J. Korean Math. Soc. **46** (2009), No. 1, pp. 13–30

# QUADRATIC RESIDUE CODES OVER $\mathbb{Z}_9$

BIJAN TAERI

ABSTRACT. A subset of $n$ tuples of elements of $\mathbb{Z}_9$ is said to be a code over $\mathbb{Z}_9$ if it is a $\mathbb{Z}_9$-module. In this paper we consider an special family of cyclic codes over $\mathbb{Z}_9$, namely quadratic residue codes. We define these codes in term 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 finite fields.

## 1. Introduction

Let $R$ be a finite commutative ring with identity. A subset $C$ of $n$ tuples of elements of $R$ is called an $R$-code (code over $R$) if it is an $R$-module. Recall that a code $C$ over $R$ is called cyclic if cyclic shift of every element of $C$ is an element of $C$, or equivalently $C$ is an ideal of $R[x]/\langle x^n - 1\rangle$. Hammons, Kumar, Calderbank, Sloane, and Solé in a seminal paper [3], discuss the $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and other codes. The structure of cyclic $\mathbb{Z}_4$-codes is considered by Pless and Qian [10], and Pless, Solé, and Qian [9]. They found generator polynomials as well as idempotent generators for cyclic $\mathbb{Z}_4$-codes. They have also outlined the necessary and sufficient conditions for these codes to be self dual.

An interesting family of cyclic codes is quadratic residue codes. Quadratic residue codes firstly defined and investigated by Andrew Gleason. The minimum weights of many modest quadratic residue codes are quite high, making this class of codes promising. Pless and Qian [10] defined quadratic residue codes over $\mathbb{Z}_4$ in terms of their idempotent generators. They showed that these codes have many good properties which are analogous in many respect to properties of quadratic residue codes over finite fields. The same results were obtained for quadratic residue codes over $\mathbb{Z}_8$ (see [2]).

In this paper we consider $\mathbb{Z}_9$ and define quadratic residue codes over $\mathbb{Z}_9$. We prove that the results of [10] and [2] remain valid over $\mathbb{Z}_9$. Our method suggests that if one has the idempotent generators of quadratic residue codes

Received April 12, 2006.

2000 *Mathematics Subject Classification.* 11T71, 94B05, 94B15, 94B99.

*Key words and phrases.* cyclic codes, quadratic residue codes, extended codes, automorphism group of a code.

This research was in part supported by a grant from IPM (No. 83200032).

over $\mathbb{Z}_{q^m}$, one can obtain idempotents over $\mathbb{Z}_{q^{m+1}}$ and define quadratic residue codes over $\mathbb{Z}_{q^{m+1}}$. We show that these quadratic residue codes over $\mathbb{Z}_9$ have large automorphism group which will be useful in decoding these codes by using the permutation decoding methods described in [5, Chapter 16]. We also define a distance preserving map from $\mathbb{Z}_9^N$ (Lee distance) to $\mathbb{Z}_2^{4N}$ (Hamming distance).

Our notation and terminology are standard and can be found in [5]. Throughout the paper we will assume that $R$ is a finite commutative ring with identity. We begin with some elementary facts (see [2, pp. 14–15], where we can replace $\mathbb{Z}_{p^m}$ by $R$).

**Theorem 1.** *Let $e_1$, $e_2$ be idempotents of $R[x]/\langle x^n - 1\rangle$ and let $C_1 = \langle e_1\rangle$, $C_2 = \langle e_2\rangle$. Then $C_1 \cap C_2$ and $C_1 + C_2$ have idempotent generators $e_1e_2$ and $e_1 + e_2 - e_1e_2$, respectively.*

**Theorem 2.** *Let $e_1(x)$ be the idempotent generator of an $R$-cyclic code $C$. Then $1 - e(x^{-1})$ is the idempotent generator of the dual code $C^\perp$.*

Recall that $f, g \in R[x]$ are called coprime if $fu+gv = 1$ for some $u, v \in R[x]$. If $x^n - 1 = fg$, where $f$ and $g$ are coprime, then it is easy to see that $C = \langle f\rangle$ in $R[x]/\langle x^n - 1\rangle$ has an idempotent generator, namely $e = fu$, which is the identity of $C$ so it is unique (see [2, Theorem 2.0.1]). Let $e_i$, $i = 1, 2, \ldots, r$ be elements of $R$. If $e_ie_j = 0$ for all $i \neq j$, and $\sum_{i=1}^r e_i = 1$, we say that $e_i$, $i = 1, 2, \ldots, r$ are primitive idempotents. In this case $R$ is the direct sum of minimal ideals $Re_i$, $i = 1, 2, \ldots, r$ (see, for example, [6, p. 95]).

**Theorem 3.** *Let $S$ and $R$ be finite commutative rings with identity and characteristic $q^m$ and $q^{m+1}$, respectively, where $q$ is a prime. Let $f : R \longrightarrow S$ be an epimorphism, with $\ker f = q^m R$.*

(a) *If $f(e) = e_1$ is an idempotent of $S$. Then $e^q$ is an idempotent of $R$.*
(b) *If $e_i$, $i = 1, 2, \ldots, r$ are primitive idempotents of $S$, and $f(\theta_i) = e_i$, $i = 1, 2, \ldots, r$, then $\theta_i^q$, $i = 1, 2, \ldots, r$, are primitive idempotents of $R$.*

*Proof.* (a) Since $e_1^2 = e_1$, we have $e^2 - e \in \ker f$. Thus $e^2 - e = q^m b_1$ for some $b_1 \in R$. Therefore, since $q$ divides $\binom{q}{i}$, $1 \leq i \leq q-1$, and $q^{mi+1} \geq q^{m+1}$, $q^{mq} \geq q^{m+1}$, we have

$$\begin{aligned} e^{2q} &= (e + q^m b_1)^q \\ &= e^q + \sum_{i=1}^{q-1} \binom{q}{i} e^{q-i}(q^m b_1)^i + (q^m b_1)^q \\ &= e^q + \sum_{i=1}^{q-1} n_i q q^{mi} e^{q-i} b_1^i + q^{mq} b_1^q \quad (n_i \in \mathbb{N}) \\ &= e^q. \end{aligned}$$

(b) In $S$ we have $\sum_{i=1}^{r} e_i = 1$ and $e_i e_j = 0$, $i \neq j$. Thus $\sum_{i=1}^{r} \theta_i = 1 + q^m a_0$ and $\theta_i \theta_j = q^m b_0$ for some $a_0, b_0 \in R$. Now

$$\left(\sum_{i=1}^{r} \theta_i\right)^q = \sum_{i=1}^{r} \theta_i^q + qu,$$

where $u$ is the sum of terms containing a factor of the form $\theta_i \theta_j$. Thus, in $R$,

$$\begin{aligned}
\sum_{i=1}^{r} \theta_i^q &= (1 + q^m a_0)^q - q^{m+1} c_0 \quad (\text{where } c_0 \in R) \\
&= 1 + \sum_{i=1}^{q} \binom{q}{i} (q^m a_0)^i \\
&= 1 + \sum_{i=1}^{q} n_i q q^{mi} a_0^i \quad (\text{where } n_i \in \mathbb{N}) \\
&= 1 \quad (\text{since } q^{mi+1} \geq q^{m+1}).
\end{aligned}$$

Finally $\theta_i^q \theta_j^q = (\theta_i \theta_j)^q = (q^m b_0)^q = q^{mq} b_0^q = 0$, since $q^{mq} \geq q^{m+1}$. □

Let $R_j$, $j = 1, 2, \ldots, m+1$ be finite commutative rings with identity and characteristic $q^j$, where $q$ is prime. Let $f_j : R_{j+1} \longrightarrow R_j$, $j = 1, 2, \ldots, m$, be epimorphisms, with $\ker f_j = q^j R_{j+1}$. Suppose that $e_1$ is an idempotent of $R_1$. Since $f_1$ is epimorphism, there exists $e_2$ in $R_2$ such that $f_1(e_2) = e_1$. By Theorem 3, $e_2^q$ is an idempotent of $R_2$. Now since $f_2$ is epimorphism, there exists $e_3$ in $R_3$ such that $f(e_3) = e_2$. Thus $f_2(e_3^q) = e_2^q$ is an idempotent of $R_2$. So, by Theorem 3, $e_3^{q^2}$ is an idempotent of $R_3$. Continuing in this way we obtain elements $e_1, e_2, \ldots, e_{m+1}$ such that $f_j(e_{j+1}) = e_j$ such that $e_{j+1}^{q^j}$ is an idempotent of $R_j$. In particular $e_{m+1}^{q^m}$ is an idempotent of $R_m$.

