/(X_0^{p^r} - 1, \ldots, X_{m-1}^{p^r} - 1)$ have the same algebraic structure. We can identify the elements of B with the elements of $\mathbb{F}_{p^r}[G]$ in the following way:

$$\sum_{0 \le i_k \le p^r - 1, 0 \le k \le m-1} g_{i_0, \ldots, i_{m-1}} x_0^{i_0} \ldots x_{m-1}^{i_{m-1}} \longleftrightarrow \sum_{0 \le i_k \le p^r - 1, 0 \le k \le m-1} g_{i_0, \ldots, i_{m-1}} X^{i_0 1 + i_1 \alpha + \ldots + i_{m-1} \alpha^{m-1}}$$

where $x_i = X_i + \left\langle X_i^{p^r} - 1 \mid 0 \le i \le m-1 \right\rangle$. In particular, B and $\mathbb{F}_{p^r}[G]$ are local algebras and the index of nilpotency of their radicals is $1 + m(p^r - 1)$. It was proved in [1] that, except for $\mathrm{Rad}(B)$ and $(\mathrm{Rad}(B))^{m(p^r-1)}$, none of the powers of $\mathrm{Rad}(B)$ is a GRM code if $r > 1$. The same result is true for $\mathbb{F}_{p^r}[G]$. Thus, a description of the GRM codes in $\mathbb{F}_{p^r}[G]$ is proposed in the next subsection.

3.3 Description of the GRM codes

We describe the GRM codes in $\mathbb{F}_{p^r}[GR(p^r, m)]$.
Set $n := q^m - 1$ where $q = p^r$, p is a prime number and r, m are integers ≥ 1. Let $A = \mathbb{F}_q[Z]/(Z^n - 1)$.
We have

$$A = \left\{a_0 + a_1 z + \ldots + a_{n-1} z^{n-1} \mid a_i \in \mathbb{F}_q\right\}$$

where $z = Z + (Z^n - 1)$.
The shortened Generalized Reed-Muller code of length n and of order ν $(0 \le \nu < m(q-1))$ over $\mathbb{F}_q$ denoted by $HC_\nu(m, q)$ is the ideal of A generated by

$$f_\nu(z) = \prod_{0 < \omega_q(i) \le m(q-1) - \nu - 1} (z - \gamma^i) \tag{3.10}$$

where γ is a primitive element of the finite field $\mathbb{F}_{q^m}$ ([8],[14]), and $\omega_q(i)$ is defined in (3.6).
Recall that G is the additive group of the Galois ring $GR(p^r, m)$.
Let us order the elements of $G = \{0, g_0, g_1, \ldots, g_{q^m - 2}\}$ as follows:

$$0 < g_0 < g_1 < \ldots < g_{q^m - 2}.$$

Thus, we have the following identification:

$$\sum_{g\in G} a_g X^g \in \mathbb{F}_q[G] \longleftrightarrow (a_g)_{g\in G} \in (\mathbb{F}_q)^{q^m}.$$

Let us order the monomials $\{X^g \mid g \in G\}$ such that

$$X^{g_i} < X^{g_j} \text{ if and only if } g_i < g_j.$$

For $a = \sum_{g\in G} a_g X^g \in \mathbb{F}_q[G]$, set $\mathrm{md}(a) := max\,\{g \in G \mid a_g \neq 0\}$ and we define the leading term of a by

$$\mathrm{LT}(a) := a_{\mathrm{md}(a)} X^{\mathrm{md}(a)}.$$

Consider the linear transformation

$$\begin{aligned} \varphi : \quad A &\longrightarrow \mathbb{F}_q[G] \\ a_0 + a_1 z + \ldots + a_{n-1} z^{n-1} &\longmapsto (-\sum_{i=0}^{n-1} a_i) X^0 + \sum_{i=0}^{n-1} a_i X^{g_i} \end{aligned} \tag{3.11}$$

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

$$C_\nu(m,q) = \varphi(HC_\nu(m,q)).$$

We have the following sequence:

$$\{0\} \subset C_0(m,q) \subset C_1(m,q) \subset \cdots \subset C_{m(q-1)-1}(m,q) \subset \mathbb{F}_q[G] \tag{3.12}$$

