Advances in Applied Mathematics **25,** 12–33 (2000)
doi:10.1006/aama.2000.0687, available online at http://www.idealibrary.com on IDEAL®

$\mathbb{Z}_8$-Cyclic Codes and Quadratic Residue Codes

Mei Hui Chiu

Department of Mathematics, National Cheng-Kung University, Tainan, Taiwan, Republic of China

Stephen S.-T. Yau

Department of Mathematics, Statistics and Computer Science (M/C 249), University of Illinois at Chicago, 851 South Morgan Street, Chicago, Illinois 60607-7045
E-mail: yau@uic.edu

and

Yung Yu

Department of Mathematics, National Cheng-Kung University, Tainan, Taiwan, Republic of China
E-mail: yungyu@mail.ncku.edu.tw

Received June 27, 1999; accepted March 1, 2000

In memory of Professor Gian-Carlo Rota for his great contributions in combinatorial and discrete geometry

A set of n-tuples over $\mathbb{Z}_8$ is called a code over $\mathbb{Z}_8$ or a $\mathbb{Z}_8$ code if it is a $\mathbb{Z}_8$ module. A particularly interesting family of $\mathbb{Z}_8$-cyclic codes are quadratic residue codes. We define such codes in terms of their idempotent generators and show that these codes also have many good properties which are analogous in many respects to properties of quadratic residue codes over a field. In particular we show that the quadratic residuce codes over $\mathbb{Z}_8$ have large automorphism groups which will be useful in decoding these codes by using the powerful permutation decoding methods described by F. J. MacWilliams and N. J. A. Sloane (1978, "Theory of Error-Correcting Codes," North-Holland, Amsterdam). We also define a distance preserving map from $\mathbb{Z}_8^N$ (Lee distance) to $\mathbb{Z}_2^{4N}$ (Hamming distance). © 2000 Academic Press

0196-8858/00 $35.00

1. INTRODUCTION

Let $\mathbb{Z}_8$ denote the integers modulo 8. $\mathbb{Z}_8$ is a ring which has 2, 4, and 6 as zero divisors. A set of n-tuples over $\mathbb{Z}_8$ is called a code over $\mathbb{Z}_8$ or a $\mathbb{Z}_8$-code if it is a $\mathbb{Z}_8$ module.

It is well known that nonlinear binary codes have excellent error-correcting capabilities. For instance, the Nordstrom–Robinson, Kerdock, Preparata, Goethals, and Delsarte–Goethals nonlinear binary codes contain more codewords than any known linear codes with the same minimum distance. (Recall that the minimum distance for a code C is $\min\{d(u, v) = wt(u - v) : u \neq v \text{ in } C\}$.) In fact many of these nonlinear binary codes satisfy a certain duality property for which a satisfactory explanation is known only in the linear code. These kinds of phenomena had been very mysterious to many experts until a breakthrough was discovered in 1994 by Hammons et al. [HKCSS]. They showed a simple connection between these nonlinear codes and linear codes over $\mathbb{Z}_4$ by means of the Gray map. This generated a lot of work on $\mathbb{Z}_4$-codes, for example, the a fundamental contribution due to Pless and Qian [Pl–Qi, Qi]. It is a natural question to ask what happens for $\mathbb{Z}_8$-cyclic codes.

In this short note, we prove that idempotent generators exist for certain $\mathbb{Z}_{p^m}$-cyclic codes. The uniqueness of idempotent generator of any cyclic code is also proven.

A particularly interesting family of $\mathbb{Z}_8$-cyclic codes is the quadratic residue codes. Quadratic residue codes were first defined by Andrew Gleason. The minimum weights of many modest quadratic codes are quite high for the codes' lengths, making this class of codes promising. We define $\mathbb{Z}_8$ quadratic residue codes in terms of their idempotent generators and show that these codes also have many good properties which are analogous in many respects to properties of quadratic residue codes over a field. In particular we show that quadratic residue codes over $\mathbb{Z}_8$ have large automorphism groups which will be useful in decoding these codes by using the powerful decoding method described in [Ma–Sl]. We also define an isometry from $\mathbb{Z}_8^N$ (Lee distance) to $\mathbb{Z}_2^{4N}$ (Hamming distance).

2. QUADRATIC RESIDUE CODES

Quadratic residue codes are cyclic codes which can be defined in terms of their idempotent generators [Le–Ma–Pl, Pl].

2.0. *Idempotent Generators of Cyclic Codes*

An idempotent in $\mathbb{Z}_{p^m}[x]/(x^n - 1)$, where p is a prime number, is defined to be a polynomial $e(x)$ such that $e(x)^2 \equiv e(x) \pmod{x^n - 1}$. We first recall the following general fact about the existence and uniqueness of idempotent generator.

THEOREM 2.0.1. *Let C be a $\mathbb{Z}_{p^m}$ cyclic code of odd length n. If $C = (f)$, where $fg = x^n - 1$ for some g such that f and g are coprime, then C has an idempotent generator in $\mathbb{Z}_p^m[x]/(x^n - 1)$. Moreover, the idempotent generator of a cyclic code is unique.*

Proof. Because f and g are coprime, there are u and v in $\mathbb{Z}_{p^m}[x]$ such that $fu + gv = 1$. Set $e = fu$. Then $e = 1 - gv$, $e^2 = e \cdot e = e(1 - gv) = e - egv = e - fugv = e \pmod{x^n - 1}$ and $fe = f - fgv = f(\text{mod } x^n - 1)$. Hence $(e) = (f)$.

Suppose e_1 is another idempotent generator of (f); i.e., $(f) = (e_1)$ and $e_1^2 = e_1$. Then $e_1 = \alpha e$ and $e = \beta e_1$ for some $\alpha, \beta \in \mathbb{Z}_{p^m}[x]/(x^n - 1)$. It follows that $e_1 = \alpha e = \alpha e^2 = e_1 e = \beta e_1^2 = \beta e_1 = e$. Q.E.D.

If we know the idempotent generator of a $\mathbb{Z}_{p^m}$ code, by the following theorem we can also find the idempotent generator of the dual code. (Recall that the dual code $C^\perp$ for a code C is $C^\perp = \{u \in V \mid u \cdot w = 0 \text{ for all } w \in C\}$ [Pl, p.8].)

THEOREM 2.0.2. *If a $\mathbb{Z}_{p^m}$ cyclic code C has the idempotent generator $e(x)$, then $C^\perp$ has the idempotent generator $1 - e(x^{-1})$.*

Proof. Since $e(x)[1 - e(x)] = e(x) - e^2(x) = 0$ in R_n, by [Pl, Theorem 47] (which holds over a ring) $e(x)$ is orthogonal to $1 - e(x^{-1})$. That is, $1 - e(x^{-1}) \in C^\perp$.

On the other hand, if C has generator polynomial g and $gh = x^n - 1$, then $C^\perp$ has generator polynomial h^*, where $h^* = x^{\deg h(x)} h(x^{-1})$. Since $e(x)$ is the idempotent generator of $C = (g)$, we have $e(x) = u(x)g(x)$ for some $u(x) \in \mathbb{Z}_8[x]$

$$\begin{aligned}
&\Rightarrow \quad h(x)(1 - e(x)) = h(x)(1 - u(x)g(x)) \\
&\Rightarrow \quad h(x)(1 - e(x)) = h(x) \qquad \text{in } \mathbb{Z}_8[x]/(x^n - 1). \\
&\Rightarrow \quad x^{\deg h} h(x^{-1})[1 - e(x^{-1})] = x^{\deg h} h(x^{-1}) \\
&\Rightarrow \quad h^*[1 - e(x^{-1})] = h^* \qquad \therefore h^* \in (1 - e(x^{-1})).
\end{aligned}$$

Since $1 - e(x^{-1}) \in C^\perp = (h^*)$, we have $C^\perp = (1 - e(x^{-1}))$. Clearly $1 - e(x^{-1})$ is the idempotent generator of $C^\perp$. Q.E.D.

