ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **11** (2022), no.11, 1033–1048
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.11.11.4

GENERALIZED REED-MULLER CODES OVER GALOIS RINGS

Harinaivo Andriatahiny[1], Desiré Arsène Ratahirinjatovo, and Sanni José Andrianalisefa

ABSTRACT. A Galois ring may be considered as a common generalization of a finite field and a prime power integer residue ring. The generalized Reed-Muller codes over finite fields were introduced by Kasami et al. and the generalized Reed-Muller codes over prime power integer residue rings were constructed by M. Bhaintwal and S. K. Wasan. In this paper, we give an unifying approach for these constructions.

1. INTRODUCTION

In the following, let $GR(p^s, r)$ denote the Galois ring of characteristic p^s and rank r, where p is a prime number and s, r are integers ≥ 1. $GR(p^s, r)$ is defined as the quotient $\mathbb{Z}_{p^s}[x]/(f(x))$ where f is a monic basic irreducible polynomial of degree r in $\mathbb{Z}_{p^s}[x]$. In particular, $GR(p^s, 1)$ is the ring $\mathbb{Z}_{p^s}$ of integers modulo p^s and $GR(p, r)$ is the finite field $\mathbb{F}_{p^r}$ of p^r elements. $GR(p^s, r)$ is a Galois extension of $\mathbb{Z}_{p^s}$ of degree r ([13]).

Codes over finite fields have been investigated by many authors (see e.g. [5, 14]). In [9], Hammons *et al.* showed that some non-linear binary codes with very good parameters are images under the Gray map of some linear codes over $\mathbb{Z}_4$. This has led to the active study of codes over rings (see e.g. [3, 4, 8, 12, 15]).

[1]*corresponding author*
2020 *Mathematics Subject Classification.* 94B05, 94B15, 12E05, 13MXX.
Key words and phrases. Reed-Muller code, Galois ring, code over ring.
Submitted: 04.10.2022; *Accepted:* 20.10.2022; *Published:* 04.11.2022.

Generalized Reed-Muller (GRM) codes over finite fields have been studied by several authors (see [5, 7, 14]). They have many applications in both theory and practice.

Reed-Muller codes over $\mathbb{Z}_4$ and over Galois rings of characteristic 2^s have been defined and studied in [6, 11].

The GRM codes over $\mathbb{Z}_{p^s}$ and the GRM codes over $\mathbb{F}_{p^r}$ are constructed in [2] and [10] respectively. Our purpose is to present a common generalization of these codes to GRM codes over $GR(p^s, r)$. The standard generator matrix, the rank, the dual, and the minimum distance are determined. We prove that the images of the GRM codes over $GR(p^s, r)$ under the projection map are the GRM codes over $\mathbb{F}_{p^r}$. We examine the trace descriptions of the Kerdock codes over $GR(p^s, r)$ and the GRM codes over $GR(p^s, r)$. We study also some properties of the shortened GRM codes over $GR(p^s, r)$.

2. Multivariate formulation

Throughout this paper, we put $L := GR(p^s, r)$. L is a local ring with maximal ideal pL and residue field $L/pL = \mathbb{F}_q$, where $q = p^r$.

Let $h(x) \in L[x]$ be a monic basic primitive polynomial of degree $m \geq 1$ dividing $x^{q^m-1} - 1$ and having ξ as a root of order $q^m - 1$ in $L[x]/(h(x)) = GR(p^s, rm)$. We denote $\mathcal{R} := GR(p^s, rm)$. $\mathcal{R}$ is a Galois extension of L of degree m. ξ is called a primitive element of $\mathcal{R}$. Let $n = q^m - 1$ and

$$\mathcal{T}_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}.$$

$\{1, \xi, \xi^2, \ldots, \xi^{m-1}\}$ is a basis of the free module $\mathcal{R}$ of rank m over L, and we have $\mathcal{R} = L[\xi]$. Each element $\xi^i \in \mathcal{T}_m$ can uniquely be expressed as

$$\xi^i = b_{1i} + b_{2i}\xi + b_{3i}\xi^2 + \ldots + b_{mi}\xi^{m-1}, \tag{2.1}$$

where $b_{ji} \in L$, $0 \leq i \leq n-1$, $1 \leq j \leq m$. We adopt the convention $\xi^\infty = 0$. Let

$$b_i = (b_{1i}, b_{2i}, b_{3i}, \ldots, b_{mi}) \ , \ 0 \leq i \leq n-1,$$

and $b_\infty = (0, 0, \ldots, 0)$.

Let X be the set of variables $x_1, x_2, \ldots, x_m$ and let $L[X]$ be the set of all polynomials in these variables with coefficients in L. The degree of a nonzero monomial

$x_1^{i_1} x_2^{i_2} \dots x_m^{i_m}$ is $\sum_{k=1}^{m} i_k$ and the degree of a polynomial $P(X)$ of $L[X]$ denoted $\deg(P(X))$ is the largest degree of a monomial in $P(X)$. We define $\deg(0) = -\infty$.

We define the evaluation map

$$\begin{aligned} ev: \quad & L[X] \longrightarrow L^{q^m} \\ & P(X) \longmapsto (P(b_\infty), P(b_0), P(b_1), \dots, P(b_{n-1})). \end{aligned} \tag{2.2}$$

Consider the L-submodule of $L[X]$

$$S = \{P(X) \in L[X] \mid \deg_{x_i}(P(X)) \leq q-1 \ , \ 1 \leq i \leq m\}.$$

Let ν be an integer such that $0 \leq \nu \leq m(q-1)$. Then the νth order Generalized Reed-Muller code of length q^m over L is defined by

$$RM_L(\nu, m) = \{ev(P(X)) \mid P(X) \in S \ , \ \deg(P(X)) \leq \nu\}.$$

The shortened Generalized Reed-Muller code of length $q^m - 1$ and order ν over L denoted by $RM_L(\nu, m)^-$ is the code obtained from $RM_L(\nu, m)$ by puncturing at the first position.

