Discrete Mathematics 128 (1994) 203–224
North-Holland

Classification of cosets of the Reed–Muller code $R(m-3,m)$

Xiang-dong Hou

Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA

Received 7 January 1992
Revised 29 April 1992

Abstract

Cosets of the Reed–Muller code $R(m-3,m)$ are classified under the actions of $\mathrm{GL}(m,2)$ and $\mathrm{GA}(m,2)$, the latter being the automorphism group of $R(m-3,m)$ for $m\geqslant 4$. The number of cosets in each class is calculated. Orphans of $R(m-3,m)$ are identified, and the normality of $R(m-3,m)$ is established. A recursive formula is given for computing weight distributions of cosets of $R(m-3,m)$. The formula gives the number of vectors of weight w in a coset of $R(m-3,m)$ with minimal weight μ rather easily when w is not far away from μ.

1. Introduction

Let C be a binary linear code of length n, and let G be an automorphism group of C. Then G acts on the set of all cosets of C. Cosets in the same G-orbit are said to be G-equivalent. G-equivalent cosets have the same coding theoretic properties.

In this paper, we concentrate on the cosets of the $(m-3)$rd order Reed–Muller code $R(m-3,m)$ of length 2^m. The general affine group $\mathrm{GA}(m,2)$ is an automorphism group of $R(m-3,m)$, and is the full automorphism group when $m\geqslant 4$. (See [13]). The general linear group $\mathrm{GL}(m,2)$ is a subgroup of $\mathrm{GA}(m,2)$. In Section 3, we see that the cosets of $R(m-3,m)$ of even weight correspond to $m\times m$ symmetric matrices over $\mathrm{GF}(2)$, and their $\mathrm{GL}(m,2)$-equivalence classes correspond to congruence classes of $m\times m$ symmetric matrices. The same thing happens with respect to the cosets of $R(m-3,m)$ of odd weight. Using the well-known classification of symmetric matrices over $\mathrm{GF}(2)$, we easily get the classification of cosets of $R(m-3,m)$ under the action of $\mathrm{GL}(m,2)$. The classification of cosets of $R(m-3,m)$ under the action of $\mathrm{GA}(m,2)$ follows immediately. The minimal weight and the number of cosets in each $\mathrm{GA}(m,2)$-equivalence class are calculated. In Section 4, we identify the orphans of $R(m-3,m)$.

Correspondence to: X-d. Hou, Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA.

SSDI 0012-365X(92)00443-I

(See [4, 5, 9] for the definition and importance of orphans of a binary linear code.) It turns out that all the orphans of $R(m-3,m)$ are 0-covered. This implies that $R(m-3,m)$ is normal. (See [8] for the definition and importance of normal codes.) In Section 5, a recursive formula is given for computing weight distributions of cosets of $R(m-3,m)$. For a coset C of $R(m-3,m)$ with minimal weight μ, the formula gives the number of vectors of weight w in C rather easily when w is not far away from μ. When w is far away from μ, the formula involves a large amount of computation.

Section 2 presents some background in Reed–Muller codes and geometry over GF(2).

2. Preliminaries

For binary vectors $x=(x_1,\dots,x_n)$, $y=(y_1,\dots,y_n)$, define $x\cap y=(x_1y_1,\dots,x_ny_n)$. Throughout this paper, h is always the all-one row vector of suitable length.

Let V be an n-dimensional vector space over GF(2). Choose a distinguished ordered basis $\varepsilon_1,\dots,\varepsilon_n$ for V, and define Hamming weight $|\circ|$ on V:

$$|x_1\varepsilon_1+\cdots+x_n\varepsilon_n|=|(x_1,\dots,x_n)|. \tag{2.1}$$

Subsets of V are binary codes of length n. Let W be another n-dimensional vector space over GF(2) with a distinguished ordered basis $\eta_1,\dots,\eta_n$, and let $\varphi: V\to W$ be the linear isomorphism given by $\varepsilon_i\mapsto\eta_i$ $(i=1,\dots,n)$. For any code $C\subset V$, $\varphi(C)$ is called the representation of C in W. Representing a code in a different ambient space sometimes is convenient. An automorphism of a code $C\subset V$ is a linear isomorphism $V\to V$ extended by a permutation of $\varepsilon_1,\dots,\varepsilon_n$ which leaves C invariant.

For $m\geqslant 0$, let GF(2) $[X_1,\dots,X_m]$ be the polynomial ring, and

$$\begin{aligned}\mathscr{P}_m&=\mathrm{GF}(2)[X_1,\dots,X_m]/(X_1^2-X_1,\dots,X_m^2-X_m)\\&\cong\{P\in\mathrm{GF}(2)[X_1,\dots,X_m]\text{: the degree of each } X_i \text{ in } P \text{ is at most } 1\}.\end{aligned} \tag{2.2}$$

$\mathscr{P}_m$ is a 2^m-dimensional vector space over GF(2). Choose ε_v $(v\in\mathrm{GF}(2)^m)$ as the distinguished ordered basis for $\mathscr{P}_m$, where

$$\varepsilon_v=(X_1-v_1+1)\cdots(X_m-v_m+1),\quad \text{for } v=\begin{bmatrix}v_1\\ \vdots\\ v_m\end{bmatrix}\in\mathrm{GF}(2)^m. \tag{2.3}$$

$(\varepsilon_v(v)=1$ and $\varepsilon_v(u)=0$ for $v\neq u\in\mathrm{GF}(2)^m.)$

For $w\geqslant 0$, let $M_{m,w}$ be the set of all $m\times w$ matrices over GF(2). Put

$$M_m=\bigcup_{w\geqslant 0} M_{m,w}. \tag{2.4}$$

For $A,B\in M_m$, we say $A\sim B$ if B can be obtained from A by a permutation of columns and by adding or deleting pairs of repeated columns. $\sim$ is an equivalence relation on

M_m. Let $q: M_m \to M_m/\sim$ be the quotient map. Define $+$ on $M_m/\sim$:

$$q(A)+q(B)=q([A,B])\,. \tag{2.5}$$

($M_m/\sim$ can be regarded as the power set of $\mathrm{GF}(2)^m$ where $+$ is the symmetric difference.) $M_m/\sim$ is a 2^m-dimensional vector space over GF(2). Choose $q(v)$ ($v\in\mathrm{GF}(2)^m$) as the distinguished ordered basis for $M_m/\sim$.

Let $\varphi: \mathscr{P}_m \to M_m/\sim$ be the linear isomorphism given by $\varepsilon_v \mapsto q(v)$ ($v\in\mathrm{GF}(2)^m$). One can prove that $\varphi^{-1}: M_m/\sim \to \mathscr{P}_m$ is given by

$$q\left(\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{bmatrix}\right) \mapsto \sum_{\substack{0\leqslant a\leqslant m\\ 1\leqslant i_1<\cdots<i_a\leqslant m}} |(\alpha_{i_1}+h)\cap\cdots\cap(\alpha_{i_a}+h)|\hat{X}_{i_1,\ldots,i_a},$$

$$\text{for any } \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{bmatrix}\in M_m, \tag{2.6}$$

where $|(\alpha_{i_1}+h)\cap\cdots\cap(\alpha_{i_a}+h)|$ is regarded as an element in GF(2), (the empty intersection of row vectors is h,) and $\hat{X}_{i_1,\ldots,i_a}=\prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_a\}} X_i$, ($\hat{X}_\phi = X_1\cdots X_m$.)

The general affine group GA(m,2) acts on $\mathrm{GF}(2)^m$, hence permutes ε_v ($v\in\mathrm{GF}(2)^m$) and $q(v)$ ($v\in\mathrm{GF}(2)^m$): for any $f\in\mathrm{GA}(m,2)$,

$$f(\varepsilon_v)=\varepsilon_{f(v)},\quad f(q(v))=q(f(v)),\qquad v\in\mathrm{GF}(2)^m\,. \tag{2.7}$$

f extends to linear automorphisms of $\mathscr{P}_m$ and $M_m/\sim$ such that the diagram

$$\begin{array}{ccc}\mathscr{P}_m & \xrightarrow{\varphi} & M_m/\sim\\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f}\\ \mathscr{P}_m & \xrightarrow{\varphi} & M_m/\sim\end{array} \tag{2.8}$$

commutes. GA(m,2) also acts on M_m: for any $f\in\mathrm{GA}(m,2)$, and $[v_1,\ldots,v_w]\in M_m$,

$$f([v_1,\ldots,v_w])=[f(v_1),\ldots,f(v_w)]\,. \tag{2.9}$$

The diagram

$$\begin{array}{ccc}M_m & \xrightarrow{q} & M_m/\sim\\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f}\\ M_m & \xrightarrow{\varphi} & M_m/\sim\end{array} \tag{2.10}$$

commutes.