Now suppose that $f_1(e_{12}) = e_{11}, f_1(e_{22}) = e_{21}, \ldots, f_1(e_{r2}) = e_{r1}$ are primitive elements of $R_1$. Then, by Theorem 3, $e_{12}^q, e_{22}^q, \ldots, e_{r2}^q$ are primitive elements of $R_2$. Now there exist elements $e_{i3}$, $i = 1, 2, \ldots, r$, such that $f_2(e_{i3}) = e_{i2}$. Thus $f_2(e_{i3}^q) = e_{i2}^q$, $i = 1, 2, \ldots, r$, are primitive elements of $R_2$ and so, by Theorem 3, $e_{i3}^{q^2}$, $i = 1, 2, \ldots, r$ are primitive elements of $R_3$. Continuing in this way we obtain elements $e_{1j}, e_{2j}, \ldots, e_{r,m+1}$ such that $f_j(e_{i,j+1}) = e_{ij}$ and $e_{1,j+1}^{q^j}, e_{2,j+1}^{q^j}, \ldots, e_{r,j+1}^{q^j}$ are primitive elements of $R_j$. In particular $e_{1,m+1}^{q^m}, e_{2,m+1}^{q^m}, \ldots, e_{r,m+1}^{q^m}$ are primitive elements of $R_m$.

Let $p$ and $q$ be primes and $m$ a positive integer. Put $R_m = \mathbb{Z}_{q^m}[x]/\langle x^p - 1 \rangle$. The epimorphism

$$\begin{aligned}
f_m : \mathbb{Z}_{q^{m+1}} &\longrightarrow \mathbb{Z}_{q^m} \\
a + \langle q^{m+1} \rangle &\mapsto a + \langle q^m \rangle
\end{aligned}$$

can be extended to an epimorphism $R_{m+1} \longrightarrow R_m$, which is again denoted by $f_m$. Thus if $e \in R_m$ is an idempotent of $R_m$ and viewed as an element of $R_{m+1}$,

then $e^q$ is an idempotent of $R_{m+1}$. In this paper we deal with some special idempotents of $\mathbb{Z}_9[x]/\langle x^p-1\rangle$, so if $e$ is an idempotent of $\mathbb{Z}_3[x]/\langle x^p-1\rangle$, then by Theorem 3, $e^3$ is an idempotent of $\mathbb{Z}_9[x]/\langle x^p-1\rangle$.

Let $Q$ be the set of quadratic residues and $N$ be the set of non-residues for $p$ (a prime). Let $e_1=\sum_{i\in Q}x^i$ and $e_2=\sum_{i\in N}x^i$. By [5, Problem (25), p. 520], 3 is quadratic residue (mod $p$) if and only if $p=12r\pm 1$. Therefore for considering quadratic residue codes over $\mathbb{Z}_3$ (and hence over $\mathbb{Z}_{3^m}$) we must assume that $p=12r\pm 1$. It is well known $2e_i$, $1+e_i$, $i=1,2$, are idempotents of $\mathbb{Z}_3[x]/\langle x^p-1\rangle$ (see [5, p. 486]). A $\mathbb{Z}_3$-cyclic code is a $\mathbb{Z}_3$-quadratic residue (QR) code if it is generated by one of the idempotents $2e_i$, $1+e_i$, $i=1,2$. If $p=12r-1$ put $Q_1=\langle 2e_1\rangle$, $Q_2=\langle 2e_2\rangle$, $Q_1'=\langle 1+e_2\rangle$ and $Q_2'=\langle 1+e_1\rangle$. If $p=12r+1$ put $Q_1=\langle 1+e_2\rangle$, $Q_2=\langle 1+e_1\rangle$, $Q_1'=\langle 2e_1\rangle$ and $Q_2'=\langle 2e_2\rangle$. Now, as we have seen, $(2e_i)^3$, $(1+e_i)^3$, $i=1,2$, are idempotents over $\mathbb{Z}_9[x]/\langle x^p-1\rangle$. In order to define quadratic residue codes over $\mathbb{Z}_9$ in terms of idempotent generators, we must compute these elements modulo 9. The following theorem is needed for such computations.

**Theorem 4** ([7], or [5, p. 519]). (i) *Suppose that $p=4k-1$ and $a$ is a number prime to $p$. Then in the set $a+(Q\cup\{0\})$, there are $k$ elements in $Q\cup\{0\}$ and $k$ elements in $N$. In the set $a+N$, there are $k$ elements in $Q\cup\{0\}$ and $k-1$ elements in $N$.*

(ii) *Suppose that $p=4k+1$ and $a$ is a number prime to $p$. Then in the set $a+(Q\cup\{0\})$, if $a\in Q$, there are $k+1$ elements in $Q\cup\{0\}$ (including 0) and $k$ elements in $N$; and if $a\in N$, there are $k$ elements in $Q$ and $k+1$ elements in $N$. In the set $a+N$, if $a\in Q$, there are $k$ elements in $Q$ and $k$ elements in $N$; and if $a\in N$, there are $k+1$ elements in $Q\cup\{0\}$ (including 0) and $k-1$ elements in $N$.*

By a routine application of Theorem 4, we obtain the following result.

**Theorem 5.** *If $p=4k-1$, then*

$$e_1^2=(k-1)e_1+ke_2,$$
$$e_2^2=ke_1+(k-1)e_2,$$
$$e_1e_2=(2k-1)+(k-1)e_1+(k-1)e_2.$$

*If $p=4k+1$, then*

$$e_1^2=(k-1)e_1+ke_2+2k,$$
$$e_2^2=ke_1+(k-1)e_2+2k,$$
$$e_1e_2=ke_1+ke_2.$$

By the above theorem and a little computations, when $p=4k-1$ we have

$$e_1^3=(3k^2-3k+1)e_1+2k(k-1)e_2+2k^2-k,$$
$$e_2^3=2k(k-1)e_1+(3k^2-3k+1)e_2+2k^2-k,$$

and when $p = 4k + 1$ we have

$$e_1^3 = (2k^2 + 1)e_1 + (2k^2 - k)e_2 + 2k^2 - 2k,$$
$$e_2^3 = (2k^2 - k)e_1 + (2k^2 + 1)e_2 + 2k^2 - 2k.$$

## 2. Quadratic residue codes over $\mathbb{Z}_9$

Throughout the paper we assume that $p$ is a prime and $h = 1 + e_1 + e_2$ is the all one vector. As mentioned in introduction, for considering quadratic residue codes over $\mathbb{Z}_3$ we must assume that $p = 12r \pm 1$. First of all we find idempotents of $\mathbb{Z}_9[x]/\langle x^p - 1\rangle$ from idempotent generators of quadratic residue codes over $\mathbb{Z}_3[x]/\langle x^p - 1\rangle$.

**Theorem 6. I.** *Suppose that* $p = 12r - 1$.

(a) *If* $r = 3k$, *then* $8e_i$, $1+e_i$, $8h$, $1+2h$ *are idempotents over* $\mathbb{Z}_9/\langle x^p - 1\rangle$, *where* $i = 1, 2$.

