ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 6, 2009

AUTOMORPHISM GROUPS OF THE EXTENDED QUADRATIC RESIDUE CODES OVER $\mathbf{Z}_{16}$ and $\mathbf{Z}_{32}$

CHUNG-LIN HSU, WEI LIANG KUO, STEPHEN S.-T. YAU AND YUNG YU

Dedicated to Professor Hirzebruch on the occasion of his 80th birthday.

1. Introduction. Let $\mathbf{Z}_{16}$ denote the integers modulo 16. $\mathbf{Z}_{16}$ is a ring which has $2, 4, 6, 8, 10, 12, 14$ as zero divisors. A set of n-tuples over $\mathbf{Z}_{16}$ is called a code over $\mathbf{Z}_{16}$ or a $\mathbf{Z}_{16}$-code if it is a $\mathbf{Z}_{16}$-module. Similarly one can define a $\mathbf{Z}_{32}$-code.

Linear codes are easy to understand, to encode and decode. However, in order to get the largest possible number of codewords with a fixed block size and correction capability, it is sometimes necessary to consider nonlinear codes. Some of the best known examples of nonlinear binary error-correcting codes that are better than any corresponding linear code are the Nordstrom-Robinson, Kerdock, and Preparata codes. In fact, some of these nonlinear binary codes satisfy a certain formal duality property for which a satisfactory explanation is known only in the linear code. In 1994, Hammons, Kumar, Calderbank, Sloane, and Solé [**3**] explained this formal duality by showing that the Kerdock and Preparata codes are in fact linear, if one views them over the ring of integers modulo 4 instead of the binary field and that, over this larger ring the two codes are algebraically dual. They showed a simple connection between these nonlinear codes and linear codes over $\mathbf{Z}_4$ by means of the Gray map. This generated a lot of interest on $\mathbf{Z}_4$-codes, see for example [**1, 10**]. It is a natural question to ask what happens for $\mathbf{Z}_{2^m}$-cyclic codes.

In [**2**], the authors prove that idempotent generators exist for certain $\mathbf{Z}_{q^m}$-cyclic codes. The uniqueness of an idempotent generator of any cyclic code is also proven. In fact Kanwar and López-Permouth [**5**] gave a systematic study of cyclic codes over $\mathbf{Z}_{q^m}$.

A particularly interesting family of cyclic codes is quadratic residue codes. Quadratic residue codes were first defined by Andrew Gleason.

Research partially supported by NSA grant.
Received by the editors on January 23, 2007, and in revised form on June 24, 2007.

DOI:10.1216/RMJ-2009-39-6-1947

The minimum weights of many modest quadratic codes are quite high for the codes' lengths, making this class of codes promising. The $\mathbf{Z}_4$ quadratic residue codes were studied by beautiful works of Bonnecaze, Solé and Calderbank [**1**] and Pless and Qian [**10**]. In [**2**], the authors studied the $\mathbf{Z}_8$ quadratic residue codes in some detail. In this paper, we define $\mathbf{Z}_{16}$ and $\mathbf{Z}_{32}$ 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 the properties of quadratic residue codes over a field. In [**4**], Kanwar has general results on quadratic residue $\mathbf{Z}_{q^m}$-codes of length p where p is an odd prime congruent to ± 1 modulo $4q$. The concept of extended quadratic residue $\mathbf{Z}_{q^m}$-codes is introduced in [**4**], and their duals are obtained. The purpose of this paper is to show that extended quadratic residue codes over $\mathbf{Z}_{16}$ or $\mathbf{Z}_{32}$ have large automorphism groups which will be useful in decoding these codes by using the powerful decoding method described in [**7**]. We also define an isometry from $\mathbf{Z}_{16}^N$ (Lee distance) to $\mathbf{Z}_2^{8N}$ (Hamming distance) and an isometry from $\mathbf{Z}_{32}^N$ (Lee distance) to $\mathbf{Z}_2^{16N}$ (Hamming distance).

In Section 2, we recall some general results on idempotent generators of cyclic codes. In Sections 3 and 5, we study some properties of quadratic residue codes over $\mathbf{Z}_{16}$ and $\mathbf{Z}_{32}$, respectively (Theorems 3.3, 3.4, 5.3, and 5.4). We also study extended quadratic residue $\mathbf{Z}_{16}$-codes and $\mathbf{Z}_{32}$-codes and obtain their duals (Theorems 3.7 and 3.9, respectively, Theorems 5.7 and 5.9). In Sections 4 and 6, we study automorphism groups of extended quadratic residue codes over $\mathbf{Z}_{16}$ and $\mathbf{Z}_{32}$, respectively. We also define an isometry from $\mathbf{Z}_{16}^N$ (Lee distance) to $\mathbf{Z}_2^{8N}$ (Hamming distance) and from $\mathbf{Z}_{32}^N$ (Lee distance) to $\mathbf{Z}_2^{16N}$ (Hamming distance).

2. Preliminaries. In this section, we recall some general results on idempotent generators of cyclic codes (cf. [**2, 5**]). An idempotent in $\mathbf{Z}_{q^m}[x]/(x^n-1)$, where q is a prime number, is defined to be a polynomial $e(x)$ such that $e(x)^2 = e(x) \pmod{x^n - 1}$. We first recall the following general facts about the existence and uniqueness of the idempotent generator. By a $\mathbf{Z}_{q^m}$-code C of length n we shall mean a linear code over $\mathbf{Z}_{q^m}$, that is, a $\mathbf{Z}_{q^m}$-module. We define an inner product of $\mathbf{Z}_{q^m}^n$ by $(a,b) = a_1b_1 + \cdots + a_nb_n \pmod{q^m}$, and then the notions of dual code ($C^\perp$), self-orthogonal code ($C \subseteq C^\perp$) and self-dual code ($C = C^\perp$) are defined in a standard way.

Theorem 2.1. *Let C be a $\mathbf{Z}_{q^m}$-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 $\mathbf{Z}_{q^m}[x]/(x^n - 1)$. Moreover, the idempotent generator of a cyclic code is unique.*

If we know the idempotent generator of a $\mathbf{Z}_{q^m}$-code, by the following theorem we can also find the idempotent generator of the dual code.

Theorem 2.2. *If a $\mathbf{Z}_{q^m}$-cyclic code C has idempotent generator $e(x)$, then $C^{\perp}$ has idempotent generator $1 - e(x^{-1})$.*

Theorem 2.3. *Let C_1 and C_2 be cyclic codes with $\mathbf{Z}_{q^m}$-idempotent generators e_1 and e_2. Then $C_1 \cap C_2$ has $\mathbf{Z}_{q^m}$-idempotent generator $e_1 e_2$ and $C_1 + C_2$ has $\mathbf{Z}_{q^m}$-idempotent generator $e_1 + e_2 - e_1 e_2$.*

3. Quadratic residue codes over $\mathbf{Z}_{16}$.

Quadratic residue (QR) codes over $\mathbf{Z}_{q^m}$ are $\mathbf{Z}_{q^m}$-cyclic codes which can be defined in terms of their idempotent generators ([**6, 8**]).

3.1. Idempotent generators of QR codes over $\mathbf{Z}_{q^m}$.

Let

$$e_1 = \sum_{i \in Q} x^i \quad \text{and} \quad e_2 = \sum_{i \in N} x^i,$$

where Q is the set of quadratic residues and N is the set of nonresidues 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.

Let the map μ_a be defined as

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

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

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

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

Note. -1 is a quadratic residue in $GF(p)$ if and only if $p \equiv 1 \pmod 4$ [**9**, Theorem 65].

The following theorems (Theorems 3.1, 3.3, 3.4, 3.7, and 3.9) are special cases of [**4**]. They are needed for Section 4.

Theorem 3.1. *Let p be a prime $\equiv \pm 1 \pmod 8$, such that $p+1$ (or $p-1$) $= 8r$.*

I. *Suppose $p+1 = 8r$.* (a) *If $r = 8k$, then $1+e_i$ and $15e_i$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i = 1, 2$.*

(b) *If $r = 8k+1$, then $3e_i+6e_j+5$ and $10e_i+13e_j+12$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(c) *If $r = 8k+2$, then $3e_i+12e_j+8$ and $4e_i+13e_j+9$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(d) *If $r = 8k+3$, then e_i+6e_j+4 and $10e_i+15e_j+13$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(e) *If $r = 8k+4$, then $8e_i+7e_j$ and $8e_i+9e_j+1$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(f) *If $r = 8k+5$, then $2e_i+5e_j+12$ and $11e_i+14e_j+5$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(g) *If $r = 8k+6$, then $4e_i+11e_j+8$ and $5e_i+12e_j+9$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(h) *If $r = 8k+7$, then $2e_i+7e_j+13$ and $9e_i+14e_j+4$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

II. *Suppose $p-1 = 8r$.* (a) *If $r = 8k$, then $1+e_i$ and $15e_i$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i = 1, 2$.*

(b) *If $r = 8k+1$, then $2e_i+7e_j+13$ and $9e_i+14e_j+4$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(c) *If $r = 8k+2$, then $4e_i+11e_j+8$ and $5e_i+12e_j+9$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(d) *If $r = 8k+3$, then $2e_i+5e_j+12$ and $11e_i+14e_j+5$ are idempotents in $\mathbf{Z}_{16}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(e) *If* $r = 8k + 4$, *then* $7e_i + 8e_j$ *and* $8e_i + 9e_j + 1$ *are idempotents in* $\mathbf{Z}_{16}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(f) *If* $r = 8k+5$, *then* e_i+6e_j+4 *and* $10e_i+15e_j+13$ *are idempotents in* $\mathbf{Z}_{16}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(g) *If* $r = 8k+6$, *then* $3e_i+12e_j+8$ *and* $4e_i+13e_j+9$ *are idempotents in* $\mathbf{Z}_{16}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(h) *If* $r = 8k+7$, *then* $3e_i+6e_j+5$ *and* $10e_i+13e_j+12$ *are idempotents in* $\mathbf{Z}_{16}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

Definition 3.2. A $\mathbf{Z}_{16}$-cyclic code is a $\mathbf{Z}_{16}$-quadratic residue (QR) code if it is generated by one of the idempotents in the above theorem.

Hence, μ_a is in the group of any $\mathbf{Z}_{16}$-Q.R. code for any $a \in Q$.