If e_1 and e_2 are $\mathbb{Z}_8$-idempotents, then it is easy to check that $e_1 e_2$ and $e_1 + e_2 - e_1 e_2$ are also $\mathbb{Z}_8$-idempotents. Let $C_1 = (e_1)$ and $C_2 = (e_2)$; then it is simple to verify that $e_1 e_2$ and $e_1 + e_2 - e_1 e_2$ are the multiplicative identities of $C_1 \cap C_2$ and $C_1 + C_2$, respectively. This proves the following theorem:

THEOREM 2.0.3. *Let C_1 and C_2 be cyclic codes with $\mathbb{Z}_8$-idempotent generators e_1 and e_2; then $C_1 \cap C_2$ has the $\mathbb{Z}_8$-idempotent generator e_1e_2 and $C_1 + C_2$ has $\mathbb{Z}_8$-idempotent generator $e_1 + e_2 - e_1e_2$.*

2.1. *Idempotent Generators of QR Codes*

Let $e_1 = \sum_{i \in Q} x^i$ and $e_2 = \sum_{i \in N} x^i$, where Q is the set of quadratic residues and N is the set of non-residues for a prime $p \equiv \pm 1 \pmod 8$. When $p \equiv -1 \pmod 8$, e_1 and e_2 are idempotents of binary $[p, (p+1)/2]$ QR codes. When $p \equiv 1 \pmod 8$, they are idempotents of binary $[p, (p-1)/2]$ QR codes. (cf. [Pl, Theorem 66])

LEMMA 2.1.1. *Let x and y be both in Q or both in N, and let $\alpha \neq 0$ in $\mathbb{Z}_p$. Then the number of pairs x, y such that $x + y = \alpha$ is $(p+1)/8$ if $p \equiv -1$* (mod 8) *and* $(p-1)/8$ *if* $p \equiv 1$ (mod 8).

Proof. From [Di, p. 46] we know that the number of ordered pairs $(X, Y) \in \mathbb{Z}_p^2$ such that $X^2 + Y^2 = \alpha$ is $p + 1$ if -1 is not a square and $p - 1$ if -1 is a square. Now if $p \equiv -1 \pmod 8$, -1 is not a square by [Pl, Theorem 65].

Case A. $x, y \in Q$, $x = X^2$, and $y = Y^2$ for some $X, Y \in \mathbb{Z}_p$.

Case A(1). $\alpha \in Q$. Among these $p + 1$ ordered solution pairs (X, Y) such that $X^2 + Y^2 = \alpha$ eight sets, $(\pm X, \pm Y), (\pm Y, \pm X)$, give the same solution $x + y = \alpha$; four sets, $(\pm X, 0), (0, \pm X)$, are not to be counted as solutions of $x + y = \alpha$, because we want x, y both to be nonzero. The other four sets, $(\pm X, \pm X)$, give the same solution $2x = \alpha$. Here we need the fact that 2 is a quadratic residue iff $p \equiv \pm 1 \pmod 8$. (See [Pl, p. 92].)

Therefore, the total number of different pairs of x, y such that $x + y = \alpha$ is $((p+1) - 8)/8 + 1 = (p+1)/8$.

Case A(2). $\alpha \in N$. Then neither x nor y can be zero and $x \neq y$. In this case, the number of pairs x, y such that $x + y = \alpha$ is again $(p+1)/8$.

Case B. Case B can be reduced to Case A in the following way. Let x, y both be in N, and let γ be in N. There are $x', y' \in Q$ such that $x = \gamma x'$, $y = \gamma y'$. The equation $x + y = \alpha$ is equivalent to the equation $x' + y' = \gamma^{-1}\alpha$.

The proof for the case $p \equiv 1 \pmod 8$ is similar. Q.E.D.

Let the map μ_a be a defined as

$$\mu_a\colon i \to ai \pmod p \text{ for any nonzero } a \in GF(p).$$

It is not hard to show that $\mu_a(fg) = \mu_a(f)\mu_a(g)$ for f and g polynomials in $R_p = \mathbb{Z}_8[x]/(x^p - 1)$.

We know that in the binary case, the all one vector $1 + e_1 + e_2$, denoted by h, is an idempotent in $\mathbb{Z}_2[x]/(x^p - 1)$. In $\mathbb{Z}_8[x]/(x^p - 1)$,

$$h^2 = (1 + e_1 + e_2)h = h + \frac{p-1}{2}h + \frac{p-1}{2}h = h + (p-1)h = ph.$$

Therefore, when $p \equiv 1 \pmod 8$, h is an idempotent in $\mathbb{Z}_8[x]/(x^p - 1)$; when $p \equiv -1 \pmod 8$, $7h$ denoted by $\tilde{h}$ is an idempotent in $\mathbb{Z}_8[x]/(x^p - 1)$.

Note. -1 is a quadratic residue in $GF(p)$ iff $p \equiv 1 \pmod 4$ [Pl, Theorem 65].

In order to prove the next theorem, we first discuss the following results. Suppose $p \equiv -1 \pmod 8$ (i.e., $p + 1 = 8r$).

1. $e_1^2 = (\sum_{i \in Q} x^i)^2 = \sum_{i \in Q} x^{2i} + \sum_{i \neq j,\, i,\, j \in Q} x^{i+j}$.

Since $2 \in Q$ (so $i \in Q \Rightarrow 2i \in Q$), the first part of the above sum is e_1. Since $-1 \notin Q$ [Pl, Theorem 65], we have $-a \notin Q$ whenever $a \in Q$. By Lemma 3.1.1, the second part of the sum is $2[(r-1)e_1 + re_2] = 2re_1 + 2re_2 - 2e_1$. So

$$e_1^2 = e_1 + 2re_1 + 2re_2 - 2e_1 = 2re_1 + 2re_2 - e_1. \tag{2.1}$$

2. $e_2^2 = (\sum_{i \in N} x^i)^2 = \sum_{i \in N} x^{2i} + \sum_{i \neq j,\, i,\, j \in N} x^{i+j}$.

Since $2 \in Q$ (so $i \in N \Rightarrow 2i \in N$), the first part of the above sum is e_2. Since $-1 \notin Q$, we have $-a \notin N$ whenever $a \in N$. By Lemma 2.1.1, the second part of the sum is $2[re_1 + (r-1)e_2] = 2re_1 + 2re_2 - 2e_2$. So

$$e_2^2 = e_2 + 2re_1 + 2re_2 - 2e_2 = 2re_1 + 2re_2 - e_2. \tag{2.2}$$

3. Since $7h = 7(1 + e_1 + e_2)$ is an idempotent in $\mathbb{Z}_8[x]/(x^n - 1)$, then $(7h)^2 = 7h$, i.e.,

$$7 + 7e_1 + 7e_2 = (7 + 7e_1 + 7e_2)^2 = 1 + e_1^2 + e_2^2 + 2e_1 + 2e_2 + 2e_1e_2$$
$$\Rightarrow \qquad 2e_1e_2 = 6 + 7e_1^2 + 7e_2^2 + 5e_1 + 5e_2. \tag{2.3}$$

Suppose $p \equiv 1 \pmod 8$ (i.e., $p - 1 = 8r$).

1. $e_1^2 = (\sum_{i \in Q} x^i)^2 = \sum_{i \in Q} x^{2i} + \sum_{i \neq j,\, i,\, j \in Q} x^{i+j}$.

Since $2 \in Q$ (so $i \in Q \Rightarrow 2i \in Q$), the first part of the above sum is e_1. Since $-1 \in Q$ by [Pl, Theorem 65], we have $-a \in Q$ whenever $a \in Q$. Thus there are $(p-1)/2 = 4r$ 1's in the second part of the sum. By Lemma 2.1.1, the second part of the sum is $2[(r-1)e_1 + re_2] + 4r = 2re_1 + 2re_2 - 2e_1 + 4r$. So

$$e_1^2 = e_1 + 2re_1 + 2re_2 - 2e_1 + 4r = 2re_1 + 2re_2 - e_1 + 4r. \tag{2.4}$$

2. $e_2^2 = (\sum_{i\in N} x^i)^2 = \sum_{i\in N} x^{2i} + \sum_{i\neq j,\, i,\, j\in N} x^{i+j}$.

Since $2 \in Q$ (so $i \in N \Rightarrow 2i \in N$), the first part of the above sum is e_2. Since $-1 \in Q$, so $a \in N \Rightarrow -a \in N$. Thus there are $(p-1)/2 = 4r$ 1's in the second part of the sum. By Lemma 2.1.1, the second part of the sum is $2[re_1 + (r-1)e_2] + 4r = 2re_1 + 2re_2 - 2e_2 + 4r$. So

$$e_2^2 = e_2 + 2re_1 + 2re_2 - 2e_2 + 4r = 2re_1 + 2re_2 - e_2 + 4r. \tag{2.5}$$

3. Since $h = 1 + e_1 + e_2$ is an idempotent in $\mathbb{Z}_8[x]/(x^p - 1)$, then $h^2 = h$, i.e.,

$$\begin{aligned} 1 + e_1 + e_2 &= (1 + e_1 + e_2)^2 = 1 + e_1^2 + e_2^2 + 2e_1 + 2e_2 + 2e_1e_2 \\ \Rightarrow \qquad 2e_1e_2 &= -e_1^2 - e_2^2 - e_1 - e_2 = 7e_1^2 + 7e_2^2 + 7e_1 + 7e_2. \end{aligned} \tag{2.6}$$

THEOREM 2.1.2. *Let p be a prime* $\equiv \pm 1 \pmod 8$.

