Reed-Muller Codes over Galois Rings of Characteristic 2⊠

メタデータ	言語: eng 出版者: 公開日: 2017-10-03 キーワード (Ja): キーワード (En): 作成者: 山田, 美枝子 メールアドレス: 所属:
URL	https://doi.org/10.24517/00011114

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 International License.

Sci. Rep. Kanazawa Univ.
Vol. 56, pp. 1–13, 2012

Reed-Muller Codes over Galois Rings of Characteristic 2^n

Soryo KAWASAKI[1], Mieko YAMADA[2]

[1] Division of Mathematical and Physical Sciences, Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa 920-1192, Japan,
E-MAIL: soryo-k@hotmail.co.jp

[2] Faculty of Mathematics and Physics, Institute of Science and Engineering, Kanazawa University, Kanazawa 920-1192, Japan,
E-MAIL: myamada@se.kanazawa-u.ac.jp

(Received November 28, 2012 and accepted in revised form January 23, 2013)

Abstract We consider the rth-order Reed-Muller codes $Z_qRM(r,m)$ of length 2^m over Galois rings of characteristic $q=2^n$ with extension degree m. This code has similar properties as a Reed-Muller code over a finite field. The Lee weight of the codeword of $Z_qRM(r,m)$ is expressed by cosine functions and qth roots of unity. We determine the minimum Lee weight of $Z_qRM(1,m)$, that is 2^m. Let $Z_qRM(1,m)^-$ be a shortened 1st-order Reed-Muller code. We show that the cyclic group generated by a shift mapping of codewords fixes $2Z_{\frac{q}{2}}RM(1,m)^-$ and acts on the cosets of $Z_qRM(1,m)^-$ modulo $2Z_{\frac{q}{2}}RM(1,m)^-$ transitively except for $2Z_{\frac{q}{2}}RM(1,m)^-$. It follows that the Lee weight distribution of $Z_qRM(1,m)^-$ can be obtained from the Lee weight distributions of the cosets of $Z_qRM(1,m)^-$ modulo $2Z_{\frac{q}{2}}RM(1,m)^-$.

Mathematics Subject Classifications(2000): 94B05, 94B15

Key words: Reed-Muller Codes, Codes over rings, Galois rings

1 Introduction

In 1994, Hammons et al. showed that the well-known binary codes, Kerdock, Preparata and Nordstrom-Robinson codes can be obtained as binary images of linear codes over Galois rings of characteristic 4 under the Gray map [3]. They also showed that the Kerdock codes over Galois rings of characteristic 4 are the dual codes of the Preparata codes over the same rings.

This led us to the active study of combinatorial topics over Galois rings. Borges et al. defined the quaternary Reed-Muller code and showed that this code has similar properties as a Reed-Muller code over a finite field [1]. They showed that a Reed-Muller code over a finite field is embedded in the ideal-part of this code. Recently Bhaintwal and Wasan [2] treated the generalized Reed-Muller codes over Z_{p^n} for a prime power p^n. They determined the minimum Hamming distance of the codes and characterized their properties.

In this paper, we restrict the characteristic q to a power of 2 and discuss the properties of Reed-Muller codes $Z_qRM(r,m)$ over these Galois rings. We give express the Lee weight of the codeword of $Z_qRM(r,m)$ in terms of cosine functions and qth roots of unity. We determine the minimum Lee weight of the 1st-order Reed-Muller code $Z_qRM(1,m)$ over this ring, which was not given in Bhaintwal and Wasan's paper [2]. Let $Z_qRM(1,m)^-$ be a shortened 1st-order Reed-Muller code. We show that the cyclic group generated by the cyclic shift mapping of codewords fixes $2Z_{\frac{q}{2}}RM(1,m)^-$ and acts on the cosets of $Z_qRM(1,m)^-$ modulo $2Z_{\frac{q}{2}}RM(1,m)^-$ transitively except for $2Z_{\frac{q}{2}}RM(1,m)^-$. It follows that the Lee weight distribution of the shortened Reed-Muller code $Z_qRM(1,m)^-$ can be obtained from the Lee weight distributions of the cosets of $Z_qRM(1,m)^-$ modulo $2Z_{\frac{q}{2}}RM(1,m)^-$.

2 Galois Rings $GR(2^n,m)$

We let $q=2^n, q'=q/2, Z_q=\boldsymbol{Z}/q\boldsymbol{Z}$ and denote a finite field with 2^m elements by F_{2^m}.

Let $h_2(x)$ be a primitive polynomial of degree m over F_2. If a monic irreducible polynomial $h_q(x)\in Z_q[x]$ satisfies $h_2(x)\equiv h_q(x) \pmod 2$ and divides $x^{2^m-1}-1$, then it is called a primitive basic polynomial of degree m over Z_q. Let ξ_q be a root of $h_q(x)$ of degree m such that $\xi_q^N=1$, where $N=2^m-1$. Then the residue ring $Z_q[x]/(h_q(x))$ is called a Galois ring of characteristic q with extension degree m and is written as $GR(q,m)$. We see $Z_q(\xi_q)\cong GR(q,m)$. If it doesn't depend on an extension degree, then we put $\mathscr{R}_q=GR(q,m)$ for convenience sake.

Every ideal of $\mathscr{R}_q$ is given by $\mathfrak{p}_q^l=2^l\mathscr{R}_q$, where $1\le l\le n-1$. The maximal ideal of $\mathscr{R}_q$ is $\mathfrak{p}_q=2\mathscr{R}_q$ and $\mathscr{R}_q/\mathfrak{p}_q\cong F_{2^m}$.

Every element $c\in\mathscr{R}_q$ has a unique 2-adic representation $c=\sum_{j=0}^{n-1}2^ja_j$, where $a_j\in\{0,1,\xi_q,\xi_q^2,\dots,\xi_q^{N-1}\}$, $0\le j\le n-1$. The automorphism $\mathscr{F}_q$ of $\mathscr{R}_q$ defined by $c^{\mathscr{F}_q}=\sum_{j=0}^{n-1}2^ja_j^2$ is called the Frobenius automorphism. The trace $T_q(c)$ of $c\in\mathscr{R}_q$ is defined by $T_q(c)=\sum_{j=0}^{m-1}c^{\mathscr{F}_q^j}$.