Let $0\leqslant r\leqslant m$. The usual definition of the rth order Reed–Muller code of length 2^m is

$$R(r,m)=\{F\in\mathscr{P}_m\colon \deg F\leqslant r\}\,. \tag{2.11}$$

By (2.6), we see that the representation of $R(r,m)$ in $M_m/\sim$ is

$$\varphi(R(r,m))=\{q(A)\in M_m/\sim : A=\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{bmatrix}\in M_m$$
$$\text{satisfies } |\alpha_{i_1}\cap\cdots\cap\alpha_{i_a}|\equiv 0 (\mathrm{mod}\, 2)$$
$$\text{for } 0\leqslant a\leqslant m-r-1,\ 1\leqslant i_1<\cdots<i_a\leqslant m\}. \tag{2.12}$$

We will work on $\varphi(R(r,m))$ and will not distinguish between $R(r,m)$ and $\varphi(R(r,m))$. $\mathrm{GA}(m,2)$ is an automorphism group of $R(r,m)$. When $1\leqslant r\leqslant m-2$, $\mathrm{GA}(m,2)$ is the full automorphism group of $R(r,m)$. (See [13].) The general linear group $\mathrm{GL}(m,2)$ is an automorphism group of $R(r,m)$.

Lemma 2.1. *Let $\mathscr{S}_m$ be the set of all $m\times m$ symmetric matrices over* GF(2), *and let $A\in\mathscr{S}_m$ have* $\mathrm{rank}(A)=t$. *If t is odd, there is a $P\in\mathrm{GL}(m,2)$ such that*

$$PAP^{\mathrm{T}}=\begin{bmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0\end{bmatrix}\Big\}t = I(m,t). \tag{2.13}$$

If t is even, there is a $P\in\mathrm{GL}(m,2)$ such that

$$PAP^{\mathrm{T}}=\begin{bmatrix}0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 0 & \\ & & & & & & \ddots \\ & & & & & & & 0\end{bmatrix}\Big\}t = K(m,t), \tag{2.14}$$

or

$$PAP^{\mathrm{T}}=\begin{bmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0\end{bmatrix}\Big\}t = I(m,t). \tag{2.15}$$

When $t\geqslant 2$ is even, (2.14) *and* (2.15), *do not both occur.*

Proof. We may assume $A \neq 0$. Without loss of generality, we may write

$$A = \begin{bmatrix} A_1 & A_2^{\mathrm{T}} \\ A_2 & A_3 \end{bmatrix},$$

where

$$A_1 = [1] \text{ or } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let

$$P_1 = \begin{bmatrix} I(s,s) & 0 \\ A_2 A_1 & I(m-s, m-s) \end{bmatrix} \in \mathrm{GL}(m,2),$$

where s is the size of A_1. Then

$$P_1 A P_1^{\mathrm{T}} = \begin{bmatrix} A_1 & 0 \\ 0 & A_3' \end{bmatrix}.$$

Now the induction on the size of A shows that there is a $P \in \mathrm{GL}(m,2)$ such that

$$PAP^{\mathrm{T}} = \begin{bmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 0 & 1 & & & & & \\ & & & 1 & 0 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 0 & 1 & & \\ & & & & & & 1 & 0 & & \\ & & & & & & & & 0 & \\ & & & & & & & & & \ddots \\ & & & & & & & & & & 0 \end{bmatrix}.$$

To prove that one of (2.13), (2.14), and (2.15) true, we only have to note

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & & \\ & 0 & 1 \\ & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}.$$

Finally, note that for any $P \in \mathrm{GL}(m,2)$, the main diagonal entries of $PK(m,t)P^{\mathrm{T}}$ are all 0. Hence, when $t \geqslant 2$ is even, (2.14) and (2.15) do not both happen. □

For any $A \in \mathscr{S}_m$, define

$$S(A) = \{P \in \mathrm{GL}(m,2) : PAP^{\mathrm{T}} = A\} < \mathrm{GL}(m,2). \tag{2.16}$$

($S(K(2n,2n))$ is the symplectic group.)

Lemma 2.2.

$$|S(I(m,t))| = \begin{cases} 2^{(1/4)t^2+(1/2)(m-t)(m+t-1)} \prod_{i=1}^{(t/2)-1} (2^{2i}-1) \prod_{i=1}^{m-t} (2^i-1), & \text{if } t \text{ is even,} \\ 2^{(1/4)(t-1)^2+(1/2)(m-t)(m+t-1)} \prod_{i=1}^{(t-1)/2} (2^{2i}-1) \prod_{i=1}^{m-t} (2^i-1), & \text{if } t \text{ is odd,} \end{cases} \tag{2.17}$$

$$|S(K(m,t))| = 2^{(1/4)t^2+(1/2)(m-t)(m+t-1)} \prod_{i=1}^{(t/2)} (2^{2i}-1) \prod_{i=1}^{m-t} (2^i-1), \quad t \text{ is even.} \tag{2.18}$$

Proof. We have

$$|S(I(t,t))| = \begin{cases} 2^{(1/4)t^2} \prod_{i=1}^{(t/2)-1} (2^{2i}-1), & \text{if } t \text{ is even,} \\ 2^{(1/4)(t-1)^2} \prod_{i=1}^{(t-1)/2} (2^{2i}-1), & \text{if } t \text{ is odd,} \end{cases} \tag{2.19}$$

$$|S(K(t,t))| = 2^{(1/4)t^2} \prod_{i=1}^{(t/2)} (2^{2i}-1), \quad \text{if } t \text{ is even.} \tag{2.20}$$

((2.19) can be obtained by induction on t; (2.20) can be found in [1, p. 147].) It is easily seen that $P \in S(I(m,t))$ iff

$$P = \begin{bmatrix} P_{11} & P_{12} \\ 0 & P_{22} \end{bmatrix}, \tag{2.21}$$

where $P_{11} \in S(I(t,t))$ and $P_{22} \in \mathrm{GL}(m-t,2)$. Hence

$$|S(I(m,t))| = |S(I(t,t))| \cdot |\mathrm{GL}(m-t,2)| \cdot 2^{t(m-t)}. \tag{2.22}$$

(2.17) follows from (2.22) and (2.19). (2.18) is proved in the same way. □

3. Classification of cosets of $R(m-3,m)$

For any $A, B \in M_m$, using (2.12) with $r=m-3$, we see that $q(A)-q(B) \in R(m-3,m)$ iff A and B have the same row size (mod 2), and $AA^{\mathrm{T}} = BB^{\mathrm{T}}$. Let $\mathscr{C}_e(\mathscr{C}_o)$ be the set of all cosets of $R(m-3,m)$ with even (odd) weight, and $\mathscr{C} = \mathscr{C}_e \cup \mathscr{C}_o$. Define $\psi: \mathscr{C} \to \mathscr{S}_m$,

$$q(A) + R(m-3,m) \mapsto AA^{\mathrm{T}}, \quad A \in M_m. \tag{3.1}$$

ψ restricts to bijections $\psi_e: \mathscr{C}_e \to \mathscr{S}_m$ and $\psi_o: \mathscr{C}_o \to \mathscr{S}_m$. Let $\mathrm{GL}(m,2)$ act on $\mathscr{S}_m$: for any $P \in \mathrm{GL}(m,2)$, $A \in \mathscr{S}_m$,

$$P(A) = PAP^{\mathrm{T}}. \tag{3.2}$$

We have the following commutative diagrams:

$$\begin{array}{ccc} \mathscr{C}_e & \xrightarrow{\psi_e} & \mathscr{S}_m \\ \downarrow P & & \downarrow P \\ \mathscr{C}_e & \xrightarrow{\psi_e} & \mathscr{S}_m \end{array} \tag{3.3}$$

$$\begin{array}{ccc} \mathscr{C}_o & \xrightarrow{\psi_o} & \mathscr{S}_m \\ \downarrow P & & \downarrow P \\ \mathscr{C}_o & \xrightarrow{\psi_o} & \mathscr{S}_m \end{array} \tag{3.4}$$