3.2. Properties of QR codes over $\mathbf{Z}_{16}$.

Theorem 3.3. *Let* p *be a prime with* $p + 1 = 8r$.

If $r = 8k$, *let*

$$\begin{aligned} Q_1 &= (15e_1), & Q_2 &= (15e_2); \\ Q_1' &= (1 + e_2), & Q_2' &= (1 + e_1). \end{aligned}$$

If $r = 8k + 1$, *let*

$$\begin{aligned} Q_1 &= (10e_1 + 13e_2 + 12), & Q_2 &= (13e_1 + 10e_2 + 12); \\ Q_1' &= (3e_1 + 6e_2 + 5), & Q_2' &= (6e_1 + 3e_2 + 5). \end{aligned}$$

If $r = 8k + 2$, *let*

$$\begin{aligned} Q_1 &= (3e_1 + 12e_2 + 8), & Q_2 &= (12e_1 + 3e_2 + 8); \\ Q_1' &= (4e_1 + 13e_2 + 9), & Q_2' &= (13e_1 + 4e_2 + 9). \end{aligned}$$

If $r = 8k + 3$, *let*

$$\begin{aligned} Q_1 &= (e_1 + 6e_2 + 4), & Q_2 &= (6e_1 + e_2 + 4); \\ Q_1' &= (10e_1 + 15e_2 + 13), & Q_2' &= (15e_1 + 10e_2 + 13). \end{aligned}$$

If $r = 8k+4$, *let*

$$\begin{aligned} Q_1 &= (8e_1 + 7e_2), & Q_2 &= (7e_1 + 8e_2);\\ Q_1' &= (9e_1 + 8e_2 + 1), & Q_2' &= (8e_1 + 9e_2 + 1). \end{aligned}$$

If $r = 8k+5$, *let*

$$\begin{aligned} Q_1 &= (2e_1 + 5e_2 + 12), & Q_2 &= (5e_1 + 2e_2 + 12);\\ Q_1' &= (11e_1 + 14e_2 + 5), & Q_2' &= (14e_1 + 11e_2 + 5). \end{aligned}$$

If $r = 8k+6$, *let*

$$\begin{aligned} Q_1 &= (4e_1 + 11e_2 + 8), & Q_2 &= (11e_1 + 4e_2 + 8);\\ Q_1' &= (5e_1 + 12e_2 + 9), & Q_2' &= (12e_1 + 5e_2 + 9). \end{aligned}$$

If $r = 8k+7$, *let*

$$\begin{aligned} Q_1 &= (9e_1 + 14e_2 + 4), & Q_2 &= (14e_1 + 9e_2 + 4);\\ Q_1' &= (2e_1 + 7e_2 + 13), & Q_2' &= (7e_1 + 2e_2 + 13). \end{aligned}$$

Then the following hold for $\mathbf{Z}_{16}$*-QR codes* Q_1, Q_2, Q_1', Q_2': (a) Q_1 *and* Q_2 *are equivalent,* Q_1' *and* Q_2' *are equivalent*;

(b) $Q_1 \cap Q_2 = (\widetilde{h})$ *and* $Q_1 + Q_2 = R_p = \mathbf{Z}_{16}[x]/(x^p - 1)$, *where* $\widetilde{h} = 15h$ *if* r *is even, and* $\widetilde{h} = 7h$ *if* r *is odd, where* $h = 1 + e_1 + e_2$;

(c) $|Q_1| = 16^{(p+1)/2} = |Q_2|$;

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

(e) $|Q_1'| = 16^{(p-1)/2} = |Q_2'|$;

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

Theorem 3.4. *Let* p *be a prime with* $p - 1 = 8r$.

If $r = 8k$, *let*

$$\begin{aligned} Q_1 &= (e_1 + 1), & Q_2 &= (e_2 + 1);\\ Q_1' &= (15e_2), & Q_2' &= (15e_1). \end{aligned}$$

If $r = 8k+1$, *let*

$$Q_1 = (2e_1 + 7e_2 + 13), \quad Q_2 = (7e_1 + 2e_2 + 13);$$
$$Q_1' = (9e_1 + 14e_2 + 4), \quad Q_2' = (14e_1 + 9e_2 + 4).$$

If $r = 8k+2$, *let*

$$Q_1 = (5e_1 + 12e_2 + 9), \quad Q_2 = (12e_1 + 5e_2 + 9);$$
$$Q_1' = (4e_1 + 11e_2 + 8), \quad Q_2' = (11e_1 + 4e_2 + 8).$$

If $r = 8k+3$, *let*

$$Q_1 = (11e_1 + 14e_2 + 5), \quad Q_2 = (14e_1 + 11e_2 + 5);$$
$$Q_1' = (2e_1 + 5e_2 + 12), \quad Q_2' = (5e_1 + 2e_2 + 12).$$

If $r = 8k+4$, *let*

$$Q_1 = (8e_1 + 9e_2 + 1), \quad Q_2 = (9e_1 + 8e_2 + 1);$$
$$Q_1' = (7e_1 + 8e_2), \quad Q_2' = (8e_1 + 7e_2).$$

If $r = 8k+5$, *let*

$$Q_1 = (10e_1 + 15e_2 + 13), \quad Q_2 = (15e_1 + 10e_2 + 13);$$
$$Q_1' = (e_1 + 6e_2 + 4), \quad Q_2' = (6e_1 + e_2 + 4).$$

If $r = 8k+6$, *let*

$$Q_1 = (4e_1 + 13e_2 + 9), \quad Q_2 = (13e_1 + 4e_2 + 9);$$
$$Q_1' = (3e_1 + 12e_2 + 8), \quad Q_2' = (12e_1 + 3e_2 + 8).$$

If $r = 8k+7$, *let*

$$Q_1 = (3e_1 + 6e_2 + 5), \quad Q_2 = (6e_1 + 3e_2 + 5);$$
$$Q_1' = (10e_1 + 13e_2 + 12), \quad Q_2' = (13e_1 + 10e_2 + 12).$$

Then the following hold for $\mathbf{Z}_{16}$*-QR codes* Q_1, Q_2, Q_1', Q_2': (a) Q_1 *and* Q_2 *are equivalent,* Q_1' *and* Q_2' *are equivalent*;

(b) $Q_1 \cap Q_2 = (\widetilde{h})$ *and* $Q_1 + Q_2 = R_p = \mathbf{Z}_{16}[x]/(x^p - 1)$, *where* $\widetilde{h} = h$ *if* r *is even, and* $\widetilde{h} = 9h$ *if* r *is odd, where* $h = 1 + e_1 + e_2$;

(c) $|Q_1| = 16^{(p+1)/2} = |Q_2|$;

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

(e) $|Q_1'| = 16^{(p-1)/2} = |Q_2'|$;

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

Definition 3.5. The extended code of a $\mathbf{Z}_{16}$-code C denoted by $\overline{C}$ is the code obtained by adding an overall parity check to each codeword of C.

Definition 3.6. When $p + 1 = 8r$ and r is odd, we define $\widetilde{Q}_1$ to be the $\mathbf{Z}_{16}$-code generated by the following matrix

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

where each row of G_1' is a cyclic shift of $3e_1 + 6e_2 + 5$ when $r = 8k + 1$, a cyclic shift of $10e_1 + 15e_2 + 13$ when $r = 8k + 3$, a cyclic shift of $11e_1 + 14e_2 + 5$ when $r = 8k + 5$ and a cyclic shift of $2e_1 + 7e_2 + 13$ when $r = 8k + 7$. We define $\widetilde{Q}_2$ similarly.

Theorem 3.7. *Suppose* $p + 1 = 8r$, *and let* Q_1, Q_2 *be the* $\mathbf{Z}_{16}$-*QR codes in Theorem* 3.3. *Let* $\overline{Q}_1$ *and* $\overline{Q}_2$ *denote their extended codes. Then* $\overline{Q}_1$ *and* $\overline{Q}_2$ *are self-dual, when* r *is even, and the dual of* $\overline{Q}_1$ *is* $\widetilde{Q}_1$ *and the dual of* $\overline{Q}_2$ *is* $\widetilde{Q}_2$ *when* r *is odd.*

Definition 3.8. When $p - 1 = 8r$, we define $\widetilde{Q}_1$ to be the $\mathbf{Z}_{16}$-code generated by the following matrix, when r is even:

$$\begin{array}{c} \begin{array}{ccccccc} \infty & 0 & 1 & \cdots & \cdots & \cdots & p-1 \end{array} \\ \begin{bmatrix} 0 & & & & & & \\ 0 & & & & & & \\ \vdots & & & G_1' & & & \\ \vdots & & & & & & \\ 1 & 1 & 1 & \cdots & \cdots & \cdots & 1 \end{bmatrix} \end{array},$$

where each row of G_1' is a cyclic shift of $15e_2$ when $r = 8k$, a cyclic shift of $4e_1 + 11e_2 + 8$ when $r = 8k + 2$, a cyclic shift of $7e_1 + 8e_2$ when $r = 8k + 4$ and a cyclic shift of $3e_1 + 12e_2 + 8$ when $r = 8k + 6$.

When r is odd:

$$\begin{array}{c} \begin{array}{ccccccc} \infty & 0 & 1 & \cdots & \cdots & \cdots & p-1 \end{array} \\ \begin{bmatrix} 0 & & & & & & \\ 0 & & & & & & \\ \vdots & & & G_1' & & & \\ \vdots & & & & & & \\ 9 & 9 & 9 & \cdots & \cdots & \cdots & 9 \end{bmatrix} \end{array},$$

where each row of G_1' is a cyclic shift of $9e_1+14e_2+4$ when $r = 8k+1$, a cyclic shift of $2e_1+5e_2+12$ when $r = 8k+3$, a cyclic shift of e_1+6e_2+4 when $r = 8k + 5$, a cyclic shift of $10e_1 + 13e_2 + 12$ when $r = 8k + 7$. We define $\widetilde{Q}_2$ similarly.

Theorem 3.9. *Suppose $p - 1 = 8r$, and let Q_1, Q_2 be the $\mathbf{Z}_{16}$-QR codes in Theorem* 3.4. *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 $\widetilde{Q}_1$.*

4. Automorphism group of the extended QR codes over $\mathbf{Z}_{16}$. Let χ be the Legendre symbol on the field $GF(p)$ which is defined as: $\chi(0) = 0$ and $\chi(i) = 1$ if i is a quadratic residue and $\chi(i) = -1$ if i is a nonresidue.