3 Codes over Z_q

If C is a Z_q-submodule of Z_q^N, then we call C a linear code of length N over Z_q. We define the Hadamard product $\boldsymbol{a}*\boldsymbol{b}$ in the usual way. We also define the Hamming weight, Hamming distance and the minimum Hamming weight in the same way of a finite field. The Lee weight of a vector $\boldsymbol{x}\in Z_q^N$ is defined by $w_L(\boldsymbol{x})=\sum_{i=1}^N\min\{x_i,q-x_i\}$ in $\boldsymbol{Z}$, the ring of rational integers, and the Lee distance of vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ is given by $d_L(\boldsymbol{x},\boldsymbol{y}) = w_L(\boldsymbol{x}-\boldsymbol{y})$. We define the minimum Lee distance of C to be the minimum Lee distance between distinct codewords. The minimum Lee distance is equal to the minimum Lee weight of the code C.

4 Reed-Muller Codes

4.1 Reed-Muller Codes over Galois Rings $GR(2^n,m)$

In [2], Bhaintwal and Wasan treated the Reed-Muller codes over a finite field and that over Galois rings of characteristic p^n, where p^n is any prime powers and any extension degree. They determined the minimum Hamming weight and gave some properties. In this paper, we restrict the characteristic to a power of 2 and discuss the properties of Reed-Muller codes over these rings.

Definition. Let ξ_q be a root of a primitive basic polynomial $h_q(x)$ of degree m. Let us consider the following $(m+1)\times(N+1)$ matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi_q & \xi_q^2 & \cdots & \xi_q^{N-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 & b_{1m} & b_{1m+1} & \cdots & b_{1N-1} \\ 0 & 0 & 1 & & 0 & b_{2m} & b_{2m+1} & \cdots & b_{2N-1} \\ \vdots & \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & & 1 & b_{mm} & b_{mm+1} & \cdots & b_{mN-1} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{1} \\ \boldsymbol{g_1} \\ \boldsymbol{g_2} \\ \vdots \\ \boldsymbol{g_m} \end{pmatrix},$$

where ξ_q^j in the second row is replaced by the m-tuple $(b_{1j}, b_{2j}, \ldots, b_{mj}) \in Z_q^m$ given by $\xi_q^j = b_{1j} + b_{2j}\xi_q + \cdots + b_{mj}\xi_q^{m-1}$, $0 \le j \le N-1$. We put $\boldsymbol{g_j^0} = \mathbf{1}$ $(1 \le j \le m)$, where $\mathbf{1}$ is the vector whose entries are all 1. Then, *rth-order Reed-Muller code* $Z_qRM(r,m)$ $(0 \le r \le m)$ of length $N+1$ over $\mathscr{R}_q$ is the code generated by the $(N+1)$-tuples of the form

$$\boldsymbol{g_1^{i_1}} * \boldsymbol{g_2^{i_2}} * \cdots * \boldsymbol{g_m^{i_m}},$$

where $i_j = 0,1$ $(1 \le j \le m)$, $\sum_{j=1}^m i_j \le r$. In particular, $Z_2RM(r,m)$ is a Reed-Muller code $RM(r,m)$ of a finite field and $Z_4RM(r,m)$ is a quaternary Reed-Muller code $QRM(r,m)$. We also see that $Z_qRM(0,m) = \{\varepsilon\mathbf{1} \mid \varepsilon \in Z_q\}$ and $Z_qRM(m,m) = Z_q^{2^m}$.

If $h_q(x) \in Z_q[x]$ is a primitive basic polynomial of degree m and d is a divisor of q, then $h_q(x) \in Z_d[x] \pmod{d\mathscr{R}_q}$ is a primitive basic polynomial of degree m. Let α be the natural homomorphism from $\mathscr{R}_q$ to $\mathscr{R}_q/\mathfrak{p}_q$. Then, we have

$$\alpha\Big(Z_qRM(r,m)\Big) = RM(r,m).$$

We define the map $\tau : \mathscr{R}_q \to \mathscr{R}_{\frac{q}{2}}$ as $\tau(c) \equiv c \pmod{\frac{q}{2}\mathscr{R}_q}$ for $c \in \mathscr{R}_q$. Then we obtain

$$\tau\Big(Z_qRM(r,m)\Big) = Z_{\frac{q}{2}}RM(r,m).$$

We notice that the commutative relationship between trace functions and the maps α or τ holds.

For the preparation, we give the Lee weight distribution of $Z_4RM(1,m)$ which was given in [1] and [3].

The case $m \geq 3$ odd;

Lee weight	number of codewords
0	1
$2^m - 2^{\frac{m-1}{2}}$	$2^{m+1}(2^m-1)$
2^m	$2^{m+2}-2$
$2^m + 2^{\frac{m-1}{2}}$	$2^{m+1}(2^m-1)$
2^{m+1}	1

The case $m \geq 2$ even;

Lee weight	number of codewords
0	1
$2^m - 2^{\frac{m}{2}}$	$2^m(2^m-1)$
2^m	$2^{m+1}(2^m+1)-2$
$2^m + 2^{\frac{m}{2}}$	$2^m(2^m-1)$
2^{m+1}	1

$Z_qRM(r,m)$ has the following properties similar to $RM(r,m)$ and $QRM(r,m)$.

Theorem 1 ([1], [2], [3])**.** (1) *The number of codewords of $Z_qRM(r,m)$ is q^k, where* $k = \sum_{s=0}^{r} \binom{m}{s}$.

(2) *$Z_qRM(r,m)$ is contained in $Z_qRM(r+1,m)$ for $0 \leq r < m$.*

(3) *The minimum Hamming weight of $Z_qRM(r,m)$ is 2^{m-r}.*

4.2 The Lee Weight $w_L(\boldsymbol{c})$ of the Codeword

The entry of the codeword of $Z_qRM(r,m)$ is given by using a trace function T_q.

