QUADRATIC RESIDUE CODES OVER $\mathbb{Z}_4 + u_1\mathbb{Z}_4 + ... + u_t\mathbb{Z}_4$ AND QUANTUM CODES FROM THESE CODES

Arezoo Soufi Karbaski[1], Karim Samei[2]

In this paper linear and cyclic codes over the ring $R = \mathbb{Z}_4+u_1\mathbb{Z}_4+...+u_t\mathbb{Z}_4$ are investigated, where $t \geq 1$. The structure of Euclidean and Hermitian linear self-dual codes over R is studied. A distance preserving Gray map from R to $\mathbb{Z}_4^{t+1}$ is also presented. Moreover, quadratic residue codes over R are defined. Further, Euclidean and Hermitian self-dual families of quadratic residue codes over R are observed and four Hermitian self-dual codes of length p over the ring R are introduced if $p \equiv -1$ (mod 8) or $p \equiv 1$ (mod 8). In particular, a method is presented to construct quantum codes over $\mathbb{F}_2$ from Gray images of quadratic residue codes over the ring R. The results are presented in the table.

Keywords: Cyclic codes, Euclidean self-dual codes, Hermitian self-dual codes, Gray map, Quadratic residue codes, Quantum codes.

MSC2010: 94B 05, 94B 15, 81P 70.

1. Introduction

Linear and cyclic codes over finite rings are an important class of codes from both a theorical and a practical viewpoint. The study of cyclic codes over finite rings have been studied in the late 1972s. In [1] and [2] the author studied the codes over finite rings. In this relation Dinh and Lopez-permouth presented the structure of cyclic and negacyclic codes over chain rings [6].

Quadratic residue (QR) codes are special cases of cyclic codes and over finite fields they have been studied for many years. More recently, Quadratic residue codes over some special rings have been studied and have generated a great deal of interest. First, Andrew Gleason introduced quadratic residue codes. The link between quadratic residue codes over $\mathbb{F}_2$ and these codes over $\mathbb{Z}_4$ was given by pless and Qian [11]. Chiu et al. and Taeri presented the structure of quadratic residue codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$, respectively, and they provided a different approach to the study of these codes [4] and [17]. In 2013, Kaya, Yildiz and Siap studied the structure of quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$ [9]. Meanwhile, Authors [14] obtained intresting results by the Gray map. Authors [15] used the Gray map for construction of some best-known binary linear quasi-cyclic codes. For see more details, we refer readers to [13] and [16].

Quantum error-correcting codes have recently generated a great deal of intrest. A method to construct quantum error-correcting codes from classical error-correcting codes was introduced by Calderbank et al. [3]. Qian gave a construction for quantum codes from cyclic codes of odd length n over $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$ [12]. More recently, Guenda and Gulliver extended the Calderbank-Shor-Steane (CSS) construction to Frobenius rings [7]. In this paper, we mainly discuss the structure of linear, cyclic and quadratic residue codes over

[1]Phd. Student, Department of Mathematics, Bu-Ali Sina University, Hamedan, Iran, e-mail: arezoosufi@yahoo.com

[2]Professor, Faculty of Sciences, Department of Mathematics, Bu-Ali Sina University, Hamedan, Iran, e-mail: samei@ipm.ir

the ring $R = \mathbb{Z}_4 + u_1\mathbb{Z}_4 + ... + u_t\mathbb{Z}_4$, where $t \geq 1$, and use the ideas of authors [9] and [11]. Moreover, we obtain quantum codes from quadratic residue codes over R using the generalized Gray map.
First we survey the known results on quadratic residue codes over $\mathbb{Z}_4$ and give general properties with quadratic residue codes over R. In section 2, we describe the brief introduction concerning linear and cyclic codes over the ring R and introduce Gray map from R to $\mathbb{Z}_4^{t+1}$. In sections 3 and 4 , we define the quadratic residue codes over R and investigate Hermitian self-dual codes over the ring R, respectively. In this correspondence, we present examples of Hermitian cyclic self-dual codes over R. Finally in the last section, we derive self-orthogonal and self-dual codes over $\mathbb{Z}_4$ as Gray images of quadratic residue codes over R and use these codes to determine the parameters of the corresponding quantum codes.