The morphism φ sets up a one to one correspondance between $HC_\nu(m,q)$ and $C_\nu(m,q)$, thus

$$\dim_{\mathbb{F}_q}(C_\nu(m,q)) = \dim_{\mathbb{F}_q}(HC_\nu(m,q)). \tag{3.13}$$

Since $HC_\nu(m,q)$ is the cyclic code of length $q^m - 1$ over $\mathbb{F}_q$ generated by $f_\nu(z)$, then

$$\dim_{\mathbb{F}_q}(HC_\nu(m,q)) = q^m - 1 - \deg(f_\nu(z)) \tag{3.14}$$

where $\deg(f_\nu(z))$ is the degree of the polynomial $f_\nu(z)$.
Set

$$\theta_\nu^j = \varphi(z^j f_\nu(z)) \tag{3.15}$$

where $0 \leq \nu \leq m(q-1) - 1$.
By (3.11), we have

$$\mathrm{LT}(\theta_\nu^j) = X^{g_{\deg(z^j f_\nu(z))}}. \tag{3.16}$$

Set

$$N(t) := \mathrm{card}(\{k \in [0, q^m - 1] \mid \omega_q(k) = t\})$$

where $[0, q^m - 1]$ is the set of integers between 0 and $q^m - 1$ (see (3.4),(3.5) and (3.6)).

Theorem 3.4. *We have*

1. $\{\theta_0^0\}$ *is a linear basis of* $C_0(m,q)$.
2. *The set* $K_\nu := \{\theta_0^0\} \cup \{\theta_i^j \mid 1 \leq i \leq \nu\ ,\ 0 \leq j \leq N(m(q-1) - i) - 1\}$ *forms a linear basis for* $C_\nu(m,q)$ *where* $1 \leq \nu \leq m(q-1) - 1$.

Proof. Let ν be an integer such that $0 \leq \nu \leq m(q-1)-1$. We have

$$\theta_0^0 = \varphi(f_0(z)) = \varphi(\prod_{i=1}^{q^m-2}(z-\gamma^i)) = \varphi(1+z+z^2+\ldots+z^{q^m-2}) = \sum_{g\in G} X^g.$$

Since $\dim_{\mathbb{F}_q}(C_0(m,q)) = \dim_{\mathbb{F}_q}(HC_0(m,q)) = q^m-1-(q^m-2) = 1$, then the first assertion is proved.
For the integer ν such that $1 \leq \nu \leq m(q-1)-1$, $f_\nu(z)$ is a monic polynomial and by (3.10), $\deg(f_\nu(z)) = \sum_{t=1}^{m(q-1)-\nu-1} N(t)$.
Thus,

$$\deg(z^j f_\nu(z)) = j + \sum_{t=1}^{m(q-1)-\nu-1} N(t)$$

for $1 \leq j \leq N(m(q-1)-\nu)-1$.
By (3.16), for the elements θ_i^j in K_ν, we have

$$\mathrm{LT}(\theta_\lambda^j) < \mathrm{LT}(\theta_\mu^k) \text{ if } \lambda > \mu, \text{ and } \mathrm{LT}(\theta_\mu^j) < \mathrm{LT}(\theta_\mu^k) \text{ if } j < k.$$

This implies that the elements of K_ν are linearly independant. And by (3.12), they are elements of $C_\nu(m,q)$.
It is clear that $\mathrm{card}(K_\nu) = 1 + \sum_{i=1}^{\nu} N(m(q-1)-i)$.
And since

$$\begin{aligned} N(m(q-1)-i) &= \deg(f_{i-1}(z)) - \deg(f_i(z)) \\ &= (q^m-1-\deg(f_i(z))) - (q^m-1-\deg(f_{i-1}(z))) \\ &= \dim_{\mathbb{F}_q}(HC_i(m,q)) - \dim_{\mathbb{F}_q}(HC_{i-1}(m,q)) \\ &= \dim_{\mathbb{F}_q}(C_i(m,q)) - \dim_{\mathbb{F}_q}(C_{i-1}(m,q)), \end{aligned}$$

then $\mathrm{card}(K_\nu) = \dim_{\mathbb{F}_q}(C_\nu(m,q))$. □

For $m=1$, we consider the case of the Reed-Solomon codes $C_\nu(1,q)$ of length q and of order ν over $\mathbb{F}_q$.