Lemma 1. *Let $1 \leq i_1 < i_2 < \cdots < i_s \leq m\,(1 \leq s \leq r)$. We put $\xi_q^{\infty} = 0$. For $\boldsymbol{g}_{i_\beta}$, $1 \leq \beta \leq s$, there exists a unique element $\mu_{i_\beta} \in \mathscr{R}_q$ such that*

$$\boldsymbol{g}_{i_\beta} = (T_q(\mu_{i_\beta}\xi_q^{\infty}), T_q(\mu_{i_\beta}), T_q(\mu_{i_\beta}\xi_q), T_q(\mu_{i_\beta}\xi_q^2), \ldots, T_q(\mu_{i_\beta}\xi_q^{N-1})).$$

Then, for $t \in \{\infty, 0, 1, \ldots, N-1\}$, the tth entry, say g_t, of $\boldsymbol{g}_{i_1} * \cdots * \boldsymbol{g}_{i_s}$ is given as

$$g_t = \sum_{l_2=0}^{m-1} \cdots \sum_{l_s=0}^{m-1} T_q(\mu_{i_1}\mu_{i_2}{}^{2^{l_2}} \cdots \mu_{i_s}{}^{2^{l_s}} \xi_q^{(1+2^{l_2}+\cdots+2^{l_s})t}).$$

Hence the tth entry, say c_t, of each codeword of $Z_qRM(r,m)$ is represented as

$$c_t = T_q(\lambda_t \xi_q^t) + \varepsilon$$

for some unique element λ_t of $\mathscr{R}_q$ and $\varepsilon \in Z_q$.

Proof. We can prove the theorem similarly to the proof of Theorem 11 in [3]. □

We notice that there exists a unique element $\mu_i \in \mathscr{R}_q$ such that

$$\begin{aligned} \boldsymbol{g_i} &= (0,\ldots,0,\overset{i}{\smile}{1},0,\ldots,0,b_{im},\ldots,b_{iN-1}) \\ &= (T_q(\mu_i\xi_q^{\infty}),T_q(\mu_i),T_q(\mu_i\xi_q),\ldots,T_q(\mu_i\xi_q^{N-1})). \end{aligned}$$

Denote the number of entries of the vector $\boldsymbol{x}$ that are equal to d by $s(d)$ and let ζ_q be a primitive qth root of unity. Then we have

$$s(d) = \sum_{x_i \in \boldsymbol{x}} \frac{1}{q} \sum_{t=0}^{q-1} \zeta_q^{t(x_i-d)}.$$

Lemma 2 gives a formula which is used in Theorem 2.

Lemma 2. *Assume $q \geq 8$. Then the following equality holds.*

$$q' + \sum_{w=1}^{\frac{q'}{2}-1} 2(q'-2w)\cos\frac{w\pi t}{q'} = q'\prod_{j=1}^{n-2}(\cos(\frac{\pi t}{2^{j+1}})+1).$$

Proof. We prove the lemma by induction on q. It is easily verified that the equality holds for $q=8$. From the induction hypothesis,

$$\begin{aligned} & q\prod_{j=1}^{n-1}(\cos(\frac{\pi t}{2^{j+1}})+1) \\ &= 2(\cos\frac{\pi t}{q}+1)\left\{q' + \sum_{w=1}^{\frac{q'}{2}-1} 2(q'-2w)\cos\frac{w\pi t}{q'}\right\} \\ &= q(\cos\frac{\pi t}{q}+1) + \sum_{w=1}^{\frac{q'}{2}-1} 4(q'-2w)\Big(\cos\frac{w\pi t}{q'} + \cos\frac{w\pi t}{q'}\cos\frac{\pi t}{q}\Big) \\ &= q(\cos\frac{\pi t}{q}+1) + \sum_{w=1}^{\frac{q'}{2}-1} 2(q'-2w)\Big(2\cos\frac{2w\pi t}{q} + \cos\frac{(2w-1)\pi t}{q} + \cos\frac{(2w+1)\pi t}{q}\Big) \end{aligned}$$

$$
\begin{aligned}
&= q + 2(q-2)\cos\frac{\pi t}{q} + \sum_{w=1}^{\frac{q'}{2}-1} 2(q-4w)\cos\frac{2w\pi t}{q} \\
&\quad + \sum_{w=1}^{\frac{q'}{2}-2} 2(q-4w-2)\cos\frac{(2w+1)\pi t}{q} + 4\cos\frac{(q'-1)\pi t}{q} \\
&= q + \sum_{w=1}^{q'-1} 2(q-2w)\cos\frac{w\pi t}{q}.
\end{aligned}
$$

□

We express the Lee weight of the codeword of $Z_qRM(r,m)$ in terms of cosine functions and qth roots of unity.

Theorem 2. *Assume that $q \geq 8$. The Lee weight of a codeword $\boldsymbol{c}$ of $Z_qRM(r,m)$ is*

$$
w_L(\boldsymbol{c}) = q2^{m-2} - \frac{1}{2} \sum_{\substack{t:odd \\ 0\leq t\leq q-1}} \prod_{j=1}^{n-2} (\cos(\frac{\pi t}{2^{j+1}}) + 1) \sum_{c_i \in \boldsymbol{c}} \zeta_q^{tc_i},
$$

where $c_i = T_q(\mu_i \xi_q^i) + \varepsilon$ in Lemma 1.

Proof. From $\zeta_q^{at} + \zeta_q^{(q-a)t} = 2\cos\pi t \cos\frac{(q-2a)\pi t}{q}$ and $\sum_{j=1}^{q'} \zeta_q^{-2jl} = 0$,