Let

$$A_{m,t}=\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{bmatrix}\Bigg\}t \in M_m, \qquad B_{m,t}=\begin{bmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ & & 0 & \end{bmatrix}\Bigg\}t \in M_m,$$

$$t=0,1,\ldots,m, \tag{3.5}$$

$$C_{m,t}=\begin{bmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \\ & & 0 & \end{bmatrix}\Bigg\}t \in M_m, \qquad D_{m,t}=\begin{bmatrix} 1 & & & 1 & 0 \\ & \ddots & & \vdots & \vdots \\ & & 1 & 1 & 0 \\ & & 0 & & \end{bmatrix}\Bigg\}t \in M_m,$$

$$t=2,4,\ldots,2\lfloor m/2 \rfloor. \tag{3.6}$$

Theorem 3.1. *The following are representatives of* GL$(m,2)$-orbits on $\mathscr{C}$:

$$q(A_{m,t})+R(m-3,m), \quad t=0,1,\ldots,m, \tag{3.7}$$

$$q(B_{m,t})+R(m-3,m), \quad t=0,1,\ldots,m, \tag{3.8}$$

$$q(C_{m,t})+R(m-3,m), \quad t=2,4,\ldots,2\lfloor m/2 \rfloor, \tag{3.9}$$

$$q(D_{m,t})+R(m-3,m), \quad t=2,4,\ldots,2\lfloor m/2 \rfloor. \tag{3.10}$$

Proof. By Lemma 2.1, $I(m,t)$ $(t=0,1,\ldots,m)$ and $K(m,t)$ $(t=2,4,\ldots,2\lfloor m/2 \rfloor)$ are representatives of GL$(m,2)$-orbits on $\mathscr{S}_m$. Therefore, by (3.3) and (3.4), $\psi_e^{-1}(I(m,t))$, $\psi_o^{-1}(I(m,t))$ $(t=0,1,\ldots,m)$ and $\psi_e^{-1}(K(m,t))$, $\psi_o^{-1}(K(m,t))$ $(t=2,4,\ldots,2\lfloor m/2 \rfloor)$ form representatives of GL$(m,2)$-orbits on $\mathscr{C}$. Note that

$$\psi_e^{-1}(I(m,t))=\begin{cases} q(A_{m,t})+R(m-3,m), & \text{if } 0\leqslant t\leqslant m,\ t \text{ is even}, \\ q(B_{m,t})+R(m-3,m), & \text{if } 0\leqslant t\leqslant m,\ t \text{ is odd}, \end{cases}$$

$$\psi_e^{-1}(I(m,t))=\begin{cases} q(B_{m,t})+R(m-3,m), & \text{if } 0\leqslant t\leqslant m,\ t \text{ is even}, \\ q(A_{m,t})+R(m-3,m), & \text{if } 0\leqslant t\leqslant m,\ t \text{ is odd}. \end{cases}$$

Also note that $\psi_o^{-1}(K(m,t))$ is $\mathrm{GL}(m,2)$-equivalent to $q(C_{m,t})+R(m-3,m)$ $(t=2,4,\ldots,2\lfloor m/2\rfloor)$, since $\psi_o(q(C_{m,t})+R(m-3,m))=C_{m,t}C_{m,t}^{\mathrm{T}}$ is $\mathrm{GL}(m,2)$-equivalent to $K(m,t)$. Similarly, $\psi_e^{-1}(K(m,t))$ is $\mathrm{GL}(m,2)$-equivalent to $q(D_{m,t})+R(m-3,m)$ $(t=2,4,\ldots,2\lfloor m/2\rfloor)$. □

For a group G acting on a set X and $x\in X$, we use $[x]_G$ to denote the G-orbit on X containing x.

Theorem 3.2. *The cardinalities of the* $\mathrm{GL}(m,2)$*-equivalence classes of* $\mathscr{C}$ *are*

$$|[q(A_{m,t})+R(m-3,m)]_{GL(m,2)}|=|[q(B_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}|$$

$$=\begin{cases} 2^{(1/4)t(t-2)}\dfrac{\prod_{i=m-t+1}^{m}(2^i-1)}{\prod_{i=1}^{t/2-1}(2^{2i}-1)}, & \text{if } 0\leqslant t\leqslant m,\ t \text{ is even},\\ 2^{(1/4)(t^2-1)}\dfrac{\prod_{i=m-t+1}^{m}(2^i-1)}{\prod_{i=1}^{(t-1)/2}(2^{2i}-1)}, & \text{if } 0\leqslant t\leqslant m,\ t \text{ is odd}, \end{cases} \tag{3.11}$$

$$|[q(C_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}|=|[q(D_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}|$$

$$=2^{(1/4)t(t-2)}\frac{\prod_{i=m-t+1}^{m}(2^i-1)}{\prod_{i=1}^{t/2}(2^{2i}-1)},\quad 2\leqslant t\leqslant m,\ t \text{ is even}. \tag{3.12}$$

Proof. By (3.3) and (3.4), we have

$$|[q(A_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}|=|[q(B_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}|$$

$$=|[I(m,t)]_{\mathrm{GL}(m,2)}|=\frac{|\mathrm{GL}(m,2)|}{|S(I(m,t))|}. \tag{3.13}$$

Equations (3.13) and (2.17) yield (3.11). Equation (3.12) is proved in the same way. □

Lemma 3.3. *For* $1\leqslant t\leqslant m$, $q(A_{m,t})+R(m-3,m)$ *is* $\mathrm{GA}(m,2)$*-equivalent to* $q(B_{m,t-1})+R(m-3,m)$.

Proof. Let $f\in\mathrm{GA}(m,2)$,

$$f(v)=\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ 1 & \cdots & 1 & & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{bmatrix}_{t} v+\begin{bmatrix} 0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0 \end{bmatrix} t,\quad v\in\mathrm{GF}(2)^m.$$

Then $f(q(A_{m,t}))=q(f(A_{m,t}))=q(B_{m,t-1})$. □

Lemma 3.4. *For* $t=2,4,\ldots,2\lfloor m/2\rfloor$, $q(C_{m,t})+R(m-3,m)$ *is* $\mathrm{GA}(m,2)$*-equivalent to* $q(B_{m,t})+R(m-3,m)$.

Proof. Let $f\in\mathrm{GA}(m,2)$,

$$f(v)=v+\begin{bmatrix}1\\ \vdots\\ 1\\ 0\\ \vdots\\ 0\end{bmatrix}\Bigg\}t, \quad v\in\mathrm{GF}(2)^m.$$

Since

$$f(C_{m,t})\cdot f(C_{m,t})^{\mathrm{T}}=\begin{bmatrix}0 & & 1 & & 0\\ & \ddots & & & \vdots\\ & 1 & & 0 & 0\\ & & 0 & & \end{bmatrix}\begin{bmatrix}0 & & 1 & & 0\\ & \ddots & & & \vdots\\ & 1 & & 0 & 0\\ & & 0 & & \end{bmatrix}^{\mathrm{T}}$$

$$=I(m,t)=B_{m,t}B_{m,t}^{\mathrm{T}},$$

we have $f(q(C_{m,t})+R(m-3,m))=q(f(C_{m,t}))+R(m-3,m)=q(B_{m,t})+R(m-3,m)$. □

Theorem 3.5.