I. *If* $p + 1 = 8r$,

(a) *If $r = 4k$, then $1 + e_i$ and $7e_i$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, where $i = 1, 2$.*

(b) *If $r = 4k + 1$, then $4 + 2e_i + 5e_j$ and $5 + 3e_i + 6e_j$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, $1 \le i \neq j \le 2$.*

(c) *If $r = 4k + 2$, then $3e_i + 4e_j$ and $1 + 4e_i + 5e_j$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, $1 \le i \neq j \le 2$.*

(d) *If $r = 4k + 3$, then $4 + 2e_i + 6e_j$ and $5 + 2e_i + 7e_j$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, $1 \le i \neq j \le 2$.*

II. *If* $p - 1 = 8r$,

(a) *If $r = 4k$, then $1 + e_i$ and $7e_i$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, where $i = 1, 2$.*

(b) *If $r = 4k + 1$, then $4 + e_i + 6e_j$ and $5 + 2e_i + 7e_j$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, $1 \le i \neq j \le 2$.*

(c) *If $r = 4k + 2$, then $3e_i + 4e_j$ and $1 + 4e_i + 5e_j$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, $1 \le i \neq j \le 2$.*

(d) *If $r = 4k + 3$, then $4 + 2e_i + 5e_j$ and $5 + 3e_i + 6e_j$ are idempotents over $\mathbb{Z}_8[x]/(x^p - 1)$, $1 \le i \neq j \le 2$.*

Proof. In all the following proofs, we shall use (2.1)–(2.6).

I. Suppose $p+1=8r$, $r=4k+1$.

$$\begin{aligned}(4+2e_1+5e_2)^2 &= 4e_1^2+e_2^2+4e_1e_2\\ &= 4e_1^2+e_2^2+2(6+7e_1^2+7e_2^2+5e_1+5e_2)\\ &= 4+2e_1^2+7e_2^2+2e_1+2e_2\\ &= 4+2(2re_1+2re_2-e_1)+7(2re_1+2re_2-e_2)+2e_1+2e_2\\ &= 4+2re_1+2re_2-5e_2\\ &= 4+2e_1+2e_2-5e_2 \qquad (\because r=4k+1)\\ &= 4+2e_1+5e_2.\end{aligned}$$

$$\begin{aligned}(5+3e_1+6e_2)^2 &= 1+e_1^2+4e_2^2+6e_1+4e_2+4e_1e_2\\ &= 1+e_1^2+4e_2^2+6e_1+4e_2+2(6+7e_1^2+e_2^2+5e_1+5e_2)\\ &= 5+7e_1^2+2e_2^2+6e_2\\ &= 5+7(2re_1+2re_2-e_1)+2(2re_1+2re_2-e_2)+6e_2\\ &= 5+2re_1+2re_2+e_1+4e_2\\ &= 5+2e_1+2e_2+e_1+4e_2 \qquad (\because r=4k+1)\\ &= 5+3e_1+6e_2.\end{aligned}$$

The proofs of other cases are similar.

II. Suppose $p-1=8r$, $r=4k+1$

$$\begin{aligned}(4+2e_1+6e_2)^2 &= e_1^2+4e_2^2+4e_1e_2\\ &= e_1^2+4e_2^2+2(7e_1^2+7e_2^2+7e_1+7e_2)\\ &= 7e_1^2+2e_2^2+6e_1+6e_2\\ &= 7(2re_1+2re_2-e_1+4r)\\ &\quad +2(2re_1+2re_2-e_2+4r)+6e_1+6e_2\\ &= 2re_1+2re_2+7e_1+4e_2+4r\\ &= 4+2e_1+2e_2+7e_1+4e_2 \qquad (\because r=4k+1)\\ &= 4+e_1+6e_2.\end{aligned}$$

$$\begin{aligned}(5+2e_1+7e_2)^2 &= 1+4e_1^2+e_2^2+4e_1+6e_2+4e_1e_2\\ &= 1+4e_1^2+e_2^2+4e_1+6e_2+2(7e_1^2+7e_2^2+7e_1+7e_2)\\ &= 1+2e_1^2+7e_2^2+2e_1+4e_2\end{aligned}$$

$$
\begin{aligned}
&= 1 + 2(2re_1 + 2re_2 - e_1 + 4r) \\
&\quad +7(2re_1 + 2re_2 - e_2 + 4r) + 2e_1 + 4e_2 \\
&= 1 + 2re_1 + 2re_2 + 5e_2 + 4r \\
&= 5 + 2e_1 + 2e_2 + 5e_2 \qquad (\because r = 4k + 1) \\
&= 5 + 2e_1 + 7e_2.
\end{aligned}
$$

The proofs of other cases are similar. Q.E.D.

DEFINITION 2.1.3. A $\mathbb{Z}_8$-cyclic code is a $\mathbb{Z}_8$-quadratic residue (QR) code if it is generated by one of the idempotents in above theorem.

Hence μ_a is in the group of any $\mathbb{Z}_8$-QR code for any $a \in Q$.

2.2. *Properties of QR Codes*

THEOREM 2.2.1. *Let p be a prime with $p + 1 = 8r$. If $r = 4k$, let $Q_1 = (7e_1)$, $Q_2 = (7e_2)$ and $Q_1' = (1 + e_2)$, $Q_2' = (1 + e_1)$. If $r = 4k + 1$, let $Q_1 = (4 + 2e_1 + 5e_2)$, $Q_2 = (4 + 5e_1 + 2e_2)$ and $Q_1' = (5 + 3e_1 + 6e_2)$, $Q_2' = (5 + 6e_1 + 3e_2)$. If $r = 4k + 2$, let $Q_1 = (3e_1 + 4e_2)$, $Q_2 = (4e_1 + 3e_2)$ and $Q_1' = (1 + 4e_1 + 5e_2)$, $Q_2' = (1 + 5e_1 + 4e_2)$. If $r = 4k + 3$, let $Q_1 = (4 + e_1 + 6e_2)$, $Q_2 = (4 + 6e_1 + e_2)$ and $Q_1' = (5 + 2e_1 + 7e_2)$, $Q_2' = (5 + 7e_1 + 2e_2)$. Then the following holds for $\mathbb{Z}_8$-*QR *codes Q_1, Q_2, Q_1', and Q_2':*

(a) *Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent*;

(b) *$Q_1 \cap Q_2 = (\tilde{h})$ and $Q_1 + Q_2 = \mathbb{R}_p = \mathbb{Z}_8[x]/(x^p - 1)$, where $\tilde{h} = 7h = 7(1 + e_1 + e_2)$;*

(c) $|Q_1| = 8^{(p+1)/2} = |Q_2|$;

(d) $Q_1 = Q_1' + (\tilde{h})$, $Q_2 = Q_2' + (\tilde{h})$;

(e) $|Q_1'| = 8^{(p-1)/2} = |Q_2'|$;

(f) *Q_1' and Q_2' are self-orthogonal and $Q_1^\perp = Q_1'$ and $Q_2^\perp = Q_2'$.*

Proof. First we prove the case $r = 4k + 1$.

Let x be an element in N; then the map μ_x interchanges e_1 and e_2, i.e., $\mu_x e_1 = e_2$, $\mu_x e_2 = e_1$. Hence $\mu_x(4 + 2e_1 + 5e_2) = (4 + 2e_2 + 5e_1)$ and $\mu_x(5 + 3e_1 + 6e_2) = (5 + 3e_2 + 6e_1)$. This proves (a).

Since $\tilde{h} = 7 + 7e_1 + 7e_2 = 7 + (4 + 2e_1 + 5e_2) + (4 + 5e_1 + 2e_2)$,

$$
\begin{aligned}
(4 + 2e_1 + 5e_2)\tilde{h} &= (4 + 2e_1 + 5e_2)[7 + (4 + 2e_1 + 5e_2) + (4 + 5e_1 + 2e_2)] \\
&= 7(4 + 2e_1 + 5e_2) + (4 + 2e_1 + 5e_2)^2 \\
&\quad +(4 + 2e_1 + 5e_2)(4 + 5e_1 + 2e_2) \\
&= (4 + 2e_1 + 5e_2)(4 + 5e_1 + 2e_2).
\end{aligned}
$$

On the other hand,

$$(4+2e_1+5e_2)\tilde{h} = 4\tilde{h} + 2\cdot\frac{p-1}{2}\tilde{h} + 5\cdot\frac{p-1}{2}\tilde{h} = \left(4+7\cdot\frac{p-1}{2}\right)\tilde{h} = \tilde{h},$$

because $4+7\cdot(p-1)/2 = 4+7\cdot(8r-1-1)/2 = 4r-3 \equiv 1 \pmod 8$. Hence $(4+2e_1+5e_2)(4+5e_1+2e_2) = \tilde{h}$.

