Generalized Extended Hamming Codes over Galois Ring of Characteristic $2^n$

MUHAMMAD ILYAS$^{1,2}$ AND MIEKO YAMADA$^3$

$^1$Graduate School of Natural Sciences and Technology, Kanazawa University, Japan,
$^2$Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Indonesia,
$^3$Institute of Science and Engineering, Kanazawa University, Japan
(reiken7@gmail.com)

Abstract

In this paper, we introduce generalized extended Hamming codes over Galois rings $GR(2^n, m)$ of characteristic $2^n$ with extension degree $m$. Furthermore we prove that the minimum Hamming weight of generalized extended Hamming codes over $GR(2^n, m)$ is 4 and the minimum Lee weight of generalized extended Hamming codes over $GR(8, m)$ is 6 for all $m \geq 3$. 

Received May 25, 2011.
This work is supported by JSPS KAKENHI (20540014).
AMS Subject Classification 94B05
1 Introduction

Preparata codes are non-linear double-error-correcting codes over finite fields, named after Franco P. Preparata who first described them in 1968. Preparata codes are nonlinear codes and these have more codewords than any comparable linear code presently known. Hammons et al. \[1\] introduced Preparata codes and Kerdock codes over the Galois ring of characteristic 4. The binary image of the Preparata code under the Gray map has the same properties of the Preparata original code over a finite field. They also show that these Preparata code is a dual code of Kerdock code over the Galois ring of characteristic 4.

We define generalized extended Hamming codes over Galois ring $GR(2^n, m)$ of characteristic $2^n$ with extension degree $m$ similarly to the definition of the extended Hamming codes over finite fields. If we restrict the characteristic to 4, then the generalized extended Hamming code turns out the Preparata code that Hammons et al. introduced. We show generalized extended Hamming codes have similar properties as the extended Hamming codes over finite fields. By using 2-adic representation, we determine the minimum Hamming weight over $GR(2^n, m)$ and the minimum Lee weight of a generalized extended Hamming code over $GR(4, m)$. We could use this method recursively to obtain the minimum Lee weight of generalized extended Hamming codes for general characteristics $2^n$.

2 Galois Rings

2.1 Galois Rings $GR(q, m)$

We let $q = 2^n$, $n \geq 1$ and $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ and we put $N = 2^m - 1$, for $m \geq 3$.

Let $h_2 (X)$ be a primitive polynomial over a finite field $\mathbb{F}_2$ with 2 elements. There exist a unique monic irreducible polynomial $h_q (X) \in \mathbb{Z}_q [X]$ of degree $m$ such that $h_2 (X) \equiv h_q (X) (\text{mod } 2)$ and $h_q (X)$ divides $X^N - 1 \in \mathbb{Z}_q [X]$. We call the polynomial $h_q (X)$ a primitive basic irreducible polynomial.

**Definition 1** (Galois Rings). Let $\xi$ be a root of $h_q (X)$, so that $\xi^N = 1$. The Galois ring $GR (q, m)$ is defined to be $\mathbb{Z}_q [X] / h_q (X)$ and isomorphic to $\mathbb{Z}_q (\xi)$. We put $R = GR (q, m)$.

We can write every element $c \in R$ as unique 2-adic representation

$$c = a_0 + 2a_1 + 4a_2 + \ldots + 2^{n-1}a_{n-1},$$

where $a_i \in \{0, 1, \xi, \xi^2, \ldots, \xi^{N-1}\}$, $0 \leq i \leq n - 1$.

We know $\xi^j$ can be represented as

$$\xi^j = a_{0,j} + a_{1,j} \xi + \ldots + a_{m-1,j} \xi^{m-1},$$

where $a_{0,j}, a_{1,j}, \ldots, a_{m-1,j} \in \mathbb{Z}_q$, $0 \leq j \leq N - 1$.

Note that $R$ contains zero divisors, these are the elements of the radical $2GR(q, m) = 2GR(\frac{q}{2}, m)$, the unique maximal ideal in $R$. 
We denote the set \( \{0, 1, \xi, \ldots, \xi^{N-1}\} \) by \( \mathcal{T} \). We define the homomorphism \( \eta \)
\[
\eta : GR(q, m) \to \mathbb{F}_{2^m} \text{ as } \eta(\xi) = \theta \text{ and } \eta(a) = a \pmod{2} \text{ for } a \in \mathbb{Z}_q,
\]
where \( \theta \) is a root of a primitive polynomial \( h_2(X) \).

Next, we define the map \( \tau : GR(q, m) \to \mathcal{T} \) as
\[
\tau(c) = c^{2^m} = a_0. \tag{2.2}
\]

### 2.2 Frobenius automorphism of \( GR(2^n, m) \)

In this subsection, we define the Frobenius automorphism over \( GR(2^n, m) \). We will use this automorphism in transforming a codeword.