2. **Preliminaries**

The ring $R = \mathbb{Z}_4 + u_1\mathbb{Z}_4 + ... + u_t\mathbb{Z}_4$ is a principal ideal ring of order 4^{t+1} and characteristic 4, subject to the restriction ${u_i}^2 = u_i$, and $u_iu_j = 0$ if $i \neq j$, where $1 \leq i \leq t$ and t is a natural number. We denote this ring by $u_0\mathbb{Z}_4+u_1\mathbb{Z}_4+...+u_t\mathbb{Z}_4$, where $u_0 = 1-\Sigma_{i=1}^{t}u_i$. The ring $\prod_{i=0}^{t} R_i$ is isomorphic to the ring R, where $R_i = \mathbb{Z}_4$ and $0 \leq i \leq t$.
A linear code C over ring R of length n is a R-submodule of R^n. A generator matrix C is a matrix whose rows generate C. The Hamming weight of a codeword is the number of non-zero components.
Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ and $\mathbf{y} = (y_1, y_2, ..., y_n)$ be two elements of R^n. The Euclidean inner product of vectors $\mathbf{x}, \mathbf{y}$ is $< \mathbf{x}, \mathbf{y} >_E = \Sigma_{i=1}^{n} x_iy_i$. The dual or orthogonal of C denoted $C^{\perp}$ is defined as

$$C^{\perp} = \{\mathbf{x} \in R^n : < \mathbf{x}, \mathbf{y} >_E = 0, \text{ for all } \mathbf{y} \in C\}.$$

The code C is (Euclidean) self-orthogonal provided $C \subseteq C^{\perp}$ and a (Euclidean) self-dual provided $C = C^{\perp}$.

Definition 2.1. *If $x_i \in \mathbb{Z}_4$, then we define the conjugate of $x = \Sigma_{i=0}^{t} u_ix_i$ as*

$$\overline{x} = \Sigma_{i=0}^{t} \overline{u_ix_i} = \Sigma_{i=0}^{t} \overline{u_i}\ x_i$$

where we define the conjugate of u_i as follows:
(1) $\overline{u_{2k}} = u_{2k+1}$, $\overline{u_{2k+1}} = u_{2k}$ and $\overline{u_t} = u_t$ if t is an even number and $0 \leq k \leq \frac{t-2}{2}$;
(2) $\overline{u_{2k}} = u_{2k+1}$ and $\overline{u_{2k+1}} = u_{2k}$ if t is an odd number and $0 \leq k \leq \frac{t-1}{2}$. It is often useful to consider another inner product, called Hermitian inner product, given by

$$< \mathbf{x}, \mathbf{y} >_H = \mathbf{x}.\overline{\mathbf{y}}$$

where $\mathbf{x} = \Sigma_{i=0}^{t} u_ix_i$ and $\mathbf{y} = \Sigma_{i=0}^{t} u_iy_i$ in R^n and $^-$, called conjugation, is given above.

The dual or orthogonal of C under the Hermitian inner product denoted $C^{\perp_H}$ is defined as

$$C^{\perp_H} = \{\mathbf{x} \in R^n : < \mathbf{x}, \mathbf{y} >_H = 0, \text{ for all } \mathbf{y} \in C\}.$$

The code C is Hermitian self-orthogonal provided $C \subseteq C^{\perp_H}$ and Hermitian self-dual provided $C = C^{\perp_H}$. We note that if $\mathbf{c} = (c_0, c_1, ..., c_{n-1}) \in R^n$, then $\overline{\mathbf{c}} = (\overline{c_0}, \overline{c_1}, ..., \overline{c_{n-1}})$. A linear code C of length n over R is said to be cyclic if for any codeword $c \in C$, we have:

$$\mathbf{c} = (c_0, c_1, ..., c_{n-2}, c_{n-1}) \in C \text{ implies that } \lambda(\mathbf{c}) = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C.$$