The minimal weight of $q(A_{m,t})+R(m-3,m)=t, \quad 0\leqslant t\leqslant m.$ (3.14)

The minimal weight of $q(B_{m,m})+R(m-3,m)=m+1,$ (3.15)

the minimal weight of $q(D_{m,t})+R(m-3,m)=t+2,\ 2\leqslant t\leqslant m,\ t$ *is even.* (3.16)

Proof. We only prove (3.16). Equations (3.14) and (3.15) are proved in the same way. Let μ be the minimal weight of $q(D_{m,t})+R(m-3,m)$. Hence, there is an $A\in M_{m,\mu}$ such that $q(A)\in q(D_{m,t})+R(m-3,m)$. Since $AA^{\mathrm{T}}=D_{m,t}D_{m,t}^{\mathrm{T}}$, we have $\mathrm{rank}(A)\geqslant \mathrm{rank}(AA^{\mathrm{T}})=\mathrm{rank}(D_{m,t}D_{m,t}^{\mathrm{T}})=t$. Note that all rows of A have even weights. Therefore, $\mu-1\geqslant\mathrm{rank}(A)\geqslant t$. Since μ and t are both even, we have $\mu\geqslant t+2$. On the other hand, $\mu\leqslant|q(D_{m,t})|=t+2$. So, $\mu=t+2$. □

Theorem 3.6. *The following are representatives of* $\mathrm{GA}(m,2)$*-orbits on* $\mathscr{C}$:

$$q(A_{m,t})+R(m-3,m), \quad t=0,1,\ldots,m, \tag{3.17}$$

$$q(B_{m,m})+R(m-3,m), \tag{3.18}$$

$$q(D_{m,t})+R(m-3,m), \quad t=2,4,\ldots,2\lfloor m/2\rfloor. \tag{3.19}$$

Proof. By Lemmas 3.3 and 3.4, it suffices to prove that the above cosets are not GA$(m,2)$-equivalent. By Theorem 3.5, it remains to prove:

(i) $q(D_{m,t})+R(m-3,m)$ is not GA$(m,2)$-equivalent to $q(A_{m,t+2})+R(m-3,m)$ $(t=2,4,\ldots,2\lfloor m/2\rfloor-2)$, and

(ii) $q(D_{m,m-1})+R(m-3,m)$ is not GA$(m,2)$-equivalent to $q(B_{m,m})+R(m-3,m)$, (m is odd).

Both (i) and (ii) follow when one notes that $q(D_{m,t})\in R(m-2,m)$ $(t=2,4,\ldots,2\lfloor m/2\rfloor)$, but $q(A_{m,t})\in R(m-1,m)\setminus R(m-2,m)$ $(t=0,1,\ldots,m)$, and $q(B_{m,m})\in R(m-1,m)\setminus R(m-2,m)$. □

Remark. In the usual ambient space $\mathscr{P}_m$ of $R(m-3,m)$, the following are representatives of GA$(m,2)$-orbits on $\mathscr{C}$:

$$t\hat{X}_\phi+\hat{X}_1+\cdots+\hat{X}_t+R(m-3,m),\quad t=0,1,\ldots,m, \tag{3.20}$$

$$(m+1)\hat{X}_\phi+\hat{X}_1+\cdots+\hat{X}_m+R(m-3,m), \tag{3.21}$$

$$\hat{X}_{1,2}+\cdots+\hat{X}_{(t/2)-1,t/2}+R(m-3,m),\quad t=2,4,\ldots,2\lfloor m/2\rfloor. \tag{3.22}$$

Theorem 3.7. *The* GA$(m,2)$*-orbits on* $\mathscr{C}$ *are*

$$[q(A_{m,0})+R(m-3,m)]_{\mathrm{GA}(m,2)}=[q(A_{m,0})+R(m-3,m)]_{\mathrm{GL}(m,2)}, \tag{3.23}$$

$$\begin{aligned}[q(A_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}=&[q(A_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}\cup\\ &[q(B_{m,t-1})+R(m-3,m)]_{\mathrm{GL}(m,2)},\\ &t=1,2,4,\ldots,2\lfloor m/2\rfloor,\end{aligned} \tag{3.24}$$

$$\begin{aligned}[q(A_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}=&[q(A_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)}\cup\\ &[q(B_{m,t-1})+R(m-3,m)]_{\mathrm{GL}(m,2)}\cup\\ &[q(C_{m,t-1})+R(m-3,m)]_{\mathrm{GL}(m,2)},\\ &t=3,5,\ldots,2\lfloor(m-1)/2\rfloor+1,\end{aligned} \tag{3.25}$$

$$[q(B_{m,m})+R(m-3,m)]_{\mathrm{GA}(m,t)}=$$

$$\begin{cases}[q(B_{m,m})+R(m-3,m)]_{\mathrm{GL}(m,2)}, & \text{if } m \text{ is odd},\\ [q(B_{m,m})+R(m-3,m)]_{\mathrm{GL}(m,2)}\cup & \\ [q(C_{m,m})+R(m-3,m)]_{\mathrm{GL}(m,2)}, & \text{if } m \text{ is even},\end{cases} \tag{3.26}$$

$$\begin{aligned}[q(D_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}=&[q(D_{m,t})+R(m-3,m)]_{\mathrm{GL}(m,2)},\\ &t=2,4,\ldots,2\lfloor m/2\rfloor,\end{aligned} \tag{3.27}$$

and they have cardinalities

$$|[q(A_{m,0})+R(m-3,m)]_{\mathrm{GA}(m,2)}|=1, \tag{3.28}$$

$$|[q(A_{m,1})+R(m-3,m)]_{\mathrm{GA}(m,2)}|=2^m, \tag{3.29}$$

$$|[q(A_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}|=2^{(1/4)t(t-2)+m-t+1}\frac{\prod_{i=m-t+2}^{m}(2^i-1)}{\prod_{i=1}^{(t/2)-1}(2^{2i}-1)},$$
$$t=2,4,\ldots,2\lfloor m/2\rfloor, \tag{3.30}$$

$$|[q(A_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}|=2^{(1/4)(t^2-1)+m-t+1}\frac{\prod_{i=m-t+2}^{m}(2^i-1)}{\prod_{i=1}^{(t-1)/2}(2^{2i}-1)},$$
$$t=3,5,\ldots,2\lfloor (m-1)/2\rfloor+1, \tag{3.31}$$

$$|[q(B_{m,m})+R(m-3,m)]_{\mathrm{GA}(m,2)}|=$$
$$\begin{cases}2^{(1/4)(m^2-1)}\dfrac{\prod_{i=1}^{m}(2^i-1)}{\prod_{i=1}^{(m-1)/2}(2^{2i}-1)}, & \text{if } m \text{ is odd},\\[2ex] 2^{(1/4)m(m+2)}\dfrac{\prod_{i=1}^{m}(2^i-1)}{\prod_{i=1}^{(m/2)}(2^{2i}-1)}, & \text{if } m \text{ is even},\end{cases} \tag{3.32}$$

$$|[q(D_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}|=2^{(1/4)t(t-2)}\frac{\prod_{i=m-t+1}^{m}(2^i-1)}{\prod_{i=1}^{(t/2)}(2^{2i}-1)},$$
$$t=2,4,\ldots,2\lfloor m/2\rfloor. \tag{3.33}$$

Proof. Equation (3.23)–(3.27) follow from Lemmas 3.3, 3.4, and Theorem 3.6. Equations (3.28)–(3.33) follow from (3.23)–(3.27) and Theorem 3.2. □

4. Orphans of $R(m-3,m)$

Let C be a binary linear code of length n, and let C' be a coset of C with minimal weight μ. Vectors of weight μ in C' are called leaders of C'. For any $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_n)\in \mathrm{GF}(2)^n$, we say $x\leqslant y$ if $x_i=1$ implies $y_i=1$ $(1\leqslant i\leqslant n)$. For any cosets C' and C'' of C, we say $C'\leqslant C''$ if $x\leqslant y$ for some leaders x of C' and y of C''. $\leqslant$ is a partial order on the set $\mathrm{GF}(2)^n/C$ of all cosets of C in $\mathrm{GF}(2)^n$. Maximal elements in $\langle \mathrm{GF}(2)^n/C, \leqslant\rangle$ are called orphans of C ([5]). A coset C' of C with minimal weight μ is an orphan of C iff the vectors of C' with weights μ and $\mu+1$ cover all coordinate positions [4, Theorem 1]. For $\varepsilon=0$ or 1, C' is called ε-covered if for each coordinate position i, there is a leader of C' with an ε in position i. Automorphisms of C send orphans to orphans and ε-covered cosets to ε-covered cosets. If C is an even code, then C' is an orphan iff it is 1-covered.