**Definition 2 (Frobenius Automorphism of \( GR(2^n, m) \)).** The **Frobenius automorphism** \( f \) from \( GR(2^n, m) \) to \( GR(2^n, m) \) is defined as
\[
c^f = a_0^2 + 2a_1^2 + 4a_2^2 + \ldots + 2^{n-1}a_{n-1}^2, \tag{2.3}
\]
for any element \( c = a_0 + 2a_1 + 4a_2 + \ldots + 2^{n-1}a_{n-1} \in GR(2^n, m) \).

### 3 Codes over \( \mathbb{Z}_q \)

#### 3.1 Codes over \( \mathbb{Z}_q \) and the minimum weight

We define a code over \( \mathbb{Z}_q \) similarly to the definition of a code over a finite field.

**Definition 3 (Codes over \( \mathbb{Z}_q \)).** If \( C \) is an additive subgroup of \( \mathbb{Z}_q^m \), then we call \( C \) a **linear block code** of length \( m \) over \( \mathbb{Z}_q \).

We need to define the minimum Hamming weight and the minimum Lee weight. Let \( c = (c_0, c_1, \ldots, c_{N-1}) \in \mathbb{Z}_q^N \) be a codeword of \( C \).

**Definition 4 (Hamming Weight).** The number of nonzero elements of the codeword \( c \in C \) is called the **Hamming weight** \( w_H(c) \) of \( c \) and the **minimum Hamming weight** of \( C \) is defined as
\[
w_H^m(C) = \min_{c \in C, c \neq 0} w_H(c).
\]

**Definition 5 (Lee Weight).** The **Lee weight** \( w_L(c) \) of the codeword \( c \in C \) is defined as
\[
w_L(c) = \sum_{i=0}^{N-1} \min \{c_i, 2^n - c_i\},
\]
and the **minimum Lee weight** of \( C \) is defined as
\[
w_L^m(C) = \min_{c \in C, c \neq 0} w_L(c).
\]
3.2 Generalized Extended Hamming Codes

Hammons et al. [1] worked on generalized extended Hamming codes and called them the "Preparata" codes over $GR(4,m)$, because the binary image of these codes over $GR(4,m)$ under the Gray map has the same properties of Preparata original codes over finite fields. Based on their paper, we define the generalized extended Hamming codes similarly to the definition of the extended Hamming codes over finite fields.

**Definition 6 (Generalized extended Hamming Codes).** We define the parity-check matrix $P$, indexed by $\infty, 0, 1, \ldots, N-1$, as follows:

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \xi & \xi^2 & \ldots & \xi^{N-1} \end{pmatrix}$$

where $\xi$ is a root of a primitive basic irreducible polynomial. Then $P_q = \{c \in \mathbb{Z}_q^{N+1} | Pc^T = 0\}$ is a code over $GR(q,m)$ and called a generalized extended Hamming code. In what follows, we abbreviate generalized extended Hamming codes as GEH codes.

In other words, if $c = (c_\infty, c_0, \ldots, c_{N-1})$ is a codeword of a GEH code, then it must satisfy the following two equations:

$$c_\infty + \sum_{i=0}^{N-1} c_i = 0, \quad (3.1)$$

$$\sum_{i=0}^{N-1} c_i \xi^i = 0. \quad (3.2)$$

We call $c_\infty$ a zero-sum check symbol. Notice that a GEH code is the dual code of a 1$^{st}$ order Reed-Muller code over $GR(q,m)$.

If $q = 2$, a GEH code coincides to an extended Hamming code over a finite field $\mathbb{F}_{2^m}$.

4 Main Theorems

We can determine the number of codewords, and the minimum Hamming weight of a GEH code $P_q$ and the minimum Lee weight of a GEH code $P_8$.

**Theorem 1 (Number of codewords).** The number of codewords of a GEH code $P_q$ is $q^k$, where $k = 2^m - m - 1$.

**Proof.** We give the number of codewords by observing a parity-check matrix of a GEH code. For simplicity, we can write the generator matrix as

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & I_m & A_k \end{pmatrix} \quad (4.1)$$

where $I_m$ is an identity matrix and $A_k$ is $m \times k$-sized square matrix where $k = 2^m - m - 1$ and $0$ is the all-zero column vector and $1$ is the all-one row vector. We can see the first column and $I_m$-block act as nullifier. Thus, the number of codewords depends only on $A_k$-block, where it is a part of a codeword with length $k$. Therefore, the number of codewords is as assigning $q$ values on $k$ column, that is $q^k$ codewords. □
**Theorem 2.** The minimum Hamming weight of $P_q$ with length $2^m$ over $GR(q, m)$ is 4.

**Proof.** Hammons et al. [1] showed that the minimum Hamming weight of $P_q$ is 4. This means that the codeword with the minimum Hamming weight has 4 non-zero entries.