3. Standard generator matrix

The component-wise product of any two elements $\mathbf{u} = (u_0, u_1, \dots, u_n)$ and $\mathbf{v} = (v_0, v_1, \dots, v_n)$ of L^{n+1} is defined by

$$\mathbf{uv} = (u_0 v_0, u_1 v_1, \dots, u_n v_n). \tag{3.1}$$

By (2.1), let us consider the $(m+1) \times q^m$ matrix

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{pmatrix}.$$

G can be expressed as

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & b_{10} & b_{11} & b_{12} & \dots & b_{1n-1} \\ 0 & b_{20} & b_{21} & b_{22} & \dots & b_{2n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & b_{m0} & b_{m1} & b_{m2} & \dots & b_{mn-1} \end{pmatrix}. \tag{3.2}$$

The ith row of G is denoted by $\mathbf{v}_i$, $0 \leq i \leq m$. Thus, the $\mathbf{v}_i$ are q^m-tuples over L. In particular, $\mathbf{v}_0$ is the all one tuple 1^{q^m}.

From section 2, each $P(X) \in S$ can be expressed as

$$P(X) = \sum_{0 \leq i_j \leq q-1} a_{i_1,\ldots,i_m} x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m},$$

where $a_{i_1,\ldots,i_m} \in L$. By (2.2), (3.1) and (3.2), we have

$$ev(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) = \mathbf{v}_1^{i_1} \mathbf{v}_2^{i_2} \ldots \mathbf{v}_m^{i_m}.$$

And since the map ev is linear, we have

$$ev(P(X)) = \sum_{0 \leq i_j \leq q-1} a_{i_1,\ldots,i_m} \mathbf{v}_1^{i_1} \mathbf{v}_2^{i_2} \ldots \mathbf{v}_m^{i_m}.$$

Let ν be an integer such that $0 \leq \nu \leq m(q-1)$. Then, the νth order Generalized Reed-Muller code $RM_L(\nu, m)$ of length q^m over L is defined to be the code generated by all tuples of the form

$$\mathbf{v}_1^{i_1} \mathbf{v}_2^{i_2} \ldots \mathbf{v}_m^{i_m} \ , \ 0 \leq i_j \leq q-1 \ , \ 1 \leq j \leq m \ , \ \sum_{j=1}^{m} i_j \leq \nu. \tag{3.3}$$

$RM_L(0, m)$ is the repetition code of length q^m over L.

Let G_ν be the matrix whose rows consist of all tuples in (3.3). G_ν is called the standard generator matrix of $RM_L(\nu, m)$. The coordinates of any tulpe in G_ν are numbered $\infty, 0, 1, \ldots, n-1$.

4. Projection map

Recall that $q = p^r$, $n = q^m - 1$ and $L = GR(p^s, r)$. Since $L/pL = \mathbb{F}_q$, consider the projection map which is defined by reduction modulo p

$$\begin{aligned} \alpha : \quad & L \longrightarrow \mathbb{F}_q \\ & a \longmapsto \bar{a} = a + pL. \end{aligned}$$

This map is extended to

$$\begin{aligned} \alpha : \quad & L[x] \longrightarrow \mathbb{F}_q[x] \\ f(x) = \sum_i a_i x^i & \longmapsto \bar{f}(x) = \sum_i \bar{a}_i x^i \end{aligned}$$

and

$$\begin{aligned} \alpha : \quad L^{q^m} &\longrightarrow (\mathbb{F}_q)^{q^m} \\ \mathbf{v} = (a_0, a_1, \ldots, a_n) &\longmapsto \bar{\mathbf{v}} = (\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_n). \end{aligned} \tag{4.1}$$

Proposition 4.1. *We have*

$$\alpha(RM_L(\nu, m)) = RM_{\mathbb{F}_q}(\nu, m),$$

where $RM_{\mathbb{F}_q}(\nu, m)$ is the usual GRM code of order ν ($0 \le \nu \le m(q-1)$) and of length q^m over the finite field $\mathbb{F}_q$ (see [5]).

Proof. By (4.1) and (3.3), we have

$$\alpha(\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\ldots\mathbf{v}_m^{i_m}) = \bar{\mathbf{v}}_1^{i_1}\bar{\mathbf{v}}_2^{i_2}\ldots\bar{\mathbf{v}}_m^{i_m}$$

and the q^m-tuples

$$\bar{\mathbf{v}}_1^{i_1}\bar{\mathbf{v}}_2^{i_2}\ldots\bar{\mathbf{v}}_m^{i_m},$$

where $0 \le i_j \le q-1$, $1 \le j \le m$, $\sum_{j=1}^{m} i_j \le \nu$ form a basis for the GRM code $RM_{\mathbb{F}_q}(\nu, m)$. □

5. RANK

Consider the q^m-tuples

$$\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\ldots\mathbf{v}_m^{i_m}\ ,\ 0 \le i_j \le q-1\ ,\ 1 \le j \le m. \tag{5.1}$$

Proposition 5.1. *The q^m-tuples in (5.1) form a basis for the free L-module L^{q^m} where $L = GR(p^s, r)$.*

Proof. Let $\bar{\mathbf{v}}_i$ be the image of $\mathbf{v}_i$ in $(\mathbb{F}_q)^{q^m}$, $0 \le i \le m$. From the theory of GRM codes over finite fields, we know that the vectors

$$\bar{\mathbf{v}}_1^{i_1}\bar{\mathbf{v}}_2^{i_2}\ldots\bar{\mathbf{v}}_m^{i_m}\ ,\ 0 \le i_j \le q-1\ ,\ 1 \le j \le m$$

form a basis for $(\mathbb{F}_q)^{q^m}$ over $\mathbb{F}_q$.