We let $R_n = \frac{R[X]}{<X^n-1>}$. Since C is a cyclic code of length n over R if and only if C is an ideal of R_n, we associate the vector $c = (c_0, c_1, ..., c_{n-1})$ in R^n with the polynomial $c(x) = c_0 + c_1x + c_2x^2 + ... + c_{n-1}x^{n-1}$ in R_n, where $x = X+ < X^n - 1 >$. A polynomial

$e(x)$ in R_n is an idempotent if $e^2(x) = e(x)$.
Two linear codes C_1 and C_2 are (permutation) equivalent provided there is a permutation of coordinates which sends C_1 to C_2.
A code is $even-like$ if it has only even-like codewords; a code is $odd-like$ if it is not even-like (A vector $\mathbf{x} = (x_0, x_1, ..., x_{n-1})$ in R^n is $even-like$ provided that $\Sigma_{i=0}^{n-1} x_i = 0$).
$X^n - 1$ has no repeated factors in $\mathbb{Z}_4[X]$ if and only if $\gcd(n, 2) = 1$, an assumption we make throughout this paper.

Remark 2.1. *The finite ring R is a principal ideal ring. Then from Chinese remainder theorem there exists a canonical R-module isomorphism*

$$\psi : R^n \to \prod_{i=0}^{t} {R_i}^n$$

where $R_i = \mathbb{Z}_4$. For $0 \leq i \leq t$, let C_i be a linear code over $\mathbb{Z}_4$ of length n, and let

$$C = CRT(C_0, C_1, ..., C_t) = \psi^{-1}(\prod_{i=0}^{t} C_i) = \{\psi^{-1}(v_0, v_1, ..., v_t) | v_i \in C_i\}.$$

The code C is called the Chinese product of codes C_0,...,C_t.

Let C be a linear code over R and let t be an even number. If

$$a = ((a_{10}, a_{11}, ..., a_{1t}), (a_{20}, a_{21}, ..., a_{2t}), ..., (a_{n0}, a_{n1}, ..., a_{nt})) \in C,$$

and p_j is the canonical projection, then

$$\psi(a) = ((a_{10}, a_{20}, ..., a_{n0}), (a_{11}, a_{21}, ..., a_{n1}), ..., (a_{1t}, a_{2t}, ..., a_{nt})),$$

and

$$p_j(\psi(a)) = (a_{1j}, a_{2j}, ..., a_{nj}),$$

where $0 \leq j \leq t$.
If j is an even and $0 \leq j < t$, we define

$$\hat{p_j}(\psi(a)) = p_{j+1}(\psi(a))$$

and if j is an odd and $0 \leq j \leq t$, we define

$$\hat{p_j}(\psi(a)) = p_{j-1}(\psi(a))$$

and if t is an even, we define

$$\hat{p_t}(\psi(a)) = p_t(\psi(a)).$$

We first give the following lemma for all PIR rings:

Theorem 2.1. [5] Let $C = CRT(C_0, C_1, ..., C_t)$ be a linear code of length n over R. Then
(1) $|C| = \prod_{i=0}^{t} |C_i|$;
(2) rank(C)=max $\{$rank $(C_i) : \ 0 \leq i \leq t\}$;
(3) $d_H(C) = min\{d(C_i) : \ 0 \leq i \leq t\}$.

Theorem 2.2. *Let $C = CRT(C_0, C_1, ..., C_t)$ be a linear code of length n over R. Then $C^{\perp} = CRT(C_0^{\perp}, C_1^{\perp}, ..., C_t^{\perp})$.*

Proof. By Remark 2.1, $a \in C^{\perp}$ if and only if $p_i(\psi(a))p_i(\psi(b)) = 0$, for any $b \in C$ and $0 \leq i \leq t$, if and only if $p_i(\psi(a)) \in C_i^{\perp}$, this is the case if and only if $\psi(a) \in \prod_{i=0}^{t} C_i^{\perp}$, and if and only if $a \in CRT(C_0^{\perp}, C_1^{\perp}, ..., C_t^{\perp})$. □

Theorem 2.3. *Let C be a linear code of length n over ring R, then $|C|.|C^{\perp}| = |R|^n$.*

Proof. Theorem 2.3 is obviously true when $R = \mathbb{Z}_4$. Then the proof follows from Theorems 2.1 and 2.2. □

In the following theorem without loss of generality, we can assume that t be an even number.