Let $c = (c_\infty, c_0, \ldots, c_{N-1})$ be the codeword with Hamming weight 4. Then we see that $2c = (2c_\infty, 2c_0, \ldots, 2c_{N-1})$ is a codeword of $P_2$ and the Hamming weight of this codeword is 4. For a general case, we can take this method recursively. Thus the minimum Hamming weight of $P_q$ is 4. \qed

**Lemma 1.** Let $q' = \frac{q}{2}$. The minimum Lee weight of $P_{q'}$ over $GR(q', m)$ are always less than or equal to the minimum Lee weight of $P_q$ over $GR(q, m)$.

**Proof.** We can write the Lee weight of a codeword $c'$ of $P_{q'}$ over $GR(q', m)$ as

$$w_L(c') = \sum_{i=1}^{q'-1} i (n'_i + n'_{q'-i}) + \frac{q'}{2} n'_{\frac{q'}{2}}$$

with the same summation index, we can write the Lee weight of a codeword $c$ of $P_q$ over $GR(q, m)$ as

$$w_L(c) = \sum_{i=1}^{q} \{i (n_i + n_{q-i}) + (q - i) (n_{q'-i} + n_{q'+i})\} + \frac{q}{2} (n_{\frac{q}{2}} + n_{\frac{q}{2}}) + q n'q$$

where $n'_i$ and $n_i$ are the numbers of entries $i$ of $c'$ and $c$ respectively.

Define the map $\mu : GR(q, m) \to GR(q', m)$ as $\mu (\xi_q) = \xi_{q'}$ and $\mu (c) \equiv c \pmod{q'}$ where $\xi_q$ and $\xi_{q'}$ are roots of the primitive basic irreducible polynomials of $P_q$ and $P_{q'}$ respectively and $c \in GR(q, m)$. Then $\mu (P_q) = P_{q'}$. From $n'_i = n_i + n_{q'+i}$, we have

$$w_L(c') = \sum_{i=1}^{q'-1} i (n'_i + n'_{q'-i}) + \frac{q'}{2} n'_{q'}$$

$$= \sum_{i=1}^{q'-1} \{i (n_i + n_{q-i}) + i (n_{q'-i} + n_{q'+i})\} + \frac{q'}{2} (n_{\frac{q}{2}} + n_{\frac{q}{2}})$$

$$\leq \sum_{i=1}^{q'-1} \{i (n_i + n_{q-i}) + (q'-i) (n_{q'-i} + n_{q'+i})\} + \frac{q'}{2} (n_{\frac{q}{2}} + n_{\frac{q}{2}}) + q' n_{q'}.$$ 

This means that $w_L(c') \leq w_L(c)$. Thus the minimum Lee weight of $P_{q'}$ over $GR(q', m)$ is always less than or equal to the minimum Lee weight of $P_q$ over $GR(q, m)$. \qed

Lemma [1] gives an important information such that the codeword of $P_q$ may have the minimum Lee weight of which image by the map $\mu$ has the minimum Lee weight of $P_{q'}$.

Thus, we show the existence of the codewords of the extended Hamming code with the Hamming weights 4 and 6 over $\mathbb{F}_{2^m}$ concretely. We consider the matrix $P$ as a parity check matrix of an extended Hamming code. Let $\theta$ be a root of $h_2(X)$. 
For $m \geq 2$, we know the sum of the following 4 vectors of length $m + 1$ is $0$.

\[
\begin{pmatrix}
1 \\
0 \\
0 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
1 \\
0 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
0 \\
1 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
1 \\
1 \\
\vdots \\
\end{pmatrix}
\]

The first vector corresponds to the column vector \( \begin{pmatrix} 1 \\ 0 \end{pmatrix} \) of $P$ in Definition [3], the second and the third vectors correspond to the column vectors \( \begin{pmatrix} 1 \\ 1 \end{pmatrix} \) and \( \begin{pmatrix} 1 \\ \theta \end{pmatrix} \) of $P$ respectively, and the fourth vector corresponds to the column vector \( \begin{pmatrix} 1 \\ \theta^2 \end{pmatrix} \) of $P$ for some $i$. If we put $c_\infty$, $c_0$, $c_1$ and $c_i$ are all 1 and the other entries are zero, then the Hamming weight of $c = (c_\infty, c_0, c_1, \ldots, c_{N-1}) = (1, 1, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$ is 4.