Corollary 3.5. *$C_\nu(1,q)$ is linearly generated over $\mathbb{F}_q$ by the set $\{\theta_i^0 \mid 0 \leq i \leq \nu\}$ where $0 \leq \nu \leq q-2$.*

3.4 Example

We consider the GRM codes of length 16 over $\mathbb{F}_4$ in $\mathbb{F}_4[GR(2^2,2)]$. Let $G = \{0, g_0, g_1, \ldots, g_{14}\}$ be the additive group of the Galois ring $GR(2^2,2)$ with $0 < g_0 < g_1 < \ldots < g_{14}$.
$C_0(2,4)$:
We have $C_0(2,4) = \varphi(HC_0(2,4))$ with $HC_0(2,4) = (f_0(z))$ and

$$f_0(z) = \prod_{0<\omega_4(i)\leq 5}(z-\gamma^i) = \prod_{i=1}^{14}(z-\gamma^i) = 1+z+z^2+\ldots+z^{14}$$

where γ is a primitive element of $\mathbb{F}_{16}$. We have $\theta_0^0 = \varphi(f_0(z)) = X^0 + X^{g_0} + X^{g_1} + \ldots + X^{g_{14}}$. Thus, $\mathrm{LT}(\theta_0^0) = X^{g_{14}}$.
By (3.13) and (3.14), we have

$$\dim_{\mathbb{F}_4}(C_0(2,4)) = \dim_{\mathbb{F}_4}(HC_0(2,4)) = 15 - \deg(f_0(z)) = 15 - 14 = 1.$$

Thus, $C_0(2,4)$ is linearly generated over $\mathbb{F}_4$ by θ_0^0.
$C_1(2,4)$:
We have $C_1(2,4) = \varphi(HC_1(2,4))$ with $HC_1(2,4) = (f_1(z))$ and

$$f_1(z) = \prod_{0<\omega_4(i)\leq 4} (z - \gamma^i).$$

Consider $N(5) := \mathrm{card}(\{k \in [0,15] \mid \omega_4(k) = 5\}) = \mathrm{card}(\{11,14\}) = 2$.
We have $\deg(f_1(z)) = \deg(f_0(z)) - N(5) = 14 - 2 = 12$.
By (3.13) and (3.14),

$$\dim_{\mathbb{F}_4}(C_1(2,4)) = \dim_{\mathbb{F}_4}(HC_1(2,4)) = 15 - \deg(f_1(z)) = 15 - 12 = 3.$$

On the other hand, by (3.16), we have $\mathrm{LT}(\theta_1^0) = X^{g_{12}}$ and $\mathrm{LT}(\theta_1^1) = X^{g_{13}}$.
From (3.12), we have

$$C_0(2,4) \subset C_1(2,4).$$

Thus, $\{\theta_0^0, \theta_1^0, \theta_1^1\} = K_1$ is a linearly independent set in $C_1(2,4)$. Then it is a linear basis of $C_1(2,4)$.
$C_2(2,4)$:
We have $C_2(2,4) = \varphi(HC_2(2,4))$ with $HC_2(2,4) = (f_2(z))$ and

$$f_2(z) = \prod_{0<\omega_4(i)\leq 3} (z - \gamma^i).$$

Consider $N(4) := \mathrm{card}(\{k \in [0,15] \mid \omega_4(k) = 4\}) = \mathrm{card}(\{7,10,13\}) = 3$.
We have $\deg(f_2(z)) = \deg(f_1(z)) - N(4) = 12 - 3 = 9$.
By (3.13) and (3.14),

$$\dim_{\mathbb{F}_4}(C_2(2,4)) = \dim_{\mathbb{F}_4}(HC_2(2,4)) = 15 - \deg(f_2(z)) = 15 - 9 = 6.$$