Theorem 2.4. *Let $C = CRT(C_0, C_1, ..., C_t)$ be a linear code of length n over R. The following hold:*
(1) $C^{\perp_H} = CRT(C_1^{\perp}, C_0^{\perp}, C_3^{\perp}, C_2^{\perp}, ..., C_t^{\perp})$;
(2) $(C^{\perp_H})^{\perp_H} = C$.

Proof. $a \in C^{\perp_H}$ if and only if $p_i(\psi(a))\hat{p}_i(\psi(b)) = 0$, and $p_t(\psi(a))p_t(\psi(b)) = 0$, for any $b \in C$ and $0 \leq \forall i \leq t-1$, if and only if $p_{2k+1}(\psi(a)) \in C_{2k}^{\perp}$, $p_{2k}(\psi(a)) \in C_{2k+1}^{\perp}$, $0 \leq \forall k \leq \frac{t-2}{2}$ and $p_t(\psi(a)) \in C_t^{\perp}$ if and only if $\psi(a) \in C_1^{\perp} \times C_0^{\perp} \times C_3^{\perp} \times ... \times C_t^{\perp}$, and if and only if $a \in CRT(C_1^{\perp}, C_0^{\perp}, ..., C_t^{\perp})$.
(2) Since $(C_i^{\perp})^{\perp} = C_i$, it follows immediately from (1). □

Theorem 2.5. *Let $C = CRT(C_0, C_1, ..., C_t)$ be a linear code over R. The following hold:*
(1) If t is an even number, then C is Hermitian self-dual code over R if and only if $C_{2k} = C_{2k+1}^{\perp}$, where $0 \leq k \leq \frac{t-2}{2}$, and C_t is a self-dual code;
(2) If t is an odd number, then C is Hermitian self-dual code over R if and only if $C_{2k} = C_{2k+1}^{\perp}$, where $0 \leq k \leq \frac{t-1}{2}$.

Proof. It follows by Theorem 2.4. □

Theorem 2.6. *Let $C = CRT(C_0, C_1, ..., C_t)$ be a linear code of length n over R. Then C is a cyclic code over R if and only if C_i is a cyclic code of length n over $\mathbb{Z}_4$, for any $0 \leq i \leq t$.*

Proof. Suppose that C is a cyclic code of length n over R and $\mathbf{c_i} \in C_i$, where $0 \leq i \leq t$. Let $\mathbf{c} = (\mathbf{c_0}, \mathbf{c_1}, ..., \mathbf{c_t})$, there exists $\mathbf{a} \in C$ such that $\psi(\mathbf{a}) = \mathbf{c}$. Hence $\lambda(\mathbf{a}) = (p_n(\mathbf{a}), p_1(\mathbf{a}), ..., p_{n-1}(\mathbf{a})) \in C$. Thus we have:

$$\psi(\lambda((\mathbf{a}))) = (\lambda(\mathbf{c_0}), \lambda(\mathbf{c_1}), ..., \lambda(\mathbf{c_t})) \in \prod_{i=0}^{t} C_i.$$

The converse is similar. □

Remark 2.2. *By Theorem* 2.6, *$C = CRT(C_0, C_1, ..., C_t)$ is an ideal of R_n if and only if C is a cyclic code of length n over R if and only if for each $0 \leq i \leq t$, C_i is a cyclic code of length n over $\mathbb{Z}_4$, and if and only if for each $0 \leq i \leq t$, C_i is an ideal of $\frac{\mathbb{Z}_4[X]}{<X^n-1>}$. On the other hand, $R[X] \cong \oplus_{i=0}^{t} u_i \mathbb{Z}_4[X]$, hence we have:*

$$\frac{R[X]}{< X^n - 1 >} \cong \bigoplus_{i=0}^{t} u_i \frac{\mathbb{Z}_4[X]}{< X^n - 1 >} \quad \text{(as ring isomorphism)}$$