Lemma 4.1. *Let $0 \leqslant r < m$. For any $q(A) \in R(r+1,m) \setminus R(r,m)$ $(A \in M_m)$, $q(A)+R(r,m)$ is an orphan of $R(r,m)$ which is both 1-covered and 0-covered.*

Proof. We may assume $A=[v_1,\ldots,v_\mu] \in M_{m,\mu}$, where $\mu \geqslant 1$ is the minimal weight of $q(A)+R(r,m)$. If B is obtained by adding $h=(1,\ldots,1)$ to any row of A, using (2.12), one can easily see that $q(B) \in q(A)+R(r,m)$ using the fact $q(A) \in R(r+1,m)$. Hence, for any $u \in \mathrm{GF}(2)^m$,

$$q([v_1+u,\ldots,v_\mu+u]) \in q(A)+R(r,m). \tag{4.1}$$

By choosing suitable u, we may make any given $v \in \mathrm{GF}(2)^m$ appear or not appear in the columns of $[v_1+u,\ldots,v_\mu+u]$. Hence, $q(A)+R(r,m)$ is both 1-covered and 0-covered. □

Theorem 4.2. (i) *If m is even, the orphans of $R(m-3,m)$ are the cosets in*

$$[q(D_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}, \quad t=2,4,\ldots,m. \tag{4.2}$$

(ii) *If m is odd, the orphans of $R(m-3,m)$ are the cosets in*

$$[q(D_{m,t})+R(m-3,m)]_{\mathrm{GA}(m,2)}, \quad t=2,4,\ldots,m-1. \tag{4.3}$$

and

$$[q(B_{m,m})+R(m-3,m)]_{\mathrm{GA}(m,2)}. \tag{4.4}$$

In both (i) *and* (ii), *all the orphans of $R(m-3,m)$ are both 1-covered and 0-covered.*

Proof. Since $q(D_{m,t}) \in R(m-2,m) \setminus R(m-3,m)$ $(t=2,4,\ldots,2\lfloor m/2 \rfloor)$, by Lemma 4.1, $q(D_{m,t})+R(m-3,m)$ is both 1-covered and 0-covered.

(i) It remains to prove that $q(A_{m,t})+R(m-3,m)$ $(t=0,1,\ldots,m)$ and $q(B_{m,m})+R(m-3,m)$ are not 1-covered. We claim that for any coset leader $q(A) \in q(A_{m,t})+R(m-3,m)$ $(A \in M_{m,t})$,

$$\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

does not appear as a column of A. Otherwise, $t \geqslant 1$, and

$$A=\begin{bmatrix} & 0 \\ A_1 & \vdots \\ & 0 \end{bmatrix}.$$

Since $AA^{\mathrm{T}}=A_{m,t}A_{m,t}^{\mathrm{T}}=I(m,t)$, we have $A_1A_1^{\mathrm{T}}=I(m,t)$. Then $q(A_1) \in q(B_{m,t})+R(m-3,m)$. There is a contradiction since $q(B_{m,t})+R(m-3,m)$ has minimal weight

$t+1$ (Lemmas 3.3 and (3.14)) and $|q(A_1)|=t-1$. Similarly, one can prove that for any coset leader $q(A)\in q(B_{m,m})+R(m-3,m)$ $(A\in M_{m,m+1})$,

$$\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

does not appear as a column of A.

(ii) As in (i), $q(A_{m,t})+R(m-3,m)$ $(t=0,1,\ldots,m)$ are not orphans. It remains to prove that $q(B_{m,m})+R(m-3,m)$ is both 1-covered and 0-covered. Since the minimal weight of $q(B_{m,m})+R(m-3,m)=m+1=$ the covering radius of $R(m-3,m)$ (Theorem 3.5), $q(B_{m,m})+R(m-3,m)$ is an orphan, hence is 1-covered. Let

$$J=\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{bmatrix}\in M_{m,m+1}.$$

Then $q(B_{m,m})$ and $q(B_{m,m}+J)$ are leaders of $q(B_{m,m})+R(m-3,m)$. For any $v\in \mathrm{GF}(2)^m$, one of $B_{m,m}$ and $B_{m,m}+J$ does not contain v as a column. Hence, $q(B_{m,m})+R(m-3,m)$ is 0-covered. □

Theorem 4.3. *$R(m-3,m)$ is normal.*

Proof. It follows immediately from [9, Lemma 2] and Theorem 4.2. □

5. Weight Distributions of Cosets of $R(m-3,m)$

For any $C\subset M_m/\sim$, and $w\geqslant 0$, let $N_w(C)$ be the number of vectors of weight w in C, and let

$$\mathscr{A}_w(C)=\{A\in M_{m,w}: q(A)\in C\}=q^{-1}(C)\cap M_{m,w}. \tag{5.1}$$

We try to derive a recursive formula for $N_w(C)$ in terms of $N_\zeta(C)$ and $|\mathscr{A}_\zeta(C)|$ $(0\leqslant\zeta\leqslant w,\ \zeta=w\,(\mathrm{mod}\,2))$. For any $A,B\in M_m$, we say $A\approx B$ if B can be obtained from A by a permutation of columns. $\approx$ is an equivalence relation on M_m. Let $p: M_m\to M_m/\approx$ be the quotient map.

Lemma 5.1.

$$\sum_{\substack{0\leqslant\zeta\leqslant w\\ \zeta\equiv w\,(\mathrm{mod}\,2)}}\binom{2^m+\dfrac{w-\zeta}{2}-1}{\dfrac{w-\zeta}{2}}N_\zeta(C)=|p(\mathscr{A}_w(C))|. \tag{5.2}$$

Proof. For $0 \leqslant i \leqslant w/2$, let

$$\mathscr{A}_w^{(i)}(C) = \{A \in \mathscr{A}_w(C) : A \text{ has exactly } i \text{ pairs of repeated columns}\}. \tag{5.3}$$

Then

$$|p(\mathscr{A}_w(C))| = \sum_{0 \leqslant i \leqslant w/2} |p(\mathscr{A}_w^{(i)}(C))|. \tag{5.4}$$

Clearly,

$$|p(\mathscr{A}_w^{(i)}(C))| = |p(\mathscr{A}_{w-2i}^{(0)}(C))| \cdot |p(M_{m,i})|.$$

Note that

$$|p(\mathscr{A}_{w-2i}^{(0)}(C))| = N_{w-2i}(C),$$

and

$$|p(M_{m,i})| = \text{the number of ways to choose } i \text{ elements from } \mathrm{GF}(2)^m \text{ with repetition allowed}$$

$$= \binom{2^m + i - 1}{i}.$$

Hence (5.4) becomes

$$|p(\mathscr{A}_w(C))| = \sum_{0 \leqslant i \leqslant w/2} \binom{2^m + i - 1}{i} N_{w-2i}(C)$$

$$= \sum_{\substack{0 \leqslant \zeta \leqslant w \\ \zeta \equiv w \pmod 2}} \binom{2^m + \dfrac{w-\zeta}{2} - 1}{\dfrac{w-\zeta}{2}} N_\zeta(C). \qquad \square$$

A partition λ of the integer w (denoted by $\lambda \vdash w$) is a sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ of nonnegative integers such that $\sum_i i\lambda_i = w$. For $w \geqslant 0$, $\zeta \geqslant 0$, define

$$g_m(w, \zeta) = \sum_{\substack{(\lambda_1, \lambda_2, \dots) \vdash w \\ \lambda_1 + \lambda_3 + \lambda_5 + \dots = \zeta}} \frac{2^{(\lambda_2 + \lambda_4 + \cdots)m}}{\prod_{i=1}^{\infty} (i^{\lambda_i} \cdot \lambda_i!)}. \tag{5.5}$$

Note that $g_m(w, \zeta) \neq 0$ only when $0 \leqslant \zeta \leqslant w$ and $\zeta \equiv w \pmod 2$.

Lemma 5.2.

$$|p(\mathscr{A}_w(C))| = \sum_{\substack{0 \leqslant \zeta \leqslant w \\ \zeta \equiv w \pmod 2}} g_m(w, \zeta) |\mathscr{A}_\zeta(C)|. \tag{5.6}$$