By Theorem 2.0.3, $Q_1 \cap Q_2$ has idempotent generator $\tilde{h}$. Therefore

$$|Q_1 \cap Q_2| = |(\tilde{h})| = 8.$$

Also by Theorem 2.0.3, $Q_1 + Q_2$ has idempotent generator

$$\begin{aligned}&(4+2e_1+5e_2) + (4+5e_1+2e_2) - (4+2e_1+5e_2)(4+5e_1+2e_2)\\ &\quad = 7e_1 + 7e_2 - (7+7e_1+7e_2) = 1.\end{aligned}$$

Hence $Q_1 + Q_2 = \mathbb{R}_p$, and $|Q_1 + Q_2| = 8^p$.

Because $|Q_1+Q_2| = |Q_1|\cdot|Q_2|/|Q_1\cap Q_2|$, $|Q_1| = |Q_2| = 8^{(p+1)/2}$. This proves (b) and (c). Observe that $(5+3e_1+6e_2)\tilde{h} = 3h + 5e_1h + 2e_2h = 3h + 5\cdot(p-1)/2\cdot h + 2\cdot(p-1)/2\cdot h = (3+7\cdot(p-1)/2)h = 0$, because $3+7\cdot(p-1)/2 = 3+7\cdot(8r-1-1)/2 = 4r-4 \equiv 0 \pmod 8$. This implies $Q_1' \cap (\tilde{h}) = \{0\}$.

By Theorem 2.0.3, $Q_1' + (\tilde{h})$ has the idempotent generator

$$\begin{aligned}(5+3e_1+6e_2) + \tilde{h} - (5+3e_1+6e_2)\tilde{h} &= 5+3e_1+6e_2\\ &\quad +7+7e_1+7e_2 = 4+2e_1+5e_2.\end{aligned}$$

Hence

$$Q_1' + (\tilde{h}) = (4+2e_1+5e_2) = Q_1.$$

Similarly, $Q_2' + (\tilde{h}) = Q_2$, and $8^{(p+1)/2} = |Q_1| = |Q_1' + (\tilde{h})| = |Q_1'|\cdot|(\tilde{h})| = 8|Q_1'|$. Hence $|Q_1'| = 8^{(p-1)/2}$. This proves (d) and (e).

Finally, by Theorem 2.0.2 and the fact that -1 is not a square, i.e., $-1 \in N$, $Q_1^{\perp}$ has the idempotent generator

$$1 - [4 + 2e_1(x^{-1}) + 5e_2(x^{-1})] = 5 + 6e_1(x^{-1}) + 3e_2(x^{-1}) = 5 + 3e_1 + 6e_2.$$

Hence $Q_1^{\perp} = Q_1'$ and $Q_1' \subseteq Q_1 = Q_1'^{\perp}$, so that Q_1' is self-orthogonal.

Similarly, we can show that $Q_2^{\perp} = Q_2'$ and Q_2' is self-orthogonal.

The proofs of other cases are similar. Q.E.D.

THEOREM 2.2.2. *Let p be a prime with $p-1 = 8r$. If $r = 4k$, let $Q_1 = (1+e_1)$, $Q_2 = (1+e_2)$ and $Q_1' = (7e_2)$, $Q_2' = (7e_1)$. If $r = 4k+1$, let $Q_1 = (5+7e_1+2e_2)$, $Q_2 = (5+2e_1+7e_2)$ and $Q_1' = (4+6e_1+e_2)$, $Q_2' = (4+e_1+6e_2)$. If $r = 4k+2$, let $Q_1 = (1+5e_1+4e_2)$, $Q_2 = (1+4e_1+5e_2)$ and $Q_1' = (4e_1+3e_2)$, $Q_2' = (3e_1+4e_2)$. If $r = 4k+3$, let $Q_1 = (5+6e_1+3e_2)$, $Q_2 = (5+3e_1+6e_2)$ and $Q_1' = (4+5e_1+2e_2)$, $Q_2' = (4+2e_1+5e_2)$.*

Then the following hold for $\mathbb{Z}_8$-QR *codes* Q_1, Q_2, Q_1', *and* Q_2':

(a) Q_1 *and* Q_2 *are equivalent and* Q_1' *and* Q_2' *are equivalent*;

(b) $Q_1 \cap Q_2 = (h)$ *and* $Q_1 + Q_2 = \mathbb{R}_p = \mathbb{Z}_8[x]/(x^p - 1)$;

(c) $|Q_1| = 8^{(p+1)/2} = |Q_2|$;

(d) $Q_1 = Q_1' + (h)$, $Q_2 = Q_2' + (h)$;

(e) $|Q_1'| = 8^{(p-1)/2} = |Q_2'|$;

(f) $Q_1^{\perp} = Q_2'$ *and* $Q_2^{\perp} = Q_1'$.

Proof. First we prove the case $r = 4k + 1$.

(a) Let x be an element in N; then the map μ_x interchanges e_1 and e_2, i.e., $\mu_x e_1 = e_2$, $\mu_x e_2 = e_1$.

Hence $\mu_x(5 + 7e_1 + 2e_2) = (5 + 7e_2 + 2e_1)$ and $\mu_x(4 + 6e_1 + e_2) = (4 + 6e_2 + e_1)$. So Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent.

(b) $h = 1 + e_1 + e_2 = 7 + (5 + 7e_1 + 2e_2) + (5 + 2e_1 + 7e_2)$,

$$\begin{aligned}(5 + 7e_1 + 2e_2)h &= (5 + 7e_1 + 2e_2)[7 + (5 + 7e_1 + 2e_2) + (5 + 2e_1 + 7e_2)] \\ &= 7(5 + 7e_1 + 2e_2) + (5 + 7e_1 + 2e_2)^2 \\ &\quad +(5 + 7e_1 + 2e_2)(5 + 2e_1 + 7e_2) \\ &= (5 + 7e_1 + 2e_2)(5 + 2e_1 + 7e_2).\end{aligned}$$

On the other hand,

$$(5 + 7e_1 + 2e_2)h = 5h + 7 \cdot \frac{p-1}{2} h + 2 \cdot \frac{p-1}{2} h = \left(5 + 1 \cdot \frac{p-1}{2}\right) h = h,$$

because $5 + 1 \cdot (p - 1)/2 = 5 + (8r + 1 - 1)/2 = 5 + 4r \equiv 1 \pmod 8$.

Hence $(5 + 7e_1 + 2e_2)(5 + 2e_1 + 7e_2) = h$. By Theorem 2.0.3, $Q_1 \cap Q_2$ has the idempotent generator h. Therefore $|Q_1 \cap Q_2| = |(h)| = 8$. Also by Theorem 2.0.3, $Q_1 + Q_2$ has the idempotent generator

$$\begin{aligned}&(5 + 7e_1 + 2e_2) + (5 + 2e_1 + 7e_2) - (5 + 7e_1 + 2e_2)(5 + 2e_1 + 7e_2) \\ &\quad = 2 + e_1 + e_2 - (1 + e_1 + e_2) = 1.\end{aligned}$$

Hence $Q_1 + Q_2 = \mathbb{R}_p$, and $|Q_1 + Q_2| = 8^p$.

(c) As $|Q_1 + Q_2| = |Q_1| \cdot |Q_2| / |Q_1 \cap Q_2|$, $|Q_1| = |Q_2| = 8^{(p+1)/2}$.

(d) Observe that $(4 + 6e_1 + e_2)h = 4h + 6e_1 h + e_2 h = 4h + 6 \cdot ((p - 1)/2)h + ((p - 1)/2)h = (4 + 7 \cdot (p - 1)/2)h = 0$, because $4 + 7 \cdot (p - 1)/2 = 4 + 7 \cdot (8r + 1 - 1)/2 = 4 + 7 \cdot 4r \equiv 0 \pmod 8$. This implies $Q_1' \cap (\tilde{h}) = \{0\}$.

By Theorem 2.0.3, $Q_1' + (h)$ has the idempotent generator

$$(4 + 6e_1 + e_2) + h - (4 + 6e_1 + e_2)h = 4 + 6e_1 + e_2$$
$$+1 + e_1 + e_2 = 5 + 7e_1 + 2e_2.$$

Hence $Q_1' + (h) = (5 + 7e_1 + 2e_2) = Q_1$. Similarly, $Q_2' + (h) = Q_2$.

(e) Since $Q_1' + (h) = Q_1$, $8^{(p+1)/2} = |Q_1| = |Q_1' + (h)| = |Q_1'| \cdot |(h)| = 8|Q_1'|$.

Hence $|Q_1'| = 8^{(p-1)/2}$. Similarly, $|Q_2'| = 8^{(p-1)/2}$.