Let $\mathbf{v} \in L^{q^m}$. Then $\bar{\mathbf{v}} \in (\mathbb{F}_q)^{q^m}$, and there exist constants $a^{(0)}_{i_1,\ldots,i_m} \in \mathbb{F}_q$ such that

$$\bar{\mathbf{v}} = \sum_{0 \le i_j \le q-1} a^{(0)}_{i_1,\ldots,i_m}\bar{\mathbf{v}}_1^{i_1}\bar{\mathbf{v}}_2^{i_2}\ldots\bar{\mathbf{v}}_m^{i_m}.$$

Then we have

$$\mathbf{v} = \sum_{0\le i_j\le q-1} a^{'(0)}_{i_1,\dots,i_m}\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\dots\mathbf{v}_m^{i_m} + p\mathbf{u}_1$$

for some $\mathbf{u}_1 \in L^{q^m}$ and $a^{'(0)}_{i_1,\dots,i_m} \in L$. There exist constants $a^{'(1)}_{i_1,\dots,i_m} \in L$ such that

$$\mathbf{u}_1 = \sum_{0\le i_j\le q-1} a^{'(1)}_{i_1,\dots,i_m}\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\dots\mathbf{v}_m^{i_m} + p\mathbf{u}_2$$

for some $\mathbf{u}_2 \in L^{q^m}$. Continuing in this way and noting that $p^s = 0$ in L, we get constants $a^{'(2)}_{i_1,\dots,i_m}, \dots, a^{'(s-1)}_{i_1,\dots,i_m} \in L$ such that

$$\mathbf{v} = \sum_{0\le i_j\le q-1} (a^{'(0)}_{i_1,\dots,i_m} + pa^{'(1)}_{i_1,\dots,i_m} + \dots + p^{s-1}a^{'(s-1)}_{i_1,\dots,i_m})\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\dots\mathbf{v}_m^{i_m}.$$

Hence, each $\mathbf{v} \in L^{q^m}$ can be expressed as a linear combination of the tuples $\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\dots\mathbf{v}_m^{i_m}$, $0 \le i_j \le q-1$, $1 \le j \le m$. Since these tuples are q^m in number and L^{q^m} is a free module of rank q^m over L, they must form a basis for L^{q^m}. □

Theorem 5.1. *Let m be a positive integer such that $rm \ge s$ and $q = p^r$. Then, for $0 \le \nu \le m(q-1)$, the GRM code $RM_L(\nu, m)$ is a free L-module of rank k, where*

$$k = \sum_{i=0}^{\nu}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{i-jq+m-1}{i-jq}.$$

Proof. By (3.3), the elements of the set

$$B = \{\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\dots\mathbf{v}_m^{i_m} \mid 0 \le i_t \le q-1\ ,\ \sum_{t=1}^{m} i_t \le \nu\}$$

span the GRM code $RM_L(\nu, m)$. Since B is a subset of the set $\{\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\dots\mathbf{v}_m^{i_m} \mid 0 \le i_t \le q-1\}$ which forms a basis for the free L-module L^{q^m}, then B must be linearly independent. Thus, B is a basis for $RM_L(\nu, m)$ and hence $RM_L(\nu, m)$ is a free module over L. The images of the elements in B under the map α generate the GRM code $RM_{\mathbb{F}_q}(\nu, m)$ over $\mathbb{F}_q$. Also, these images are linearly independent over $\mathbb{F}_q$. Therefore, the elements $\bar{\mathbf{v}}$, where $\mathbf{v} \in B$, form a basis for $RM_{\mathbb{F}_q}(\nu, m) = \alpha(RM_L(\nu, m))$, and we have $\operatorname{rank} RM_L(\nu, m) = \operatorname{rank} RM_{\mathbb{F}_q}(\nu, m)$. It is known from the theory of GRM codes over finite fields that

$$\operatorname{rank} RM_{\mathbb{F}_q}(\nu, m) = \sum_{i=0}^{\nu}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{i-jq+m-1}{i-jq}.$$

□

Notice that the rank of the GRM code $RM_L(\nu, m)$ is just the number of ways we can place ν or fewer objects in m cells where no cell is to contain more than $q-1$ objects.

6. TRACE DESCRIPTIONS

Each element $c \in \mathcal{R} = GR(p^s, rm)$ has a unique p-adic representation

$$c = \epsilon_0 + p\epsilon_1 + p^2\epsilon_2 + \ldots + p^{s-1}\epsilon_{s-1},$$

where $\epsilon_0, \epsilon_1, \epsilon_2, \ldots, \epsilon_{s-1} \in \mathcal{T}_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. Under this representation, the Frobenius automorphism is defined by

$$f: \quad \mathcal{R} \longrightarrow \mathcal{R},$$
$$c = \epsilon_0 + p\epsilon_1 + \ldots + p^{s-1}\epsilon_{s-1} \longmapsto c^f = \epsilon_0^q + p\epsilon_1^q + \ldots + p^{s-1}\epsilon_{s-1}^q,$$

where $q = p^r$. f is an automorphism of $\mathcal{R}$, fixes only elements of $L = GR(p^s, r)$, and generates the group of automorphisms of $\mathcal{R}$, which is cyclic of order m. Note that when $s = 1$, f is the usual Frobenius automorphism for $\mathbb{F}_{q^m}$.