On the other hand, by (3.16), we have $\mathrm{LT}(\theta_2^0) = X^{g_9}$, $\mathrm{LT}(\theta_2^1) = X^{g_{10}}$ and $\mathrm{LT}(\theta_2^2) = X^{g_{11}}$.
From (3.12), we have

$$C_0(2,4) \subset C_1(2,4) \subset C_2(2,4).$$

Thus, $\{\theta_0^0, \theta_1^0, \theta_1^1, \theta_2^0, \theta_2^1, \theta_2^2\} = K_2$ is a linearly independent set in $C_2(2,4)$. Then it is a linear basis of $C_2(2,4)$.
$C_3(2,4)$:
We have $C_3(2,4) = \varphi(HC_3(2,4))$ with $HC_3(2,4) = (f_3(z))$ and

$$f_3(z) = \prod_{0<\omega_4(i)\leq 2} (z - \gamma^i).$$

Consider $N(3) := \mathrm{card}(\{k \in [0,15] \mid \omega_4(k) = 3\}) = \mathrm{card}(\{3,6,9,12\}) = 4$.
We have $\deg(f_3(z)) = \deg(f_2(z)) - N(3) = 9 - 4 = 5$.
By (3.13) and (3.14),

$$\dim_{\mathbb{F}_4}(C_3(2,4)) = \dim_{\mathbb{F}_4}(HC_3(2,4)) = 15 - \deg(f_3(z)) = 15 - 5 = 10.$$

On the other hand, by (3.16), we have $\mathrm{LT}(\theta_3^0) = X^{g_5}$, $\mathrm{LT}(\theta_3^1) = X^{g_6}$, $\mathrm{LT}(\theta_3^2) = X^{g_7}$ and $\mathrm{LT}(\theta_3^3) = X^{g_8}$.
From (3.12), we have

$$C_0(2,4) \subset C_1(2,4) \subset C_2(2,4) \subset C_3(2,4).$$

Thus, $\{\theta_0^0, \theta_1^0, \theta_1^1, \theta_2^0, \theta_2^1, \theta_2^2, \theta_3^0, \theta_3^1, \theta_3^2, \theta_3^3\} = K_3$ is a linearly independent set in $C_3(2,4)$. Then it is a linear basis of $C_3(2,4)$.

$C_4(2,4)$:
We have $C_4(2,4) = \varphi(HC_4(2,4))$ with $HC_4(2,4) = (f_4(z))$ and

$$f_4(z) = \prod_{0<\omega_4(i)\leq 1} (z - \gamma^i).$$

Consider $N(2) := \mathrm{card}(\{k \in [0,15] \mid \omega_4(k) = 2\}) = \mathrm{card}(\{2,5,8\}) = 3$.
We have $\deg(f_4(z)) = \deg(f_3(z)) - N(2) = 5 - 3 = 2$.
By (3.13) and (3.14),

$$\dim_{\mathbb{F}_4}(C_4(2,4)) = \dim_{\mathbb{F}_4}(HC_4(2,4)) = 15 - \deg(f_4(z)) = 15 - 2 = 13.$$

On the other hand, by (3.16), we have $\mathrm{LT}(\theta_4^0) = X^{g_2}$, $\mathrm{LT}(\theta_4^1) = X^{g_3}$ and $\mathrm{LT}(\theta_4^2) = X^{g_4}$.
From (3.12), we have

$$C_0(2,4) \subset C_1(2,4) \subset C_2(2,4) \subset C_3(2,4) \subset C_4(2,4).$$

Thus, $\{\theta_0^0, \theta_1^0, \theta_1^1, \theta_2^0, \theta_2^1, \theta_2^2, \theta_3^0, \theta_3^1, \theta_3^2, \theta_3^3, \theta_4^0, \theta_4^1, \theta_4^2\} = K_4$ is a linearly independent set in $C_4(2,4)$. Then it is a linear basis of $C_4(2,4)$.
$C_5(2,4)$:
We have $C_5(2,4) = \varphi(HC_5(2,4))$ with $HC_5(2,4) = (f_5(z))$ and

$$f_5(z) = \prod_{0<\omega_4(i)\leq 0} (z - \gamma^i) = 1.$$

Then $\deg(f_5(z)) = 0$.
By (3.13) and (3.14),

$$\dim_{\mathbb{F}_4}(C_5(2,4)) = \dim_{\mathbb{F}_4}(HC_5(2,4)) = 15 - \deg(f_5(z)) = 15.$$

On the other hand, by (3.16), $\mathrm{LT}(\theta_5^0) = X^{g_0}$ and $\mathrm{LT}(\theta_5^1) = X^{g_1}$.
From (3.12), we have

$$C_0(2,4) \subset C_1(2,4) \subset C_2(2,4) \subset C_3(2,4) \subset C_4(2,4) \subset C_5(2,4).$$

Thus, $\{\theta_0^0, \theta_1^0, \theta_1^1, \theta_2^0, \theta_2^1, \theta_2^2, \theta_3^0, \theta_3^1, \theta_3^2, \theta_3^3, \theta_4^0, \theta_4^1, \theta_4^2, \theta_5^0, \theta_5^1\} = K_5$ is a linearly independent set in $C_5(2,4)$. Then it is a linear basis of $C_5(2,4)$.