(b) *If* $r = 3k+1$, *then* $3+6e_i+8e_j$, $7+e_i+3e_j$, $5h$, $1+5h$ *are idempotents over* $\mathbb{Z}_9/\langle x^p - 1\rangle$, *where* $1 \le i \ne j \le 2$.

(c) *If* $r = 3k+2$, *then* $6+3e_i+8e_j$, $4+e_i+6e_j$, $2h$, $8+8h$ *are idempotents over* $\mathbb{Z}_9/\langle x^p - 1\rangle$, *where* $1 \le i \ne j \le 2$.

**II.** *Let* $p = 12r + 1$.

(a) *If* $r = 3k$, *then* $1 + e_i$, $8e_i$, $h$, $1 + h$ *are idempotents over* $\mathbb{Z}_9/\langle x^p - 1\rangle$, *where* $i = 1, 2$.

(b) *If* $r = 3k+1$, *then* $4+e_i+6e_j$, $6+3e_i+8e_j$, $7h$, $1+2h$ *are idempotents over* $\mathbb{Z}_9/\langle x^p - 1\rangle$, *where* $1 \le i \ne j \le 2$.

(c) *If* $r = 3k+2$, *then* $7+e_i+3e_j$, $3+6e_i+8e_j$, $4h$, $1+5h$ *are idempotents over* $\mathbb{Z}_9/\langle x^p - 1\rangle$, *where* $1 \le i \ne j \le 2$.

*Proof.* **I.** Let $p = 12r - 1$. Since $2e_1$ is an idempotent of $\mathbb{Z}_3[x]/\langle x^p - 1\rangle$, $(2e_1)^3$ is an idempotent $\mathbb{Z}_9[x]/\langle x^p - 1\rangle$. By Theorem 5, in $\mathbb{Z}_9[x]/\langle x^p - 1\rangle$ we have

$$\begin{aligned}
(2e_1)^3 &= 8e_1^3 \\
&= -[(18r^2 - 9r + 1)e_1 + 6r(3r - 1)e_2 + 18r^2 - 3r] \\
&= 3r + 8e_1 + 6re_2 \\
&= \begin{cases} 8e_1 & r = 3k \\ 3 + 8e_1 + 6e_2 & r = 3k + 1 \\ 6 + 8e_1 + 3e_2 & r = 3k + 2. \end{cases}
\end{aligned}$$

Similarly,

$$\begin{aligned}
(1 + e_1)^3 &= 1 + 3e_1 + 3e_1^2 + e_1^3 \\
&= 1 + 3e_1 + 3[(3r - 1)e_1 + 3re_2] + [e_1 - 6re_2 - 3r] \\
&= 1 - 3r + e_1 - 6re_2 \\
&= \begin{cases} 1 + e_1 & r = 3k \\ 7 + e_1 + 3e_2 & r = 3k + 1 \\ 4 + e_1 + 6e_2 & r = 3k + 2. \end{cases}
\end{aligned}$$

Other cases are proved similarly. □

A $\mathbb{Z}_9$-cyclic code is called a $\mathbb{Z}_9$-quadratic residue (QR) code if it is generated by one of the idempotents in the above theorem. Let $a$ be a nonzero element of $\mathbb{Z}_p$. The map $\mu_a$ is defined as $\mu_a(i) = ai \pmod p$. It is easy to see that $\mu_a(fg) = \mu_a(f)\mu_a(g)$ for polynomials $f$ and $g$ in $\mathbb{Z}_9[x]/\langle x^p - 1\rangle$. In the following theorem we investigate some properties of QR-codes over $\mathbb{Z}_9$.

**Theorem 7.** *Suppose that $p = 12r - 1$. If $r = 3k$, let $Q_1 = \langle 8e_1\rangle$, $Q_2 = \langle 8e_2\rangle$ and $Q_1' = \langle 1 + e_2\rangle$, $Q_2' = \langle 1 + e_1\rangle$. If $r = 3k + 1$, let $Q_1 = \langle 3 + 6e_1 + 8e_2\rangle$, $Q_2 = \langle 3 + 8e_1 + 6e_2\rangle$ and $Q_1' = \langle 7 + e_1 + 3e_2\rangle$, $Q_2' = \langle 7 + 3e_1 + e_2\rangle$. If $r = 3k + 2$, let $Q_1 = \langle 6 + 3e_1 + 8e_2\rangle$, $Q_2 = \langle 6 + 8e_1 + 3e_2\rangle$ and $Q_1' = \langle 4 + e_1 + 6e_2\rangle$, $Q_2' = \langle 4 + 6e_1 + e_2\rangle$. Then the following hold for $\mathbb{Z}_9$-QR codes $Q_1$, $Q_2$, $Q_1'$, $Q_2'$ :*

(a) *$Q_1$ and $Q_2$ are equivalent and $Q_1'$ and $Q_2'$ are equivalent;*
(b) *$Q_1 \cap Q_2 = \langle \widetilde{h}\rangle$ and $Q_1 + Q_2 = \mathbb{Z}_9[x]/\langle x^p - 1\rangle$, where $\widetilde{h}$ is a suitable element in $\{8h, 5h, 2h\}$ listed in the Theorem 6;*
(c) *$|Q_1| = 9^{(p+1)/2} = |Q_2|$;*
(d) *$Q_1 = Q_1' + \langle \widetilde{h}\rangle$, $Q_2 = Q_2' + \langle \widetilde{h}\rangle$;*
(e) *$|Q_1'| = 9^{(p-1)/2} = |Q_2'|$;*
(f) *$Q_1'$ and $Q_2'$ are self-orthogonal and $Q_1^{\perp} = Q_1'$ and $Q_2^{\perp} = Q_2'$;*
(g) *$Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = \langle 1 - \widetilde{h}\rangle$; also $Q_i' \cap Q_j' = \{0\}$ and $Q_i' + Q_j' = \mathbb{Z}_9[x]/\langle x^p - 1\rangle$, where $1 \le i \ne j \le 2$.*

*Proof.* Since $p = 4(3r) - 1$, $-1 \in N$, by [8, Theorem 65]. We prove the case $r = 3k + 2$. The proof of other cases are similar.

(a) Let $a$ be an element of $N$. Then $\mu_a e_1 = e_2$ and $\mu_a e_2 = e_1$. Thus $\mu_a\langle 6 + 3e_1 + 8e_2\rangle = \langle 6 + 8e_1 + 3e_2\rangle$ and $\mu_a\langle 4 + 6e_1 + e_2\rangle = \langle 4 + e_1 + 6e_2\rangle$.

(b) Since $(6 + 3e_1 + 8e_2) + (6 + 8e_1 + 3e_2) = 1 + 2h$, we have

$$\begin{aligned} & (6 + 3e_1 + 8e_2)(5h) \\ = \ & (6 + 3e_1 + 8e_2)[8 + (6 + 3e_1 + 8e_2) + (6 + 8e_1 + 3e_2)] \\ = \ & 8(6 + 3e_1 + 8e_2) + (6 + 3e_1 + 8e_2)^2 + (6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2) \\ = \ & (6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2). \end{aligned}$$

Now since $p = 12(3k + 2) - 1 = 36k + 23$ and $\frac{p-1}{2} \equiv 2 \bmod 9$, we have

$$(6+3e_1+8e_2)(2h) = 6(2h)+3\frac{p-1}{2}(2h)+8\frac{p-1}{2}(2h) = (6+2\frac{p-1}{2})(2h) = 2h.$$

Therefore $(6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2) = 2h$. By Theorem 1, $Q_1 \cap Q_2$ has idempotent generator $2h$. Hence

$$|Q_1 \cap Q_2| = |\langle 2h\rangle| = 9.$$

Also, by Theorem 1, $Q_1 + Q_2$ has idempotent generator

$$(6 + 3e_1 + 8e_2) + (6 + 8e_1 + 3e_2) - (6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2)$$
$$= 3 + 2e_1 + 2e_2 - (2 + 2e_1 + 2e_2) = 1.$$

Thus $Q_1 + Q_2 = \mathbb{Z}_9[x]/\langle x^p - 1\rangle$.