The relative trace map is defined by

$$T: \quad \mathcal{R} \longrightarrow L$$
$$c \longmapsto T(c) = c + c^f + c^{f^2} + \ldots + c^{f^{m-1}}.$$

T is a linear transformation over L.

6.1. **Kerdock codes over** $GR(p^s, r)$**.** Let m be a positive integer such that $rm \geq s$ and $n = q^m - 1$ with $q = p^r$. Let $h(x) \in L[x]$ be a monic basic primitive polynomial of degree m dividing $x^n - 1$ and having ξ as a root of order n in $\mathcal{R}$. Let $g(x)$ be the reciprocal polynomial of $\frac{x^n-1}{(x-1)h(x)}$. The shortened Kerdock code $\mathcal{K}^-$ is the cyclic code of length n over $L = GR(p^s, r)$ with generator polynomial $g(x)$.

Since $g(x) \mid x^n - 1$, $\mathcal{K}^-$ is a free cyclic code of rank $n - \deg g(x) = m + 1$ over L. A generator matrix of $\mathcal{K}^-$ is

$$G^- := \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \xi & \xi^2 & \ldots & \xi^{n-1} \end{pmatrix}.$$

The Kerdock code $\mathcal{K}$ of length $n+1$ over L is obtained by adding an overall parity-check to $\mathcal{K}^-$.

Since $rm \geq s$ and $\sum_{i=0}^{n-1} \xi^i = 0$, the zero-sum check for the first row of G^- is 1 and for the second row, it is 0. Thus, a generator matrix for $\mathcal{K}$ is

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{pmatrix}$$

where the elements in the second row of G are considered to be m-tuples over L. Thus we have $\mathcal{K} = RM_L(1, m)$.

Theorem 6.1. *Let m be a positive integer such that $rm \geq s$ and $n = q^m - 1$ with $q = p^r$. Let ξ be a primitive element of $\mathcal{R} = GR(p^s, rm)$. Then $\mathcal{K}^-$ and $\mathcal{K}$ have the following trace descriptions over $\mathcal{R}$*

(i) $\mathcal{K}^- = \{\epsilon 1^n + v^{(\lambda)} \mid \epsilon \in L\ ,\ \lambda \in \mathcal{R}\}$, *where 1^n is the all one tuple of length n and*

$$v^{(\lambda)} = (T(\lambda), T(\lambda\xi), T(\lambda\xi^2), \dots, T(\lambda\xi^{n-1})),$$

(ii) $\mathcal{K} = \{\epsilon 1^{n+1} + u^{(\lambda)} \mid \epsilon \in L\ ,\ \lambda \in \mathcal{R}\}$, *where*

$$u^{(\lambda)} = (0, T(\lambda), T(\lambda\xi), T(\lambda\xi^2), \dots, T(\lambda\xi^{n-1})).$$

Proof.

(i) Let $\mathcal{C} = \{\epsilon 1^n + v^{(\lambda)} \mid \epsilon \in L\ ,\ \lambda \in \mathcal{R}\}$. Let $h(x)$ be the monic basic primitive polynomial of degree m in $L(x)$ dividing $x^n - 1$ such that $h(\xi) = 0$. Let $h^*(x)$ be the reciprocal polynomial of $h(x)$, i.e. $h^*(x) = x^m h(\frac{1}{x})$. From the definition of $\mathcal{K}^-$, the check polynomial of $\mathcal{K}^-$ is $(1-x)h^*(x)$. Clearly, $1-x$ annihilates the tuple $\epsilon 1^n$ and $h^*(x)$ annihilates $v^{(\lambda)}$. Thus $(1-x)h^*(x)$ annihilates $\mathcal{C}$. It follows that $\mathcal{C} \subseteq \mathcal{K}^-$. On the other hand, we have $\operatorname{card}\mathcal{C} = \operatorname{card}\mathcal{K}^- = (p^{sr})^{m+1}$.

(ii) $\mathcal{K}$ is a parity check extension of $\mathcal{K}^-$ and the zero-sum check for $\epsilon 1^n$ is ϵ and the zero-sum check for $v^{(\lambda)}$ is 0. Thus, the result follows from (i).

□

6.2. **GRM codes over** $GR(p^s, r)$**.** Let j be any integer such that $0 \le j \le q^m - 1$, where $q = p^r$. Then, j can uniquely be expressed as

$$j = \sum_{d=0}^{m-1} j_d q^d \ , \ \ 0 \le j_d \le q-1 \ , \ \ 0 \le d \le m-1.$$

The q-weight of j is defined by

$$w_q(j) = \sum_{d=0}^{m-1} j_d.$$

According to Section 5, we have

$$\operatorname{rank} RM_L(\nu, m) = \operatorname{card}(\{j \mid 0 \le j \le q^m - 2 \ , \ w_q(j) \le \nu\}).$$

Theorem 6.2. *Let m be a positive integer such that $rm \ge s$ and $n = q^m - 1$ with $q = p^r$. Let $1 \le \nu \le m(q-1)$. Then, $RM_L(\nu, m)$ is generated by the repetition code $RM_L(0, m)$ together with all q^m-tuples of the form*

$$(0, T(\lambda_j), T(\lambda_j \xi^j), T(\lambda_j \xi^{2j}), \ldots, T(\lambda_j \xi^{(n-1)j})), \tag{6.1}$$

where j ranges over a system of representatives of those cyclotomic cosets modulo $q^m - 1$ for which $w_q(j) \le \nu$ and λ_j ranges over $\mathcal{R} = GR(p^s, rm)$.