We use the following theorem extensively.

Theorem 4.1 (Perron [**8**]). (i) *Suppose $p = -1 + 8r$ and a is a number prime to p. Then, in the set $\{q + a$, where $q \in Q \cup \{0\}\}$, there* *are* $2r$ *elements in* $Q \cup \{0\}$ *and* $2r$ *elements in* N. *In the set* $\{n + a,$ *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* $\{q + a,$ *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* $\{n+a,$ *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 4.2. *Let* G *be the group generated by the following elements:*

$\sigma : i \to i + 1 \pmod p$, $\infty \to \infty$; $\mu_a : i \to ai \pmod p$, *for* $a \in Q$, $\infty \to \infty$; $\rho : i \to -(1/i) \pmod p$ *followed by multiplication by* $-\chi(i)$ *for* $i \neq 0, \infty$.

The action of ρ *on* 0 *and* ∞ *is defined as follows.*

(I) $p + 1 = 8r$. *If* $r = 8k$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 1,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 15.$$

If $r = 8k + 1$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 11,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 13.$$

If $r = 8k + 2$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 9,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 7.$$

If $r = 8k + 3$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 13,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 11.$$

If $r = 8k + 4$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 15,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 1.$$

If $r = 8k + 5$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 11,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 13.$$

If $r = 8k + 6$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 7,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 9.$$

If $r = 8k + 7$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 13,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 11.$$

(II) $p - 1 = 8r$. *If* $r = 8k$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 1,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 1.$$

If $r = 8k + 1$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 3,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 11.$$

If $r = 8k + 2$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 9,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 9.$$

If $r = 8k + 3$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 5,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 13.$$

If $r = 8k + 4$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 15,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 15.$$

If $r = 8k + 5$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 3,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 11.$$

If $r = 8k + 6$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 7,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 7.$$

If $r = 8k + 7$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 5,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 13.$$

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

Proof. 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 [**7**, page 492] to show that the extended code is also fixed by the map ρ.

(I) We suppose that $p + 1 = 8r$ and $r = 8k$. The extended code is generated by $(p + 1/2)$ rows of the following $(p + 1) \times (p + 1)$ matrix

$$\begin{array}{c|cccccc|}
r_0 & 0 & & & & & \\
\cdot & 0 & & & & & \\
\vdots & \vdots & & & G_1' & & \\
r_s & \vdots & & & & & \\
\vdots & \vdots & & & & & \\
r_\infty & 15 & 15 & \cdots & \cdots & \cdots & 15
\end{array},$$

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

1. Since $p = 8r - 1$, -1 is a nonresidue $\bmod p$. Hence, ρ sends Q to N and vice versa. In particular,

$$r_0 = (0, 1 + e_2) \Longrightarrow \rho(r_0) = (1, e_1) = 15r_0 + 15r_\infty.$$

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

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

Hence,

$$\rho(r_s) = \left(1, 15x^{-1/s} + 15 \sum_{n+s \in Q} x^{-1/(n+s)} + \sum_{n+s \in N} x^{-1/(n+s)}\right)$$

because the set $\{n+s\}$ has element 0; therefore, in the ∞ position of $\rho(r_s)$ it is 1. We claim that $\rho(r_s) = 15r_0 + 15r_{-1/s} + 15r_\infty$. By Perron's theorem and $-1 \in N$, 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, 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

$$15x^{-1/s} + 15 \sum_{n+s \in Q} x^{-1/(n+s)} + x^{-1/s} + \sum_{n-(1/s) \in N} x^{n-(1/s)}.$$

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

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

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

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

$$\rho(r_s) + r_{-1/s} = (1, e_1) = 15r_0 + 15r_\infty;$$

i.e., $\rho(r_s) = 15r_{-1/s} + 15r_0 + 15r_\infty$, for $s \in Q$.

3. For any $s \in N$,

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

Hence, $\rho(r_s) = (0, x^{-1/s} + 15 \sum_{n+s \in Q} x^{-1/(n+s)} + \sum_{n+s \in N} x^{-1/(n+s)})$.

Because the set $\{q+s\}$ has element 0, therefore in the ∞ position of $\rho(r_s)$ it is 0. We claim that $\rho(r_s) = 15r_0 + r_{-1/s}$.

By Perron's theorem and $-1 \in N$, the set $\{-1/n+s\}$ has $2r-1$ elements in Q and $2r$ elements in N; the set $\{n-(1/s)\}$ has $2r-1$ elements in Q and $2r-1$ elements in N, one element is 0. In the residue position of $\rho(r_s) + 15r_{-1/s}$ it is

$$x^{-1/s} + \sum_{n+s \in N} x^{-1/(n+s)} + 15x^{-1/s} + 15 \sum_{n-(1/s) \in Q} x^{n-(1/s)}.$$

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

In the nonresidue position of $\rho(r_s) + 15r_{-1/s}$, it is

$$15 \sum_{n+s \in Q} x^{-1/(n+s)} + 15 \sum_{n-(1/s) \in N} x^{n-(1/s)}.$$

Since for any $-1/(n+s) \in N$, there is a $q \in Q$ such that $-1/(n+s) = q - (1/s)$. There are $2r + 2r - 1 = 4r - 1$ terms in the above, so the sum is $15e_2$.

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

$$\rho(r_s) + 15r_{-1/s} = (0, 15 + 15e_2) = 15r_0;$$

i.e., $\rho(r_s) = r_{-1/s} + 15r_0$, for $s \in N$.

4. Since

$$r_\infty = (15, 15 + 15e_1 + 15e_2) \Longrightarrow \rho(r_\infty) = (15, 1 + e_2 + 15e_1) = 2r_0 + r_\infty,$$

by similar proofs, we also get the following results:

When $r = 8k + 1$,

$$\begin{gathered} r_0 = (0, 3e_1 + 6e_2 + 5) \\ \rho(r_0) = 13r_0 + 9r_\infty, \quad \rho(r_s) = 13r_0 + 15r_{1/s} + 14r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 13r_0 + 15r_\infty, \quad s \in N, \\ \rho(r_\infty) = 6r_0 + 3r_\infty. \end{gathered}$$

When $r = 8k + 2$,

$$\begin{gathered} r_0 = (0, 4e_1 + 13e_2 + 9) \\ \rho(r_0) = 7r_0 + 15r_\infty, \quad \rho(r_s) = 7r_0 + 15r_{1/s} + 11r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 7r_0 + 12r_\infty, \quad s \in N, \\ \rho(r_\infty) = 2r_0 + 9r_\infty. \end{gathered}$$

When $r = 8k + 3$,

$$\begin{gathered} r_0 = (0, 10e_1 + 15e_2 + 13) \\ \rho(r_0) = 11r_0 + 7r_\infty, \quad \rho(r_s) = 11r_0 + 15r_{1/s} + 13r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 11r_0 + 14r_\infty, \quad s \in N, \\ \rho(r_\infty) = 10r_0 + 5r_\infty. \end{gathered}$$

When $r = 8k + 4$,

$$\begin{gathered} r_0 = (0, 9e_1 + 8e_2 + 1) \\ \rho(r_0) = r_0 + r_\infty, \quad \rho(r_s) = r_0 + 15r_{1/s} + 8r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + r_0 + 9r_\infty, \quad s \in N, \\ \rho(r_\infty) = 14r_0 + 15r_\infty. \end{gathered}$$

When $r = 8k + 5$,

$$\begin{gathered} r_0 = (0, 11e_1 + 14e_2 + 5) \\ \rho(r_0) = 13r_0 + 9r_\infty, \quad \rho(r_s) = 13r_0 + 15r_{1/s} + 6r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 13r_0 + 7r_\infty, \quad s \in N, \\ \rho(r_\infty) = 6r_0 + 3r_\infty. \end{gathered}$$

When $r = 8k+6$,

$$r_0 = (0, 5e_1 + 12e_2 + 9)$$
$$\rho(r_0) = 9r_0 + r_\infty, \quad \rho(r_s) = 9r_0 + 15r_{1/s} + 12r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 9r_0 + 13r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 14r_0 + 7r_\infty.$$

When $r = 8k+7$,

$$r_0 = (0, 2e_1 + 7e_2 + 13)$$
$$\rho(r_0) = 11r_0 + 7r_\infty, \quad \rho(r_s) = 11r_0 + 15r_{1/s} + 5r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 11r_0 + 6r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 5r_\infty.$$

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

$$\begin{array}{c} r_0 \\ . \\ \vdots \\ r_s \\ \vdots \\ r_\infty \end{array} \left(\begin{array}{cccccc} 0 & & & & & \\ 0 & & & & & \\ \vdots & & & G_1' & & \\ \vdots & & & & & \\ \vdots & & & & & \\ 15 & 1 & \cdots & \cdots & \cdots & 1 \end{array}\right),$$

where each row of G_1' is a cyclic shift of $15e_2$.

1. Since $r_0 = (0, 15e_2) \Rightarrow \rho(r_0) = (0, 15e_2) = r_0$.
2. For any $s \in Q$ (in the following proofs $q \in Q$ and $n \in N$),

$$r_s = \Big(0, 15\sum x^{n+s}\Big), \quad r_{-1/s} = \Big(0, 15\sum x^{n-(1/s)}\Big).$$

Hence, $\rho(r_s) = (0, \sum_{n+s\in Q} x^{-1/(n+s)} + 15\sum_{n+s\in N} x^{-1/(n+s)})$.

Because the set $\{q+s\}$ has element 0, therefore in the ∞ position of $\rho(r_s)$ it is 0. We claim that $\rho(r_s) = r_0 + 15r_{-1/s}$. By Perron's theorem and $-1 \in Q$, 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, $2r$ 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

$$\sum_{n+s\in Q} x^{-1/n+s} + 15 \sum_{n-(1/s)\in Q} x^{n-(1/s)},$$

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

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

$$15\sum_{n+s\in N} x^{-1/(n+s)} + 15 \sum_{n-(1/s)\in N} x^{n-(1/s)}.$$

Since for any $-1/(n+s)\in N$, there is a $q\in Q$ such that $-1/(n+s) = q-(1/s)$. And there are $2r+2r=4r$ terms, so the sum of the above is $15e_2$. Since the set $\{q-(1/s)\}$ has element 0, therefore

$$\rho(r_s)+r_{-1/s} = (0, 15e_2) = r_0;$$

i.e., $\rho(r_s) = 15r_{-1/s}+r_0$, for $s\in Q$.