Therefore when $C = CRT(C_0, C_1, ..., C_t)$ is a cyclic code over R, the ideal C is corresponding to $\oplus_{i=0}^{t} u_i C_i$. Thus without loss of generality, we can assume that $C = \oplus_{i=0}^{t} u_i C_i$ and by Theorem 2.2, *$C^{\perp} = \oplus_{i=0}^{t} C_i^{\perp}$.*

Corollary 2.1. *Let $C = u_0 C_0 \oplus u_1 C_1 \oplus ... \oplus u_t C_t$ be a cyclic code of length n over R. Then $C =< u_0 f_1(x), u_1 f_2(x), ..., u_t f_t(x) >=< f(x) >$ such that $f_i(x)$ is the generator polynomial of cyclic code C_i and $f(x) = \Sigma_{i=0}^{t} u_i f_i(x)$, with $0 \leq i \leq t$. Moreover, if for each $0 \leq \forall i \leq t$, $f_i(X) | X^n - 1$, then $f(X) | X^n - 1$.*

Proof. The first part follows from Remark 2.2 and [[18], Theorem 7.26]. If for each $0 \leq i \leq t$, $f_i(X) | X^n - 1$, therefore there exists $r_i(X) \in \frac{\mathbb{Z}_4[X]}{<X^n-1>}$ such that $X^n - 1 = r_i(X) f_i(X)$. Put $r(X) = \Sigma_{i=0}^{t} u_i r_i(X)$, we have $X^n - 1 = f(X) r(X)$, i.e., $f(X) | X^n - 1$. □

Corollary 2.2. *R_n is a principal ideal ring.*

Proposition 2.1. [8] *Let R be a finite commutative ring with identity and let $t(x)$ be the idempotent generator of a cyclic code C. Then $1-t(x^{-1})$ is the idempotent generator of the dual code $C^{\perp}$.*

Theorem 2.7. [8] *Let R be a finite commutative ring with identity and let $f(x)$, $g(x)$ be idempotents of R_n and let $C_1 =< f(x) >$, $C_2 =< g(x) >$ be cyclic codes over R. Then $C_1 \cap C_2$ and $C_1 + C_2$ have idempotent generators $f(x)g(x)$ and $f(x) + g(x) - f(x)g(x)$, respectively.*

Corollary 2.3. *Let $C = u_0C_0 \oplus u_1C_1 \oplus ... \oplus u_tC_t$ be a cyclic code of length n over R. If each generator polynomial of cyclic code C_i is a divisor of $X^n - 1$, then there exists unique generating idempotent for C of the form $e(x) = \Sigma_{i=0}^{t} u_i e_i(x)$, where $e_i(x)$ is unique generating idempotent for C_i and $C^{\perp} =< 1 - e(x^{-1}) >$.*

Proof. Since C_i is a cyclic code of length n over $\mathbb{Z}_4$, then by [[18], Theorem 7.27] there exists unique idempotent $e_i(x)$ in $\frac{\mathbb{Z}_4[X]}{<X^n-1>}$ such that $C_i =< e_i(x) >$.
It is obvious that $e(x) = u_0e_0(x) + u_1e_1(x) + ... + u_te_t(x)$ is idempotent and $C =< \Sigma_{i=0}^{t} u_i e_i(x) >$. If there exists another idempotent $e'(x) \in C$ such that $C =< e'(x) >$, then $e'(x) = r(x)e(x)$ for some $r(x) \in \frac{R[X]}{<X^n-1>}$. So $e'(x)e(x) = e'(x)$. Similarly, $e'(x)e(x) = e(x)$, then $e(x) = e'(x)$. The last statement is immediate consequence of Theorem 2.7. □

First, the Euclidean weights of $0, 1, 2, 3$ of $\mathbb{Z}_4$ are defined to be $0, 1, 4, 1$, respectively. For later applications let us introduce the Euclidean weight of vectors in the ring R. Let τ be the function from $\mathbb{Z}_4$ to $\mathbb{Z}_4$ which $\tau(0) = 0$, $\tau(1) = \tau(3) = 1$ and $\tau(2) = 4$.