Proof. Let $\mathcal{C}$ be the code generated by the repetition code $RM_L(0, m)$ together with all tuples in (6.1). Since the matrix G in (3.2) is a generator matrix for the Kerdock code $\mathcal{K}$, then from Theorem 6.1, for each row $\mathbf{v}_j$, $j = 1, 2, \ldots, m$ of G, there exists a unique $\lambda_j \in \mathcal{R}$ such that

$$\mathbf{v}_j = (0, T(\lambda_j), T(\lambda_j \xi), T(\lambda_j \xi^2), \ldots, T(\lambda_j \xi^{n-1})).$$

Thus, the lth coordinate of a tuple

$$\mathbf{v}_1^{i_1} \mathbf{v}_2^{i_2} \ldots \mathbf{v}_m^{i_m} \ , \ 0 \le i_d \le q-1 \ , \ 1 \le d \le m \ , \ \sum_{d=1}^{m} i_d \le \nu$$

in the standard generator matrix of the GRM code $RM_L(\nu, m)$ is of the form

$$T(\lambda_1 z)^{i_1} T(\lambda_2 z)^{i_2} \ldots T(\lambda_m z)^{i_m},$$

where $0 \le i_d \le q-1$, $\sum_{d=1}^{m} i_d \le \nu$, $z = \xi^l$ with $\xi^\infty = 0$. Now for some i and j, we have

$$\begin{aligned} T(\lambda_i z)T(\lambda_j z) &= \sum_{u=0}^{m-1}(\lambda_i z)^{f^u}\sum_{v=0}^{m-1}(\lambda_j z)^{f^v} \\ &= \sum_{u=0}^{m-1}\lambda_i^{f^u} z^{q^u}\sum_{v=0}^{m-1}\lambda_j^{f^v} z^{q^v} \\ &= T(\lambda_i\lambda_j z^2) + T(\lambda_i\lambda_j^f z^{1+q}) + \ldots + T(\lambda_i\lambda_j^{f^{m-1}} z^{1+q^{m-1}}) \\ &= \sum_{u=0}^{m-1} T(\lambda_i\lambda_j^{f^u} z^{1+q^u}). \end{aligned}$$

We have $w_q(1+q^u) \leq 2$, $\forall u = 0, 1, \ldots, m-1$. For some i, j and k, we have

$$T(\lambda_i z)T(\lambda_j z)T(\lambda_k z) = \sum_{u=0}^{m-1}\sum_{v=0}^{m-1} T(\lambda_i\lambda_j^{f^u}\lambda_k^{f^v} z^{1+q^u+q^v}).$$

Since $z^{q^m} = z$, for some u and v, we have $1 + q^u + q^v = e \mod q^m - 1$ for some integer $e \in [0, q^m - 2]$ with $w_q(e) \leq 3$. In general, if $\sum_{d=1}^{m} i_d = a \geq 1$, then

$$T(\lambda_1 z)^{i_1} T(\lambda_2 z)^{i_2} \ldots T(\lambda_m z)^{i_m} = \sum_t T(\mu_t z^t),$$

where $t = 1 + q^{j_1} + q^{j_2} + \ldots + q^{j_{a-1}}$, $0 \leq j_\delta \leq m-1$, $1 \leq \delta \leq a-1$, and μ_t is the corresponding product of the powers of $\lambda_1, \lambda_2, \ldots, \lambda_m$.

It is easy to see that in this expansion of any $T(\lambda_1 z)^{i_1} \ldots T(\lambda_m z)^{i_m}$, the corresponding powers t of z are some representatives of cyclotomic cosets modulo $q^m - 1$ and $w_q(t) \leq \sum_{d=1}^{m} i_d$. It follows that each tuple $\mathbf{v}_1^{i_1}\mathbf{v}_2^{i_2}\ldots\mathbf{v}_m^{i_m}$ in the generator matrix of the GRM code $RM_L(\nu, m)$ is a linear combination of the all one tuple 1^{q^m} and the tuples $(0, T(\lambda_j), T(\lambda_j\xi^j), T(\lambda_j\xi^{2j}), \ldots, T(\lambda_j\xi^{(n-1)j}))$, where j ranges over a set of coset representatives modulo $q^m - 1$ with $w_q(j) \leq \sum_{d=1}^{m} i_d \leq \nu$ and λ_j ranges over $\mathcal{R}$. Hence $RM_L(\nu, m) \subseteq \mathcal{C}$.

Conversely, let $\mathcal{C}^-$ be the code obtained from $\mathcal{C}$ by puncturing at the first position. That is, $\mathcal{C}^-$ is generated by the all one tuple 1^n together with all tuples of the form $(T(\lambda_j), T(\lambda_j\xi^j), T(\lambda_j\xi^{2j}), \ldots, T(\lambda_j\xi^{(n-1)j}))$, where j and λ_j are as in (6.1).