3. For any $s\in N$,

$$r_s = (0, 15\sum x^{n+s}),$$
$$r_{-1/s} = (0, 15\sum x^{n-(1/s)}).$$

Hence, $\rho(r_s) = (15, \sum_{n+s\in Q} x^{-1/(n+s)} + 15\sum_{n+s\in N} x^{-1/(n+s)})$.

Because the set $\{n+s\}$ has element 0, therefore in the ∞ position of $\rho(r_s)$ it is 15. We claim that $\rho(r_s) = r_0 + r_{-1/s} + r_\infty$.

By Perron's theorem and $-1\in Q$, 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 $\rho(r_s)+15r_{-1/s}$ it is

$$15\sum_{n+s\in N} x^{-1/(n+s)} + \sum_{n-(1/s)\in N} x^{n-(1/s)}.$$

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

In the residue position of $\rho(r_s)+15r_{-(1/s)}$ it is

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

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

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

$$\rho(r_s)+15r_{-1/s} = (15, 1+e_1) = r_0 + r_\infty;$$

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

4. Since

$$r_\infty = (15, 15+1+e_1+e_2) \Longrightarrow \rho(r_\infty) = (1, 15+15e_1+e_2) = 14r_0+15r_\infty,$$

by similar proofs, we also get the following results:

When $r = 8k+1$,

$$r_0 = (0, 9e_1+14e_2+4)$$
$$\rho(r_0) = 11r_0+4r_\infty, \quad \rho(r_s) = 15r_{1/s}+11r_0+5r_\infty, \quad s \in Q,$$
$$\rho(r_s) = 11r_0 + r_{1/s} + 6r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0+5r_\infty.$$

When $r = 8k+2$,

$$r_0 = (0, 4e_1+11e_2+8)$$
$$\rho(r_0) = 9r_0+8r_\infty, \quad \rho(r_s) = 15r_{1/s}+9r_0+12r_\infty, \quad s \in Q$$
$$\rho(r_s) = 9r_0 + r_{1/s} + 13r_\infty, \quad s \in N$$
$$\rho(r_\infty) = 14r_0+7r_\infty.$$

When $r = 8k+3$,

$$r_0 = (0, 2e_1+5e_2+12)$$
$$\rho(r_0) = 13r_0+4r_\infty, \quad \rho(r_s) = 15r_{1/s}+13r_0+6r_\infty, \quad s \in Q,$$
$$\rho(r_s) = 13r_0 + r_{1/s} + 7r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 6r_0+3r_\infty.$$

When $r = 8k+4$,

$$\begin{gathered} r_0 = (0, 7e_1 + 8e_2) \\ \rho(r_0) = 15r_0, \quad \rho(r_s) = 15r_{1/s} + 15r_0 + 7r_\infty, \quad s \in Q, \\ \rho(r_s) = 15r_0 + r_{1/s} + 8r_\infty, \quad s \in N, \\ \rho(r_\infty) = 2r_0 + r_\infty. \end{gathered}$$

When $r = 8k+5$,

$$\begin{gathered} r_0 = (0, e_1 + 6e_2 + 4) \\ \rho(r_0) = 11r_0 + 4r_\infty, \quad \rho(r_s) = 15r_{1/s} + 11r_0 + 13r_\infty, \quad s \in Q, \\ \rho(r_s) = 11r_0 + r_{1/s} + 14r_\infty, \quad s \in N, \\ \rho(r_\infty) = 10r_0 + 5r_\infty. \end{gathered}$$

When $r = 8k+6$,

$$\begin{gathered} r_0 = (0, 3e_1 + 12e_2 + 8) \\ \rho(r_0) = 7r_0 + 8r_\infty \quad \rho(r_s) = 15r_{1/s} + 7r_0 + 11r_\infty, \quad s \in Q, \\ \rho(r_s) = 7r_0 + r_{1/s} + 12r_\infty, \quad s \in N, \\ \rho(r_\infty) = 2r_0 + 9r_\infty. \end{gathered}$$

When $r = 8k+7$,

$$\begin{gathered} r_0 = (0, 10e_1 + 13e_2 + 12) \\ \rho(r_0) = 13r_0 + 4r_\infty, \quad \rho(r_s) = 15r_{1/s} + 13r_0 + 14r_\infty, s \in Q, \\ \rho(r_s) = 13r_0 + r_{1/s} + 15r_\infty, \quad s \in N, \\ \rho(r_\infty) = 6r_0 + 3r_\infty. \qquad \square \end{gathered}$$

We call a vector in a $\mathbf{Z}_{q^m}$-code "even-like" if the sum of its coordinates is $0 \pmod{q^m}$; otherwise, we call it "odd-like." The following corollary 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 $\mathbf{Z}_{16}$-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 [**9**, page 33].)

Corollary 4.3. *The minimum* (*Hamming*) *weight vectors of a* $\mathbf{Z}_{16}$-QR $(p,(p+1)/2)$ *code are odd-like.*

Definition 4.4. The Lee weights of the elements count $\pm a$ as a for $1 \leq a \leq 7$, 8 as 8 and 0 as 0. The Lee weight of a vector is the sum of the Lee weights of its components.

Definition 4.5. The Euclidean weights of the elements count $\pm a$ as a^2 for $1 \leq a \leq 7$, 8 as 64 and 0 as 0. The Euclidean weight of a vector is the sum of the Euclidean weights of its components.

By direct computation using a computer, we have

Theorem 4.6. *The* $\mathbf{Z}_{16}$-QR $(7,4)$ *code of length* 7 *has minimum Lee weight* 7*, minimum Euclidean weight* 7 *and minimum Hamming weight* 3*.*

We define maps α *and* β_i*,* $i = 1,\dots,8$*, from* $\mathbf{Z}_{16}$ *to* $\mathbf{Z}_2$ *by*

c	$\alpha(c)$	$\beta_1(c)$	$\beta_2(c)$	$\beta_3(c)$	$\beta_4(c)$	$\beta_5(c)$	$\beta_6(c)$	$\beta_7(c)$	$\beta_8(c)$
0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	0	1	1
3	1	0	0	0	0	0	1	1	1
4	0	0	0	0	0	1	1	1	1
5	1	0	0	0	1	1	1	1	1
6	0	0	0	1	1	1	1	1	1
7	1	0	1	1	1	1	1	1	1
8	0	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1	0
10	0	1	1	1	1	1	1	0	0
11	1	1	1	1	1	1	0	0	0
12	0	1	1	1	1	0	0	0	0
13	1	1	1	1	0	0	0	0	0
14	0	1	1	0	0	0	0	0	0
15	1	1	0	0	0	0	0	0	0

and extend them componentwise to maps from $\mathbf{Z}_{16}^N$ *to* $\mathbf{Z}_2^N$*. Then the Gray map* $\phi : \mathbf{Z}_{16}^N \to \mathbf{Z}_2^{8N}$ *is given by* $\phi(c) = (\beta_1(c), \beta_2(c), \dots, \beta_8(c))$*.*

Note that $\alpha(c) + \beta_1(c) + \beta_2(c) + \cdots + \beta_8(c) = 0$ for all $c \in \mathbf{Z}_{16}$.

Observe that ϕ is a distance-preserving map or isometry from $\mathbf{Z}_{16}^N$ (Lee distance) to $\mathbf{Z}_2^{8N}$ (Hamming distance).

The weight distribution of the image of the length 7 $\mathbf{Z}_{16}$-QR $(7,4)$ code under the Gray map is as follows.

i	A_i	i	A_i	i	A_i
$0,56$	1	$14,42$	296	$22,34$	2814
$7,49$	2	$15,41$	518	$23,33$	3052
$8,48$	14	$16,40$	700	$24,32$	3269
$9,47$	70	$17,39$	882	$25,31$	3556
$10,46$	42	$18,38$	1162	$26,30$	3878
$11,45$	28	$19,37$	1582	$27,29$	4200
$12,44$	182	$20,36$	1876	28	4300
$13,43$	224	$21,35$	2270		

Since the symmetrized Lee weight enumerator of the $\mathbf{Z}_{16}$-QR $(7,4)$ code of length 7 takes a few pages long to write it down, we omit it here.

5. Quadratic residue codes over $\mathbf{Z}_{32}$.

The following theorems (Theorems 5.1, 5.3, 5.4, 5.7 and 5.9) are special cases of [**4**]. They are needed for Section 6.

Theorem 5.1. *Let p be a prime $p \equiv \pm 1 \pmod 8$, such that $p+1$ (or $p-1$) $= 8r$.*

I. *Suppose $p+1 = 8r$.*

(a) *If $r = 16k$, then e_i+1 and $31e_i$ are idempotents in $\mathbf{Z}_{32}[x]/(x^p-1)$, where $i = 1, 2$.*

(b) *If $r = 16k+1$, then $19e_i + 22e_j + 5$ and $13e_i + 10e_j + 28$ are idempotents in $\mathbf{Z}_{32}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(c) *If $r = 16k+2$, then $29e_i + 20e_j + 9$ and $3e_i + 12e_j + 24$ are idempotents in $\mathbf{Z}_{32}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(d) *If $r = 16k+3$, then $31e_i + 26e_j + 13$ and $e_i + 6e_j + 20$ are idempotents in $\mathbf{Z}_{32}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(e) *If $r = 16k+4$, then $25e_i + 8e_j + 17$ and $7e_i + 24e_j + 16$ are idempotents in $\mathbf{Z}_{32}[x]/(x^p-1)$, where $i, j = 1, 2$ and $i \neq j$.*

(f) *If* $r = 16k + 5$, *then* $11e_i + 30e_j + 21$ *and* $21e_i + 2e_j + 12$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(g) *If* $r = 16k + 6$, *then* $21e_i + 28e_j + 25$ *and* $11e_i + 4e_j + 8$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(h) *If* $r = 16k + 7$, *then* $23e_i + 2e_j + 29$ *and* $9e_i + 30e_j + 4$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(i) *If* $r = 16k+8$, *then* $17e_i+16e_j+1$ *and* $15e_i+16e_j$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(j) *If* $r = 16k + 9$, *then* $3e_i + 6e_j + 5$ *and* $29e_i + 26e_j + 28$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(k) *If* $r = 16k + 10$, *then* $13e_i + 4e_j + 9$ *and* $19e_i + 28e_j + 24$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(l) *If* $r = 16k + 11$, *then* $15e_i + 10e_j + 13$ *and* $17e_i + 22e_j + 20$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(m) *If* $r = 16k + 12$, *then* $9e_i + 24e_j + 17$ *and* $23e_i + 8e_j + 16$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(n) *If* $r = 16k + 13$, *then* $27e_i + 14e_j + 21$ *and* $5e_i + 18e_j + 12$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(o) *If* $r = 16k + 14$, *then* $5e_i + 12e_j + 25$ *and* $27e_i + 20e_j + 8$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(p) *If* $r = 16k + 15$, *then* $7e_i + 18e_j + 29$ *and* $25e_i + 14e_j + 4$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

II. *Suppose* $p - 1 = 8r$.

(a) *If* $r = 16k$, *then* e_i+1 *and* $31e_i$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p-1)$, *where* $i = 1, 2$.