4 CONCLUSIONS

a In the subsection (2.1), we recall the definition and some properties of the Galois ring $GR(p^r, m)$.

b In the subsection (2.2), we summarize some results on the group algebra $\mathbb{F}_{p^r}[\mathbb{F}_{p^m}]$ developed by Assmus and Key in [2]. In particular, some facts about a linear basis of the group algebra $\mathbb{F}_{p^r}[\mathbb{F}_{p^m}]$ called Jennings basis ([7]) are pointed out.

c In the subsection (3.1), We give some generalizations of the properties of $\mathbb{F}_{p^r}[\mathbb{F}_{p^m}]$ presented in subsection (2.2) by considering the group algebra $\mathbb{F}_{p^r}[G]$ where G is the additive group of the Galois ring $GR(p^r, m)$.

d In the subsection (3.2), we establish a natural isomorphism between $\mathbb{F}_{p^r}[G]$ and $\mathbb{F}_{p^r}[X_0, X_1, \ldots, X_{m-1}]/(X_0^{p^r} - 1, \ldots, X_{m-1}^{p^r} - 1)$.

e In the subsection (3.3), we describe the GRM codes over a finite field $\mathbb{F}_{p^r}$ in $\mathbb{F}_{p^r}[G]$ by using the fact that GRM codes are extended cyclic codes.

f In the subsection (3.4), an example is given.

A possible future work is to determine a new decoding algorithm according to this description of the GRM codes.
A binary Reed-Muller code was used to transmit excellent pictures of the planet Mars taken by the Satellite Mariner to Earth. I think that if one can propose a new decoding method from the algebraic structure of the GRM codes and construct a fast decoding algorithm, the GRM codes become a more powerful tool in the area of communication.

Competing Interests

The author declare that no competing interests exist.

References

[1] Andriatahiny H., The Generalized Reed-Muller codes and the Radical Powers of a modular algebra, British Journal of Mathematics and Computer Science, 18(5):1-14, 2016.

[2] Assmus EF. and Key JD., Polynomial codes and finite geometries, Handbook of Coding Theory, 1994.

[3] Berman SD., On the theory of group codes, Kibernetika 3(1) :31-39, 1967.

[4] Charpin P., Une généralisation de la construction de Berman des codes de Reed et Muller p-aires, Communications in algebra 16 :2231-2246, 1988.

[5] Couselo E., Gonzalez S., Markov VT., Martinez C., Nechaev AA., Ideal representation of Reed-Solomon and Reed-Muller codes, Algebra and Logic, 51(3), 2012.

[6] Cox D., Little J. and O'Shea D., Ideals, Varieties and Algorithms, Springer, 1992.

[7] Jennings SA., The structure of the group ring of a p-group over a modular field, Trans.Amer.Math.Soc., 50:175-185, 1941.

[8] Kasami T., Lin S. and Peterson WW., New generalizations of the Reed-Muller codes, IEEE Transactions on Information Theory 14(2):189-205, 1968.

[9] Landrock P. and Manz O., Classical Codes as Ideals in Group Algebras, Designs, Codes and Cryptography, 2:273-285, 1992.

[10] McDonald BR., Finite Rings with identity, Dekker, 1974.

[11] Rolland R., The second Weight of Generalized Reed-Muller codes in Mosts Cases, Cryptography and Communications - Discrete Structure, Boolean Function and Sequences 2(1):19-40, 2010.

[12] Tumaikin IN., Basic Reed-Muller codes and their connections with powers of radical of group algebra over a non-prime field, Moscow University Bulletin, 68(6):295-298, 2013.

[13] Tumaikin IN., Basic Reed-Muller codes as group codes, Journal of Mathematical Sciences, 206(6):699-710, 2015.

[14] Van Lint JH., Introduction to Coding Theory, 3rd ed., Springer, 1998.

©2011 Author1 & Author2; This is an Open Access article distributed under the terms of the Creative Commons Attribution License http://creativecommons.org/licenses/by/2.0, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.