Since $w_q(j) \leq \nu$, it is easy to verify that all these generators are annihilated by the polynomial

$$f_\nu^*(x) = (1-x)\prod_{\substack{1\leq j\leq q^m-2 \\ w_q(j)\leq\nu}} (1-\xi^j x),$$

where $f_\nu^*(x)$ is the reciprocal polynomial of

$$f_\nu(x) = (x-1) \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) \le \nu}} (x - \xi^j) = \prod_{\substack{0 \le j \le q^m-2 \\ w_q(j) \le \nu}} (x - \xi^j).$$

Let $g_\nu(x)$ be the reciprocal polynomial to the polynomial

$$g_\nu^*(x) = \frac{x^{q^m-1}-1}{f_\nu(x)} = \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) > \nu}} (x - \xi^j)$$

and denote by $\mathcal{C}_\nu = (g_\nu(x))$ the L-cyclic code generated by $g_\nu(x)$. Then, $f_\nu^*(x)$ is the check polynomial of $\mathcal{C}_\nu$. Therefore, $\mathcal{C}^- \subseteq \mathcal{C}_\nu$. Thus, $RM_L(\nu, m)^- \subseteq \mathcal{C}^- \subseteq \mathcal{C}_\nu$. Clearly,

$$g_\nu(x) = \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) > \nu}} (1 - \xi^j x).$$

We have

$$\begin{aligned} \operatorname{rank} \mathcal{C}_\nu &= q^m - 1 - \deg g_\nu(x) \\ &= \operatorname{card}(\{j \mid 0 \le j \le q^m - 2\ ,\ w_q(j) \le \nu\}) \\ &= \operatorname{rank} RM_L(\nu, m) \\ &= \operatorname{rank} RM_L(\nu, m)^-. \end{aligned}$$

It follows that $RM_L(\nu, m)^- = \mathcal{C}^- = \mathcal{C}_\nu$. □

Corollary 6.1. *$RM_L(\nu, m)^-$ is a L-cyclic code generated by the polynomial*

$$g_\nu(x) = \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) \le m(q-1)-\nu-1}} (x - \xi^j). \tag{6.2}$$

Proof. By the proof of Theorem 6.2, we have $RM_L(\nu, m)^- = (g_\nu(x))$ with

$$g_\nu(x) = \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) > \nu}} (1 - \xi^j x).$$

The zeros of $g_\nu(x)$ are all ξ^{-j} with $w_q(j) > \nu$. Since $\xi^{-j} = \xi^{q^m-1-j}$ and $w_q(q^m - 1 - j) = m(q-1) - w_q(j)$, we have

$$g_\nu(x) = \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) > \nu}} (x - \xi^{-j}) = \prod_{\substack{1 \le j \le q^m-2 \\ w_q(j) > \nu}} (x - \xi^{q^m-1-j}).$$

Let $J = q^m - 1 - j$. We have $J \neq 0$ and $w_q(J) = m(q-1) - w_q(j)$. Thus, $w_q(j) = m(q-1) - w_q(J) > \nu$. This implies that $w_q(J) < m(q-1) - \nu$. Then

$$g_\nu(x) = \prod_{0<w_q(J)\leq m(q-1)-\nu-1} (x - \xi^J).$$

Finally, we have

$$g_\nu(x) = \prod_{\substack{1\leq j\leq q^m-2 \\ w_q(j)\leq m(q-1)-\nu-1}} (x - \xi^j).$$

□

7. Dual code

We have the following property.

Proposition 7.1. *Let m be a positive integer such that $rm \geq s$ and $n = q^m - 1$ with $q = p^r$. Let ν be an integer such that $0 \leq \nu < m(q-1)$. Then, for any $c = (c_\infty, c_0, c_1, \ldots, c_{n-1}) \in RM_L(\nu, m)$, we have $c_\infty + c_0 + c_1 + \ldots + c_{n-1} = 0$.*

Proof. It is enough to prove our Proposition for all generators of the GRM code $RM_L(\nu, m)$ given in Theorem 6.2. First, since $rm \geq s$, then for 1^{q^m}, we have $\underbrace{1 + 1 + \ldots + 1}_{q^m terms} = q^m = p^{rm} = 0$. Second, for the q^m-tuples (6.1), we have

$$\begin{aligned}\sum_{i=0}^{n-1} T(\lambda_j \xi^{ij}) &= \sum_{i=0}^{n-1}\sum_{k=0}^{m-1} (\lambda_j \xi^{ij})^{f^k} \\ &= \sum_{k=0}^{m-1} \lambda_j^{f^k} \sum_{i=0}^{n-1} \xi^{ijq^k} \\ &= \sum_{k=0}^{m-1} \lambda_j^{f^k} \frac{1 - \xi^{jnq^k}}{1 - \xi^{jq^k}} = 0\end{aligned}$$

because $\xi^n = 1$. □

Theorem 7.1. *Let m be a positive integer such that $rm \geq s$ and $0 \leq \nu < m(q-1)$ with $q = p^r$. Then*

$$RM_L(\nu, m)^\perp = RM_L(\mu, m),$$

where $\mu = m(q-1) - \nu - 1$.

Proof. First, we prove that the all one q^m-tuple $1^{q^m} \in RM_L(\nu, m)$ belongs to $RM_L(\nu, m)^\perp$. Since $rm \geq s$, then $1^{q^m} \cdot 1^{q^m} = 0$. Moreover, we have to prove that 1^{q^m} is orthogonal to all q^m-tuples of the form (6.1), where $w_q(j) \leq \nu$. By the proof of Proposition 7.1, we have

$$\sum_{i=0}^{n-1} T(\lambda_j \xi^{ij}) = 0.$$

Therefore, $1^{q^m} \in RM_L(\nu, m)^\perp$.