For $m \geq 4$, we know the sum of the following 6 vectors of length $m + 1$ is $0$.

\[
\begin{pmatrix}
1 \\
0 \\
0 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
1 \\
0 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
0 \\
1 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
0 \\
0 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
1 \\
1 \\
\vdots \\
\end{pmatrix}
\quad
\begin{pmatrix}
1 \\
1 \\
1 \\
\vdots \\
\end{pmatrix}
\]

The first vector corresponds to the column vector \( \begin{pmatrix} 1 \\ 0 \end{pmatrix} \) of $P$, the second to the fifth vectors correspond to the column vectors \( \begin{pmatrix} 1 \\ 1 \end{pmatrix} \), \( \begin{pmatrix} 1 \\ \theta \end{pmatrix} \), \( \begin{pmatrix} 1 \\ \theta^2 \end{pmatrix} \), \( \begin{pmatrix} 1 \\ \theta^3 \end{pmatrix} \) of $P$ respectively, and the sixth vector corresponds to the column vector \( \begin{pmatrix} 1 \\ \theta^i \end{pmatrix} \) of $P$ for some $i$. If we put $c_\infty$, $c_0$, $c_1$, $c_2$, $c_3$ and $c_i$ are all 1 and the other entries are zero, then the Hamming weight of $c = (c_\infty, c_0, c_1, \ldots, c_{N-1}) = (1, 1, 1, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$ is 6.

We give the dependencies among the powers of $\gamma$ where $\gamma$ is a root of $h_4(X)$ used in the proof of theorems.

**Lemma 2.** ([1] and [4]). Let $\gamma$ be a root of a primitive basic irreducible polynomial $h_4(X)$. We have

1. $\pm \gamma^j \pm \gamma^k$ is invertible for $0 \leq j < k < N$, $m \geq 2$.
2. $\gamma^j - \gamma^k \neq \pm \gamma^l$ for distinct $j$, $k$, $l$ in $[0, N - 1]$, $m \geq 2$.
3. If $m \geq 3$ and $i \neq j$, $k \neq l$ in $[0, N - 1]$, then $\gamma^i - \gamma^j = \gamma^k - \gamma^l \Rightarrow i = k$ and $j = l$.
4. If $m \geq 3$ and $m$ odd, then $\gamma^i + \gamma^j + \gamma^k + \gamma^l = 0 \Rightarrow i = j = k = l$.
Hammons et al. [1] determined the minimum Lee weight of $P_4$ and just showed the existence of the codewords with minimum Lee weight. Next we list all the codewords with the minimum Lee weight of $P_4$ by transforming the codewords of the extended Hamming code over $\mathbb{F}_{2^n}$.

On the following theorems, the coordinates $\{0, a, b, c, d, e\}$ correspond to the coordinates of nonzero entries of the codewords of the extended Hamming code with the Hamming weights 4 or 6.

**Theorem 3.** For odd $m \geq 3$, the minimum Lee weight of $P_4$ with length $2^m$ is 6. The codeword $c = (c_\infty, c_0, \ldots, c_{N-1})$ of $P_4$ with the minimum Lee weight 6 has one of the following forms:

| Case | $c_\infty$ | $c_0$ | $c_a$ | $c_b$ | $c_c$ | $c_d$ | $c_e$ |
|------|------------|-------|-------|-------|-------|-------|-------|
| Case 1 | -1 | 1 | 1 | 1 | 2 | 0 | 0 |
| Case 2 | 1 | -1 | 1 | 1 | 2 | 0 | 0 |
| Case 3 | 2 | -1 | 1 | 1 | 1 | 0 | 0 |
| Case 4 | 0 | -1 | 1 | 1 | 1 | 2 | 0 |
| Case 5 | 0 | -1 | 1 | 1 | 1 | 1 | 1 |
| Case 6 | 0 | -1 | -1 | 1 | 1 | 1 | 1 |
| Case 7 | -1 | 1 | 1 | 1 | 1 | 1 | 0 |
| Case 8 | 1 | -1 | 1 | 1 | 1 | 1 | 0 |
| Case 9 | -1 | -1 | 1 | 1 | 1 | 0 | 0 |
| Case 10 | 1 | -1 | -1 | 1 | 1 | 0 | 0 |

Table 1: List of codewords with the minimum Lee weight of $P_4$ for odd $m \geq 3$

The codewords for Cases 1 to 4 are obtained from the codewords of the extended Hamming code over $\mathbb{F}_{2^m}$ with the minimum Hamming weight 4 and the codewords for Cases 5 to 10 are obtained from the codewords with the Hamming weight 6.

For even $m \geq 4$, the minimum Lee weight of $P_4$ with length $2^m$ is 4. The codeword of $P_4$ with the minimum Lee weight 4 has one of the following 2 forms:

| Case | $c_\infty$ | $c_0$ | $c_a$ | $c_b$ | $c_c$ |
|------|------------|-------|-------|-------|-------|
| Case 11 | 1 | 1 | 1 | 1 | 0 |
| Case 12 | 0 | 1 | 1 | 1 | 1 |

Table 2: List of codewords with the minimum Lee weight of $P_4$ for even $m \geq 4$

Proof. The equation (3.1) implies that every codeword has even number of odd entries. Therefore Lee weight is even. So, the minimum Lee weight is even. The codeword obtained from multiplying the nonzero entries of the other codeword by $-1$ has the same Lee weight as that of the other. Therefore we may choose one of these codewords.