(c) By (a) and (b) we have

$$9^p = |Q_1 + Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{9},$$

so $|Q_1| = |Q_2| = 9^{(p+1)/2}$.

(d) By Theorem 1, $Q_1' \cap \langle 2h\rangle$ has idempotent generator

$$(4 + 6e_1 + e_2)(2h) = 4(2h) + 6\frac{p-1}{2}(2h) + \frac{p-1}{2}(2h) = (4 + 7\frac{p-1}{2})(2h) = 0.$$

Thus $Q_1' \cap \langle 2h\rangle = \{0\}$. By Theorem 1, $Q_1' + \langle 2h\rangle$ has idempotent generator $(4 + 6e_1 + e_2) + 2h - (4 + 6e_1 + e_2)(2h) = 6 + 8e_1 + 3e_2$. Hence

$$Q_1' + \langle 2h\rangle = \langle 6 + 8e_1 + 3e_2\rangle = Q_1.$$

Similarly $Q_2' + \langle 2h\rangle = Q_2$.

(e) $9^{(p+1)/2} = |Q_1| = |Q_1' + \langle 2h\rangle| = |Q_1'||\langle 2h\rangle| = 9|Q_1'|$. Thus $|Q_1'| = 9^{(p-1)/2}$.

(f) By Theorem 2 and the fact that $-1 \in N$, $Q_1^\perp$ has idempotent generator

$$1 - [6 + 3e_1(x^{-1}) + 8e_2(x^{-1})] = 4 + 6e_1(x^{-1}) + e_2(x^{-1}) = 4 + e_1 + 6e_2.$$

Hence $Q_1^\perp = Q_1'$. Similarly $Q_2^\perp = Q_2'$. By (d), $Q_1 \subseteq Q_2' = Q_1^\perp$ and $Q_1 \subseteq Q_2' = Q_1^\perp$, so $Q_1$ and $Q_2$ are self-orthogonal.

(g) Since $(4 + e_1 + 6e_2) + (4 + 6e_1 + e_2) = 1 + 7h$, we have

$$\begin{aligned} & (4 + e_1 + 6e_2)(7h) \\ = \; & (4 + e_1 + 6e_2)[8 + (4 + e_1 + 6e_2) + (4 + 6e_1 + e_2)] \\ = \; & 8(4 + e_1 + 6e_2) + (4 + e_1 + 6e_2)^2 + (4 + e_1 + 6e_2)(4 + 6e_1 + e_2) \\ = \; & (4 + e_1 + 6e_2)(4 + 6e_1 + e_2). \end{aligned}$$

Now since $\frac{p-1}{2} \equiv 2 \bmod 9$, we have

$$(4 + e_1 + 6e_2)(7h) = 4(7h) + \frac{p-1}{2}(7h) + 6\frac{p-1}{2}(7h) = (4 + 7\frac{p-1}{2})(2h) = 0.$$

Therefore $(6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2) = 0$. By Theorem 1, $Q_1' \cap Q_2' = \{0\}$, and $Q_1' + Q_2'$ has idempotent generator $(4 + e_1 + 6e_2) + (4 + 6e_1 + e_2) = 1 + 7h$, so $Q_1' + Q_2' = \langle 1 + 7h\rangle$. □

**Theorem 8.** *Let $p = 12r + 1$ be a prime. If $r = 3k$, let $Q_1 = \langle 1 + e_1\rangle$, $Q_2 = \langle 1 + e_2\rangle$ and $Q_1' = \langle 8e_2\rangle$, $Q_2' = \langle 8e_1\rangle$. If $r = 3k+1$, let $Q_1 = \langle 4 + e_1 + 6e_2\rangle$, $Q_2 = \langle 4 + 6e_1 + e_2\rangle$ and $Q_1' = \langle 6 + 3e_1 + 8e_2\rangle$, $Q_2' = \langle 6 + 8e_1 + 3e_2\rangle$. If $r = 3k+2$, let $Q_1 = \langle 7 + e_1 + 3e_2\rangle$, $Q_1 = \langle 7 + 3e_2 + e_1\rangle$ and $Q_1' = \langle 3 + 6e_1 + 8e_2\rangle$, $Q_2' = \langle 3 + 8e_1 + 6e_2\rangle$. Then the following hold for $\mathbb{Z}_9$-QR codes $Q_1$, $Q_2$, $Q_1'$, $Q_2'$:*

(a) $Q_1$ *and* $Q_2$ *are equivalent and* $Q_1'$ *and* $Q_2'$ *are equivalent;*
(b) $Q_1 \cap Q_2 = \langle \widetilde{h} \rangle$ *and* $Q_1 + Q_2 = \mathbb{Z}_9[x]/\langle x^p - 1 \rangle$, *where* $\widetilde{h}$ *is a suitable element in* $\{h, 4h, 7h\}$ *listed in the Theorem* 6;
(c) $|Q_1| = 9^{(p+1)/2} = |Q_2|$;
(d) $Q_1 = Q_1' + \langle \widetilde{h} \rangle$, $Q_2 = Q_2' + \langle \widetilde{h} \rangle$;
(e) $|Q_1'| = 9^{(p-1)/2} = |Q_2'|$;
(f) $Q_1^{\perp} = Q_2'$ *and* $Q_2^{\perp} = Q_1'$;
(g) $Q_1' \cap Q_2' = \{0\}$ *and* $Q_1' + Q_2' = \langle 1 - \widetilde{h} \rangle$; *also* $Q_i' \cap Q_j' = \{0\}$ *and* $Q_i' + Q_j' = \langle u \rangle$, *where* $1 \leq i \neq j \leq 2$, *and* $u$ *is a suitable element of* $\{1 + 2h, 1 + 5h, 1 + h\}$ *listed in the Theorem* 6.

*Proof.* We prove the case $r = 3k + 1$. The proof of other cases are similar.

(a) Let $a$ be an element of $N$. Then $\mu_a e_1 = e_2$ and $\mu_a e_2 = e_1$. Thus $\mu_a\langle 4 + 6e_1 + e_2 \rangle = \langle 4 + e_1 + 6e_2 \rangle$ and $\mu_a\langle 3 + 8e_1 + 6e_2 \rangle = \langle 3 + 6e_1 + 8e_2 \rangle$.

(b) Since $(4 + 6e_1 + e_2) + (4 + e_1 + 6e_2) = 1 + 7h$, we have

$$\begin{aligned} & (4 + 6e_1 + e_2)(7h) \\ = \; & (4 + 6e_1 + e_2)[8 + (4 + 6e_1 + e_2) + (4 + e_1 + 6e_2)] \\ = \; & 8(4 + 6e_1 + e_2) + (4 + 6e_1 + e_2)^2 + (4 + 6e_1 + e_2)(4 + e_1 + 6e_2) \\ = \; & (4 + 6e_1 + e_2)(4 + e_1 + 6e_2). \end{aligned}$$

Now since $p = 12(3k + 1) + 1 = 36k + 13$ and $\frac{p-1}{2} \equiv 6 \bmod 9$, we have

$$(4 + 6e_1 + e_2)(7h) = 4(7h) + 6\frac{p-1}{2}(7h) + \frac{p-1}{2}(7h) = (4 + 7\frac{p-1}{2})(7h) = 7h.$$

Therefore $(4 + 6e_1 + e_2)(4 + e_1 + 6e_2) = 7h$. By Theorem 1, $Q_1 \cap Q_2$ has idempotent generator $7h$. Hence

$$|Q_1 \cap Q_2| = |\langle 7h \rangle| = 9.$$

Also, by Theorem 1, $Q_1 + Q_2$ has idempotent generator

$$\begin{aligned} & (4 + 6e_1 + e_2) + (4 + e_1 + 6e_2) - (4 + 6e_1 + e_2)(4 + e_1 + 6e_2) \\ = \; & 8 + 7e_1 + 7e_2 - (7 + 7e_1 + 7e_2) = 1. \end{aligned}$$

Thus $Q_1 + Q_2 = \mathbb{Z}_9[x]/\langle x^p - 1 \rangle$.