$$
\begin{aligned}
w_L(\boldsymbol{c}) = &\sum_{c_i \in \boldsymbol{c}} \left\{ \sum_{j=1}^{q'} \frac{j}{q} \sum_{t=0}^{q-1} \zeta_q^{t(c_i-j)} + \sum_{j=q'+1}^{q-1} \frac{q-j}{q} \sum_{t=0}^{q-1} \zeta_q^{t(c_i-j)} \right\} \\
= &\frac{1}{q} \sum_{c_i \in \boldsymbol{c}} \left\{ q'^2 + \sum_{\substack{t:odd \\ 0\leq t\leq q-1}} \zeta_q^{tc_i} \left(\zeta_q^{-t} + 2\zeta_q^{-2t} + \cdots + q'\zeta_q^{-q't} \right.\right. \\
&\left.\left. + (q'-1)\zeta_q^{-(q'+1)t} + \cdots + \zeta_q^{-(q-1)t} \right) \right\} \\
&+ \frac{1}{q} \sum_{c_i \in \boldsymbol{c}} \sum_{l=1}^{q'-1} \zeta_q^{2lc_i} \left(\zeta_q^{-2l} + 2\zeta_q^{-4l} + \cdots + q'\zeta_q^{-ql} + (q'-1)\zeta_q^{-(q+2)l} + \cdots + \zeta_q^{-2(q-1)l} \right) \\
= &\frac{1}{q} \sum_{c_i \in \boldsymbol{c}} \left\{ q'^2 + \sum_{\substack{t:odd \\ 0\leq t\leq q-1}} \zeta_q^{tc_i} \left(q'\cos\pi t + \sum_{j=1}^{q'-1} 2j\cos\pi t \cos\frac{(q-2j)\pi t}{q} \right) \right\} \\
&+ \frac{1}{q} \sum_{c_i \in \boldsymbol{c}} \sum_{l=1}^{q'-1} \zeta_q^{2lc_i} \left(\zeta_q^{-2l} + 2\zeta_q^{-4l} + \cdots + q'\zeta_q^{-ql} + (q'-1)\zeta_q^{-2l} + \cdots + \zeta_q^{-(q-2)l} \right)
\end{aligned}
$$

$$
\begin{aligned}
=&\frac{1}{q}\sum_{c_i\in \boldsymbol{c}}\Big\{q'^2-\sum_{\substack{t:odd\\0\le t\le q-1}}\zeta_q^{tc_i}\Big(q'+\sum_{j=1}^{q'-1}2j\cos\frac{(q'-j)\pi t}{q'}\Big)\Big\}\\
&+\frac{1}{q}\sum_{c_i\in \boldsymbol{c}}\sum_{l=1}^{q'-1}\zeta_q^{2lc_i}q'(\zeta_q^{-2l}+\zeta_q^{-4l}+\cdots+\zeta_q^{-ql})\\
=&\frac{1}{q}\sum_{c_i\in \boldsymbol{c}}q'^2-\frac{1}{q}\sum_{\substack{t:odd\\0\le t\le q-1}}\Big(q'+\sum_{j=1}^{q'-1}2j\cos\frac{(q'-j)\pi t}{q'}\Big)\sum_{c_i\in \boldsymbol{c}}\zeta_q^{tc_i}\\
=&q'2^{m-1}-\frac{1}{q}\sum_{\substack{t:odd\\0\le t\le q-1}}\Big(q'+\sum_{w=1}^{\frac{q'}{2}-1}2(q'-2w)\cos\frac{w\pi t}{q'}\Big)\sum_{c_i\in \boldsymbol{c}}\zeta_q^{tc_i}.
\end{aligned}
$$

From Lemma 2, we obtain

$$
w_L(\boldsymbol{c})=q2^{m-2}-\frac{1}{2}\sum_{\substack{t:odd\\0\le t\le q-1}}\prod_{j=1}^{n-2}(\cos(\frac{\pi t}{2^{j+1}})+1)\sum_{c_i\in \boldsymbol{c}}\zeta_q^{tc_i}.
$$

□

4.3 An Embedding System of $Z_qRM(r,m)$

We will show that if $q\ge 8$, then $Z_{\frac{q}{2}}RM(r,m)$ is embedded in the ideal part $Z_qRM(r,m)\cap\mathfrak{p}_q$ of $Z_qRM(r,m)$.

Theorem 3. *The code $Z_qRM(r,m)$ has the following partition.*

$$
\begin{aligned}
Z_qRM(r,m)=\bigcup_{e_0,e_1,\dots,e_{k-1}\in Z_2}\Big(&2Z_{q'}RM(r,m)+\big(e_0\mathbf{1}+e_1\boldsymbol{g_1}+\cdots+e_m\boldsymbol{g_m}\\
&+e_{m+1}\boldsymbol{g_1}*\boldsymbol{g_2}+\cdots+e_{k-1}\boldsymbol{g}_{m-r+1}*\boldsymbol{g}_{m-r+2}*\cdots*\boldsymbol{g_m}\big)\Big),
\end{aligned}
$$

where $k=\sum_{s=0}^{r}\binom{m}{s}$.

Proof. First we prove that the subsets $2Z_{q'}RM(r,m)+e_0\mathbf{1}+e_1\boldsymbol{g_1}+\cdots+e_{k-1}\boldsymbol{g}_{m-r+1}*\boldsymbol{g}_{m-r+2}*\cdots*\boldsymbol{g_m}$ are disjoint. We denote the $(N+1)$-tuples of the form $\boldsymbol{g_1}^{i_1}*\boldsymbol{g_2}^{i_2}*\cdots*\boldsymbol{g_m}^{i_m}$ by $\boldsymbol{r_i}$ $(1\le i\le k-1)$, where $i_j=0,\ 1$ $(1\le j\le m)$. Assume that

$$
2\boldsymbol{x}+a_0\mathbf{1}+a_1\boldsymbol{r_1}+\cdots+a_{k-1}\boldsymbol{r}_{k-1}=2\boldsymbol{y}+b_0\mathbf{1}+b_1\boldsymbol{r_1}+\cdots+b_{k-1}\boldsymbol{r}_{k-1},
$$

where $\boldsymbol{x},\boldsymbol{y}\in Z_{q'}RM(r,m)$. Thus,

$$
2(\boldsymbol{x}-\boldsymbol{y})=(b_0-a_0)\mathbf{1}+(b_1-a_1)\boldsymbol{r_1}+\cdots+(b_{k-1}-a_{k-1})\boldsymbol{r}_{k-1},
$$

and applying the map α,

$$\mathbf{0} = (b_0 - a_0)\mathbf{1} + (b_1 - a_1)\alpha(\boldsymbol{r_1}) + \cdots + (b_{k-1} - a_{k-1})\alpha(\boldsymbol{r}_{k-1}).$$

Since $\mathbf{1}$ and $\alpha(\boldsymbol{r_1}), \alpha(\boldsymbol{r_2}), \ldots, \alpha(\boldsymbol{r}_{k-1})$ are basis vectors of $RM(r,m)$, then $a_i = b_i$, $0 \le i \le k-1$. Therefore, the cosets are disjoint.