Next, we prove that any $c = (c_\infty, c_0, c_1, \ldots, c_{n-1}) \in RM_L(\mu, m)$ belongs to $RM_L(\nu, m)^\perp$. Clearly, $c \in RM_L(\mu, m)$ if and only if $c - c_\infty 1^{q^m} \in RM_L(\mu, m)$, and $c \in RM_L(\nu, m)^\perp$ if and only if $c - c_\infty 1^{q^m} \in RM_L(\nu, m)^\perp$. Therefore, it is sufficient to show that for c with $c_\infty = 0$, $c \in RM_L(\mu, m)$ implies $c \in RM_L(\nu, m)^\perp$.

Let $c = (0, c') \in RM_L(\mu, m)$, where $c' = (c_0, c_1, \ldots, c_{n-1})$. Then $c' \in RM_L(\mu, m)^-$. By Corollary 6.1, $RM_L(\mu, m)^-$ is a L-cyclic code with generator polynomial

$$g_\mu(x) = \prod_{\substack{1 \leq j \leq q^m - 2 \\ w_q(j) \leq \nu}} (x - \xi^j).$$

So, $c'(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ is a multiple of $g_\mu(x)$. By Proposition 7.1, $c'(1) = c_0 + c_1 + \ldots + c_{n-1} = 0$. Then $c'(x)$ is also a multiple of $x - 1$.

Since $\bar{g}_\mu(1) \neq 0$, $g_\mu(1)$ is an invertible element of L. It follows that $c'(x)$ is a multiple of $(x-1)g_\mu(x)$. Then, $c'(x)$ is annihilated by the polynomial

$$f_\mu(x) = \frac{x^n - 1}{(x-1)g_\mu(x)} = \prod_{\substack{1 \leq j \leq q^m - 2 \\ w_q(j) > \nu}} (x - \xi^j)$$

i.e. $c'(x) f_\mu(x) = 0$. Therefore $c'(x)$ belongs to the dual code of the L-cyclic code with generator polynomial

$$\begin{aligned} f^*_\mu(x) &= \prod_{\substack{1 \leq j \leq q^m - 2 \\ w_q(j) > \nu}} (1 - \xi^j x) = \prod_{\substack{1 \leq j \leq q^m - 2 \\ w_q(j) \leq m(q-1) - \nu - 1}} (x - \xi^j) \\ &= g_\nu(x). \end{aligned}$$

By Corollary 6.1, $RM_L(\nu, m)^- = (g_\nu(x))$. Thus $c'(x) \in (RM_L(\nu, m)^-)^\perp$. Since $c_\infty = 0$, $c \in RM_L(\nu, m)^\perp$. Therefore, we have proved that $RM_L(\mu, m) \subseteq RM_L(\nu, m)^\perp$.

To check the ranks, we note that $\operatorname{rank} RM_L(\nu, m) = \operatorname{rank} RM_L(\nu, m)^-$ as $RM_L(\nu, m)$ is a parity check extension of $RM_L(\nu, m)^-$. According to Corollary 6.1, $RM_L(\nu, m)^-$

has the generator polynomial $g_\nu(x)$ as given in (6.2), and $RM_L(\mu,m)^-$ has the generator polynomial $g_\mu(x)$. $g_\mu(x)$ is the reciprocal polynomial of $\frac{x^n-1}{(x-1)g_\nu(x)}$. Therefore, we have

$$\begin{aligned}\operatorname{rank} RM_L(\nu,m)^- &+ \operatorname{rank} RM_L(\mu,m)^- \\ &= (n-\deg g_\nu(x)) + (n-\deg g_\mu(x)) \\ &= n+1 = q^m.\end{aligned}$$

It follows that $\operatorname{rank} RM_L(\nu,m) + \operatorname{rank} RM_L(\mu,m) = q^m$. Thus, $\operatorname{rank} RM_L(\mu,m) = \operatorname{rank} RM_L(\nu,m)^\perp$. And we have $RM_L(\mu,m) = RM_L(\nu,m)^\perp$. □

8. Minimum distance

We have the following result.

Theorem 8.1. *The shortened GRM code $RM_L(\nu,m)^-$ is a subcode of a BCH code of length q^m-1 over L whose roots include*

$$\xi, \xi^2, \ldots, \xi^{(R+1)q^Q-2}$$

where ξ is a primitive element of $\mathcal{R} = GR(p^s, rm)$, and Q and R are the quotient and remainder respectively, resulting from dividing $\mu+1 = m(q-1)-\nu$ by $q-1$.

Proof. Let d be the smallest integer such that $w_q(d) = m(q-1)-\nu = (q-1)Q + R$, $0 \le R < q-1$. Therefore, we must have $d = Rq^Q + (q-1)q^{Q-1} + (q-1)q^{Q-2} + \ldots + (q-1)q + (q-1) = (R+1)q^Q - 1$.

Also, every integer less than d has q-weight less than or equal to $m(q-1)-\nu-1$. It follows from (6.2) that all elements $\xi, \xi^2, \ldots, \xi^{(R+1)q^Q-2}$ are roots of $RM_L(\nu,m)^-$. Thus, $RM_L(\nu,m)^-$ is a subcode of a primitive BCH code of length q^m-1 over L. □

Consequently, from BCH bound on codes over Galois rings [1], $RM_L(\nu,m)^-$ has minimum distance at least $(R+1)q^Q-1$, where Q and R are the quotient and remainder respectively, resulting from dividing $\mu+1 = m(q-1)-\nu$ by $q-1$. It can be easily seen from the structure of $RM_L(\nu,m)$ that the minimum distance of $RM_L(\nu,m)$ is equal to the minimum distance of $RM_L(\nu,m)^-$. Hence the minimum distance of $RM_L(\nu,m)$ is at least $(R+1)q^Q-1$.