We assume $m$ is odd. We know the minimum Hamming weight of the extended Hamming code $H$ over a finite field is 4. If the codeword of $P_4$ has the Lee weight 6 and its image has the Hamming weight 4, then the nonzero entries are determined as $\{-1, 1, 1, 1, 2\}$. 
If the codewords of $P_4$ has the Lee weight 6 and its image has the Hamming weight 6, then we have the following 2 cases:

1. Codewords with nonzero entries $\{-1, 1, 1, 1, 1\}$.

2. Codewords with nonzero entries $\{-1, -1, -1, 1, 1\}$.

We need to check that the codeword with this form satisfy equation (3.2). Every element $\alpha_4 \in GR(4, m)$ has a unique representation

$$\alpha_4 = a_0 + 2a_1$$

(4.2)

where $a_0, a_1 \in T = \{0, 1, \gamma, \ldots, \gamma^{n-1}\}$. We fix the codeword of the extended Hamming code $H$ with the minimum Hamming weight 4, so that it will satisfy $\theta^a + \theta^b + \theta^c + \theta^d = 0$ for some $a, b, c$ and $d$. We can write this equivalently as $\theta^a (1 + \theta^{b-a} + \theta^{c-a} + \theta^{d-a}) = 0$. Therefore, without loss of generality, we may assume that $1 + \theta^a + \theta^b + \theta^c = 0$ is satisfied for some $a, b$ and $c$. We choose the vector of $GR(4, m)$ with nonzero entries $\{-1, 1, 1, 1, 2\}$. We assume that $c_\infty$ is 0 or 2. The coordinates 0, $a, b$ and $c$ correspond to the nonzero entries of the codeword of $H$. We may assume $c_0 = -1$ without loss of generality. Otherwise, for example, for the case $c_0 = -1$, it can be reduced to the case $c_0 = -1$ by multiplying $1 - \gamma^a + \gamma^b + \gamma^c = a_0 + 2a_1$ by $\gamma^{-a}$. We put

$$-1 + \gamma^a + \gamma^b + \gamma^c = a_0 + 2a_1, \quad a_0, a_1 \in T.$$  

(4.3)

By applying the map $\tau$ in (1.3), we can obtain

$$a_0 = (-1 + \gamma^a + \gamma^b + \gamma^c)^{2^m} = 1 + \gamma^a + \gamma^b + \gamma^c + 2 \left( \gamma^{2^{m-1}a} + \gamma^{2^{m-1}b} + \gamma^{2^{m-1}c} + \gamma^{2^{m-1}(a+b)} + \gamma^{2^{m-1}(a+c)} + \gamma^{2^{m-1}(b+c)} \right).$$  

(4.4)

If we multiply (4.4) by 2, then we have

$$2a_0 = 2 \left( -1 + \gamma^a + \gamma^b + \gamma^c \right).$$  

(4.5)

From $2 \left( -1 + \gamma^a + \gamma^b + \gamma^c \right) = 2 (1 + \theta^a + \theta^b + \theta^c) = 0$, we see $a_0$ is zero.

We can calculate $a_1$ as follows:

$$2a_1 = \left( -1 + \gamma^a + \gamma^b + \gamma^c \right) - \left( -1 + \gamma^a + \gamma^b + \gamma^c \right)^{2^m} = 2 \left( 1 + \gamma^{2^{m-1}a} + \gamma^{2^{m-1}b} + \gamma^{2^{m-1}c} + \gamma^{2^{m-1}(a+b)} + \gamma^{2^{m-1}(a+c)} + \gamma^{2^{m-1}(b+c)} \right),$$

$$a_1 = 1 + \theta^{2^{m-1}a} + \theta^{2^{m-1}b} + \theta^{2^{m-1}c} + \theta^{2^{m-1}(a+b)} + \theta^{2^{m-1}(a+c)} + \theta^{2^{m-1}(b+c)}. $$

(4.6)

By using the Frobenius automorphism, we have

$$1 + \theta^{2^{m-1}a} + \theta^{2^{m-1}b} + \theta^{2^{m-1}c} = (1 + \theta^a + \theta^b + \theta^c)^{2^{m-1}} = 0.$$  

Thus we have

$$a_1 = \theta^{2^{m-1}(a+b)} + \theta^{2^{m-1}(a+c)} + \theta^{2^{m-1}(b+c)}. $$  

(4.7)

Hence the coordinate $d$ such that

$$-1 + \gamma^a + \gamma^b + \gamma^c = 2\gamma^d,$$

(4.8)
is determined as \( 2\gamma^d = 2\left(\theta^{2m-1(a+b)} + \theta^{2m-1(a+c)} + \theta^{2m-1(b+c)}\right) \). Otherwise \(-1 + \gamma^a + \gamma^b + \gamma^c = 0\).