(c) By (a) and (b) we have

$$9^p = |Q_1 + Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{9},$$

so $|Q_1| = |Q_2| = 9^{(p+1)/2}$.

(d) By Theorem 1, $Q_1' \cap \langle 7h \rangle$ has idempotent generator

$$(6 + 3e_1 + 8e_2)(7h) = 6(7h) + 3\frac{p-1}{2}(7h) + 8\frac{p-1}{2}(7h) = (6 + 2\frac{p-1}{2})(7h) = 0.$$

Thus $Q_1' \cap \langle 7h \rangle = \{0\}$. By Theorem 1, $Q_1' + \langle 7h \rangle$ has idempotent generator $(6 + 3e_1 + 8e_2) + 7h - (6 + 3e_1 + 8e_2)(7h) = 4 + e_1 + 6e_2$. Hence

$$Q_1' + \langle 7h \rangle = \langle 4 + e_1 + 6e_2 \rangle = Q_1.$$

Similarly $Q_2' + \langle 7h \rangle = Q_2$.

(e) $9^{(p+1)/2} = |Q_1| = |Q_1' + \langle 7h \rangle| = |Q_1'||\langle 7h \rangle| = 9|Q_1'|$. Thus $|Q_1'| = 9^{(p-1)/2}$.

(f) By Theorem 2 and the fact that $-1 \in Q$, $Q_1^{\perp}$ has idempotent generator

$$1 - [4 + e_1(x^{-1}) + 6e_2(x^{-1})] = 6 + 8e_1(x^{-1}) + 3e_2(x^{-1}) = 6 + 8e_1 + 3e_2.$$

Hence $Q_1^{\perp} = Q_2'$.

(g) Since $(6 + 3e_1 + 8e_2) + (6 + 8e_1 + 3e_2) = 1 + 2h$, we have

$$\begin{aligned} & (6 + 3e_1 + 8e_2)(2h) \\ = \; & (6 + 3e_1 + 8e_2)[8 + (6 + 3e_1 + 8e_2) + (6 + 8e_1 + 3e_2)] \\ = \; & 8(6 + 3e_1 + 8e_2) + (6 + 3e_1 + 8e_2)^2 + (6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2) \\ = \; & (6 + 3e_1 + 8e_2)(6 + 8e_1 + 3e_2). \end{aligned}$$

Now since $\frac{p-1}{2} \equiv 6 \bmod 9$, we have

$$(6+3e_1+8e_2)(2h) = 6(2h)+3\frac{p-1}{2}(2h)+8\frac{p-1}{2}(2h) = (6+11\frac{p-1}{2})(2h) = 0.$$

Therefore $(6+3e_1+8e_2)(6+8e_1+3e_2) = 0$. By Theorem 1, $Q_1' \cap Q_2' = \{0\}$, and $Q_1' + Q_2'$ has idempotent generator $(6+3e_1+8e_2)+(6+8e_1+3e_2) = 1+2h$. □

The extended code of an $R$ code $C$ will be denoted by $\overline{C}$, which is the code obtained by adding an overall parity check to each codeword of $C$.

**Theorem 9.** *Suppose $p = 12r - 1$ and $Q_1$, $Q_2$ are the $\mathbb{Z}_9$-QR codes in Theorem 7. Then $\overline{Q}_1$ and $\overline{Q}_2$ are self-dual.*

*Proof.* We prove the case $p = 3k + 2$. The proof of other cases are similar. We know, by Theorem 7, that $Q_1 = Q_1' + \langle 2h \rangle$, and $\overline{Q}_1$ has the $\frac{p+1}{2} \times (p+1)$ generator matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \dots & p-1 \\ 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 8 & 2 & 2 & 2 & \dots & 2 \end{pmatrix},$$

where each row of $G_1'$ is a cyclic shift of the vector $4 + e_1 + 6e_2$. We know that $G_1'$ generates $Q_1'$. Since $Q_1'$ is self-orthogonal (Theorem 7(f)), the rows of $G_1'$ are orthogonal to each other and obviously also orthogonal to $2h$. Since the vector $(8, 2h)$ is orthogonal to itself and $|\overline{Q}_1| = |Q_1| = 9^{(p+1)/2}$, 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. □

When $p = 12r + 1$, we define $\widetilde{Q}_1$ to be the $\mathbb{Z}_9$-code generated by the matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \dots & p-1 \\ 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 1 & 1 & 1 & 1 & \dots & 1 \end{pmatrix},$$

where each row of $G_1'$ is a cyclic shift of $8e_1$ when $r = 3k$, a cyclic shift of $6 + 3e_1 + 8e_2$ when $r = 3k + 1$, a cyclic shift of $3 + 6e_1 + 8e_2$ when $r = 3k + 2$. We define $\widetilde{Q}_2$ similarly. Note that these are not extended codes of $Q_1$ and $Q_2$, since the sum of the components of the all one vector is not 0 (mod 9).

**Theorem 10.** *Suppose $p = 12r + 1$ and $Q_1$, $Q_2$ are the $\mathbb{Z}_9$-QR codes in Theorem 8. 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 $p = 3k + 2$. The proof of other cases are similar. In this case, since $Q_1 = Q_1' + \langle 4h \rangle$ (Theorem 8(d)), $\overline{Q}_1$ has the $\frac{p+1}{2} \times (p + 1)$ generator matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \dots & p-1 \\ 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 8 & 4 & 4 & 4 & \dots & 4 \end{pmatrix},$$

where each row of $G_1'$ is a cyclic shift of the vector $3 + 6e_1 + 8e_2$. Since $G_1'$ generates $Q_1'$ and $Q_2^{\perp} = Q_1'$, by Theorem 8(f), any row in the above matrix is orthogonal to any row in the matrix which defines $\widetilde{Q}_2$. By comparing the order of the dual of $\overline{Q}_1$ and the order of $\widetilde{Q}_2$, we find that $\overline{Q}_1^{\perp} = \widetilde{Q}_2$. □

For $p = 12r \pm 1$, the extended codes $\overline{Q}_1$ and $\overline{Q}_2$ are equivalent, since $Q_1$ and $Q_2$ are equivalent. They are also equivalent to $\overline{Q}_1^{\perp}$ and $\overline{Q}_2^{\perp}$. Therefore the group of extended codes, which will investigated in the next section, is the group of either one of the extended codes.