Proof. Let the symmetric group S_w act on $\mathscr{A}_w(C)$ by column permutation. Then $|p(\mathscr{A}_w(C))|$ is the number of S_w-orbits in $\mathscr{A}_w(C)$. By Burnside's Lemma ([3, Theorem 1.2.5]),

$$|p(\mathscr{A}_w(C))| = \frac{1}{w!} \sum_{\alpha \in S_w} |F(\alpha)|, \tag{5.7}$$

where

$$F(\alpha) = \{A \in \mathscr{A}_w(C) : \alpha(A) = A\} \tag{5.8}$$

is the set of elements fixed by α. Let $\alpha \in S_w$ be a disjoint product of ξ cycles of even length and ζ cycles of odd length. Without loss of generality, write

$$\alpha = \underbrace{(1,2,\dots)}_{i_1} \cdots \underbrace{(\quad)}_{i_\zeta} \underbrace{(\quad)}_{j_1} \cdots \underbrace{(\cdots, w-1, w)}_{j_\xi}, \tag{5.9}$$

where $i_1, \dots, i_\zeta$ are odd and $j_1, \dots, j_\xi$ are even. Then any $A \in F(\alpha)$ is of the form

$$A = [\underbrace{v_1 \dots v_1}_{i_1}, \ \cdots, \ \underbrace{v_\zeta \dots v_\zeta}_{i_\zeta}, \ \underbrace{u_1 \dots u_1}_{j_1}, \ \dots \ \underbrace{u_\xi \dots, u_\xi}_{j_\xi}], \tag{5.10}$$

where $[v_1, \dots, v_\zeta] \in \mathscr{A}_\zeta(C)$, and $u_1, \dots, u_\xi \in \mathrm{GF}(2)^m$ are arbitrary. Hence

$$|F(\alpha)| = |\mathscr{A}_\zeta(C)| 2^{\xi m}. \tag{5.11}$$

For any $\alpha \in S_w$ and $\lambda = (\lambda_1, \lambda_2, \dots) \vdash w$, we say α is of type λ if α is a disjoint product of λ_i cycles of length i ($i = 1, 2 \dots$). There are

$$\frac{w!}{\prod_{i=1}^{\infty} (i^{\lambda_i} \cdot \lambda_i!)} \tag{5.12}$$

$\alpha \in S_w$ of type λ, and for each such α, (5.11) gives

$$|F(\alpha)| = |\mathscr{A}_{\lambda_1 + \lambda_3 + \lambda_5 + \dots}(C)| 2^{(\lambda_2 + \lambda_4 + \cdots)m}. \tag{5.13}$$

By (5.8) and (5.13),

$$\begin{aligned}
|p(\mathscr{A}_w(C))| &= \sum_{(\lambda_1, \lambda_2, \cdots) \vdash w} \frac{2^{(\lambda_2 + \lambda_4 + \cdots)m}}{\prod_{i=1}^{\infty} (i^{\lambda_i} \cdot \lambda_i!)} |\mathscr{A}_{\lambda_1 + \lambda_3 + \lambda_5 + \dots}(C)| \\
&= \sum_{\zeta = 0}^{w} \left(\sum_{\substack{(\lambda_1, \lambda_2, \cdots) \vdash w \\ \lambda_1 + \lambda_3 + \lambda_5 + \cdots = \zeta}} \frac{2^{(\lambda_2 + \lambda_4 + \cdots)m}}{\prod_{i=1}^{\infty} (i^{\lambda_i} \cdot \lambda_i!)} \right) |\mathscr{A}_\zeta(C)| \\
&= \sum_{\zeta = 0}^{w} g_m(w, \zeta) |\mathscr{A}_\zeta(C)| \\
&= \sum_{\substack{0 \leqslant \zeta \leqslant w \\ \zeta \equiv w \pmod 2}} g_m(w, \zeta) |\mathscr{A}_\zeta(C)|. \qquad \square
\end{aligned}$$

The function $g_m(w, \zeta)$ is difficult to compute in general. However, when ζ ($\leqslant w$) is close to w, $g_m(w, \zeta)$ takes rather simple expressions:

$$g_m(w, w)=\frac{1}{w!}, \tag{5.14}$$

$$g_m(w, w-2)=\begin{cases} 2^{m-1}, & w=2, \\ \dfrac{2^{m-1}}{(w-2)!}+\dfrac{1}{3\cdot(w-3)!}, & w\geqslant 3, \end{cases} \tag{5.15}$$

Theorem 5.3. *Let $C\subset M_m/\sim$. Then the minimal weight of C is*

$$\mu=\min\{\zeta: \mathscr{A}_\zeta(C)\neq\phi\}. \tag{5.16}$$

The weight distribution of C is given by the recursive formula

$$N_w(C)=\sum_{\substack{\mu\leqslant\zeta\leqslant w \\ \zeta\equiv w \pmod 2}} g_m(w, \zeta)|\mathscr{A}_\zeta(C)|-\sum_{\substack{\mu\leqslant\zeta\leqslant w-2 \\ \zeta\equiv w \pmod 2}} \binom{2^m+\dfrac{w-\zeta}{2}-1}{\dfrac{w-\zeta}{2}} N_\zeta(C),$$

$$w\geqslant \mu+2, \tag{5.17}$$

with initial conditions

$$N_\mu(C)=\frac{1}{\mu!}|\mathscr{A}_\mu(C)|, \tag{5.18}$$

$$N_{\mu+1}(C)=\frac{1}{(\mu+1)!}|\mathscr{A}_{\mu+1}(C)|. \tag{5.19}$$

Proof. Equation (5.16) is obvious. Equation (5.17) follows from (5.2) and (5.6). Equations (5.18) and (5.19) also follow from (5.2) and (5.6) using (5.14). □

When w ($\geqslant\mu$) is close to μ, (5.17) gives rather simple formulae for $N_w(C)$ in terms of $|\mathscr{A}_\zeta(C)|$:

$$N_{\mu+2}(C)=\begin{cases} -2^{m-1}+\dfrac{1}{2!}|\mathscr{A}_2(C)|, & \mu=0, \\ \left(-\dfrac{2^{m-1}}{\mu!}+\dfrac{1}{3\cdot(\mu-1)!}\right)|\mathscr{A}_\mu(C)|+\dfrac{1}{(\mu+2)!}|\mathscr{A}_{\mu+2}(C)|, & \mu\geqslant 1, \end{cases} \tag{5.20}$$

$$N_{\mu+3}(C)=\left(-\frac{2^{m-1}}{(\mu+1)!}+\frac{1}{3\cdot\mu!}\right)|\mathscr{A}_{\mu+1}(C)|+\frac{1}{(\mu+3)!}|\mathscr{A}_{\mu+3}(C)|, \tag{5.21}$$

We now turn to weight distributions of cosets of $R(m-3,m)$. For any $A\in M_m$, let $\tilde{A}=q(A)+R(m-3,m)$. By Theorem 3.6, it suffices to look at the weight distributions of $\widetilde{A_{m,t}}$ $(t=0,1,\ldots,m)$, $\widetilde{B_{m,m}}$ and $\widetilde{D_{m,t}}$ $(t=2,4,\ldots,2\lfloor m/2\rfloor)$. By Theorem 5.3, we only have to know $|\mathscr{A}_\zeta(\ \ )|$ $(\zeta\geqslant 0)$ of these cosets.

Let V be a vector space over GF(2) with nondegenerate inner product $l: V\times V\to \mathrm{GF}(2)$. (V,l) is called a symplectic space if $l(v,v)=0$ for all $v\in V$, and is called an Euclidean space otherwise. A subspace W of V is called isotropic if $l(u,v)=0$ for all $u,v\in W$. Let

$$\Phi_{n,k}=\text{the number of } k\text{-dimensional isotropic subspaces of an } n\text{-dimensional Euclidean space, } \quad 0\leqslant k\leqslant n/2,\ n\geqslant 1, \tag{5.22}$$

$$\Psi_{n,k}=\text{the number of } k\text{-dimensional isotropic subspaces of an } n\text{-dimensional symplectic space, } \quad 0\leqslant k\leqslant n/2,\ n \text{ is even.} \tag{5.23}$$

Lemma 5.4. (i) For $0\leqslant k\leqslant n/2$, $n\geqslant 1$,

$$\Phi_{n,k}=\begin{cases} 1 & k=0,\\ \dfrac{\prod_{i=1}^{k}(2^{n+1-2i}-1)}{\prod_{i=1}^{k}(2^i-1)}, & n \text{ is odd},\\ (2^{n-k}-1)\dfrac{\prod_{i=1}^{k-1}(2^{n-2i}-1)}{\prod_{i=1}^{k}(2^i-1)}, & n \text{ is even},\ k\geqslant 1. \end{cases} \tag{5.24}$$

(ii) *For* $0\leqslant k\leqslant n/2$, n *even*,

$$\Psi_{n,k}=\frac{\prod_{i=1}^{k}(2^{n+2-2i}-1)}{\prod_{i=1}^{k}(2^i-1)}. \tag{5.25}$$

Proof. We omit the details. One can see [12]. □

For $\zeta\geqslant 0$, let

$$\mathscr{I}(m,t,\zeta)=\{A\in M_{m,\zeta}: AA^{\mathrm{T}}=I(m,t)\},\quad t=0,1,\ldots,m, \tag{5.26}$$

$$\mathscr{K}(m,t,\zeta)=\{A\in M_{m,\zeta}: AA^{\mathrm{T}}=K(m,t)\},\quad t=2,4,\ldots,2\lfloor m/2\rfloor, \tag{5.27}$$