(f) Finally, by Theorem 2.0.2 and the fact that -1 is a square, i.e., $-1 \in Q$, $Q_1^{\perp}$ has the idempotent generator

$$1 - [5 + 7e_1(x^{-1}) + 2e_2(x^{-1})] = 4 + e_1(x^{-1}) + 6e_2(x^{-1}) = 4 + e_1 + 6e_2$$

which is the idempotent generator of Q_2'; this proves that $Q_1^{\perp} = Q_2'$. Similarly, we can show that $Q_2^{\perp} = Q_1'$.

The proofs of other cases are similar. Q.E.D.

Definition 2.2.3. The extended code of a $\mathbb{Z}_8$ code C denoted by $\overline{C}$ is the code obtained by adding an overall parity check to each codeword of C.

Theorem 2.2.4. *Suppose* $p + 1 = 8r$; *let* Q_1, Q_2 *be the* $\mathbb{Z}_8$-QR *codes in Theorem* 2.2.1. *Let* $\overline{Q_1}$ *and* $\overline{Q_2}$ *denote their extended codes. Then* $\overline{Q_1}$ *and* $\overline{Q_2}$ *are self-dual.*

Proof. We first prove the case $r = 4k + 1$. We know that $Q_1 = Q_1' + (\tilde{h})$, and $\overline{Q_1}$ has the $(p + 1)/2 \cdot (p + 1)$ generator matrix

$$\begin{array}{cccccc} \infty & 0 & 1 & 2 & \cdots & p-1 \\ \hline 0 & & & & & \\ 0 & & & & & \\ \vdots & & & G_1' & & \\ \vdots & & & & & \\ 7 & 7 & 7 & 7 & \cdots & 7 \end{array},$$

where each row of G_1' is a cyclic shift of the vector $5 + 3e_1 + 6e_2$. We know that G_1' generates Q_1'. Since Q_1' is self-orthogonal, the rows of G_1' are orthogonal to each other and clearly also orthogonal to $\tilde{h}$. Because the vector $(7, \tilde{h})$ is orthogonal to itself and $|\overline{Q_1}| = |Q_1| = 8^{(p+1)/2}$, by comparing the order of $\overline{Q_1}$ and $\overline{Q_1}^{\perp}$, $\overline{Q_1}$ is self-dual. Similarly, $\overline{Q_2}$ is self-dual.

The proofs of other cases $r = 4k$, $r = 4k + 2$, $r = 4k + 3$ are also similar. Q.E.D.

When $p-1=8r$, we define $\widetilde{Q_1}$ to be the $\mathbb{Z}_8$ code generated by the matrix

$$\begin{array}{c} \begin{array}{cccccc} \infty & 0 & 1 & 2 & \cdots & p-1 \end{array} \\ \left[\begin{array}{cccccc} 0 & & & & & \\ 0 & & & & & \\ \vdots & & & G_1' & & \\ \vdots & & & & & \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{array}\right] \end{array},$$

where each row of G_1' is a cyclic shift of $4+6e_1+e_2$ when $r=4k+1$, a cyclic shift of $7e_2$ when $r=4k$, a cyclic shift of $4e_1+3e_2$ when $r=4k+2$, and a cyclic shift of $4+5e_1+2e_2$ when $r=4k+3$. We define $\widetilde{Q_2}$ similarly. Notice that these are not the extended codes of Q_1 and Q_2 because the sum of the components of the all one vector is not 0 (mod 8).

THEOREM 2.2.5. *Suppose $p-1=8r$; let Q_1, Q_2 be the $\mathbb{Z}_8$-*QR *codes in Theorem* 2.2.2. *Let $\overline{Q_1}$ and $\overline{Q_2}$ denote their extended codes. Then the dual of $\overline{Q_1}$ is $\widetilde{Q_2}$ and the dual of $\overline{Q_2}$ is $\widetilde{Q_1}$.*

Proof. We prove the case with $r=4k+1$ only. In this case $\overline{Q_1}$ has the $(p+1)/2 \cdot (p+1)$ generator matrix

$$\begin{array}{c} \begin{array}{cccccc} \infty & 0 & 1 & 2 & \cdots & p-1 \end{array} \\ \left[\begin{array}{cccccc} 0 & & & & & \\ 0 & & & & & \\ \vdots & & & G_1' & & \\ \vdots & & & & & \\ 7 & 1 & 1 & 1 & \cdots & 1 \end{array}\right] \end{array},$$

where each row of G_1' is a cyclic shift of the vector $4+6e_1+e_2$. Since G_1' generates Q_1' and $Q_2^{\perp}=Q_1'$ by Theorem 2.2.2, any row in the above matrix is orthogonal to any row in the matrix which defines $\widetilde{Q_2}$. By comparing the order of dual of $\overline{Q_1}$ with the order of $\widetilde{Q_2}$, we know the dual of $\overline{Q_1}$ is $\widetilde{Q_2}$. Q.E.D.

Remark. For both $p \equiv 1 \pmod 8$ and $p \equiv -1 \pmod 8$, the extended codes $\overline{Q_1}$ and $\overline{Q_2}$ are equivalent because Q_1 and Q_2 are equivalent. They are also equivalent to $\overline{Q_1}^{\perp}$ and $\overline{Q_2}^{\perp}$. Due to this property, the group of the extended codes we mention in the Theorem 2.3.2 will be the group of either one of the extended codes.

2.3. *Automorphism Group of the Extended QR Codes*

Let χ be the Legendre symbol on the field $GF(p)$ which is defined as $\chi(0) = 0$, $\chi(i) = 1$ if i is a quadratic residue and $\chi(i) = -1$ if i is a nonresidue.

We use the following theorem extensively.

THEOREM 2.3.1. [*Pe*]. (i) *Suppose* $p = -1 + 8r$, *and* a *is a number prime to* p. *Then in the set* $\{q + a,\ \text{where } q \in Q \cup \{0\}\}$, *there are* $2r$ *elements in* $Q \cup \{0\}$ *and* $2r$ *elements in* N. *In the set* $\{n + a,\ \text{where } n \in N\}$, *there are* $2r$ *elements in* $Q \cup \{0\}$ *and* $2r - 1$ *elements in* N.

(ii) *Suppose* $p = 1 + 8r$, *and* a *is a number prime to* p. *Then in the set* $\{q + a,\ \text{where } q \in Q \cup \{0\}\}$, *if* $a \in Q$, *there are* $2r + 1$ *elements in* $Q \cup \{0\}$ *and* $2r$ *elements in* N, *and if* $a \in N$, *there are* $2r$ *elements in* Q *and* $2r + 1$ *elements in* N. *In the set* $\{n + a,\ \text{where } n \in N\}$, *if* $a \in Q$, *there are* $2r$ *elements in* Q *and* $2r$ *elements in* N, *and, if* $a \in N$, *there are* $2r + 1$ *elements in* $Q \cup \{0\}$ *and* $2r - 1$ *elements in* N.

THEOREM 2.3.2. *Let* G *be the group generated by the following elements*:

$$\sigma: i \to i + 1 \pmod p), \quad \infty \to \infty,$$

$$\mu_a: i \to ai \ (\mathrm{mod}\ p), \qquad \text{for } a \in Q, \infty \to \infty,$$

$$\rho: i \to -\frac{1}{i} \ (\mathrm{mod}\ p), \qquad \text{followed by multiplication by} - \chi(i).$$

I. *When* $p + 1 = 8r$,

$r = 4k$ and $r = 4k + 2$,

$\infty \to 0$ followed by multiplication by -1,

$0 \to \infty$ followed by multiplication by 1;

$r = 4k + 1$,

$\infty \to 0$ followed by multiplication by -3,

$0 \to \infty$ followed by multiplication by 3;

$r = 4k + 3$,

$\infty \to 0$ followed by multiplication by -5,

$0 \to \infty$ followed by multiplication by 5.

II. *When* $p - 1 = 8r$,

$r = 4k$ and $r = 4k + 2$,

$\infty \to 0$ followed by multiplication by 1,

$$\begin{array}{rl} 0 \to \infty & \text{followed by multiplication by } 1; \\ r = 4k+1, & \\ \infty \to 0 & \text{followed by multiplication by } 5, \\ 0 \to \infty & \text{followed by multiplication by } 5; \\ r = 4k+3, & \\ \infty \to 0 & \text{followed by multiplication by } 3, \\ 0 \to \infty & \text{followed by multiplication by } 3. \end{array}$$

Then G is contained in the group of the extended QR *code.*

When $p \equiv -1 \pmod 8$, $G/(\pm I) \simeq PSL_2(p)$; when $p \equiv 1 \pmod 8$, $G \simeq PSL_2(p)$.