We put $\boldsymbol{g_0} = \mathbf{1}$. From now on, we will show that

$$Z_q RM(r,m) \subseteq \bigcup_{e_0, e_1, \ldots, e_{k-1} \in Z_2} \Big(2Z_{q'} RM(r,m) + \big(e_0 \mathbf{1} + e_1 \boldsymbol{g_1} + \cdots + e_m \boldsymbol{g_m} + e_{m+1} \boldsymbol{g_1} * \boldsymbol{g_2} + \cdots + e_{k-1} \boldsymbol{g}_{m-r+1} * \boldsymbol{g}_{m-r+2} * \cdots * \boldsymbol{g_m}\big)\Big).$$

First, we consider the case $r = 1$. We put

$$C_1 = \left\{ 2\boldsymbol{x_1} + \sum_{i=0}^{m} d_i \boldsymbol{g_i} \mid 2\boldsymbol{x_1} \in 2Z_{q'} RM(1,m), d_i \in Z_2 \right\}.$$

If we put $a_i = 2\delta_i + \nu_i \in Z_q, \delta_i \in Z_{q'}, \nu_i \in Z_2$, then $\sum_{i=0}^{m} a_i \boldsymbol{g_i} = \sum_{i=0}^{m} (2\delta_i + \nu_i) \boldsymbol{g_i} \in C_1$, that is, $Z_q RM(1,m) \subseteq C_1$. Since $\big|C_1\big| = \Big|Z_q RM(1,m)\Big| = q^{m+1}$ from Theorem 1, we obtain $Z_q RM(1,m) = C_1$.

Next, we assume $r = 2$. We put

$$C_2 = \left\{ 2\boldsymbol{x_2} + \sum_{i=0}^{m} d_i \boldsymbol{g_i} + \sum_{1 \le i < j \le m} e_{ij} \boldsymbol{g_i} * \boldsymbol{g_j} \mid 2\boldsymbol{x_2} \in 2Z_{q'} RM(2,m), d_i, e_{ij} \in Z_2 \right\}.$$

If we put $b_{ij} = 2\delta_{ij} + \nu_{ij}, \delta_{ij} \in Z_{q'}, \nu_{ij} \in Z_2$, then $2\delta_{ij} \boldsymbol{g_i} * \boldsymbol{g_j} \in 2Z_{q'} RM(2,m)$, $\nu_{ij} \boldsymbol{g_i} * \boldsymbol{g_j} \in C_2$, and

$$\sum_{1 \le i < j \le m} b_{ij} \boldsymbol{g_i} * \boldsymbol{g_j} = \sum_{1 \le i < j \le m} (2\delta_{ij} + \nu_{ij}) \boldsymbol{g_i} * \boldsymbol{g_j} \in C_2,$$

so that $\sum_{i=0}^{m} a_i \boldsymbol{g_i} + \sum_{1 \le i < j \le m} b_{ij} \boldsymbol{g_i} * \boldsymbol{g_j} \in C_2$. It yields $Z_q RM(2,m) \subseteq C_2$.

From Theorem 1, $\big|C_2\big| = q^k$ and $\Big|Z_q RM(2,m)\Big| = q^k$, where $k = \sum_{s=0}^{2} \binom{m}{s}$. Therefore $Z_q RM(2,m) = C_2$.

It can be proved in a similar way for the case $r \ge 3$. □

The above theorem implies that $Z_{\frac{q}{2}} RM(r,m)$ is embedded in the ideal-part of $Z_q RM(r,m)$.

4.4 Minimum Lee Weight of $Z_qRM(1,m)$

It is easily verified that $w_L^{(q)}(\tau(\boldsymbol{c})) \leq w_L^{(2q)}(\boldsymbol{c})$ where $w_L^{(q)}(\tau(\boldsymbol{c}))$ and $w_L^{(2q)}(\boldsymbol{c})$ are the Lee weights of the codewords of $\tau(\boldsymbol{c})$ of $Z_qRM(r,m)$ and $\boldsymbol{c}$ of $Z_{2q}RM(r,m)$ respectively.

Theorem 4. *Suppose that $q \geq 8, m \geq 3$ and $(q,m) \neq (8,3)$. The minimum Lee weight of $Z_qRM(1,m)$ is 2^m and $\mathbf{1}, -\mathbf{1}$ are the codewords with minimum Lee weight. For the case $(q,m) = (8,3)$, the minimum Lee weight is 6.*

Proof. It is sufficient to prove the minimum Lee weight of $Z_8RM(1,m)$ is 2^m. We put $C = Z_8RM(1,m)$. The Lee weight of every codeword $\boldsymbol{c} \in C$ is written as

$$w_L(\boldsymbol{c}) = n_1 + n_7 + 2(n_2 + n_6) + 3(n_3 + n_5) + 4n_4,$$

where n_i is the number of entries of the codeword $\boldsymbol{c}$ that are equal to i for $0 \leq i < 8$.

We assume that $w_L(\boldsymbol{c}) < 2^m$ for every $\boldsymbol{c} \in C, \boldsymbol{c} \neq \varepsilon\mathbf{1}, \varepsilon \in Z_q$. Since the minimum Hamming weight of $RM(1,m)$ is 2^{m-1}, $2^m > w_L(\boldsymbol{c}) \geq 2(n_2 + n_6 + n_4) + n_1 + n_7 + n_3 + n_5 = 3 \cdot 2^{m-1} - 2n_0$. Thus

$$n_0 > 2^{m-2}. \tag{4.1}$$

We put $a = n_0 - n_4, b = n_1 - n_5, c = n_2 - n_6, d = n_3 - n_7$. By (4.1), we have $a = n_0 - n_4 > 0$. Let ζ be a primitive 8th root of unity. From the theorem by Kumar et al. [4, Theorem 1], we obtain

$$\left| a + b\zeta + c\zeta^2 + d\zeta^3 \right| < 3\sqrt{2^m}.$$

We substitute $\zeta = \frac{\sqrt{2}}{2}(1 + \sqrt{-1})$ to the above inequality.