## 3. Extended quadratic residue codes over $\mathbb{Z}_9$

Let $a \in Q$. Define permutations $\sigma$ and $\mu_a$ on $\{\infty, 0, 1, \dots, p-1\}$ by

$$\sigma : i \mapsto i + 1 \bmod p, \qquad \infty \mapsto \infty;$$
$$\mu_a : i \mapsto ai \bmod p, \qquad \infty \mapsto \infty.$$

Clearly, the extended $QR$-codes are fixed by $\sigma$ and $\mu_a$. So the group generated by $\sigma$ and $\mu_a$, $a \in Q$, is contained in the group of extended $QR$-codes. Let $\chi$ be

the Legendre symbol on $GF(p)$ which is defined by

$$\chi(i) = \begin{cases} 1 & i \in Q \\ -1 & i \in N \\ 0 & \text{otherwise.} \end{cases}$$

Now we define a permutation $\rho$ on extended quadratic residue codes as follows:

$$\rho : i \mapsto -\frac{1}{i} \bmod p, \quad \text{followed by multiplication by } -\chi(i),$$

that is, $\rho : x^i \mapsto -\chi(i)x^{-1/i}$, and when $p = 12r - 1$,

| | | | |
|---|---|---|---|
| $r = 3k$ | $\infty \mapsto 0$ | followed by multiplication by | 8 |
| $r = 3k$ | $0 \mapsto \infty$ | followed by multiplication by | 1 |
| $r = 3k + 1$ | $\infty \mapsto 0$ | followed by multiplication by | 7 |
| $r = 3k + 1$ | $0 \mapsto \infty$ | followed by multiplication by | 2 |
| $r = 3k + 2$ | $\infty \mapsto 0$ | followed by multiplication by | 4 |
| $r = 3k + 2$ | $0 \mapsto \infty$ | followed by multiplication by | 5, |

and when $p = 12r + 1$,

| | | | |
|---|---|---|---|
| $r = 3k$ | $\infty \mapsto 0$ | followed by multiplication by | 1 |
| $r = 3k$ | $0 \mapsto \infty$ | followed by multiplication by | 8 |
| $r = 3k + 1$ | $\infty \mapsto 0$ | followed by multiplication by | 4 |
| $r = 3k + 1$ | $0 \mapsto \infty$ | followed by multiplication by | 5 |
| $r = 3k + 2$ | $\infty \mapsto 0$ | followed by multiplication by | 7 |
| $r = 3k + 2$ | $0 \mapsto \infty$ | followed by multiplication by | 2. |

Let $G$ be the group generated by elements $\sigma$, $\rho$, $\mu_a$, $a \in Q$. Note that when $p = 12r - 1$, $G/(\pm I) \simeq PSL_2(p)$, and when $p = 12r - 1$, $G \simeq PSL_2(p)$. In the following theorem we prove that $G$ is contained in the group of the extended $QR$-code.

**Theorem 11.** *Let $G$ be as above. Then $G$ is contained in the group of the extended $QR$-code.*

*Proof.* Suppose that $p = 12r - 1$ and $r = 3k + 1$.

Since $p = 4(3r) - 1$, $-1 \in N$, by [8, Theorem 65]. Since $Q_1 = Q_1' + \langle 5h \rangle$, (Theorem 7(d)), the extended code $\overline{Q}_1$ is generated by $\frac{p+1}{2}$ rows of the $(p + 1) \times (p + 1)$ matrix

$$\begin{array}{c} r_0 \\ . \\ \vdots \\ \vdots \\ r_\infty \end{array} \begin{pmatrix} 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ & & & & & \\ 8 & 5 & 5 & 5 & \cdots & 5 \end{pmatrix},$$

where each row of $G_1'$ is a cyclic shift of the vector $7 + e_1 + 3e_2$. Since $-1$ is a nonresidue, $\rho(e_1) = -e_2$ and $\rho(e_2) = e_1$.

By definition of $\rho$ we have $x^0 \mapsto 2x_\infty$ and $x_\infty \mapsto 5x^0$. Now $r_0 = (0, 7 + e_1 + 3e_2)$ and so

$$\rho(r_0) = (2 \cdot 7, 5 \cdot 0 - e_2 + 3e_1) = (5, 3e_1 + 8e_2) = 7r_0 + 5h \in \overline{Q}_1,$$

where $h$ is the all one vector of length $p+1$, i.e., $h = (1, 1 + e_1 + e_2)$. Since $r_\infty = (8, 5 + 5e_1 + 5e_2)$, we have $\rho(r_\infty) = (2 \cdot 5, 7 \cdot 8 - 5e_2 + 5e_1) = (1, 2 + 5e_1 + 4e_2) = 4r_0 + h \in \overline{Q}_1$. Now we prove that $\rho(r_s) \in \overline{Q}_1$. In all the following proofs we let $q \in Q$ and $n \in N$. We have

$$\begin{aligned} r_s &= \left(0, 7x^s + \sum x^{q+s} + 3\sum x^{n+s}\right) \\ r_{-1/s} &= \left(0, 7x^{-1/s} + \sum x^{q-1/s} + 3\sum x^{n-1/s}\right). \end{aligned}$$

We consider two cases $s \in Q$ and $s \in N$:

**Case 1.** $s \in Q$. We have $\rho(r_s) = (2 \cdot 3, -7\chi(s)x^{-1/s} - \sum \chi(q+s)x^{-1/(q+s)} - 3\sum \chi(n+s)x^{-1/(n+s)})$. Since $-1 \in N$ and $s \in Q$, $0 \in s + N$, the $\infty$ position of $\rho(r_s)$ is $2 \cdot 3 = 6$. We show that $\rho(r_s) = 8r_{-1/s} + 7r_0 + 3r_\infty$. Since $-1 \in N$ and $s \in Q$, the nonresidue position of $\rho(r_s) + r_{-1/s}$ is:

$$\begin{aligned} &-7x^{-1/s} - \sum_{q+s\in Q} x^{-1/(q+s)} - 3\sum_{n+s\in Q} x^{-1/(n+s)} \\ &+7x^{-1/s} + \sum_{q-1/s\in N} x^{q-1/s} + 3\sum_{n-1/s\in N} x^{n-1/s}. \end{aligned}$$

By Theorem 4, the set $s+Q$ has $3r-1$ elements in $Q$, $3r$ elements in $N$. Thus, since $-1 \in N$, the set $\{-1/(q+s)\}$ has $3r-1$ elements in $N$ and $3r$ elements in $Q$. Similarly the set $\{-1/(n+s), n+s \neq 0\}$ has $3r-1$ elements in $N$ and $3r-1$ elements in $Q$; the set $-1/s + Q$ has $3r-1$ elements in $N$ and $3r-1$ elements in $Q$, and one element is 0; the set $-1/s + N$ has $3r-1$ elements in $N$ and $3r$ elements in $Q$.

Also 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 a $n' \in N$ such that $-1/(n+s) = n' - 1/s$, the nonresidue position is equal to

$$-\sum_{q'-1/s\in N} x^{q'-1/s} - 3\sum_{n'-1/s\in N} x^{n'-1/s} + \sum_{q-1/s\in N} x^{q-1/s} + 3\sum_{n-1/s\in N} x^{n-1/s} = 0.$$

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

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

Since for any $-1/(q+s) \in Q$, there is a $n' \in N$ such that $-1/(q+s) = n' - 1/s$ and for any $-1/(n+s) \in Q$, there is a $q' \in Q$ such that $-1/(n+s) = q' - 1/s$, there are $3r + 3r - 1 = 6r - 1$ terms appearing, so the residue position is equal

to

$$\sum_{n'-1/s\in Q} x^{q'-1/s}+3\sum_{q'-1/s\in Q} x^{n'-1/s}+\sum_{q-1/s\in Q} x^{q-1/s}+3\sum_{n-1/s\in Q} x^{n-1/s}=4e_1.$$

Thus, since $0\in -1/s+Q$, we have

$$\rho(r_s)+r_{-1/s}=(6,1+4e_1)=7r_0+3r_\infty;$$

that is, $\rho(r_s)=8r_{-1/s}+7r_0+5h$.

**Case 2.** $s\in N$. We have $\rho(r_s)=(2\cdot 1,-7\chi(s)x^{-1/s}-\sum\chi(q+s)x^{-1/(q+s)}-3\sum\chi(n+s)x^{-1/(n+s)})$. Since $0\in s+Q$, the $\infty$ position of $\rho(r_s)$ is $2\cdot 1=2$. We show that $\rho(r_s)=r_{-1/s}+7r_0+3h$. Since $-1\in N$ and $s\in N$, the residue position of $\rho(r_s)-r_{-1/s}$ is

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

By Theorem 4, the set $s+Q$ has $3r-1$ elements in $Q$, $3r-1$ elements in $N$ and one element is 0. Thus the set $\{-1/(q+s), q+s\neq 0\}$ has $3r-1$ elements in $N$ and $3r-1$ elements in $Q$. Similarly the set $\{-1/(n+s)\}$ has $3r$ elements in $N$ and $3r-1$ elements in $Q$; the set $-1/s+Q$ has $3r$ elements in $N$ and $3r-1$ elements in $Q$; the set $-1/s+N$ has $3r-1$ elements in $N$ and $3r-1$ elements in $Q$, and one element is 0.