For the case \(-1 + \gamma^a + \gamma^b + \gamma^c = 0\), the codeword must have \(c_\infty = 2\) to satisfy the first row equation (3.1) and its image satisfies \(\theta^{a+b} + \theta^{a+c} + \theta^{b+c} = 0\). Thus the codeword with Lee weight 6 is given as follows:

\[
\begin{pmatrix}
c_\infty & \ldots & c_0 & \ldots & c_a & \ldots & c_b & \ldots & c_c & \ldots \\
2 & \ldots & -1 & \ldots & 1 & \ldots & 1 & \ldots & 1 & \ldots
\end{pmatrix}
\] (4.9)

This is Case 3 in Table 1 of the theorem.

For the case \(-1 + \gamma^a + \gamma^b + \gamma^c = 2\gamma^d\) where \(2\gamma^d = 2\left(\theta^{2m-1(a+b)} + \theta^{2m-1(a+c)} + \theta^{2m-1(b+c)}\right)\), the codewords must have \(c_\infty = 0\) to satisfy the first row equation (3.1). Thus the codeword with Lee weight 6 is given as follows:

\[
\begin{pmatrix}
c_\infty & \ldots & c_0 & \ldots & c_a & \ldots & c_b & \ldots & c_c & \ldots & c_d & \ldots \\
0 & \ldots & -1 & \ldots & 1 & \ldots & 1 & \ldots & 1 & \ldots & 2 & \ldots
\end{pmatrix}
\] (4.10)

This is Case 4 in Table 1 of the theorem. If we assume \(c_\infty = \pm 1\), then we obtain Cases 1 and 2 by similar calculations and the coordinate \(c\) is determined from the codeword of the extended Hamming code.

We consider the vector of \(GR(4, m)\) whose image by \(\eta\) is the codeword of \(H\) with Hamming weight 6. Then we obtain Cases 5 and 6 if \(c_\infty = 0\) and Cases 7, 8, 9 and 10 if \(c_\infty = \pm 1\) in the same way.

Next, we assume \(m\) is even. To satisfy (3.1), the codewords of \(P_4\) with the Lee weight 4 have nonzero values \(\{1, 1, -1, -1\}\) or \(\{1, 1, 1, 1\}\).

If we consider the codewords with nonzero values \(\{1, 1, -1, -1\}\) and \(c_\infty = 0\), then it must satisfy \(\gamma^a + \gamma^b - \gamma^c - \gamma^d = 0\), that is \(a = d\) and \(b = c\) from Lemma 2. It contradicts the assumption. On the other hand, if the codeword has \(c_\infty = \pm 1\) it will also contradict point (2) of Lemma 2.

Hammons et al. [1] showed that \(\gamma^{2t} + \gamma^t + 1 = 0\) is satisfied where \(t = (2^m - 1)/3\) and the codeword with nonzero entries \(c_\infty = c_0 = c_1 = c_2t = 1\) has the Lee weight 4. The codeword with \(c_\infty = 0\) and 4 other nonzero entries also has the Lee weight 4. Hence we have Case 11 and Case 12.

We find the minimum Lee weight of \(P_8\) over Galois rings of characteristic 8 by transformation of the codewords of \(P_4\) in Tables 1 and 2.

**Theorem 4.** The minimum Lee weight of \(P_8\) over Galois rings of characteristic 8 with length \(2^m\) is 6, for \(m \geq 3\).

**Proof.** We know that the minimum Lee weight of \(P_4\) is 6 for odd extensions and 4 for even extensions [1]. For even extension, if there exists the codeword with Lee weight 6 of \(P_8\), then the minimum Lee weight of \(P_8\) is 6 from Lemma [1].

The image by the map \(\mu\) of this codeword is a codeword of \(P_4\) with Lee weight 6 and the image under the map \(\eta\) is a codeword of an extended Hamming code with the Hamming weight 4 or 6.

Notice that any element \(\alpha_8 \in GR(8, m)\) has the unique representation

\[\alpha_8 = a_0 + 2a_1 + 4a_2\]
where \( a_0, a_1, a_2 \in T \) and \( \mu (\alpha_8) \in GR(4, m) \) and \( \tau (\alpha_8) = \alpha_8^{2m} = a_0 \).

We assume that the image of the codeword of \( P_8 \) by the map \( \mu \) is the codeword of \( P_4 \) which satisfies \( 1 + \gamma^a + \gamma^b = 2\gamma^c, a \neq b \neq c \), for Case 1 in Table 1 of Theorem 3.