$$a + b\zeta + c\zeta^2 + d\zeta^3 = (a + \frac{\sqrt{2}}{2}b - \frac{\sqrt{2}}{2}d) + \sqrt{-1}(c + \frac{\sqrt{2}}{2}b + \frac{\sqrt{2}}{2}d).$$

Therefore

$$\begin{aligned}
&\left| a + b\zeta + c\zeta^2 + d\zeta^3 \right|^2 \\
= \ & (a + \frac{\sqrt{2}}{2}b - \frac{\sqrt{2}}{2}d)^2 + (c + \frac{\sqrt{2}}{2}b + \frac{\sqrt{2}}{2}d)^2 \\
= \ & \frac{\sqrt{2}}{2}(a + b + c + d)^2 + (1 - \frac{\sqrt{2}}{2})(a^2 + b^2 + c^2 + d^2) - \sqrt{2}(a(2d + c) + bd) \qquad (4.2) \\
< \ & 9 \cdot 2^m.
\end{aligned}$$

We assume that m is odd. By the table in Subsection 4.1, we have

$$n_0 + n_4 = 2^{m-2} + 2^{\frac{m-3}{2}}, \quad n_2 + n_6 = 2^{m-2} - 2^{\frac{m-3}{2}},$$
$$n_1 + n_5 = 2^{m-2} + \delta 2^{\frac{m-3}{2}}, \quad n_3 + n_7 = 2^{m-2} - \delta 2^{\frac{m-3}{2}},$$

where $\delta = \pm 1$. Then it follows

$$\begin{aligned}2^m > w_L(\boldsymbol{c}) &\geq n_1 + n_7 + 3(n_3 + n_5) + 2(n_2 + n_6)\\ &= 3 \cdot 2^{m-1} - 2(n_1 + n_7) + 2(2^{m-2} - 2^{\frac{m-3}{2}})\\ &= 2^{m+1} - 2^{\frac{m-1}{2}} - 2(n_1 + n_7).\end{aligned}$$

Therefore $n_1 + n_7 > 2^{m-1} - 2^{\frac{m-3}{2}}$.

Since $w_L(\boldsymbol{c}) = w_L(-\boldsymbol{c})$ for $\boldsymbol{c} \in C$, we may assume $n_1 > n_7$ without loss of generality. Since $2n_1 > n_1 + n_7 > 2^{m-1} - 2^{\frac{m-3}{2}}$,

$$n_1 > 2^{m-2} - 2^{\frac{m-5}{2}}, \tag{4.3}$$

and

$$n_3 + n_5 = 2^{m-1} - (n_1 + n_7) < 2^{m-1} - (2^{m-1} - 2^{\frac{m-3}{2}}) = 2^{\frac{m-3}{2}}.$$

Then $n_1 > 2^{m-2} - 2^{\frac{m-5}{2}} > 2^{\frac{m-3}{2}} > n_3 + n_5 \geq n_5$, so that $b > 0$. Furthermore from $n_1 + n_7 > 2^{m-1} - 2^{\frac{m-3}{2}}$ and $2^{m-2} - 2^{\frac{m-5}{2}} < n_1 \leq 2^{m-2} + 2^{\frac{m-3}{2}}$,

$$n_7 > 2^{m-2} - 2^{\frac{m-1}{2}}. \tag{4.4}$$

For $m > 3$, we have $n_7 > 2^{m-2} - 2^{\frac{m-1}{2}} > 2^{\frac{m-3}{2}} > n_3 + n_5 \geq n_3$, so that $d < 0$ and $bd < 0$. Thus

$$\begin{aligned}d &< 2^{\frac{m-3}{2}} - (2^{m-2} - 2^{\frac{m-1}{2}}) = -2^{m-2} + 2^{\frac{m-3}{2}} + 2^{\frac{m-1}{2}},\\ c &\leq 2^{m-2} - 2^{\frac{m-3}{2}}.\end{aligned}$$

Then we have

$$\begin{aligned}2d + c &< 2(-2^{m-2} + 2^{\frac{m-3}{2}} + 2^{\frac{m-1}{2}}) + 2^{m-2} - 2^{\frac{m-3}{2}}\\ &= -2^{m-2} + 2^{\frac{m-3}{2}} + 2^{\frac{m+1}{2}}.\end{aligned}$$

Furthermore we assume $m \geq 7$, then $2d + c < 0$. We see the last term $-\sqrt{2}(a(2d + c) + bd) > 0$ of the equality (4.2). Also we see $\delta = 1$ as $n_5 = 2^{m-2} + \delta 2^{\frac{m-3}{2}} - n_1 < \delta 2^{\frac{m-3}{2}} + 2^{\frac{m-5}{2}}$ from (4.3).

Consequently from $(1 - \frac{\sqrt{2}}{2})(a^2 + b^2 + c^2 + d^2) > \frac{1}{4}(a^2 + b^2 + c^2 + d^2)$, we obtain

$$\frac{1}{4}(a^2 + b^2 + c^2 + d^2) < \left| a + b\zeta + c\zeta^2 + d\zeta^3 \right|^2 < 9 \cdot 2^m.$$

On the other hand,

$$\begin{aligned}a^2 + b^2 + c^2 + d^2 = (n_0 + n_4)^2 &+ (n_1 + n_5)^2\\ &+ (n_2 + n_6)^2 + (n_3 + n_7)^2 - 4(n_0 n_4 + n_1 n_5 + n_2 n_6 + n_3 n_7)\\ = 4(2^{2m-4} &+ 2^{m-3}) - 4(n_0 n_4 + n_1 n_5 + n_2 n_6 + n_3 n_7).\end{aligned}$$

Thus it follows

$$\frac{1}{4}(a^2+b^2+c^2+d^2) = 2^{2m-4}+2^{m-3}-(n_0n_4+n_1n_5+n_2n_6+n_3n_7) < 9\cdot 2^m.$$