Also 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 a $n'\in N$ such that $-1/(n+s)=n'-1/s$, the nonresidue position is equal to

$$\sum_{q'-1/s\in Q} x^{q'-1/s}+3\sum_{n'-1/s\in Q} x^{n'-1/s}-\sum_{q-1/s\in Q} x^{q-1/s}-3\sum_{n-1/s\in Q} x^{n-1/s}=0.$$

Now the nonresidue position of $\rho(r_s)-r_{-1/s}$ is:

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

Since for any $-1/(q+s)\in N$, there is a $n'\in N$ such that $-1/(q+s)=n'-1/s$ and for any $-1/(n+s)\in N$, there is a $q'\in Q$ such that $-1/(n+s)=q'-1/s$, and there are $3r+3r-1=6r-1$ terms appearing, so the residue position is equal to $-4e_2=5e_2$. Thus, since $0\in -1/s+N$, we have

$$\rho(r_s)-r_{-1/s}=(2,6+5e_1)=7r_0+2h;$$

that is, $\rho(r_s)=r_{-1/s}+7r_0+2h\in\overline{Q}_1$.

By similar proofs, we obtain the following results:
When $r = 3k$,

$$r_0 = (0, 1 + e_2), \quad \rho(r_0) = 8r_0 + h, \quad \rho(r_s) = 8r_{-1/s} + r_0, \quad s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 8r_0, \quad s \in N, \quad \rho(r_\infty) = 2r_0 + 8h.$$

When $r = 3k + 2$,

$$r_0 = (0, 4 + e_1 + 6e_2),\ \rho(r_0) = 4r_0 + 2h,\ \rho(r_s) = 8r_{-1/s} + 4r_0 + 3h,\ s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 4r_0 + 5h, \quad s \in N, \quad \rho(r_\infty) = r_0 + h.$$

Now suppose that $p = 12r + 1$ and $r = 3k + 1$. Since $Q_1 = Q_1' + \langle 7h \rangle$ (Theorem 8(d)), the extended code $\overline{Q}_1$ is generated by $\frac{p+1}{2}$ rows of the $(p + 1) \times (p + 1)$ matrix

$$\begin{array}{c} r_0 \\ . \\ \vdots \\ \vdots \\ r_\infty \end{array} \begin{pmatrix} 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ & & & & & \\ 8 & 7 & 7 & 7 & \cdots & 7 \end{pmatrix},$$

where each row of $G_1'$ is a cyclic shift of the vector $6 + 3e_1 + 8e_2$. Since $p = 4(3r) + 1$, $-1$ is a residue mod $p$, by [8, Theorem 65]. Thus $\rho(e_1) = -e_1$ and $\rho(e_2) = e_2$.

By definition of $\rho$ we have $x^0 \mapsto 5x_\infty$ and $x_\infty \mapsto 4x^0$. Now $r_0 = (0, 6 + 3e_1 + 8e_2)$ and so

$$\rho(r_0) = (5 \cdot 6, 4 \cdot 0 - 3e_1 + 8e_2) = (3, 6e_1 + 8e_2) = 4r_0 + 5h \in \overline{Q}_1.$$

Since $r_\infty = (8, 7 + 7e_1 + 7e_2)$ we have $\rho(r_\infty) = (5 \cdot 7, 4 \cdot 8 - 7e_1 + 7e_2) = (8, 5 + 2e_1 + 7e_2) = r_0 + 8h \in \overline{Q}_1$. Now we prove that $\rho(r_s) \in \overline{Q}_1$. In all the following proofs we let $q \in Q$ and $n \in N$. We have

$$r_s = \left(0, 6x^s + 3\sum x^{q+s} + 8\sum x^{n+s}\right),$$
$$r_{-1/s} = \left(0, 6x^{-1/s} + 3\sum x^{q-1/s} + 8\sum x^{n-1/s}\right).$$

We consider two cases $s \in Q$ and $s \in N$:

**Case 1.** $s \in Q$. We have $\rho(r_s) = (5 \cdot 3, -6\chi(s)x^{-1/s} - 3\sum \chi(q+s)x^{-1/(q+s)} - 8\sum \chi(n+s)x^{-1/(n+s)})$. Since $0 \in s + Q$, the $\infty$ position of $\rho(r_s)$ is $5 \cdot 3 = 6$. We show that $\rho(r_s) = 8r_{-1/s} + 4r_0 + 6h$. Since $-1 \in Q$ and $s \in Q$, the residue position of $\rho(r_s) + r_{-1/s}$ is:

$$-6x^{-1/s} - 3\sum_{q+s \in Q} x^{-1/(q+s)} - 8\sum_{n+s \in Q} x^{-1/(n+s)}$$
$$+6x^{-1/s} + 3\sum_{q-1/s \in Q} x^{q-1/s} + 8\sum_{n-1/s \in Q} x^{n-1/s}.$$

By Theorem 4, the set $s+Q$ has $3r-1$ elements in $Q$, $3r$ elements in $N$, and one element is 0. Thus, since $-1 \in Q$, the set $\{-1/(q+s), q+s \neq 0\}$ has $3r-1$ elements in $Q$ and $3r$ elements in $N$. Similarly the set $\{-1/(n+s)\}$ has $3r$ elements in $Q$ and $3r$ elements in $N$; the set $-1/s+Q$ has $3r-1$ elements in $Q$ and $3r$ elements in $N$, and one element is 0; the set $-1/s+N$ has $3r$ elements in $Q$ and $3r$ elements in $Q$.

Also 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 a $n' \in N$ such that $-1/(n+s) = n' - 1/s$, the nonresidue position is equal to

$$-3 \sum_{q'-1/s \in Q} x^{q'-1/s} - 8 \sum_{n'-1/s \in Q} x^{n'-1/s} + 3 \sum_{q-1/s \in Q} x^{q-1/s} + 8 \sum_{n-1/s \in Q} x^{n-1/s} = 0.$$

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

$$3 \sum_{q+s \in N} x^{-1/(q+s)} + 8 \sum_{n+s \in N} x^{-1/(n+s)} + 3 \sum_{q-1/s \in N} x^{q-1/s} + 8 \sum_{n-1/s \in N} x^{n-1/s}.$$

Since for any $-1/(q+s) \in N$, there is a $n' \in N$ such that $-1/(q+s) = n' - 1/s$ and for any $-1/(n+s) \in N$, there is a $q' \in Q$ such that $-1/(n+s) = q' - 1/s$, and there are $3r + 3r = 6r$ terms appearing, so the residue position is equal to

$$3 \sum_{q'-1/s \in N} x^{q'-1/s} + 8 \sum_{n'-1/s \in N} x^{n'-1/s} + 3 \sum_{q-1/s \in N} x^{q-1/s} + 8 \sum_{n-1/s \in N} x^{n-1/s} = 2e_2.$$

Thus, since the $0 \in -1/s+Q$, we have

$$\rho(r_s) + r_{-1/s} = (6, 3 + 2e_1) = 4r_0 + 6h;$$

that is, $\rho(r_s) = 8r_{-1/s} + 4r_0 + 6h$.