We put
\[
1 + \xi^a + \xi^b = a_0 + 2a_1 + 4a_2, \quad a_0, a_1, a_2 \in T.
\] (4.11)

By applying the map \( \tau \) to the equation (4.11), we can write
\[
\begin{align*}
a_0 &= (1 + \xi^a + \xi^b)^{2m} \\
&= 1 + \xi^a + \xi^b + 4 \left( 1 + \xi^{2m-1}a + \xi^{2m-1}b \right) \cdot \left( \xi^{2m-2}a + \xi^{2m-2}b + \xi^{2m-2(a+b)} \right) \quad (4.12) \\
&+ 6 \left( \xi^{2m-1}a + \xi^{2m-1}b + \xi^{2m-1(a+b)} \right).
\end{align*}
\]

From
\[
4 \left( 1 + (\xi^a)^{2m-1} + (\xi^b)^{2m-1} \right) = 4 \left( 1 + (\theta^a)^{2m-1} + (\theta^b)^{2m-1} \right) = 4 \left( 1 + \theta^a + \theta^b \right)^{2m-1} = 0,
\]
we have
\[
a_0 = 1 + \xi^a + \xi^b + 6 \left( \xi^{2m-1}a + \xi^{2m-1}b + \xi^{2m-1(a+b)} \right). \quad (4.13)
\]

We can verify \( a_0 = 0 \), by multiplying (4.13) by 4,
\[
4a_0 = 4 \left( 1 + \xi^a + \xi^b \right) = 4 \left( 1 + \theta^a + \theta^b \right) = 0.
\]

We can calculate \( a_1 \) and \( a_2 \).
\[
\begin{align*}
2a_1 + 4a_2 &= (1 + \xi^a + \xi^b) - (1 + \xi^a + \xi^b)^{2m}, \\
2a_1 + 4a_2 &= 2 \left( \xi^{2m-1}a + \xi^{2m-1}b + \xi^{2m-1(a+b)} \right), \\
a_1 + 2a_2 &= \gamma^{2m-1}a + \gamma^{2m-1}b + \gamma^{2m-1(a+b)}. \quad (4.14)
\end{align*}
\]

Let \( \gamma^u = \gamma^{2m-1}a \) and \( \gamma^v = \gamma^{2m-1}b \). We can calculate \( a_1 \) by applying the map \( \tau \),
\[
a_1 = (\gamma^u + \gamma^v + \gamma^{u+v})^{2m} = \gamma^u + \gamma^v + \gamma^{u+v} + 2\gamma^{2m-1(u+v)} \left( 1 + \gamma^{2m-1u} + \gamma^{2m-1v} \right).
\]

From
\[
2 \left( 1 + (\gamma^u)^{2m-1} + (\gamma^v)^{2m-1} \right) = 2 \left( 1 + (\theta^a)^{2m-2} + (\theta^b)^{2m-2} \right) = 0,
\]
we have
\[
a_1 = (\gamma^u + \gamma^v + \gamma^{u+v})^{2m} = \gamma^u + \gamma^v + \gamma^{u+v} = \gamma^{2m-1a} + \gamma^{2m-1b} + \gamma^{2m-1(a+b)}. \quad (4.15)
\]

By substituting (4.15) to (4.14), we can get \( a_2 = 0 \). Hence we have
\[
\begin{align*}
a_0 &= 0, \\
a_1 &= \gamma^{2m-1a} + \gamma^{2m-1b} + \gamma^{2m-1(a+b)}, \\
a_2 &= 0.
\end{align*}
\]

Consequently, the coordinate \( c \) such that
\[
1 + \xi^a + \xi^b = 2\xi^c
\]
is determined as \( 2\xi^c = 2 \left( \gamma^{2m-1}a + \gamma^{2m-1}b + \gamma^{2m-1}(a+b) \right) \). For the cases when \( c = 0, a \) and \( b \), it contradicts the minimum Lee weight of \( P_4 \) is 6.

The codewords is as follows:

\[
\left( \begin{array}{cccccccc}
  c_\infty & c_0 & \ldots & c_a & \ldots & c_b & \ldots & c_c & \ldots \\
 -1 & 1 & \ldots & 1 & \ldots & 1 & \ldots & 6 & \ldots 
\end{array} \right)
\]

The Lee weight of this codeword is 6. In subsection 3.1, we showed the existence of a codeword of the extended Hamming code with Hamming weight 4. It ensures the existence of this codeword. We also prove the codewords corresponding to Case 9 and 10 in Table 1 has the Lee weight 6 and it ensures the existence of these codewords from the codeword of the extended Hamming code mentioned in subsection 3.1.

Next we assume the image of the codeword of \( P_8 \) by the map \( \mu \) satisfies \( 1 + \gamma^t + \gamma^{2t} = 0 \) where \( \gamma^{3t} = 1 \) and \( t = \frac{2m-1}{3} \) for Case 11 of Table 1 of Theorem 3. So, \( 1 + \theta^t + \theta^{2t} = 0 \) is also satisfied.