Therefore we obtain

$$2^{2m-4}-71\cdot 2^{m-3} < n_0n_4+n_1n_5+n_2n_6+n_3n_7.$$

From (4.1), we have $n_0n_4 = n_0(2^{m-2}+2^{\frac{m-3}{2}}-n_0) < 2^{m-2+\frac{m-3}{2}}$. We have $n_1n_5 < 3\cdot 2^{\frac{m-5}{2}}(2^{m-2}-2^{\frac{m-5}{2}})$, $n_3n_7 < 2^{\frac{m-3}{2}}(2^{m-2}-2^{\frac{m-1}{2}})$ by using (4.3) and (4.4). When $n_2 = \frac{1}{2}(2^{m-2}-2^{\frac{m-3}{2}})$, $n_2n_6 = n_2(2^{m-2}-2^{\frac{m-3}{2}}-n_2)$ has the maximal value, it leads $n_2n_6 \le \frac{1}{4}(2^{m-2}-2^{\frac{m-3}{2}})^2$. From the above result, we have

$$\begin{aligned}
&2^{2m-4}-71\cdot 2^{m-3}\\
&\quad < n_0n_4+n_1n_5+n_2n_6+n_3n_7\\
&\quad < 2^{m-2+\frac{m-3}{2}}+\frac{1}{4}(2^{m-2}-2^{\frac{m-3}{2}})^2+3\cdot 2^{\frac{m-5}{2}}(2^{m-2}-2^{\frac{m-5}{2}})+2^{\frac{m-3}{2}}(2^{m-2}-2^{\frac{m-1}{2}})\\
&\quad = 6\cdot 2^{m-3+\frac{m-3}{2}}+2^{2m-6}-5\cdot 2^{m-4}.
\end{aligned}$$

If we put $x = 2^{\frac{m-3}{2}} \ge 4$, then the above inequality is written as

$$\frac{x^2}{2}(6x^2-12x-137) < 0.$$

The inequality does not hold for $x \ge 6$, namely $m \ge 9$. Therefore we have $w_L(\boldsymbol{c}) \ge 2^m$ for odd $m > 7$.

Next, we assume that m is even. By the table in Subsection 4.1, we know n_j+n_{j+4} is one of the following values $0, 2^{m-2}\pm 2^{\frac{m-2}{2}}, 2^{m-2}, 2^{m-1}, 2^m$ for $0 \le j < 4$. The Lee weight of the codeword $w_L(\boldsymbol{c})$ is greater than or equal to 2^m if $n_j+n_{j+4} = 2^m$ for some j, $n_1+n_3+n_5+n_7 = 2^m$, or $n_2+n_6 = 2^{m-1}$. For the case $n_0+n_4 = n_2+n_6 = 2^{m-2}$ and $n_1+n_3+n_5+n_7 = 2^{m-1}$, $w_L(\boldsymbol{c}) = 2(n_2+n_6)+4n_4+2^{m-1}+2(n_3+n_5) \ge 2^m$.

We discuss in a similar way to the proof of odd m for the other cases. We put $x = 2^{\frac{m-2}{2}}$. For $n_0+n_4 = 2^{m-2}+2^{\frac{m-2}{2}}, n_2+n_6 = 2^{m-2}-2^{\frac{m-2}{2}}, n_{l+1}+n_{l+5} = 2^{m-2}+\delta 2^{\frac{m-2}{2}}$, $\delta = \pm 1$, $l = 0,2$, we obtain

$$\frac{x^2}{4}(3x^2-12x-130) < 0$$

and for $n_0+n_4 = 2^{m-2}+2^{\frac{m-2}{2}}, n_2+n_6 = 2^{m-2}-2^{\frac{m-2}{2}}, n_{l+1}+n_{l+5} = 2^{m-2}$, $l = 0,2$, we obtain

$$\frac{x^2}{4}(3x^2-8x-138) < 0.$$

Thus we have $w_L(\boldsymbol{c}) \ge 2^m$ for even $m > 8$.

We see the codewords $\mathbf{1}$ and $-\mathbf{1}$ have the minimum Lee weight 2^m. Hence the minimum Lee weight of $Z_qRM(1,m)$ is 2^m for $m > 8$ and $q \geq 8$. It remains to verify the case for $m \leq 8$. We obtain the minimum Lee weight is 2^m for $4 \leq m \leq 8$ and $q = 8$ by a computer search. We also obtain the minimum Lee weight of $Z_8RM(1,3)$ is 6 and that of $Z_{16}RM(1,3)$ is 2^3 by a computer search. Thus the minimum Lee weight of $Z_qRM(1,m)$ for $q \geq 8,\ 3 \leq m \leq 8,\ (q,m) \neq (8,3)$ is 2^m. □

4.5 Lee Weight Distribution of $Z_qRM(1,m)^-$

Let $\bar{\boldsymbol{g}}_1, \bar{\boldsymbol{g}}_2, \ldots, \bar{\boldsymbol{g}}_m$ be the vectors obtained from $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_m$ by removing the first entry. The cyclic code $Z_qRM(1,m)^-$ is defined from $\bar{\boldsymbol{g}}_1, \bar{\boldsymbol{g}}_2, \ldots, \bar{\boldsymbol{g}}_m$ in the same way as $Z_qRM(1,m)$, which is called a shortened 1st-order Reed-Muller code. The shift mapping S is defined as

$$\begin{aligned} S : Z_qRM(1,m)^- &\to \quad Z_qRM(1,m)^-, \\ \boldsymbol{v} = (a_1, a_2, \ldots, a_N) &\mapsto \quad S(\boldsymbol{v}) = \boldsymbol{v}^{(1)} = (a_N, a_1, a_2, \ldots, a_{N-1}). \end{aligned}$$

We denote a cyclic group of order N with a generater S by G. We can show that $Z_qRM(1,m)^-$ has the following partition similarly to Theorem 3:

$$Z_qRM(1,m)^- = \bigcup_{D_1,D_2,\ldots,D_m \in Z_2} \left(2Z_{q'}RM(1,m)^- + D_1\bar{\boldsymbol{g}}_1 + D_2\bar{\boldsymbol{g}}_2 + \cdots + D_m\bar{\boldsymbol{g}}_m\right).$$

Let

$$\begin{aligned} &Z_qRM(1,m)^-/2Z_{q'}RM(1,m)^- \\ &\qquad = \left\{2Z_{q'}RM(1,m)^- + D_1\bar{\boldsymbol{g}}_1 + D_2\bar{\boldsymbol{g}}_2 + \cdots + D_m\bar{\boldsymbol{g}}_m \mid D_1, D_2, \ldots, D_m \in Z_2\right\} \end{aligned}$$

be the quotient group of $Z_qRM(1,m)^-$ modulo the ideal-part $2Z_{q'}RM(1,m)^-$.