Theorem 8.2. *The GRM code $RM_L(\nu, m)$ has minimum distance $(R+1)q^Q - 1$, where Q and R are the quotient and remainder respectively, resulting from dividing $\mu + 1 = m(q-1) - \nu$ by $q-1$.*

Proof. Since the minimum distance of $RM_L(\nu, m)$ is at least $(R+1)q^Q - 1$, we only need to show a tuple of weight $(R+1)q^Q - 1$ in $RM_L(\nu, m)$. The image $\alpha(RM_L(\nu, m)) = RM_{\mathbb{F}_q}(\nu, m)$ has minimum distance exactly $(R+1)q^Q - 1$. Let $\mathbf{u} = (u_\infty, u_0, u_1, \ldots, u_{n-1})$ be a vector of weight $(R+1)q^Q - 1$ in $RM_{\mathbb{F}_q}(\nu, m)$. Let $I = \mathrm{supp}(\mathbf{u}) = \{i \mid u_i \neq 0\}$ the support of $\mathbf{u}$. Thus, $\mathrm{card}(I) = (R+1)q^Q - 1$. Then, there exists a vector $\mathbf{v} = (v_\infty, v_0, v_1, \ldots, v_{n-1}) \in RM_L(\nu, m)$ such that $\alpha(\mathbf{v}) = \bar{\mathbf{v}} = \mathbf{u}$ i.e. $(\bar{v}_\infty, \bar{v}_0, \bar{v}_1, \ldots, \bar{v}_{n-1}) = (u_\infty, u_0, u_1, \ldots, u_{n-1})$. Thus, $\bar{v}_i = u_i$ for all i.

If $i \notin I$, then $u_i = 0$. Thus, v_i is in pL, and $p^{s-1}v_i = 0$.

If $i \in I$, then $u_i \neq 0$ and $v_i \notin pL$, i.e. v_i is an invertible element of L, and $p^{s-1}v_i \neq 0$. Therefore, $p^{s-1}\mathbf{v} \in RM_L(\nu, m)$ and $p^{s-1}\mathbf{v}$ is of weight $(R+1)q^Q - 1$. Hence, $RM_L(\nu, m)$ has minimum distance $(R+1)q^Q - 1$. □

REFERENCES

[1] M. BHAINTWAL, S.K. WASAN: *On quasi-cyclic codes over $\mathbb{Z}_q$*, Appl. Algebra Eng.Comm.Comput., (2009).

[2] M. BHAINTWAL, S.K. WASAN: *Generalized Reed-Muller codes over $\mathbb{Z}_q$*, Des. Codes Cryptogr., **54** (2010), 149–166.

[3] J.T. BLACKFORD, D.K. RAY-CHAUDHURI: *A transform approach to permutation groups of cyclic codes over Galois rings*, IEEE Trans. Inform. Theory, **46** (2000), 2350–2358.

[4] I.F. BLAKE: *Codes over certain rings*, Inform. Control, **20** (1972), 396–404.

[5] I.F. BLAKE, R.C. MULLIN: *The mathematical theory of coding*, Academic Press, 1975.

[6] J. BORGES, C. FERNANDEZ, K.T. PHELPS: *Quaternary Reed-Muller codes*, IEEE Trans. Inform. Theory, **51** (2005), 2686–2691.

[7] P. DELSARTE, J.M. GOETHALS, F.J. MAC WILLIAMS: *On Generalized Reed-Muller Codes and Their Relatives*, Inform. Control, **16** (1970), 403–442.

[8] B.K. DEY, B.S. RAJAN: *Affine invariant extended cyclic codes over Galois rings*, IEEE Trans. Inform. Theory, **50**(4) (2004), 160.

[9] A.R. HAMMONS, P.V. KUMAR, A.R. CALDERBANK, N.J.A. SLOANE, P. SOLÉ: *The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

[10] T. KASAMI, S. LIN, W.W. PETERSON: *New generalizations of the Reed-Muller codes*, IEEE Trans. Inform. Theory, **14**(2) (1968), 189–205.

[11] S. KAWASAKI, M. YAMADA: *Reed-Muller codes over Galois rings of characteristic* 2^n, Sci.Rep.Kanazawa Univ., **56** (2012), 1–13.
[12] T. KIRAN, B.S. RAJAN: *Abelian codes over Galois rings closed under certain permutations*, IEEE Trans. Inform. Theory, **49**(9) (2003), 2242–2253
[13] B.R. MCDONALD: *Finite rings with identity*, Marcel Dekker, New York, 1974.
[14] J.H. VAN LINT: *Introduction to coding theory*, 3rd ed., Springer, 1998.
[15] Z.X. WAN: *Quaternary codes*, World Scientific, Singapore, 1997.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF ANTANANARIVO
ANTANANARIVO (101)
MADAGASCAR.
Email address: hariandriatahiny@gmail.com

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF ANTANANARIVO
ANTANANARIVO (101)
MADAGASCAR.
Email address: ratahirinjatovo@gmail.com

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF ANTANANARIVO
ANTANANARIVO (101)
MADAGASCAR.
Email address: sunnysfat@gmail.com