We put

\[
1 + \xi^t + \xi^{2t} = a_0 + 2a_1 + 4a_2, \quad a_0, a_1, a_2 \in \mathcal{T}.
\]

By applying the map \( \tau \) in (4.16), we can write

\[
a_0 = (1 + \xi^t + \xi^{2t})^{2m} = 1 + \xi^t + \xi^{2t} + 4 \left( 1 + \xi^{2m-1} + \xi^{2m-1} + \xi^{2m-1} + \xi^{2m-1} \right) \cdot \left( \xi^{2m-2t} + \xi^{2m-2t} + 1 \right) + 6 \left( \xi^{2m-1} + \xi^{2m-1} + 1 \right).
\]

From \( 4 \left( (1 + \xi^t)^{2m-1} + (\xi^{2t})^{2m-1} \right) = 4 \left( (1 + \theta^t)^{2m-1} + (\theta^{2t})^{2m-1} \right) = 4 (1 + \theta^t + \theta^{2t})^{2m-1} = 0 \), we obtain

\[
a_0 = 1 + \xi^t + \xi^{2t} + 6 \left( \xi^{2m-1} + \xi^{2m-1} + 1 \right).
\]

Thus we verify \( a_0 = 0 \) from \( 4a_0 = 0 \). We can calculate \( a_1 \) and \( a_2 \).

\[
2a_1 + 4a_2 = (1 + \xi^t + \xi^{2t}) - (1 + \xi^t + \xi^{2t})^{2m},
\]

\[
2a_1 + 4a_2 = 2 \left( \xi^{2m-1} + \xi^{2m-1} + 1 \right),
\]

\[
a_1 + 2a_2 = \gamma^{2m-1} + \gamma^{2m-1} + 1.
\]

From applying the Frobenius automorphism, we have \( (1 + \gamma^t + \gamma^{2t})^{2m-1} = 0 \), that is \( a_1 + 2a_2 = 0 \). Thus we obtain \( a_0 = a_1 = a_2 = 0 \), then

\[
1 + \xi^t + \xi^{2t} = 0.
\]

The codewords is as follows:

\[
\left( \begin{array}{cccccccc}
  c_\infty & c_0 & \ldots & c_t & \ldots & c_{2t} & \ldots \\
  5 & 1 & \ldots & 1 & \ldots & 1 & \ldots 
\end{array} \right)
\]

and the Lee weight of this codeword is 6. It concludes that the minimum Lee weight of \( P_8 \) is 6.

\( \blacksquare \)
We will give some examples of the codewords with the minimum Lee weight 6 to clarify our proof.

Examples of the codewords with the minimum Lee weight of $P_8$

1. We give the example of the codeword with minimum Lee weight which generated by searching the weight of the codewords over $GR(8, m)$ by computer programs.
   - For case $m = 3$, we found the codeword $c = (7, 1, 1, 6, 0, 0, 1, 0)$ has the minimum Lee weight 6 by computer search.
   - For case $m = 4$, we found the codeword $c = (7, 1, 1, 6, 0, 0, 0, 0, 0, 1, 1, 0, 0)$ and $c = (5, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$ have the minimum Lee weight 6 by computer search. By consider Table 1 and Table 2 of Theorem 3, we can see that the first codeword transformed from Case 1 and the second codeword transformed from Case 11.

2. For $m = 3$, it is easy to see $1 + \theta + \theta^5 = 0$ is satisfied where $\theta$ is a root of the primitive polynomial $h_2(X) = X^3 + X^2 + 1$. Next we assign the value of $c$ which satisfies $1 + \gamma + \gamma^5 = 2\gamma^c$, where $\gamma$ is a root of the primitive basic irreducible polynomial $h_2(X) = X^3 - X^2 - 2X - 1$. We obtain $c = 2$. From the equation $1 + \gamma + \gamma^5 = 2\gamma^2$, it is sufficient to determine the sign of the equation $1 + \xi + \xi^5 = \pm 2\xi^2$, where $\xi$ is a root of the primitive basic irreducible polynomial $h_8(X) = X^3 - 5X^2 - 6X - 1$. Thus we obtain the codeword $c = (7, 1, 1, 6, 0, 0, 1, 0)$ of $P_8$ with the minimum Lee weight 6. We do the same scheme for the case $m = 4$ and know the codeword $c = (7, 1, 1, 0, 0, 1, 6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$ has the minimum Lee weight 6.

References

[1] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, "The $\mathbb{Z}_4$- Linearity of Kerdock, Preparata, Goethals, and Related Codes," IEEE Transactions on Information Theory, 40:301-319, 1994.

[2] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger and J. R. Wall. Coding Theory : The Essentials. New York : Marcel Dekker Inc. 1991.

[3] R. Lidl and H. Niederreiter. Introduction to Finite Fields and their Applications. Cambridge : Cambridge University Press. 2000.

[4] J. H. van Lint. Introduction to Coding Theory. New York : Springer-Verlag. 1999.