(b) *If* $r = 16k + 1$, *then* $18e_i + 7e_j + 29$ *and* $14e_i + 25e_j + 4$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(c) *If* $r = 16k + 2$, *then* $12e_i + 5e_j + 25$ *and* $20e_i + 27e_j + 8$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(d) *If* $r = 16k + 3$, *then* $14e_i + 27e_j + 21$ *and* $18e_i + 5e_j + 12$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(e) *If* $r = 16k + 4$, *then* $24e_i + 9e_j + 17$ *and* $8e_i + 23e_j + 16$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(f) *If* $r = 16k + 5$, *then* $10e_i + 15e_j + 13$ *and* $22e_i + 17e_j + 20$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(g) *If* $r = 16k + 6$, *then* $4e_i + 13e_j + 9$ *and* $28e_i + 19e_j + 24$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(h) *If* $r = 16k + 7$, *then* $6e_i + 3e_j + 5$ *and* $26e_i + 29e_j + 28$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(i) *If* $r = 16k+8$, *then* $16e_i+17e_j+1$ *and* $16e_i+15e_j$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(j) *If* $r = 16k+9$, *then* $2e_i+23e_j+29$ *and* $30e_i+9e_j+4$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(k) *If* $r = 16k + 10$, *then* $28e_i + 21e_j + 25$ *and* $4e_i + 11e_j + 8$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(l) *If* $r = 16k + 11$, *then* $30e_i + 11e_j + 21$ *and* $2e_i + 21e_j + 12$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(m) *If* $r = 16k + 12$, *then* $8e_i + 25e_j + 17$ *and* $24e_i + 7e_j + 16$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(n) *If* $r = 16k + 13$, *then* $26e_i + 31e_j + 13$ *and* $6e_i + e_j + 20$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(o) *If* $r = 16k + 14$, *then* $20e_i + 29e_j + 9$ *and* $12e_i + 3e_j + 24$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

(p) *If* $r = 16k + 15$, *then* $22e_i + 19e_j + 5$ *and* $10e_i + 13e_j + 28$ *are idempotents in* $\mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $i, j = 1, 2$ *and* $i \neq j$.

Definition 5.2. A $\mathbf{Z}_{32}$-cyclic code is a $\mathbf{Z}_{32}$-quadratic residue (QR) code if it is generated by one of the idempotents in the above theorem.

Hence, μ_a is in the group of any $\mathbf{Z}_{32}$-Q.R. code for any $a \in Q$.

Properties of QR codes over $\mathbf{Z}_{32}$.

Theorem 5.3. *Let* p *be a prime with* $p + 1 = 8r$.

If $r = 16k$, *let*

$$Q_1 = (31e_1), \qquad Q_2 = (31e_2);$$
$$Q_1' = (e_2 + 1), \quad Q_2' = (e_1 + 1).$$

If $r = 16k+1$, *let*

$$Q_1 = (13e_1 + 10e_2 + 28), \quad Q_2 = (10e_1 + 13e_2 + 28);$$
$$Q_1' = (22e_1 + 19e_2 + 5), \quad Q_2' = (19e_1 + 22e_2 + 5).$$

If $r = 16k+2$, *let*

$$Q_1 = (3e_1 + 12e_2 + 24), \quad Q_2 = (12e_1 + 3e_2 + 24);$$
$$Q_1' = (20e_1 + 29e_2 + 9), \quad Q_2' = (29e_1 + 20e_2 + 9).$$

If $r = 16k+3$, *let*

$$Q_1 = (e_1 + 6e_2 + 20), \quad Q_2 = (6e_1 + e_2 + 20);$$
$$Q_1' = (26e_1 + 31e_2 + 13), \quad Q_2' = (31e_1 + 26e_2 + 13).$$

If $r = 16k+4$, *let*

$$Q_1 = (7e_1 + 24e_2 + 16), \quad Q_2 = (24e_1 + 7e_2 + 16);$$
$$Q_1' = (8e_1 + 25e_2 + 17), \quad Q_2' = (25e_1 + 8e_2 + 17).$$

If $r = 16k+5$, *let*

$$Q_1 = (21e_1 + 2e_2 + 12), \quad Q_2 = (2e_1 + 21e_2 + 12);$$
$$Q_1' = (30e_1 + 11e_2 + 21), \quad Q_2' = (11e_1 + 30e_2 + 21).$$

If $r = 16k+6$, *let*

$$Q_1 = (11e_1 + 4e_2 + 8), \quad Q_2 = (4e_1 + 11e_2 + 8);$$
$$Q_1' = (28e_1 + 21e_2 + 25), \quad Q_2' = (21e_1 + 28e_2 + 25).$$

If $r = 16k+7$, *let*

$$Q_1 = (9e_1 + 30e_2 + 4), \quad Q_2 = (30e_1 + 9e_2 + 4);$$
$$Q_1' = (2e_1 + 23e_2 + 29), \quad Q_2' = (23e_1 + 2e_2 + 29).$$

If $r = 16k+8$, *let*

$$Q_1 = (15e_1 + 16e_2), \quad Q_2 = (16e_1 + 15e_2);$$
$$Q_1' = (16e_1 + 17e_2 + 1), \quad Q_2' = (17e_1 + 16e_2 + 1).$$

If $r = 16k + 9$, *let*

$$\begin{aligned} Q_1 &= (29e_1 + 26e_2 + 28), & Q_2 &= (26e_1 + 29e_2 + 28); \\ Q_1' &= (6e_1 + 3e_2 + 5), & Q_2' &= (3e_1 + 6e_2 + 5). \end{aligned}$$

If $r = 16k + 10$, *let*

$$\begin{aligned} Q_1 &= (19e_1 + 28e_2 + 24), & Q_2 &= (28e_1 + 19e_2 + 24); \\ Q_1' &= (4e_1 + 13e_2 + 9), & Q_2' &= (13e_1 + 4e_2 + 9). \end{aligned}$$

If $r = 16k + 11$, *let*

$$\begin{aligned} Q_1 &= (17e_1 + 22e_2 + 20), & Q_2 &= (22e_1 + 17e_2 + 20); \\ Q_1' &= (10e_1 + 15e_2 + 13), & Q_2' &= (15e_1 + 10e_2 + 13). \end{aligned}$$

If $r = 16k + 12$, *let*

$$\begin{aligned} Q_1 &= (23e_1 + 8e_2 + 16), & Q_2 &= (8e_1 + 23e_2 + 16); \\ Q_1' &= (24e_1 + 9e_2 + 17), & Q_2' &= (9e_1 + 24e_2 + 17). \end{aligned}$$

If $r = 16k + 13$, *let*

$$\begin{aligned} Q_1 &= (5e_1 + 18e_2 + 12), & Q_2 &= (18e_1 + 5e_2 + 12); \\ Q_1' &= (14e_1 + 27e_2 + 21), & Q_2' &= (27e_1 + 14e_2 + 21). \end{aligned}$$

If $r = 16k + 14$, *let*

$$\begin{aligned} Q_1 &= (27e_1 + 20e_2 + 8), & Q_2 &= (20e_1 + 27e_2 + 8); \\ Q_1' &= (12e_1 + 5e_2 + 25), & Q_2' &= (5e_1 + 12e_2 + 25). \end{aligned}$$

If $r = 16k + 15$, *let*

$$\begin{aligned} Q_1 &= (25e_1 + 14e_2 + 4), & Q_2 &= (14e_1 + 25e_2 + 4); \\ Q_1' &= (18e_1 + 7e_2 + 29), & Q_2' &= (7e_1 + 18e_2 + 29). \end{aligned}$$

Then the following hold for $\mathbf{Z}_{32}$-QR *codes* Q_1, Q_2, Q_1', Q_2':

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

(b) $Q_1 \cap Q_2 = (\widetilde{h})$ *and* $Q_1 + Q_2 = R_p = \mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $\widetilde{h} = 31h$ *if* $r = 4k$, $\widetilde{h} = 23h$ *if* $r = 4k+1$, $\widetilde{h} = 15h$ *if* $r = 4k+2$ *and* $\widetilde{h} = 7h$ *if* $r = 4k+3$, *where* $h = e_1 + e_2 + 1$;

(c) $|Q_1| = 32^{(p+1)/2} = |Q_2|$;

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

(e) $|Q_1'| = 32^{(p-1)/2} = |Q_2'|$;

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

Theorem 5.4. *Let* p *be a prime with* $p - 1 = 8r$.