Definition 2.2. *We define the Euclidean weight of $a = a_0 + u_1a_1 + u_2a_2 + ... + u_ta_t$ in R:*

$$w_E(a) = \tau(a_0) + \tau(a_0 + a_1) + \tau(a_0 + a_2) + ... + \tau(a_0 + a_t).$$

Then the Euclidean weight of an n-tuple in R is defined to be the integral sum of the Euclidean weights of its components. Let μ be the map from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ which $\mu(0) = (0, 0)$, $\mu(1) = (0, 1)$, $\mu(2) = (1, 1)$ and $\mu(3) = (1, 0)$. The map μ is extended to $\mathbb{Z}_4^n$ componentwise; naturally.

Definition 2.3. *We define two maps as*

$$\phi : R \to \mathbb{F}_2^{2(t+1)}$$

$$a_0 + u_1a_1 + u_2a_2 + ... + u_ta_t \to (\mu(a_0), \mu(a_0 + a_1), \mu(a_0 + a_2), ..., \mu(a_0 + a_t))$$

and

$$\phi' : R \to \mathbb{Z}_4^{(t+1)}$$

$$a_0 + u_1a_1 + u_2a_2 + ... + u_ta_t \to (a_0, a_0 + a_1, a_0 + a_2, ..., a_0 + a_t).$$

The maps ϕ and ϕ' are extended to R^n componentwise, naturally.

The Lee weight of an element c in R is defined as the Hamming weight of its image over $\mathbb{F}_2$; in other words

$$w_L(c)\text{=the number of nonzero components of } \phi(c)$$

where $c = a_0 + u_1a_1 + ... + u_ta_t$. We can easily verify that $d_L(x, y) = d(\phi(x), \phi(y))$ for all $x, y \in R$.

Corollary 2.4. *Let $C = CRT(C_0, C_1, ..., C_t)$ be a linear code of length n over R. The following hold:*
(1) If d_L be the minimum Lee weight of a code C, then

$$d_L(C) = min\{d_L(C_i) : \ 0 \le i \le t\};$$

(2) If d_E be the minimum Euclidean weight of a code C, then

$$d_E(C) = min\{d_E(C_i) : \ 0 \leq i \leq t\};$$

where $d_L(C_i)$ and $d_E(C_i)$ denote the minimum Lee and Euclidean weight of the code C_i over $\mathbb{Z}_4$, respectively.

Corollary 2.5. *Let ϕ' be the Gray map which is described in Definition* 2.3. *The following hold:*
(1) ϕ' is $\mathbb{Z}_4$-linear;
(2) The image of a self-dual code over R is a self-dual code over $\mathbb{Z}_4$.