**Case 2.** $s \in N$. We have $\rho(r_s) = (5 \cdot 8, -6\chi(s)x^{-1/s} - 3\sum \chi(q+s)x^{-1/(q+s)} - 8\sum \chi(n+s)x^{-1/(n+s)})$. Since $0 \in s+N$, the $\infty$ position of $\rho(r_s)$ is $5 \cdot 8 = 4$. We show that $\rho(r_s) = r_{-1/s} + 4r_0 + 4h$. Since $-1 \in Q$ and $s \in N$, the nonresidue position of $\rho(r_s) - r_{-1/s}$ is:

$$6x^{-1/s} + 3 \sum_{q+s \in N} x^{-1/(q+s)} + 8 \sum_{n+s \in N} x^{-1/(n+s)} - \left( 6x^{-1/s} + 3 \sum_{q-1/s \in N} x^{q-1/s} + 8 \sum_{n-1/s \in N} x^{n-1/s} \right).$$

Since $-1 \in Q$, by Theorem 4 the set $\{-1/(q+s)\}$ has $3r$ elements in $Q$ and $3r$ elements in $N$. Similarly, the set $\{-1/(n+s), n+s \neq 0\}$ has $3r$ elements in $Q$ and $3r-1$ elements in $N$; the set $-1/s+Q$ has $3r$ elements in $Q$ and $3r$ elements in $N$; the set $-1/s+N$ has $3r$ elements in $Q$ and $3r-1$ elements in $N$, and one element is 0.

Also 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 a $n' \in N$ such that $-1/(n+s) = n' - 1/s$, the nonresidue position is 0.

The residue position of $\rho(r_s) - r_{-1/s}$ is:

$$-3 \sum_{q+s \in Q} x^{-1/(q+s)} - 8 \sum_{n+s \in Q} x^{-1/(n+s)} - \left( 3 \sum_{q-1/s \in Q} x^{q-1/s} + 8 \sum_{n-1/s \in Q} x^{n-1/s} \right).$$

Since for any $-1/(q+s) \in Q$, there is a $n' \in N$ such that $-1/(q+s) = n' - 1/s$ and for any $-1/(n+s) \in Q$, there is a $q' \in Q$ such that $-1/(n+s) = q' - 1/s$, there are $3r + 3r = 6r$ terms appearing, so the residue position is equal to $-11e_1 = 7e_1$. Thus since $0 \in -1/s+N$, $\rho(r_s) - r_{-1/s} = (4, 1+7e_1) = 4r_0 + 4h$; that is, $\rho(r_s) = r_{-1/s} + 4r_0 + 4h \in \overline{Q}_1$.

By similar proofs, we obtain the following results: When $r = 3k+1$,

$$r_0 = (0, 6+3e_1+8e_2),\ \rho(r_0) = 4r_0 + 5h,\ \rho(r_s) = 8r_{-1/s} + 4r_0 + 6h,\ s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 4r_0 + 4h,\quad s \in N,\quad \rho(r_\infty) = r_0 + 8h.$$

When $r = 3k$,

$$r_0 = (0, 8e_2),\ \rho(r_0) = r_0,\ \rho(r_s) = 8r_{-1/s} + r_0,\ s \in Q,$$
$$\rho(r_s) = r_{-1/s} + r_0 + 8r_\infty,\quad s \in N,\quad \rho(r_\infty) = 8r_\infty.$$

When $r = 3k+2$,

$$r_0 = (0, 3+6e_1+8e_2),\ \rho(r_0) = 7r_0 + 6h,\ \rho(r_s) = 8r_{-1/s} + 7r_0 + 3r_\infty,\ s \in Q,$$
$$\rho(r_s) = r_{-1/s} + 7r_0 + 7h,\quad s \in N,\quad \rho(r_\infty) = 4r_0 + 8h.$$ □

Recall that the Lee weight of $a \in \mathbb{Z}_m$ is defined as $\min\{a, m-a\}$, and the Lee wight of a vector is the sum of the Lee wight of its components. Thus in $\mathbb{Z}_9$, the Lee wight of 0 is 0; the Lee wight of $1, 8$ is 1; the Lee wight of $2, 7$ is 2; the Lee wight of $3, 6$ is 3 and the Lee wight of $4, 5$ is 4. The Euclidian weight of $a \in \mathbb{Z}_m$ is defined as the square of the Lee wight of $a$, i.e., $(\min\{a, m-a\})^2$; and the Euclidian weight of a vector is the sum of the Euclidian wight of its components. By direct computation with the aid of a computer, we have

**Theorem 12.** *The $\mathbb{Z}_9$-QR code of length* 11 *has minimum Lee weight* 7, *minimum Euclidian weight* 9, *and minimum Hamming weight* 5.

We define the maps $\beta_i$, $i = 1, 2, 3, 4$, from $\mathbb{Z}_9$ to $\mathbb{Z}_2$, by

| $c$ | $\beta_1(c)$ | $\beta_2(c)$ | $\beta_3(c)$ | $\beta_4(c)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 1 | 1 |
| 3 | 0 | 1 | 1 | 1 |
| 4 | 1 | 1 | 1 | 1 |
| 5 | 1 | 1 | 1 | 1 |
| 6 | 1 | 1 | 1 | 0 |
| 7 | 1 | 1 | 0 | 0 |
| 8 | 1 | 0 | 0 | 0 |

The map $\beta_i$ can be extended on $N$-tuples which is also denoted by $\beta_i$. The Gray map $\phi : \mathbb{Z}_9^N \longrightarrow \mathbb{Z}_2^{4N}$ is given by $\phi(c) = (\beta_1(c), \beta_2(c), \beta_3(c), \beta_4(c))$. Clearly $\phi$ is a distance-preserving map from ($\mathbb{Z}_9^N$, Lee distance) to ($\mathbb{Z}_2^{4N}$, Hamming distance). The weight distribution of the image of the QR-code of length 11 under the Gray map is given in the following table;

| $i$ | $A_i$ | $i$ | $A_i$ |
|---|---|---|---|
| 0 | 1 | 24 | 51700 |
| 7, 8, 42 | 22 | 25 | 45232 |
| 9, 39 | 110 | 26 | 39292 |
| 10 | 220 | 27 | 47102 |
| 11 | 112 | 28 | 38632 |
| 12 | 550 | 29 | 24618 |
| 13 | 2002 | 30 | 20570 |
| 14 | 3454 | 31 | 16852 |
| 15 | 4862 | 32 | 13684 |
| 16 | 7854 | 33 | 6404 |
| 17 | 11352 | 34 | 3652 |
| 18 | 13992 | 35 | 2222 |
| 19 | 23122 | 36 | 1804 |
| 20 | 32582 | 37 | 660 |
| 21 | 33484 | 38 | 132 |
| 22 | 38656 | 44 | 2 |
| 23 | 46354 | | |

**Acknowledgment.** The author thanks the Center of Excellence of Mathematics of Isfahan University of Technology (CEAMA).

## References

[1] A. Bonneaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), no. 2, 366–377.

[2] M. H. Chiu, S. S.-T. Yau, and Y. Yu, *$Z_8$-cyclic codes and quadratic residue codes*, Adv. in Appl. Math. **25** (2000), no. 1, 12–33.

[3] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $Z_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.
[4] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
[5] F. J. MacWilliams and N. J. A. Sloan, *The theory of error-correcting codes*, North Hoalland, Amsterdam, 1977.
[6] B. R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974.
[7] O. Perron, *Bemerkungen über die Verteilung der quadratischen Reste*, Math. Z. **56** (1952), 122–130.
[8] V. Pless, *Introduction to The Theory of Error Correcting Codes*, John Wiley & Sons, Inc., New York, 1989.
[9] V. Pless, P. Solé, and Z. Qian, *Cyclic self-dual $Z_4$-codes*, Finite Fields Appl. **3** (1997), no. 1, 48–69.
[10] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $Z_4$*, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600.

Department of Mathematical Sciences
Isfahan University of Technology
Isfahan 84156-83111
and
Institute for Studies in Theoretical Physics and Mathematics
Iran
*E-mail address*: b.taeri@cc.iut.ac.ir