If $r = 16k$, *let*

$$\begin{aligned} Q_1 &= (e_1 + 1), & Q_2 &= (e_2 + 1); \\ Q_1' &= (31e_2), & Q_2' &= (31e_1). \end{aligned}$$

If $r = 16k + 1$, *let*

$$\begin{aligned} Q_1 &= (18e_1 + 7e_2 + 29), & Q_2 &= (7e_1 + 18e_2 + 29); \\ Q_1' &= (25e_1 + 14e_2 + 4), & Q_2' &= (14e_1 + 25e_2 + 4). \end{aligned}$$

If $r = 16k + 2$, *let*

$$\begin{aligned} Q_1 &= (12e_1 + 5e_2 + 25), & Q_2 &= (5e_1 + 12e_2 + 25); \\ Q_1' &= (27e_1 + 20e_2 + 8), & Q_2' &= (20e_1 + 27e_2 + 8). \end{aligned}$$

If $r = 16k + 3$, *let*

$$\begin{aligned} Q_1 &= (14e_1 + 27e_2 + 21), & Q_2 &= (27e_1 + 14e_2 + 21); \\ Q_1' &= (5e_1 + 18e_2 + 12), & Q_2' &= (18e_1 + 5e_2 + 12). \end{aligned}$$

If $r = 16k + 4$, *let*

$$\begin{aligned} Q_1 &= (24e_1 + 9e_2 + 17), & Q_2 &= (9e_1 + 24e_2 + 17); \\ Q_1' &= (23e_1 + 8e_2 + 16), & Q_2' &= (8e_1 + 23e_2 + 16). \end{aligned}$$

If $r = 16k + 5$, *let*

$$\begin{aligned} Q_1 &= (10e_1 + 15e_2 + 13), & Q_2 &= (15e_1 + 10e_2 + 13); \\ Q_1' &= (17e_1 + 22e_2 + 20), & Q_2' &= (22e_1 + 17e_2 + 20). \end{aligned}$$

If $r = 16k + 6$, *let*

$$\begin{aligned} Q_1 &= (4e_1 + 13e_2 + 9), & Q_2 &= (13e_1 + 4e_2 + 9); \\ Q_1' &= (19e_1 + 28e_2 + 24), & Q_2' &= (28e_1 + 19e_2 + 24). \end{aligned}$$

If $r = 16k + 7$, *let*

$$\begin{aligned} Q_1 &= (6e_1 + 3e_2 + 5), & Q_2 &= (3e_1 + 6e_2 + 5); \\ Q_1' &= (29e_1 + 26e_2 + 28), & Q_2' &= (26e_1 + 29e_2 + 28). \end{aligned}$$

If $r = 16k + 8$, *let*

$$\begin{aligned} Q_1 &= (16e_1 + 17e_2 + 1), & Q_2 &= (17e_1 + 16e_2 + 1); \\ Q_1' &= (15e_1 + 16e_2), & Q_2' &= (16e_1 + 15e_2). \end{aligned}$$

If $r = 16k + 9$, *let*

$$\begin{aligned} Q_1 &= (2e_1 + 23e_2 + 29), & Q_2 &= (23e_1 + 2e_2 + 29); \\ Q_1' &= (9e_1 + 30e_2 + 4), & Q_2' &= (30e_1 + 9e_2 + 4). \end{aligned}$$

If $r = 16k + 10$, *let*

$$\begin{aligned} Q_1 &= (28e_1 + 21e_2 + 25), & Q_2 &= (21e_1 + 28e_2 + 25); \\ Q_1' &= (11e_1 + 4e_2 + 8), & Q_2' &= (4e_1 + 11e_2 + 8). \end{aligned}$$

If $r = 16k + 11$, *let*

$$\begin{aligned} Q_1 &= (30e_1 + 11e_2 + 21), & Q_2 &= (11e_1 + 30e_2 + 21); \\ Q_1' &= (21e_1 + 2e_2 + 12), & Q_2' &= (2e_1 + 21e_2 + 12). \end{aligned}$$

If $r = 16k + 12$, *let*

$$\begin{aligned} Q_1 &= (8e_1 + 25e_2 + 17), & Q_2 &= (25e_1 + 8e_2 + 17); \\ Q_1' &= (7e_1 + 24e_2 + 16), & Q_2' &= (24e_1 + 7e_2 + 16). \end{aligned}$$

If $r = 16k + 13$, *let*

$$\begin{aligned} Q_1 &= (26e_1 + 31e_2 + 13), & Q_2 &= (31e_1 + 26e_2 + 13); \\ Q_1' &= (e_1 + 6e_2 + 20), & Q_2' &= (6e_1 + e_2 + 20). \end{aligned}$$

If $r = 16k + 14$, *let*

$$\begin{aligned} Q_1 &= (20e_1 + 29e_2 + 9), & Q_2 &= (29e_1 + 20e_2 + 9); \\ Q_1' &= (3e_1 + 12e_2 + 24), & Q_2' &= (12e_1 + 3e_2 + 24). \end{aligned}$$

If $r = 16k + 15$, *let*

$$\begin{aligned} Q_1 &= (22e_1 + 19e_2 + 5), & Q_2 &= (19e_1 + 22e_2 + 5); \\ Q_1' &= (13e_1 + 10e_2 + 28), & Q_2' &= (10e_1 + 13e_2 + 28). \end{aligned}$$

Then the following hold for $\mathbf{Z}_{32}$-QR *codes* Q_1, Q_2, Q_1', Q_2':

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

(b) $Q_1 \cap Q_2 = (\widetilde{h})$ *and* $Q_1 + Q_2 = R_p = \mathbf{Z}_{32}[x]/(x^p - 1)$, *where* $\widetilde{h} = h$ *if* $r = 4k$, $\widetilde{h} = 25h$ *if* $r = 4k + 1$, $\widetilde{h} = 17h$ *if* $r = 4k + 2$ *and* $\widetilde{h} = 9h$ *if* $r = 4k + 3$, *where* $h = e_1 + e_2 + 1$;

(c) $|Q_1| = 32^{(p+1)/2} = |Q_2|$;

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

(e) $|Q_1'| = 32^{(p-1)/2} = |Q_2'|$;

(f) $Q_1^\perp = Q_2'$, $Q_2^\perp = Q_1'$.

Definition 5.5. The extended code of a $\mathbf{Z}_{32}$-code C denoted by $\overline{C}$ is the code obtained by adding an overall parity check to each codeword of C.

Definition 5.6. When $p+1 = 8r$, we defined $\widetilde{Q}_1$ to be the $\mathbf{Z}_{32}$-code generated by the following matrix. When $r = 4k + 1$:

$$\begin{array}{ccccccc} \infty & 0 & 1 & \cdots & \cdots & \cdots & p-1 \\ \end{array}$$
$$\left[\begin{array}{c|c} 0 & \\ \vdots & \\ \vdots & G_1' \\ 0 & \\ 23 & 23 \quad 23 \quad \cdots \quad \cdots \quad \cdots \quad 23 \end{array}\right],$$

where each row of G_1' is a cyclic shift of $22e_1+19e_2+5$ when $r = 16k+1$, a cyclic shift of $30e_1 + 11e_2 + 21$ when $r = 16k + 5$, a cyclic shift of

$6e_1 + 3e_2 + 5$ when $r = 16k + 9$ and a cyclic shift of $14e_1 + 27e_2 + 21$ when $r = 16k + 13$.

When $r = 4k + 3$:

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

where each row of G_1' is a cyclic shift of $26e_1 + 31e_2 + 13$ when $r = 16k + 3$, a cyclic shift of $2e_1 + 23e_2 + 29$ when $r = 16k + 7$, a cyclic shift of $10e_1 + 15e_2 + 13$ when $r = 16k + 11$ and a cyclic shift of $18e_1 + 7e_2 + 29$ when $r = 16k + 15$. We define $\widetilde{Q}_2$ similarly.

Theorem 5.7. *Suppose $p + 1 = 8r$, and let Q_1, Q_2 be the $\mathbf{Z}_{32}$-QR codes in Theorem 5.3. Let $\overline{Q}_1$ and $\overline{Q}_2$ denoted their extended codes. Then $\overline{Q}_1$ and $\overline{Q}_2$ are self-dual, when $r = 4k$ and $4k + 2$. The dual of $\overline{Q}_1$ is $\widetilde{Q}_1$ and the dual of $\overline{Q}_2$ is $\widetilde{Q}_2$, when $r = 4k + 1$ and $4k + 3$.*

Definition 5.8. When $p - 1 = 8r$, we define $\widetilde{Q}_1$ to be the $\mathbf{Z}_{32}$-code generated by the following matrix.

When $r = 4k$:

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

where each row of G_1' is a cyclic shift of $31e_2$ when $r = 16k$, a cyclic shift of $23e_1 + 8e_2 + 16$ when $r = 16k + 4$, a cyclic shift of $15e_1 + 16e_2$ when $r = 16k + 8$ and a cyclic shift of $7e_1 + 24e_2 + 16$ when $r = 16k + 12$.

When $r = 4k + 1$:

$$\begin{array}{c} \begin{array}{ccccccc} \infty & 0 & 1 & \cdots & \cdots & \cdots & p-1 \end{array} \\ \begin{bmatrix} 0 & & & & & & \\ \vdots & & & & & & \\ \vdots & & & G_1' & & & \\ 0 & & & & & & \\ 25 & 25 & 25 & \cdots & \cdots & \cdots & 25 \end{bmatrix} \end{array},$$

where each row of G_1' is a cyclic shift of $25e_1+14e_2+4$ when $r = 16k+1$, a cyclic shift of $17e_1 + 22e_2 + 20$ when $r = 16k + 5$, a cyclic shift of $9e_1 + 30e_2 + 4$ when $r = 16k+9$ and a cyclic shift of $e_1 + 6e_2 + 20$ when $r = 16k + 13$.

When $r = 4k + 2$:

$$\begin{array}{c} \begin{array}{ccccccc} \infty & 0 & 1 & \cdots & \cdots & \cdots & p-1 \end{array} \\ \begin{bmatrix} 0 & & & & & & \\ \vdots & & & & & & \\ \vdots & & & G_1' & & & \\ 0 & & & & & & \\ 17 & 17 & 17 & \cdots & \cdots & \cdots & 17 \end{bmatrix} \end{array},$$

where each row of G_1' is a cyclic shift of $27e_1+20e_2+8$ when $r = 16k+2$, a cyclic shift of $19e_1 + 28e_2 + 24$ when $r = 16k + 6$, a cyclic shift of $11e_1 + 4e_2 + 8$ when $r = 16k + 10$ and a cyclic shift of $3e_1 + 12e_2 + 24$ when $r = 16k + 14$.