Proof. (1) It follows immediately from definition of ϕ'.
(2) Let C be a self-dual code of length n over R and $\mathbf{a} = \mathbf{a_0} + u_1\mathbf{a_1} + ... + u_t\mathbf{a_t}$, $\mathbf{b} = \mathbf{b_0} + u_1\mathbf{b_1} + ... + u_t\mathbf{b_t}$ be two codewords of C, where $\mathbf{a_i}, \mathbf{b_i} \in \mathbb{Z}_4^n$, $0 \leq i \leq t$. Then $\mathbf{ab} = \mathbf{0}$. It follows that, $\mathbf{a_0b_0} + u_1(\mathbf{a_0b_1} + \mathbf{a_1b_0} + \mathbf{a_1b_1}) + ... + u_t(\mathbf{a_0b_t} + \mathbf{a_tb_0} + \mathbf{a_tb_t}) = 0$. Thus $\phi'(\mathbf{a})\phi'(\mathbf{b}) = (\mathbf{a_0}, \mathbf{a_0} + \mathbf{a_1}, ..., \mathbf{a_0} + \mathbf{a_t})(\mathbf{b_0}, \mathbf{b_0} + \mathbf{b_1}, ..., \mathbf{b_0} + \mathbf{b_t}) = \mathbf{0}$. Then $\phi'(C)$ is self-orthogonal. On the other hand by Theorem 2.3, $|\phi'(C^\perp)| = |C^\perp| = \frac{|R^n|}{|C|} = |\phi'(C)^\perp|$, then $|\phi'(C)| = |\phi'(C^\perp)| = |\phi'(C)^\perp|$ and $\phi'(C)$ is a self-dual code of length $n(t+1)$ over $\mathbb{Z}_4$. □

By Definition 2.3, we have the following corollary.

Corollary 2.6. *Let $C = CRT(C_0, C_1, ..., C_t)$ be a (n, M, d_L) linear code over R. Then $\phi'(C)$ is a $((t+1)n, M, d_L)$ linear code over $\mathbb{Z}_4$.*

Not that for n odd, the $\mathbb{Z}_4$ cyclic code generated by 2 is self-dual. We call this a trivial cyclic self-dual code.

Theorem 2.8. *Let n be an odd number. Then self-dual code over R of length n exists.*

Proof. Let C be the trivial cyclic self-dual code of length n over $\mathbb{Z}_4$. Then the code $C' = CRT(C, C, ..., C)$ is self-dual code of length n over R. □

Theorem 2.9. *Let n be an odd number. The following hold:*
(1) Nontrivial cyclic self-dual codes of odd length n over R exist if and only if $n \nmid 2^i + 1$ for any i;
(2) There exist Hermitian cyclic self-dual codes of any odd length n over R.

Proof. (1) By [[10], Theorem 3], nontrivial cyclic self-dual codes of length n over $\mathbb{Z}_4$ exist if and only if $n \nmid 2^i + 1$ for any i. Then we can prove (1) in a similar way to the one which was used in Theorem 2.8.
(2) Without loss of generality, we can assume that t is an even number. Let $C = CRT(C_0, C_0^\perp, C_2, C_2^\perp, ..., C_t)$, where C_t is cyclic self-dual code of length n over $\mathbb{Z}_4$ and C_i is cyclic code of length n over $\mathbb{Z}_4$, where $i = 0, 2, ..., t-2$. Then the proof is complete from Theorem 2.5. □

Theorem 2.10. *Let n be an odd number. If $X^n - 1 \in \mathbb{Z}_4[X]$ be unique expressed as $X^n - 1 = f_1(X)f_2(X)...f_r(X)$, where $f_i(X)$ is a basic irreducible polynomial and $1 \leq i \leq r$, then the number of the cyclic codes of length n over R is $3^{r(t+1)}$.*

Proof. Since the number of the cyclic codes of length n over $\mathbb{Z}_4$ is 3^r, then the number of the cyclic codes of length n over R is $3^{r(t+1)}$.

□

Theorem 2.11. *Let n be an odd number. If $X^n - 1 \in \mathbb{Z}_4[X]$ be unique expressed as $X^n - 1 = f_1(X)f_2(X)...f_r(X)$, where $f_i(X)$ is a basic irreducible polynomial and $1 \leq i \leq r$, then the following hold:*
(1) If t is an odd number, the number of the Hermitian cyclic self-dual codes of length n over R is $3^{r(\frac{t+1}{2})}$;
(2) If t is an even number and the number of the Euclidean cyclic self-dual codes of length

n over $\mathbb{Z}_4$ is k, then the number of the Hermitian cyclic self-dual codes of length n over R is $3^{r(\frac{t}{2})} \times k$.