Proof. (I) We suppose that $p+1 = 8r$ and $r = 4k+2$. It is obvious that the extended code is fixed by the map σ. The extended code is fixed by μ_a for $a \in Q$ because μ_a does not change the ∞ position and it fixes the QR codes. We use the method in [Ma–Sl, p. 492] to show that the extended code is also fixed by the map ρ. The extended code is generated by $(p+1)/2$ rows of the $(p+1) \cdot (p+1)$ matrix

$$\begin{array}{c|ccccc|} r_0 & 0 & & & & \\ \cdot & 0 & & & & \\ \vdots & \vdots & & G_1' & & \\ r_s & \vdots & & & & \\ \vdots & \vdots & & & & \\ r_\infty & 7 & 7 & 7 & \cdots & 7 \end{array},$$

where each row of G_1' is a cyclic shift of $1 + 4e_1 + 5e_2$.

1. Since $p = 8r - 1 = 4(8k+3) + 3$, -1 is a nonresidue mod p (see [Ma–Sl, p. 46]).

Hence ρ sends Q to N and vice versa. In particular

$$r_0 = (0, 1 + 4e_1 + 5e_2) \qquad \Rightarrow \qquad \rho(r_0) = (1, 4e_2 + 5e_1) = 7r_0 + h,$$

where h is all one vector of length $p+1$; i.e., $h = (1, 1 + e_1 + e_2)$.

2. For $s \in Q$, we have $-1/s \in N$. In all the following proofs $q \in Q$ and $n \in N$.

$$r_s = (0, x^s + 4\sum x^{q+s} + 5\sum x^{n+s}).$$
$$r_{-1/s} = (0, x^{-1/s} + 4\sum x^{q-1/s} + 5\sum x^{n-1/s}).$$

Hence $\rho(r_s) = \big(5, 7x^{-1/s} + 4\sum_{q+s\in Q} x^{-1/(q+s)} + 4\sum_{q+s\in N} x^{-1/(q+s)} + 3\sum_{n+s\in Q} x^{-1/(n+s)} + 5\sum_{n+s\in N} x^{-1/(n+s)}\big)$ because the set $\{n+s\}$ has the element 0; therefore in the ∞ position of $\rho(r_s)$ it is 5.
We claim that $\rho(r_s) = 7r_{-1/s} + 7r_0 + 5h$. By Theorem 2.3.1, the set $\{q+s\}$ has $2r-1$ elements in Q, $2r$ elements in N. Since $-1 \in N$, then the set $\{-1/(q+s)\}$ has $2r-1$ elements in N, and $2r$ elements in Q.

Similarly,

the set $\{-1/(n+s), n+s \neq 0\}$ has $2r-1$ elements in N and $2r-1$ elements in Q;

the set $\{q-1/s\}$ has $2r-1$ elements in N and $2r-1$ elements in Q, and one element is 0;

the set $\{n-1/s\}$ has $2r-1$ elements in N and $2r$ elements in Q.

In the nonresidue position of $\rho(r_s) + r_{-1/s}$ it is

$$7x^{-1/s} + 4\sum_{q+s\in Q} x^{-1/(q+s)} + 3\sum_{n+s\in Q} x^{-1/(n+s)} + x^{-1/s}$$
$$+4\sum_{q-\frac{1}{s}\in N} x^{q-1/s} + 5\sum_{n-\frac{1}{s}\in N} x^{n-1/s}.$$

Since for any $-1/(q+s) \in N$, there is a $q' \in Q$ such that $-1/(q+s) = q' - 1/s$ and for any $-1/(n+s) \in N$, there is an $n' \in N$ such that $-1/(n+s) = n' - 1/s$, the sum of above is 0.

In the residue position of $\rho(r_s) + r_{-1/s}$ it is

$$4\sum_{q+s\in N} x^{-1/(q+s)} + 5\sum_{n+s\in N} x^{-1/(n+s)} + 5\sum_{n-1/s\in Q} x^{n-1/s} + 4\sum_{q-1/s\in Q} x^{q-1/s}.$$

Since for any $-1/(q+s) \in Q$, there is an $n \in N$ such that $-1/(q+s) = n - 1/s$ and for any $-1/(n+s) \in Q$, there is an $q \in Q$ such that $-1/(n+s) = q - 1/s$, there are $2r + 2r - 1 = 4r - 1$ terms appearing, so the sum of above is e_1.

Since the set $\{q - 1/s\}$ has the element 0, therefore

$$\rho(r_s) + r_{-1/s} = (5, 4 + e_1) = 7r_0 + 5h;$$

i.e., $\rho(r_s) = 7r_{-1/s} + 7r_0 + 5h$, for $s \in Q$.

3. For any $s \in N$, $r_s = (0, x^s + 4\sum x^{q+s} + 5\sum x^{n+s})$. $r_{-\frac{1}{s}} = (0, x^{-1/s} + 4\sum x^{q-1/s} + 5\sum x^{n-1/s})$.

Hence $\rho(r_s) = \big(4, x^{-1/s} + 4\sum_{q+s\in N} x^{-1/(q+s)} + 4\sum_{q+s\in Q} x^{-1/(q+s)} + 5\sum_{n+s\in N} x^{-1/(n+s)} + 3\sum_{n+s\in Q} x^{-1/(n+s)}\big)$ because the set $\{q+s\}$ has the element 0; therefore in the ∞ position of $\rho(r_s)$ it is 4.
We claim that $\rho(r_s) = r_{-1/s} + 7r_0 + 4h$. By Theorem 2.3.1 and $-1 \in N$, $\{-1/(q+s), q+s \neq 0\}$ has $2r-1$ elements in Q and $2r-1$ elements in N.

Similarly,

the set $\{\frac{-1}{n+s}\}$ has $2r-1$ elements in Q and $2r$ elements in N;

the set $\{q-\frac{1}{s}\}$ has $2r-1$ elements in Q and $2r$ elements in N;

the set $\{n-\frac{1}{s}\}$ has $2r-1$ elements in Q and $2r-1$ elements in N, and one element is 0.

In the residue position of $\rho(r_s)+7r_{-1/s}$ it is

$$x^{-1/s}+4\sum_{q+s\in N}x^{-1/(q+s)}+5\sum_{n+s\in N}x^{-1/(n+s)}+7x^{-1/s}$$
$$+4\sum_{q-1/s\in Q}x^{q-1/s}+3\sum_{n-1/s\in Q}x^{n-1/s}.$$

Since for any $-1/(q+s)\in Q$, there is a $q'\in Q$ such that $-1/(q+s)=q'-1/s$ and for any $-1/(n+s)\in Q$, there is an $n'\in N$ such that $-1/(n+s)=n'-1/s$, the sum of the above is 0.
In the nonresidue position of $\rho(r_s)+7r_{-1/s}$ it is

$$4\sum_{q+s\in Q}x^{-1/(q+s)}+3\sum_{n+s\in Q}x^{-1/(n+s)}+3\sum_{n-1/s\in N}x^{n-1/s}+4\sum_{q-1/s\in N}x^{q-1/s}.$$

Since for any $-1/(q+s)\in N$, there is an $n\in N$ such that $-1/(q+s)=n-1/s$ and for any $-1/(n+s)\in N$, there is a $q\in Q$ such that $-1/(n+s)=q-1/s$, the terms of the above are $2r+2r-1=4r-1$, so the sum is $7e_2$.
Since the set $\{n-1/s\}$ has the element 0, therefore

$$\rho(r_s)+7r_{-1/s}=(4,3+7e_2)=7r_0+4h;$$

i.e., $\rho(r_s)=r_{-1/s}+7r_0+4h$, for $s\in N$.

4. Since

$$r_\infty=(7,7+7e_1+7e_2)\qquad\Rightarrow\qquad\rho(r_\infty)=(7,1+7e_1+e_2)=2r_0+7h,$$

by similar proofs, we also get the following results:
When $r=4k$,

$$r_0=(0,1+e_2)\quad\rho(r_0)=7r_0+h\quad\rho(r_s)=7r_{-1/s}+7r_0+h,\quad s\in Q$$
$$\rho(r_s)=r_{-1/s}+7r_0,\quad s\in N\quad\rho(r_\infty)=2r_0+7h.$$

When $r=4k+1$,

$$r_0=(0,5+3e_1+6e_2)\quad\rho(r_0)=5r_0+7h$$
$$\rho(r_s)=7r_{-1/s}+5r_0+2h,\quad s\in Q$$
$$\rho(r_s)=r_{-1/s}+5r_0+h\quad s\in N\quad\rho(r_\infty)=6r_0+5h.$$

When $r = 4k + 3$,

$$\begin{aligned} &r_0 = (0, 5 + 2e_1 + 7e_2) \quad \rho(r_0) = 3r_0 + h \\ &\rho(r_s) = 7r_{-1/s} + 3r_0 + 3h, \quad s \in Q \\ &\rho(r_s) = r_{-1/s} + 3r_0 + 2h, \quad s \in N \quad \rho(r_\infty) = 2r_0 + 3h. \end{aligned}$$

(II) Suppose $p - 1 = 8r$ and $r = 4k + 2$. The extended code is generated by $(p+1)/2$ rows of the $(p+1) \cdot (p+1)$ matrix

$$\begin{array}{c} r_0 \\ \cdot \\ \vdots \\ r_s \\ \vdots \\ r_\infty \end{array} \begin{bmatrix} 0 & & & & \\ 0 & & & & \\ \vdots & & G_1' & & \\ \vdots & & & & \\ \vdots & & & & \\ 7 & 1 & 1 & \cdots & 1 \end{bmatrix},$$

where each row of G_1' is a cyclic shift of $4e_1 + 3e_2$.