Theorem 5. *G acts on $Z_qRM(1,m)^-/2Z_{q'}RM(1,m)^-$ transitively except for $2Z_{q'}RM(1,m)^-$. That is, the cosets of $Z_qRM(1,m)^-/2Z_{q'}RM(1,m)^-$ have the same Lee weight distribution. The ideal-part $2Z_{q'}RM(1,m)^-$ is fixed by G.*

Proof. We put $\boldsymbol{v} = (a_1, a_2, \ldots, a_N) \in 2Z_{q'}RM(1,m)^- + b_1\bar{\boldsymbol{g}}_1 + b_2\bar{\boldsymbol{g}}_2 + \cdots + b_m\bar{\boldsymbol{g}}_m$, and $\boldsymbol{v}^{(s)} = (a_1^{(s)}, a_2^{(s)}, \ldots, a_N^{(s)}) \in 2Z_{q'}RM(1,m)^- + b_1^{(s)}\bar{\boldsymbol{g}}_1 + b_2^{(s)}\bar{\boldsymbol{g}}_2 + \cdots + b_m^{(s)}\bar{\boldsymbol{g}}_m$. We know $b_i = \alpha(a_i)$ and $b_i^{(s)} = \alpha(a_i^{(s)})$ for $i \in \{1, 2, \ldots, m\}$ easily.

We prove $(b_1, b_2, \ldots, b_m) \neq (b_1^{(s)}, b_2^{(s)}, \ldots, b_m^{(s)})$. The vector $\bar{\boldsymbol{g}}_i$ is written as

$$\bar{\boldsymbol{g}}_i = (T_q(\mu_i), T_q(\mu_i\xi_q), T_q(\mu_i\xi_q^2), \ldots, T_q(\mu_i\xi_q^{N-1}))$$

for some element $\mu_i \in \mathscr{R}_q$ from Lemma 1. Let $\lambda_i = \alpha(\mu_i)$ and $\theta = \alpha(\xi_q)$. From the commutability of the trace function and the map α, the l-th entry of $\alpha(\boldsymbol{v})$ is given as

$$\begin{aligned} b_1T_2(\lambda_1\theta^l)+b_2T_2(\lambda_2\theta^l)+\cdots+b_mT_2(\lambda_m\theta^l) &= T_2((b_1\lambda_1+b_2\lambda_2+\cdots+b_m\lambda_m)\theta^l) \\ &= T_2(\theta^{j+l}) \end{aligned}$$

for some integer j. Thus we obtain

$$\alpha(\boldsymbol{v}) = (T_2(\theta^j), T_2(\theta^{j+1}), \ldots, T_2(\theta^{j+N-1}))$$

and also

$$\alpha(\boldsymbol{v}^{(s)}) = (T_2(\theta^t), T_2(\theta^{t+1}), \ldots, T_2(\theta^{t+N-1}))$$

for some integer t.

Since the sequence $T_2(\theta^n)$, $n = 0, 1, \ldots, N-1$, has period N (cf. [5]), we have $T_2(\theta^{j+l}) \neq T_2(\theta^{t+l})$ for some l, which implies $\alpha(\boldsymbol{v}) \neq \alpha(\boldsymbol{v}^{(s)})$. Therefore $(b_1, b_2, \ldots, b_m)$ $\neq (b_1^{(s)}, b_2^{(s)}, \ldots, b_m^{(s)})$, namely $\boldsymbol{v}$ and $\boldsymbol{v}^{(s)}$ belong to different cosets.

Now, we show that G acts on $Z_qRM(1,m)^-/2Z_{q'}RM(1,m)^-$ transitively. Assume that the codewords $\boldsymbol{v}$, $\boldsymbol{v}'$ are contained in the same coset. It is equivalent to $\boldsymbol{v}-\boldsymbol{v}' \in 2Z_{q'}RM(1,m)^-$. The vector $\boldsymbol{v}-\boldsymbol{v}'$ is represented by trace function T_q from Lemma 1. Therefore $\boldsymbol{v}^{(1)} - \boldsymbol{v}'^{(1)} = (\boldsymbol{v}-\boldsymbol{v}')^{(1)} \in 2Z_{q'}RM(1,m)^-$. Therefore $\boldsymbol{v}^{(1)}$, $\boldsymbol{v}'^{(1)}$ are contained in the same coset. It completes the proof. □

Theorem 5 says every coset except for $2Z_{q'}RM(1,m)^-$ has the same Lee weight distribution. It turns out that the Lee weight distribution of $Z_qRM(1,m)^-$ can be obtained from the Lee weight distributions of the cosets of $Z_qRM(1,m)^-$ modulo $2Z_{q'}RM(1,m)^-$.

Acknowledgement The authors would like to thank anonymous referees for their careful reading and many comments. This work has been supported by JSPS KAKENHI(90540014).

References

[1] Borges, J., Fernández, C., Phelps, K.T.: Quaternary Reed-Muller codes. IEEE Trans. Inf. Theory **51**, 2686-2691 (2005)

[2] Bhaintwal, M., Wasan, S.K.: Generalized Reed-Muller codes over Z_q. Des. Codes Cryptogr. **54**, 149-166 (2010)

[3] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The Z_4-linearity of Kerdock, Preparata, Goethals, and Related codes. IEEE Trans. Inf. Theory **40**, 301-319 (1994)

[4] Kumar, P.V., Helleseth, T., Calderbank, A.R.: An upper bound for Weil exponential sums over Galois rings and applications. IEEE Trans. Inf. Theory **41**, 456-468 (1995)

[5] Lidl, R., Niederreiter, H.: Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge (2000)