When $r = 4k + 3$:

$$\begin{array}{c} \begin{array}{ccccccc} \infty & 0 & 1 & \cdots & \cdots & \cdots & p-1 \end{array} \\ \begin{bmatrix} 0 & & & & & & \\ \vdots & & & & & & \\ \vdots & & & G_1' & & & \\ 0 & & & & & & \\ 9 & 9 & 9 & \cdots & \cdots & \cdots & 9 \end{bmatrix} \end{array},$$

where each row of G_1' is a cyclic shift of $5e_1+18e_2+12$ when $r=16k+3$, a cyclic shift of $29e_1+26e_2+28$ when $r=16k+7$, a cyclic shift of $21e_1+2e_2+12$ when $r=16k+11$ and a cyclic shift of $13e_1+10e_2+28$ when $r=16k+15$. We define $\widetilde{Q}_2$ similarly.

Theorem 5.9. *Suppose $p-1=8r$, and let Q_1, Q_2 be the $\mathbf{Z}_{32}$-QR codes in Theorem 5.4. 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 $\widetilde{Q}_1$.*

6. Automorphism group of the extended QR code over $\mathbf{Z}_{32}$.

Theorem 6.1. *Let G be the group generated by the following elements:*

$$\sigma : i \longrightarrow i+1 \pmod p, \quad \infty \to \infty;$$
$$\mu_a : i \longrightarrow ai \pmod p, \ \textit{for } a \in Q, \ \infty \to \infty;$$
$$\rho : i \longrightarrow -\frac{1}{i} \pmod p$$

followed by multiplication by $-\chi(i)$ for $i \neq 0, \infty$.

The action of ρ on 0 and ∞ is defined as follows.

(I) *$p+1=8r$. If $r=16k$, let*

$0 \longrightarrow \infty$ *followed by multiplication by* 1,
$\infty \longrightarrow 0$ *followed by multiplication by* 15.

If $r=16k+1$, let

$0 \longrightarrow \infty$ *followed by multiplication by* 21,
$\infty \longrightarrow 0$ *followed by multiplication by* 3.

If $r=16k+2$, let

$0 \longrightarrow \infty$ *followed by multiplication by* 25,
$\infty \longrightarrow 0$ *followed by multiplication by* 23.

If $r=16k+3$, let

$0 \longrightarrow \infty$ *followed by multiplication by* 13,
$\infty \longrightarrow 0$ *followed by multiplication by* 27.

If $r = 16k + 4$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 17,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 15.$$

If $r = 16k + 5$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 5,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 19.$$

If $r = 16k + 6$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 9,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 7.$$

If $r = 16k + 7$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 29,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 11.$$

If $r = 16k + 8$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 1,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 31.$$

If $r = 16k + 9$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 21,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 3.$$

If $r = 16k + 10$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 25,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 23.$$

If $r = 16k + 11$, *let*

$$0 \longrightarrow \infty \text{ followed by multiplication by } 13,$$
$$\infty \longrightarrow 0 \text{ followed by multiplication by } 27.$$

If $r = 16k + 12$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 17,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 15.$$

If $r = 16k + 13$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 5,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 19.$$

If $r = 16k + 14$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 9,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 7.$$

If $r = 16k + 15$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 29,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 11.$$

(II) $p - 1 = 8r$. *If* $r = 16k$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 1,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 1.$$

If $r = 16k + 1$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 3,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 11.$$

If $r = 16k + 2$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 23,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 7.$$

If $r = 16k + 3$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 27,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 19.$$

If $r = 16k + 4$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 15,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 15.$$

If $r = 16k + 5$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 19,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 27.$$

If $r = 16k + 6$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 7,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 23.$$

If $r = 16k + 7$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 11,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 3.$$

If $r = 16k + 8$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 31,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 31.$$

If $r = 16k + 9$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 3,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 11.$$

If $r = 16k + 10$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 29,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 7.$$

If $r = 16k + 11$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 27,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 19.$$

If $r = 16k + 12$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 15,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 15.$$

If $r = 16k + 13$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 19,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 27.$$

If $r = 16k + 14$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 7,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 23.$$

If $r = 16k + 15$, *let*

$$0 \longrightarrow \infty \textit{ followed by multiplication by } 11,$$
$$\infty \longrightarrow 0 \textit{ followed by multiplication by } 3.$$

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

Proof. 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.

By a similar proof as in Theorem 4.2, we can show that the extended code is also fixed by the map ρ. Here we just give the results of the action of ρ.

(I) $p + 1 = 8r$. When $r = 16k$,

$$r_0 = (0, 1 + e_2),$$
$$\rho(r_0) = 31r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 31r_0 + 31r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-/s} + 31r_0, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + r_\infty.$$

When $r = 16k + 1$,

$$r_0 = (0, 5 + 22e_1 + 19e_2),$$
$$\rho(r_0) = 3r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 3r_0 + 17r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 3r_0 + 18r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 29r_\infty.$$

When $r = 16k + 2$,

$$r_0 = (0, 9 + 20e_1 + 29e_2),$$
$$\rho(r_0) = 23r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 23r_0 + 11r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 23r_0 + 12r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 18r_0 + 9r_\infty.$$

When $r = 16k + 3$,

$$r_0 = (0, 13 + 26e_1 + 31e_2),$$
$$\rho(r_0) = 27r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 27r_0 + 13r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 27r_0 + 14r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 5r_\infty.$$

When $r = 16k + 4$,

$$r_0 = (0, 17 + 8e_1 + 25e_2),$$
$$\rho(r_0) = 15r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 15r_0 + 23r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 15r_0 + 24r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + 17r_\infty.$$

When $r = 16k + 5$,

$$r_0 = (0, 21 + 30e_1 + 11e_2),$$
$$\rho(r_0) = 19r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 19r_0 + 9r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 19r_0 + 10r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 13r_\infty.$$

When $r = 16k + 6$,

$$r_0 = (0, 25 + 28e_1 + 21e_2),$$
$$\rho(r_0) = 7r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 7r_0 + 3r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 7r_0 + 4r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 18r_0 + 25r_\infty.$$

When $r = 16k + 7$,

$$r_0 = (0, 29 + 2e_1 + 23e_2),$$
$$\rho(r_0) = 11r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 11r_0 + 5r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 11r_0 + 6r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 21r_\infty.$$

When $r = 16k + 8$,

$$r_0 = (0, 1 + 16e_1 + 17e_2),$$
$$\rho(r_0) = 31r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 31r_0 + 15r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 31r_0 + 16r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + r_\infty.$$

When $r = 16k + 9$,

$$r_0 = (0, 5 + 6e_1 + 3e_2),$$
$$\rho(r_0) = 3r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 3r_0 + r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 3r_0 + 2r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 29r_\infty.$$

When $r = 16k + 10$,

$$r_0 = (0, 9 + 4e_1 + 13e_2)$$
$$\rho(r_0) = 23r_0 + 31r_\infty \quad \rho(r_s) = 31r_{-1/s} + 23r_0 + 27r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 23r_0 + 28r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 18r_0 + 9r_\infty.$$

When $r = 16k + 11$,

$$r_0 = (0, 13 + 10e_1 + 15e_2),$$
$$\rho(r_0) = 27r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 27r_0 + 29r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 27r_0 + 30r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 5r_\infty.$$

When $r = 16k + 12$,

$$r_0 = (0, 17 + 24e_1 + 9e_2),$$
$$\rho(r_0) = 15r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 15r_0 + 7r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 15r_0 + 8r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + 17r_\infty.$$

When $r = 16k + 13$,

$$r_0 = (0, 21 + 14e_1 + 27e_2),$$
$$\rho(r_0) = 19r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 19r_0 + 25r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 19r_0 + 26r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 13r_\infty.$$

When $r = 16k + 14$,

$$\begin{gathered} r_0 = (0, 25 + 12e_1 + 5e_2), \\ \rho(r_0) = 7r_0 + 31r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 7r_0 + 19r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 7r_0 + 20r_\infty, \quad s \in N, \\ \rho(r_\infty) = 18r_0 + 25r_\infty. \end{gathered}$$

When $r = 16k + 15$,

$$\begin{gathered} r_0 = (0, 29 + 18e_1 + 7e_2), \\ \rho(r_0) = 11r_0 + 23r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 11r_0 + 21r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 11r_0 + 22r_\infty, \quad s \in N, \\ \rho(r_\infty) = 10r_0 + 21r_\infty. \end{gathered}$$

(II) $p - 1 = 8r$. When $r = 16k$,

$$\begin{gathered} r_0 = (0, 31e_2), \quad \rho(r_0) = r_0, \quad \rho(r_s) = 31r_{-1/s} + r_0, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + r_0 + r_\infty, \quad s \in N, \qquad \rho(r_\infty) = 30r_0 + 31r_\infty. \end{gathered}$$

When $r = 16k + 1$,

$$\begin{gathered} r_0 = (0, 4 + 25e_1 + 14e_2), \\ \rho(r_0) = 11r_0 + 20r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 11r_0 + 21r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 21r_0 + 22r_\infty, \quad s \in N, \\ \rho(r_\infty) = 10r_0 + 21r_\infty. \end{gathered}$$

When $r = 16k + 2$,

$$\begin{gathered} r_0 = (0, 8 + 27e_1 + 20e_2), \\ \rho(r_0) = 7r_0 + 8r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 7r_0 + 19r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 7r_0 + 20r_\infty, \quad s \in N, \\ \rho(r_\infty) = 18r_0 + 25r_\infty. \end{gathered}$$

When $r = 16k + 3$,

$$\begin{gathered} r_0 = (0, 12 + 5e_1 + 18e_2), \\ \rho(r_0) = 19r_0 + 28r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 19r_0 + 25r_\infty, \quad s \in Q, \\ \rho(r_s) = r_{-1/s} + 19r_0 + 26r_\infty, \quad s \in N, \\ \rho(r_\infty) = 26r_0 + 13r_\infty. \end{gathered}$$

When $r = 16k + 4$,

$$r_0 = (0, 16 + 23e_1 + 8e_2),$$
$$\rho(r_0) = 15r_0 + 16r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 15r_0 + 7r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 15r_0 + 8r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + 17r_\infty.$$

When $r = 16k + 5$,

$$r_0 = (0, 20 + 17e_1 + 22e_2),$$
$$\rho(r_0) = 27r_0 + 4r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 27r_0 + 29r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 27r_0 + 30r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 5r_\infty.$$

When $r = 16k + 6$,

$$r_0 = (0, 24 + 19e_1 + 28e_2),$$
$$\rho(r_0) = 23r_0 + 24r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 23r_0 + 27r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 23r_0 + 28r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 18r_0 + 9r_\infty.$$