1. $r_0 = (0, 4e_1 + 3e_2) \Rightarrow \rho(r_0) = (0, 4e_1 + 3e_2) = r_0$.
2. For $s \in Q$ (in all the following proofs $q \in Q$ and $n \in N$),

$$r_s = (0, 4\sum x^{q+s} + 3\sum x^{n+s}).$$

$$r_{-1/s} = (0, 4\sum x^{q-1/s} + 3\sum x^{n-1/s}).$$

Hence $\rho(r_s) = \left(4, 4\sum_{q+s\in Q} x^{-1/(q+s)} + 4\sum_{q+s\in N} x^{-1/(q+s)} + 5\sum_{n+s\in Q} x^{-1/(n+s)} + 3\sum_{n+s\in N} x^{-1/(n+s)}\right)$ because the set $\{q+s\}$ has the element 0; therefore in the ∞ position of $\rho(r_s)$ it is 4.

We claim that $\rho(r_s) = 7r_{-1/s} + r_0 + 4r_\infty$. By Theorem 2.3.1, the set $\{q + s, q + s \neq 0\}$ has $2r - 1$ elements in Q and $2r$ elements in N. Since $-1 \in Q$, then the set $\{-1/(q+s)\}$ has $2r - 1$ elements in Q and $2r$ elements in N. Similarly,

the set $\{-1/(n+s)\}$ has $2r$ elements in Q and $2r$ elements in N;

the set $\{q - 1/s\}$ has $2r - 1$ elements in Q and $2r$ elements in N, and one element is 0;

the set $\{n - 1/s\}$ has $2r$ elements in Q and $2r$ elements in N.

In the residue position of $\rho(r_s) + r_{-1/s}$ it is

$$4\sum_{q+s\in Q} x^{-1/(q+s)} + 5\sum_{n+s\in Q} x^{-1/(n+s)} + 4\sum_{q-1/s\in Q} x^{q-1/s} + 3\sum_{n-1/s\in Q} x^{n-1/s}.$$

Since for any $-1/(q+s) \in Q$, there is a $q' \in Q$ such that $-1/(q+s) = q' - 1/s$ and for any $-1/(n+s) \in Q$, there is an $n' \in N$ such that $-1/(n+s) = n' - 1/s$, the sum of above is 0.

In the nonresidue position of $\rho(r_s) + r_{-1/s}$ it is

$$4 \sum_{q+s \in N} x^{-1/(q+s)} + 3 \sum_{n+s \in N} x^{-1/(n+s)} + 3 \sum_{n-1/s \in N} x^{n-1/s} + 4 \sum_{q-1/s \in N} x^{q-1/s}.$$

Since for any $-1/(q+s) \in N$, there is an $n \in N$ such that $-1/(q+s) = n - 1/s$, for any $-1/(n+s) \in N$, there is an $q \in Q$ such that $-1/(n+s) = q - 1/s$, and there are $2r + 2r = 4r$ terms appearing, the sum of above is $7e_2$.

Since the set $\{q - 1/s\}$ has the element 0, therefore

$$\rho(r_s) + r_{-1/s} = (4, 4 + 7e_2) = r_0 + 4r_\infty;$$

i.e., $\rho(r_s) = 7r_{-1/s} + r_0 + 4_\infty, \quad$ for $s \in Q$.

3. For any $s \in N$,

$$r_s = (0, 4\sum x^{q+s} + 3\sum x^{n+s}) \qquad r_{-1/s} = (0, 4\sum x^{q-1/s} + 3\sum x^{n-1/s}).$$

Hence $\rho(r_s) = \big(3, 4\sum_{q+s\in Q} x^{-1/(q+s)} + 4\sum_{q+s\in N} x^{-1/(q+s)} + 5\sum_{n+s\in Q} x^{-1/(n+s)} + 3\sum_{n+s\in N} x^{-1/(n+s)}\big)$ because the set $\{n + s\}$ has the element 0; therefore in the ∞ position of $\rho(r_s)$ it is 3.

We claim that $\rho(r_s) = r_{-1/s} + r_0 + 5r_\infty$. By Theorem 2.3.1 and $-1 \in Q$, $\{-1/(q+s)\}$ has $2r$ elements in Q and $2r$ elements in N. Similarly,

the set $\{-1/(n+s), n+s \neq 0\}$ has $2r$ elements in Q and $2r - 1$ elements in N;

the set $\{q - 1/s\}$ has $2r$ elements in Q and $2r$ elements in N;

the set $\{n - 1/s\}$ has $2r$ elements in Q and $2r - 1$ elements in N, and one element is 0.

In the nonresidue position of $\rho(r_s) + 7r_{-1/s}$ it is

$$4 \sum_{q+s \in N} x^{-1/(q+s)} + 3 \sum_{n+s \in N} x^{-1/(n+s)} + 4 \sum_{q-1/s \in N} x^{q-1/s} + 5 \sum_{n-1/s \in N} x^{n-1/s}.$$

Since for any $-1/(q+s) \in N$, there is a $q' \in Q$ such that $-1/(q+s) = q' - 1/s$ and for any $-1/(n+s) \in N$, there is an $n' \in N$ such that $-1/(n+s) = n' - 1/s$, the sum of above is 0.

In the residue position of $\rho(r_s) + 7r_{-1/s}$ it is

$$4 \sum_{q+s \in Q} x^{-1/(q+s)} + 5 \sum_{n+s \in Q} x^{-1/(n+s)} + 5 \sum_{n-1/s \in Q} x^{n-1/s} + 4 \sum_{q-1/s \in Q} x^{q-1/s}.$$

Since for any $-1/(q+s) \in Q$, there is an $n \in N$ such that $-1/(q+s) = n - 1/s$ and for any $-1/(n+s) \in Q$, there is a $q \in Q$ such that $-1/(n+s) = q - 1/s$, the terms of the above $2r + 2r = 4r$ appearing, so the sum is e_1. Since the set $\{n - 1/s\}$ has the element 0, therefore

$$\rho(r_s) + 7r_{-1/s} = (3, 5 + e_1) = r_0 + 5r_\infty;$$

i.e., $\rho(r_s) = r_{-1/s} + r_0 + 5r_\infty$, for $s \in N$.

4. Since

$$r_\infty = (7, 1 + e_1 + e_2) \qquad \Rightarrow \qquad \rho(r_\infty) = (1, 7 + 7e_1 + e_2) = 6r_0 + 7r_\infty,$$

by similar proofs, we also get the following results:

When $r = 4k$,

$$r_0 = (0, 7e_2) \quad \rho(r_0) = r_0 \quad \rho(r_s) = 7r_{-1/s} + r_0, \quad s \in Q$$
$$\rho(r_s) = r_{-1/s} + r_0 + r_\infty, \quad s \in N \quad \rho(r_\infty) = 6r_0 + 7r_\infty.$$

When $r = 4k + 1$,

$$r_0 = (0, 4 + 6e_1 + e_2) \quad \rho(r_0) = 5r_0 + 4r_\infty$$
$$\rho(r_s) = 7r_{-1/s} + 5r_0 + 2r_\infty, \quad s \in Q$$
$$\rho(r_s) = r_{-1/s} + 5r_0 + 3r_\infty, \quad s \in N \quad \rho(r_\infty) = 6r_0 + 3r_\infty.$$

When $r = 4k + 3$,

$$r_0 = (0, 4 + 5e_1 + 2e_2) \quad \rho(r_0) = 3r_0 + 4r_\infty$$
$$\rho(r_s) = 7r_{-1/s} + 3r_0 + r_\infty, \quad s \in Q$$
$$\rho(r_s) = r_{-1/s} + 3r_0 + 2r_\infty, \quad s \in N \quad \rho(r_\infty) = 2r_0 + 5r_\infty.$$

Q.E.D.