Clearly,

$$\mathscr{I}(m,t,\zeta)=\phi,\quad \text{for } \zeta<t, \tag{5.28}$$

$$\mathscr{K}(m,t,\zeta)=\phi,\quad \text{for } \zeta<t+1. \tag{5.29}$$

Let $l:\mathrm{GF}(2)^\zeta\times\mathrm{GF}(2)^\zeta\to\mathrm{GF}(2)$ be the usual dot product, and for $\zeta\geqslant t\geqslant 0$, define

$$\mathscr{I}_e(t,\zeta)=\{A=\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_t\end{bmatrix}\in\mathscr{I}(t,t,\zeta): l \text{ restricts to an}$$

Euclidean inner product on $\langle \alpha_1, \ldots, \alpha_t \rangle^{\perp}\}$, (5.30)

$$\mathscr{I}_s(t,\zeta)=\{A=\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_t\end{bmatrix}\in\mathscr{I}(t,t,\zeta)\colon l \text{ restricts to a}$$

symplectic inner product on $\langle \alpha_1, \ldots, \alpha_t \rangle^{\perp}\}$. (5.31)

Also define $\mathscr{K}_e(t,\zeta)$, $\mathscr{K}_s(t,\zeta)$ ($\zeta \geqslant t+1$, $t \geqslant 2$ even) similarly. Then

$$\mathscr{I}(t,t,\zeta)=\mathscr{I}_e(t,\zeta)\cup\mathscr{I}_s(t,\zeta), \quad \zeta\geqslant t\geqslant 0, \tag{5.32}$$

$$\mathscr{K}(t,t,\zeta)=\mathscr{K}_e(t,\zeta),\ \mathscr{K}_s(t,\zeta)=\phi, \quad \zeta\geqslant t+1,\ t\geqslant 2 \text{ even}. \tag{5.33}$$

Lemma 5.5.

$$|\mathscr{I}_e(0,\zeta)|=\begin{cases}0, & \text{if } \zeta=0,\\ 1, & \text{if } \zeta>0,\end{cases} \tag{5.34}$$

$$|\mathscr{I}_s(0,\zeta)|=\begin{cases}1, & \text{if } \zeta=0,\\ 0, & \text{if } \zeta>0,\end{cases} \tag{5.35}$$

$$|\mathscr{I}_e(t,\zeta)|=\begin{cases}2^{(1/4)(t-1)(2\zeta-t-1)}\prod_{i=(\zeta-t)/2}^{(\zeta-1)/2}(2^{2i}-1), & \zeta\geqslant t\geqslant 0,\ \zeta \text{ and } t \text{ both odd},\\ 2^{(1/4)t(2\zeta-t-2)}\prod_{i=(\zeta-t+1)/2}^{(\zeta-1)/2}(2^{2i}-1), & \zeta\geqslant t\geqslant 2,\ \zeta \text{ odd}, t \text{ even},\\ 2^{(1/4)(t+1)(2\zeta-t-1)}\prod_{i=(\zeta-t+1)/2}^{(\zeta/2)-1}(2^{2i}-1), & \zeta\geqslant t\geqslant 1,\ \zeta \text{ even}, t \text{ odd},\\ 2^{(1/4)t(2\zeta-t)}\prod_{i=(\zeta-t)/2}^{(\zeta/2)-1}(2^{2i}-1), & \zeta\geqslant t\geqslant 2,\ \zeta \text{ and } t \text{ both even},\end{cases} \tag{5.36}$$

$$|\mathscr{I}_s(t,\zeta)|=\begin{cases}2^{(1/4)(t-1)(2\zeta-t-1)}\prod_{i=(\zeta-t)/2+1}^{(\zeta-1)/2}(2^{2i}-1), & \zeta\geqslant t\geqslant 1,\ \zeta \text{ and } t \text{ both odd},\\ 0, & \zeta\geqslant t\geqslant 2,\ \zeta \text{ odd}, t \text{ even},\\ 0, & \zeta\geqslant t\geqslant 1,\ \zeta \text{ even}, t \text{ odd},\\ 2^{(1/4)t(2\zeta-t)}\prod_{i=(\zeta-t)/2+1}^{(\zeta/2)-1}(2^{2i}-1), & \zeta\geqslant t\geqslant 2,\ \zeta \text{ and } t \text{ both even},\end{cases} \tag{5.37}$$

$$|\mathscr{K}_e(t,\zeta)|=\begin{cases}2^{(1/4)t(2\zeta-t-2)}\prod_{i=(\zeta-t+1)/2}^{(\zeta-1)/2}(2^{2i}-1), & \zeta\geqslant t+1,\ \zeta\geqslant 2 \text{ even},\\ 2^{(1/4)t(2\zeta-t)}\prod_{i=(\zeta-t)/2}^{(\zeta/2)-1}(2^{2i}-1), & \zeta\geqslant t+1,\ \zeta \text{ even},\ t\geqslant 2 \text{ even}.\end{cases} \tag{5.38}$$

Proof. We omit the details. □

Lemma 5.6. *For* $\zeta \geqslant 0$,

$$|\mathscr{I}(m,t,\zeta)| = \sum_{0 \leqslant k \leqslant \min(m-t,\,(\zeta-t)/2)} [|\mathscr{I}_e(t,\zeta)|\,\Phi_{\zeta-t,k} + |\mathscr{I}_s(t,\zeta)|\,\Psi_{\zeta-t,k}]\,2^{(1/2)k(k-1)} \times \prod_{i=m-t-k+1}^{m-t} (2^i-1), \quad t=0,1,\ldots,m, \tag{5.39}$$

$$|\mathscr{K}(m,t,\zeta)| = |\mathscr{K}_e(t,\zeta)| \sum_{0 \leqslant k \leqslant \min(m-t,\,(\zeta-t)/2)} \Phi_{\zeta-t,k}\,2^{(1/2)k(k-1)} \times \prod_{i=m-t-k+1}^{m-t} (2^i-1), \quad t=2,4,\ldots,2\lfloor m/2 \rfloor. \tag{5.40}$$

Proof. Any $A \in \mathscr{I}(m,t,\zeta)$ is of the form

$$A = \begin{bmatrix} X \\ Y \end{bmatrix}, \tag{5.41}$$

where $X \in \mathscr{I}(t,t,\zeta)$, $YX^{\mathrm{T}}=0$, $YY^{\mathrm{T}}=0$. For any

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_t \end{bmatrix} \in \mathscr{I}(t,t,\zeta), \tag{5.42}$$

let

$$\mathscr{Y}_X = \{ Y \in M_{m-t,\zeta} \colon YX^{\mathrm{T}}=0,\ YY^{\mathrm{T}}=0 \}. \tag{5.43}$$

For any isotropic subspace $V \subset \langle x_1,\ldots,x_t\rangle^{\perp}$ with $\dim V \leqslant m-t$, let

$$\mathscr{Y}_{X,V} = \left\{ Y = \begin{bmatrix} y_1 \\ \vdots \\ y_{m-t} \end{bmatrix} \colon \langle y_1,\ldots,y_{m-t}\rangle = V \right\}. \tag{5.44}$$

Then

$$\mathscr{Y}_X = \bigcup_{V \subset \langle x_1,\ldots,x_t\rangle^{\perp} \text{ is isotropic, } \dim V \leqslant m-t} \mathscr{Y}_{X,V}, \tag{5.45}$$

where the union is disjoint. For any isotropic subspace $V \subset \langle x_1,\ldots,x_t\rangle^{\perp}$ with $\dim V = k \leqslant m-t$, choose a basis $v_1,\ldots,v_k$ for V. Then $\mathrm{GL}(m-t,2)$ acts transitively on $\mathscr{Y}_{X,V}$ by left multiplication, and the stabilizer of

$$\begin{bmatrix} v_1 \\ \vdots \\ v_k \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathscr{Y}_{X,V}$$

is

$$\left\{ \begin{bmatrix} I(k,k) & * \\ 0 & Q \end{bmatrix} : Q \in \mathrm{GL}(m-t-k,2) \right\}.$$