When $r = 16k + 7$,

$$r_0 = (0, 28 + 29e_1 + 26e_2),$$
$$\rho(r_0) = 3r_0 + 12r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 3r_0 + r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 3r_0 + 2r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 29r_\infty.$$

When $r = 16k + 8$,

$$r_0 = (0, 15e_1 + 16e_2),$$
$$\rho(r_0) = 31r_0, \quad \rho(r_s) = 31r_{-1/s} + 31r_0 + 15r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 31r_0 + 16r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + r_\infty.$$

When $r = 16k + 9$,

$$r_0 = (0, 4 + 9e_1 + 30e_2),$$
$$\rho(r_0) = 11r_0 + 20r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 11r_0 + 5r_\infty, \quad s \in Q,$$
$$\rho(\gamma_s) = \gamma_{-1/s} + 11\gamma_0 + 6\gamma_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 21r_\infty.$$

When $r = 16k + 10$,

$$r_0 = (0, 8 + 11e_1 + 4e_2),$$
$$\rho(r_0) = 7r_0 + 8r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 7r_0 + 3r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 7r_0 + 4r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 18r_0 + 25r_\infty.$$

When $r = 16k + 11$,

$$r_0 = (0, 12 + 21e_1 + 2e_2),$$
$$\rho(r_0) = 19r_0 + 28r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 19r_0 + 9r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 19r_0 + 10r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 13r_\infty.$$

When $r = 16k + 12$,

$$r_0 = (0, 16 + 7e_1 + 24e_2),$$
$$\rho(r_0) = 15r_0 + 16r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 15r_0 + 23r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 15r_0 + 24r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 2r_0 + 17r_\infty.$$

When $r = 16k + 13$,

$$r_0 = (0, 20 + e_1 + 6e_2),$$
$$\rho(r_0) = 27r_0 + 4r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 27r_0 + 13r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 27r_0 + 14r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 10r_0 + 5r_\infty.$$

When $r = 16k + 14$,

$$r_0 = (0, 24 + 3e_1 + 12e_2),$$
$$\rho(r_0) = 23r_0 + 24r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 23r_0 + 11r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 23r_0 + 12r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 18r_0 + 9r_\infty.$$

When $r = 16k + 15$,

$$r_0 = (0, 28 + 13e_1 + 10e_2),$$
$$\rho(r_0) = 3r_0 + 12r_\infty, \quad \rho(r_s) = 31r_{-1/s} + 3r_0 + 17r_\infty, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 3r_0 + 18r_\infty, \quad s \in N,$$
$$\rho(r_\infty) = 26r_0 + 29r_\infty. \qquad \square$$

The following corollary is an immediate result of the fact that group G which appears in the above theorem is transitive; hence, all codes obtained from an extended $\mathbf{Z}_{32}$-QR code by puncturing must be equivalent.

Corollary 6.2. *The minimum (Hamming) weight vectors of a* $\mathbf{Z}_{32}$-QR $(p,(p+1)/2)$ *code are odd-like.*

Definition 6.3. The Lee weights of the elements count $\pm a$ as a for $1 \leq a \leq 15$; 16 as 16; and 0 as 0. The Lee weight of a vector is the sum of the Lee weights of its components.

Definition 6.4. The Euclidean weights of the elements count $\pm a$ as a^2 for $1 \leq a \leq 15$; 16 as 256; and 0 as 0. The Euclidean weight of a vector is the sum of the Euclidean weights of its components.

By direct computation using a computer, we have

Theorem 6.5. *The* $\mathbf{Z}_{32}$-QR $(7,4)$ *code of length* 7 *has minimum Lee weight* 7, *minimum Euclidean weight* 7, *and minimum Hamming weight* 3.

We define maps α and β_i, $i = 1, \ldots, 16$, from $\mathbf{Z}_{32}$ to $\mathbf{Z}_2$ by

c	$\alpha(c)$	$\beta_1(c)$	$\beta_2(c)$	$\beta_3(c)$	$\beta_4(c)$	$\beta_5(c)$	$\beta_6(c)$	$\beta_7(c)$
0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	1	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	1	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	1
11	1	0	0	0	0	0	1	1
12	0	0	0	0	0	1	1	1
13	1	0	0	0	1	1	1	1

c	$\alpha(c)$	$\beta_1(c)$	$\beta_2(c)$	$\beta_3(c)$	$\beta_4(c)$	$\beta_5(c)$	$\beta_6(c)$	$\beta_7(c)$
14	0	0	0	1	1	1	1	1
15	1	0	1	1	1	1	1	1
16	0	1	1	1	1	1	1	1
17	1	1	1	1	1	1	1	1
18	0	1	1	1	1	1	1	1
19	1	1	1	1	1	1	1	1
20	0	1	1	1	1	1	1	1
21	1	1	1	1	1	1	1	1
22	0	1	1	1	1	1	1	1
23	1	1	1	1	1	1	1	1
24	0	1	1	1	1	1	1	1
25	1	1	1	1	1	1	1	1
26	0	1	1	1	1	1	1	0
27	1	1	1	1	1	1	0	0
28	0	1	1	1	1	0	0	0
29	1	1	1	1	0	0	0	0
30	0	1	1	0	0	0	0	0
31	1	1	0	0	0	0	0	0

c	$\beta_8(c)$	$\beta_9(c)$	$\beta_{10}(c)$	$\beta_{11}(c)$	$\beta_{12}(c)$	$\beta_{13}(c)$	$\beta_{14}(c)$	$\beta_{15}(c)$	$\beta_{16}(c)$
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	0	1	1
3	0	0	0	0	0	0	1	1	1
4	0	0	0	0	0	1	1	1	1
5	0	0	0	0	1	1	1	1	1
6	0	0	0	1	1	1	1	1	1
7	0	0	1	1	1	1	1	1	1
8	0	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1
14	1	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1	1
16	1	1	1	1	1	1	1	1	1
17	1	1	1	1	1	1	1	1	0

c	$\beta_8(c)$	$\beta_9(c)$	$\beta_{10}(c)$	$\beta_{11}(c)$	$\beta_{12}(c)$	$\beta_{13}(c)$	$\beta_{14}(c)$	$\beta_{15}(c)$	$\beta_{16}(c)$
18	1	1	1	1	1	1	1	0	0
19	1	1	1	1	1	1	0	0	0
20	1	1	1	1	1	0	0	0	0
21	1	1	1	1	0	0	0	0	0
22	1	1	1	0	0	0	0	0	0
23	1	1	0	0	0	0	0	0	0
24	1	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0

and extend them in the obvious way to maps from $\mathbf{Z}_{32}^N$ to $\mathbf{Z}_2^N$. Then the Gray map $\phi : \mathbf{Z}_{32}^N \to \mathbf{Z}_2^{16N}$ is given by $\phi(c) = (\beta_1(c), \beta_2(c), \dots, \beta_{16}(c))$.

Note that $\alpha(c) + \beta_1(c) + \beta_2(c) + \cdots + \beta_{16}(c) = 0$ for all $c \in \mathbf{Z}_{32}$.

Observe that ϕ is a distance-preserving map or isometry from $\mathbf{Z}_{32}^N$ (Lee distance) to $\mathbf{Z}_2^{16N}$ (Hamming distance).

The weight distribution of the image of length 7 $\mathbf{Z}_{32}$-QR $(7,4)$ code under the Gray map is as follows.

i	A_i
$0, 112$	1
$7, 105$	2
$8, 9, 103, 104$	14
$13, 99$	56
$14, 98$	86
$15, 97$	42
$16, 96$	28
$17, 95$	154
$18, 94$	224
$19, 93$	252
$20, 92$	392
$21, 91$	478
$22, 90$	560

i	A_i
$23, 89$	686
$24, 88$	1190
$25, 87$	1442
$26, 86$	1666
$27, 85$	2016
$28, 84$	2312
$29, 83$	3136
$30, 82$	3990
$31, 81$	4704
$32, 80$	4984
$33, 79$	5978
$34, 78$	7042
$35, 77$	8346
$36, 76$	9800
$37, 75$	10696
$38, 74$	11970
$39, 73$	13202
$40, 72$	15176
$41, 71$	16674
$42, 70$	18482
$43, 69$	19754
$44, 68$	21000
$45, 67$	22736
$46, 66$	24416
$47, 65$	26656
$48, 64$	27587
$49, 63$	28618
$50, 62$	29218
$51, 61$	31010
$52, 60$	32032
$53, 59$	32592
$54, 58$	33418
$55, 57$	32900
56	33112

Since the symmetrized Lee weight enumerator of the $\mathbf{Z}_{32}$-QR $(7, 4)$ code of length 7 takes a few pages' length to write down, we omit it here.

Acknowledgments. We would like to thank Professor Margaret Bayer, the editor of this paper, who read the paper carefully and made a lot of suggestions to improve the presentation of our paper.

REFERENCES

1. A. Bonnecaze, P. Solé and A.R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), 366–h377.

2. Mei Hui Chiu, Yung Yu and Stephen S.-T. Yau, $\mathbf{Z}_8$*-cyclic codes and quadratic residue codes*, Adv. Appl. Math. **25** (2000), 12–33.

3. A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, *The* $\mathbf{Z}_4$*- linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

4. P. Kanwar, *Quadratic residue codes over the integers modulo* q^m, Contemp. Math. **259** (2000), 299-312.

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

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

7. F.J. MacWilliams and N.J.A. Sloane, *Theory of error–Correcting codes*, North-Holland, Amsterdam, 1978.

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

9. V. Pless, *Introduction to the theory of error-correcting codes*, Second edition, Wiley Interscience, 1989.

10. V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbf{Z}_4$, IEEE Trans. Inform. Theory **42** (1996), 1594–1600.

Department of Mathematics, National Cheng Kung University, Tainan, Taiwan, R.O.C.
Email address: loveinmath@yahoo.com.tw

Department of Mathematics, National Cheng Kung University, Tainan, Taiwan, R.O.C.
Email address: gwego@msn.com

University of Illinois at Chicago, 851 South Morgan Street, Chicago, IL 60607-7045
Email address: yau@uic.edu

Department of Mathematics, National Cheng Kung University, Tainan, Taiwan, R.O.C.
Email address: yungyu@mail.ncku.edu.tw