We call a vector in a $\mathbb{Z}_8$-code "even-like" if the sum of its coordinates is 0 (mod 8); otherwise, we call it "odd-like." The following theorem is an immediate result of the fact that the group G appearing in the above theorem is transitive; hence all codes obtained from an extended $\mathbb{Z}_8$-QR code by puncturing must be equivalent. (Recall that the code we obtain by removing a column of a generator matrix of C is called a punctured C [Pl, p. 33].)

COROLLARY 2.3.3. *The minimum* (*Hamming*) *weight vectors of a* $\mathbb{Z}_8$-QR $(p, (p+1)/2)$ *code are odd-like.*

Proof. Suppose that a QR code Q has even-like minimum weight vector x of minimum weight d. Consider the extended QR code $\overline{Q}$, the vector $\overline{x}$ with the same component in x, and 0 at its ∞. Since x is even-like, therefore, $wt(\overline{x}) = wt(x) = d$.

Puncture $\overline{Q}$ on a coordinate position where $\overline{x}$ has a nonzero coordinate. Call the punctured code Q^*, so Q^* is equivalent to Q. But Q^* has vector in it of weight less than d (since the punctured x). This is a contradiction that Q^* and Q has the same minimum weight. So that x is odd-like. Q.E.D.

DEFINITION. The Lee weights of the elements count 1, 7 as 1; 2, 6 as 2; 3, 5 as 3; 4 as 4; and 0 as 0. The Lee weight of a vector is the sum of the Lee weight of its components.

DEFINITION. The Euclidean weights of the elements count 1, 7 as 1; 2, 6 as 4; 3, 5 as 9; 4 as 16; and 0 as 0. The Euclidean weight of a vector is the sum of the Euclidean weight of its components.

By direct computation using a computer, we have

THEOREM 2.3.4. *The* $\mathbb{Z}_8$-QR *code of length* 7 *has minimum Lee weight* 5, *minimum Euclidean weight* 7, *and minimum Hamming weight* 3.

We define maps α and β_i $(i = 1, \ldots, 4)$ from $\mathbb{Z}_8^N$ to $\mathbb{Z}_2^N$ by

c	$\alpha(c)$	$\beta_1(c)$	$\beta_2(c)$	$\beta_3(c)$	$\beta_4(c)$
0	0	0	0	0	0
1	1	0	0	0	1
2	0	0	0	1	1
3	1	0	1	1	1
4	0	1	1	1	1
5	1	1	1	1	0
6	0	1	1	0	0
7	1	1	0	0	0

Then the Gray map $\phi: \mathbb{Z}_8^N \to \mathbb{Z}_2^{4N}$ is given by $\phi(c) = (\beta_1(c), \beta_2(c), \beta_3(c), \beta_4(c))$.

Note that $\alpha(c) + \beta_1(c) + \beta_2(c) + \beta_3(c) + \beta_4(c) = 0$ for all $c \in \mathbb{Z}_8$.

Observe that ϕ is a distance-preserving map or isometry from $\mathbb{Z}_8^N$ (Lee distance) to $\mathbb{Z}_2^{4N}$ (Hamming distance).

The weight distribution of the image of the length 7 $\mathbb{Z}_8$-QR code under the Gray map is as follows.

i	A_i
0,28	1
5,6,22,23	14
7,21	44
8,10,18,20	140
9,19	154
11,17	350
12,16	595
13,15	462
14	268

The following is the symmetrized Lee weight enumerator of the $\mathbb{Z}_8$-QR code of length 7 (the powers of w_0, w_1, w_2, w_3, and w_4 are numbers of 0, 1 or 7, 2 or 6, 3 or 5 and 4 components, respectively):

$$\begin{aligned}
& w_0^7 + 7w_0^4w_4^3 + 14w_0^3w_1^3w_2 + 14w_0^3w_1^3w_3 + 42w_0^3w_1^2w_2w_3 + 42w_0^3w_1w_2w_3^2 \\
&\quad + 14w_0^3w_1w_3^3 + 14w_0^3w_2^4 + 56w_0^3w_2^3w_4 + 14w_0^3w_2w_3^3 + 7w_0^3w_4^4 \\
&\quad + 84w_0^2w_1^3w_2w_3 + 42w_0^2w_1^3w_2w_4 + 42w_0^2w_1^3w_3w_4 + 126w_0^2w_1^2w_2w_3w_4 \\
&\quad + 84w_0^2w_1w_2w_3^3 + 126w_0^2w_1w_2w_3^2w_4 + 42w_0^2w_1w_3^3w_4 + 42w_0^2w_2^4w_4 \\
&\quad + 42w_0^2w_2w_3^3w_4 + 42w_0w_1^4w_2^2 + 56w_0w_1^3w_2^3 + 168w_0w_1^3w_2w_3w_4 \\
&\quad + 42w_0w_1^3w_2w_4^2 + 42w_0w_1^3w_3w_4^2 + 168w_0w_1^2w_2^3w_3 + 252w_0w_1^2w_2^2w_3^2 \\
&\quad + 126w_0w_1^2w_2w_3w_4^2 + 168w_0w_1w_2^3w_3^2 + 168w_0w_1w_2w_3^3w_4 \\
&\quad + 126w_0w_1w_2w_3^2w_4^2 + 42w_0w_1w_3^3w_4^2 + 42w_0w_2^4w_4^2 + 56w_0w_2^3w_3^3 \\
&\quad + 56w_0w_2^3w_4^3 + 42w_0w_2^2w_3^4 + 42w_0w_2w_3^3w_4^2 \\
&\quad + 2w_1^7 + 14w_1^6w_3 + 42w_1^5w_3^2 \\
&\quad + 28w_1^4w_2^3 + 42w_1^4w_2^2w_4 + 70w_1^4w_3^3 + 56w_1^3w_2^3w_4 + 84w_1^3w_2w_3w_4^2 \\
&\quad + 14w_1^3w_2w_4^3 + 70w_1^3w_3^4 + 14w_1^3w_3w_4^3 + 168w_1^2w_2^3w_3^2 + 168w_1^2w_2^3w_3w_4 \\
&\quad + 252w_1^2w_2^2w_3^2w_4 + 42w_1^2w_2w_3w_4^3 + 42w_1^2w_3^5 + 168w_1w_2^3w_3^2w_4 \\
&\quad + 84w_1w_2w_3^3w_4^2 + 42w_1w_2w_3^2w_4^3 + 14w_1w_3^6 + 14w_1w_3^3w_4^3 + 16w_2^7 \\
&\quad + 14w_2^4w_4^3 + 28w_2^3w_3^4 + 56w_2^3w_3^3w_4 \\
&\quad + 42w_2^2w_3^4w_4 + 14w_2w_3^3w_4^3 + 2w_3^7 + w_4^7.
\end{aligned}$$

REFERENCES

[Ca–Sl] A. R. Calderbank and N. J. A. Sloane, Modular and p-adic cyclic codes, *Des. Codes Cryptogr.* **6** (1995), 21–35.

[Co] S. R. Costa et al. The symmetry group of $\mathbb{Z}_p^n$ in the lee space and the $\mathbb{Z}_{p^n}$-linear codes, *Lecture Notes in Computer Sci.* **1225** (1997), 66–77.

[Di] L. E. Dickson, “Linear Groups,” Dover, New York, 1958.

[HKCSS] 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 Trans. Inform. Theory* **40** (1994), 301–319.

[Hu] T. W. Hungerford, “Algebra,” Springer-Verlag, New York, 1974.

[Ka–Lp] P. Kanwar and S. López-Permouth, Cyclic codes over the integers modulo p^m, *Finite Fields Appl.* **3** (1997), 334–352.

[Le–Ma–Pl] J. S. Leon, J. M. Masley, and V. Pless, Duadic codes, *IEEE Trans. Inform. Theory* **30** (1994), 709–714.

[Ma–Sl] F. J. MacWilliams and N. J. A. Sloane, “Theory of Error-Correcting Codes,” North-Holland, Amsterdam, 1978.

[Mc] B. R. McDonald, “Finite Rings With Identity,” Dekker, New York, 1974.

[Pe] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, *Math. Z.* **56** (1952), 122–130.

[Pl] V. Pless, “Introduction to the Theory of Error-Correcting Codes,” 2nd ed., Wiley–Interscience, New York, 1989.

[Pl-Qi] V. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **42**, No. 5 (1996), 1594–1600.

[Qi] Z. Qian, “Cyclic Codes over $\mathbb{Z}_4$,” Ph.D. dissertation, Univ. of Illinois at Chicago, 1996.

[Ra-Si] B. Sundar Rajan and M. U. Siddiqi, Transform domain characterization of cyclic codes over $\mathbb{Z}_m$, *J. AAECC* **5** (1994), 261–275.