Hence

$$|\mathscr{Y}_{X,V}| = \frac{|\mathrm{GL}(m-t,2)|}{2^{k(m-t-k)}|\mathrm{GL}(m-t-k,2)|} = 2^{(1/2)k(k-1)} \prod_{i=m-t-k+1}^{m-t} (2^i-1). \quad (5.46)$$

Therefore

$$\begin{aligned} |\mathscr{I}(m,t,\zeta)| &= \sum_{X \in \mathscr{I}(t,t,\zeta)} \sum_{V \subset \langle x_1, \cdots, x_t \rangle^\perp \text{ is isotropic, } \dim V \leqslant m-t} |\mathscr{Y}_{X,V}| \\ &= \sum_{X \in \mathscr{I}(t,t,\zeta)} \sum_{0 \leqslant k \leqslant \min(m-t,(\zeta-t)/2)} \sum_{V \subset \langle x_1, \cdots, x_t \rangle^\perp \text{ is isotropic, } \dim V = k} |\mathscr{Y}_{X,V}| \\ &= \sum_{0 \leqslant k \leqslant \min(m-t,(\zeta-t)/2)} 2^{(1/2)k(k-1)} \prod_{i=m-t-k+1}^{m-t} (2^i-1) \\ &\quad \times \sum_{X \in \mathscr{I}(t,t,\zeta)} \sum_{V \subset \langle x_1, \cdots, x_t \rangle^\perp \text{ is isotropic, } \dim V = k} 1 \\ &= \sum_{0 \leqslant k \leqslant \min(m-t,(\zeta-t)/2)} [|\mathscr{I}_e(t,\zeta)| \Phi_{\zeta-t,k} + |\mathscr{I}_s(t,\zeta)| \Psi_{\zeta-t,k}] 2^{(1/2)k(k-1)} \\ &\quad \times \prod_{i=m-t-k+1}^{m-t} (2^i-1). \end{aligned}$$

Equation (5.40) is proved similarly. □

Theorem 5.7. (i) *For* $\zeta \geqslant 0$,

$$|\mathscr{A}_\zeta(\widetilde{A_{m,0}})| =$$

$$\begin{cases} 0, & \text{if } \zeta \text{ is odd,} \\ 1 + \displaystyle\sum_{1 \leqslant k \leqslant \min(m,\zeta/2)} 2^{(1/2)k(k-1)} (2^{\zeta-k}-1) \frac{\prod_{i=1}^{k-1} (2^{\zeta-2i}-1) \prod_{i=m-k+1}^{m} (2^i-1)}{\prod_{i=1}^{k} (2^i-1)}, & \\ & \text{if } \zeta \text{ is even,} \end{cases} \quad (5.47)$$

(ii) *For* $t=1,,\dots,m$, *and* $\zeta\geqslant 0$,

$$|\mathscr{A}_\zeta(\widetilde{A_{m,t}})|=\begin{cases}0, & \text{if } \zeta<t, \text{ or } \zeta\not\equiv t \pmod 2,\\ 2^{(1/4)(t-1)(2\zeta-t-1)+\zeta-t}\sum_{0\leqslant k\leqslant \min(m-t,(\zeta-t)/2)}2^{(1/2)k(k-3)} & \\ \quad\dfrac{\prod_{i=(\zeta-t)/2-k+1}^{(\zeta-1)/2}(2^{2i}-1)\prod_{i=m-t-k+1}^{m-t}(2^i-1)}{\prod_{i=1}^{k}(2^i-1)}, & \\ \qquad \text{if } \zeta\geqslant t\geqslant 1,\ t \text{ and } \zeta \text{ both odd},\\ 2^{(1/4)t(2\zeta-t)+\zeta-t}\sum_{0\leqslant k\leqslant \min(m-t,(\zeta-t)/2)}2^{(1/2)k(k-3)} & \\ \quad\dfrac{\prod_{i=(\zeta-t)/2-k+1}^{(\zeta/2)-1}(2^{2i}-1)\prod_{i=m-t-k+1}^{m-t}(2^i-1)}{\prod_{i=1}^{k}(2^i-1)}, & \\ \qquad \text{if } \zeta\geqslant t\geqslant 2,\ t \text{ and } \zeta \text{ both even},\end{cases}\tag{5.48}$$

(iii) *For* $\zeta\geqslant 0$,

$$|\mathscr{A}_\zeta(\widetilde{B_{m,m}})|=\begin{cases}0, & \text{if } \zeta<m+1, \text{ or } \zeta\not\equiv m+1 \pmod 2,\\ 2^{(1/4)m(2\zeta-t-2)}\prod_{i=(\zeta-m+1)/2)}^{(\zeta-1)/2}(2^{2i}-1), & \\ \qquad \text{if } m \text{ even}, \zeta\geqslant m+1 \text{ odd},\\ 2^{(1/4)(m+1)(2\zeta-m-1)}\prod_{i=(\zeta-m+1)/2}^{(\zeta/2)-1}(2^{2i}-1), & \\ \qquad \text{if } m \text{ odd}, \zeta\geqslant m+1 \text{ even},\end{cases}\tag{5.49}$$

(iv) *For* $t=2,4,\dots,2\lfloor m/2\rfloor$, *and* $\zeta\geqslant 0$,

$$|\mathscr{A}_\zeta(\widetilde{D_{m,t}})|=\begin{cases}0, & \text{if } \zeta<t+2, \text{ or } \zeta \text{ is odd},\\ 2^{(1/4)t(2\zeta-t)}\sum_{0\leqslant k\leqslant \min(m-t,(\zeta-t)/2)}2^{(1/2)k(k-1)}(2^{\zeta-t-k}-1) & \\ \quad\times\dfrac{\prod_{i=(\zeta-t)/2-k+1}^{(\zeta/2)-1}(2^{2i}-1)\prod_{i=m-t-k+1}^{m-t}(2^i-1)}{\prod_{i=1}^{k}(2^i-1)}, & \\ \qquad \text{if } \zeta\geqslant t+2 \text{ is even}.\end{cases}\tag{5.50}$$

Proof. Note that

$$|\mathscr{A}_\zeta(\widetilde{A_{m,t}})|=\begin{cases}\Phi, & \text{if } \zeta\not\equiv t \pmod 2,\\ \mathscr{I}(m,t,\zeta), & \text{if } \zeta\equiv t \pmod 2.\end{cases}\tag{5.51}$$

Then (5.47) and (5.48) follow from (5.51) and (5.39). We omit the details of computation. Equations (5.49) and (5.50) are proved similarly. □

References

[1] E. Artin, Geometric Algebra (Wiley, New York, 1988).
[2] E. Berlekamp and L.R. Welch, Weight distributions of the cosets of the (32, 6) Reed–Muller code, IEEE Trans. Inform. Theory 18 (1972) 203–207.
[3] N.L. Biggs and A.T. White, Permutation Groups and Combinatorial Structures (Cambridge Univ. Press, Cambridge, 1979).
[4] R.A. Brualdi, N. Cai and V.S. Pless, Orphans structure of the first order Reed–Muller codes, Discrete Math. 102 (1992) 239–247.
[5] R.A. Brualdi and V.S. Pless, Orphans of the first order Reed–Muller codes, IEEE Trans. Inform. Theory 36 (1990) 399–401.
[6] G.D. Cohen, M.G. Karpovsky, H.F. Mattson Jr and J.R. Schatz, Covering radius – survey and recent results, IEEE Trans. Inform. Theory 31 (1985) 328–343.
[7] L.E. Dickson, Linear Groups (Dover, New York, 1958).
[8] R.L. Graham and N.J.A. Sloane, On the covering radius of codes, IEEE Trans. Inform. Theory 31 (1985) 385–401.
[9] X. Hou, Binary linear quasi-perfect codes are normal, IEEE Trans. Inform. Theory 37 (1991) 378–379.
[10] F.J. MacWilliams and N.J. Sloane, The Theory of Error-Correcting Codes, Vol. II (North-Holland, Amsterdam, 1977).
[11] A. McLoughlin, The covering radius of the $(m-3)$rd Reed–Muller codes and a lower bound on the $(m-4)$th order Reed–Muller codes, SIAM J. Appl. Math. 37 (1979) 419–422.
[12] V. Pless, The number of isotropic subspaces in a finite geometry, Accad, Naz. Lincei, Rend. Cl. Sci. Fiz., Mat. e Nat. (8) 39 (1965) 418–421.
[13] J. Simonis, Reed–Muller codes, Report 87–23, Delft Univ. of Tech., Delft, 1987.