Proof. The (1) and (2) immediately follow from Theorem 2.5 and the fact that the number of the cyclic codes of length n over $\mathbb{Z}_4$ is 3^r. We note that there is a trivial Euclidean cyclic self-dual code of any odd length n over $\mathbb{Z}_4$. □

3. Quadratic residue codes over R

Throughout this chapter, we assume that p is an odd prime and $p = \pm 1 \pmod 8$. Then QR-codes of length p over $\mathbb{Z}_4$ exist. Let $D_1 =< a_1(x) >$, $D_2 =< b_1(x) >$ and $C_1 =< a_2(x) >$, $C_2 =< b_2(x) >$ be QR-codes of type $4^{\frac{p+1}{2}}$ and $4^{\frac{p-1}{2}}$ over $\mathbb{Z}_4$, respectively, such that $a_i(x)$ and $b_i(x)$ are the idempotent generators of QR-codes, with $i = 1, 2$, see [[18], ch. 11].
In this section, without loss of generality, we can assume that t is an odd number. Denote Q_p and N_p are the sets of quadratic residues and quadratic non-residues modulo p, respectively. We let $e_1(x) = \Sigma_{i \in Q_p} x^i$ and $e_2(x) = \Sigma_{i \in N_p} x^i$.

Definition 3.1. *With above notation, we define four QR-codes over R as follows:*
$Q_1 = u_0D_1 \oplus u_1D_2 \oplus u_2D_1 \oplus ... \oplus u_tD_2$;
$Q_2 = u_0D_2 \oplus u_1D_1 \oplus u_2D_2 \oplus ... \oplus u_tD_1$;
$Q'_1 = u_0C_1 \oplus u_1C_2 \oplus u_2C_1 \oplus ... \oplus u_tC_2$;
$Q'_2 = u_0C_2 \oplus u_1C_1 \oplus u_2C_2 \oplus ... \oplus u_tC_1$.

Let $p_1(x) = u_0a_1(x) + u_1b_1(x) + u_2a_1(x) + ... + u_tb_1(x)$, $q_1(x) = u_0b_1(x) + u_1a_1(x) + u_2b_1(x) + ... + u_ta_1(x)$, $p_2(x) = u_0a_2(x) + u_1b_2(x) + u_2a_2(x) + ... + u_tb_2(x)$ and $q_2(x) = u_0b_2(x) + u_1a_2(x) + u_2b_2(x) + ... + u_ta_2(x)$. By Corollary 2.3, $p_1(x)$, $q_1(x)$, $p_2(x)$ and $q_2(x)$ are idempotent generators of Q_1, Q_2, Q'_1 and Q'_2, respectively. We note that $j(x) = 1 + x + x^2 + ... + x^{p-1}$ is the polynomial corresponding to the all one vector of length p.

3.1.

Case I. If $p-1 = 8r$ and r is odd, then two QR-codes of type $4^{\frac{p+1}{2}}$ and two QR-codes of type $4^{\frac{p-1}{2}}$ over $\mathbb{Z}_4$ have generating idempotents $1 + 3e_1(x) + 2e_2(x)$, $1 + 2e_1(x) + 3e_2(x)$ and $2e_1(x) + e_2(x)$, $e_1(x) + 2e_2(x)$, respectively.

3.2.

Case II. If $p - 1 = 8r$ and r is even, then two QR-codes of type $4^{\frac{p+1}{2}}$ and two QR-codes of type $4^{\frac{p-1}{2}}$ over $\mathbb{Z}_4$ have generating idempotents $1 + e_1(x)$, $1 + e_2(x)$ and $3e_2(x)$, $3e_1(x)$, respectively.
QR-codes over R have the following properties.

Theorem 3.1. *Let the situation be as in definition 3.1 and $p \equiv 1 \pmod 8$. Then the following hold:*
(1) Q_1 and Q'_1 are equivalent to Q_2 and Q'_2, respectively;
(2) $Q_1 \cap Q_2 =< j(x) >$ and $Q_1 + Q_2 = R_p$;
(3) $|Q_1| = 4^{\frac{(p+1)(t+1)}{2}} = |Q_2|$;
(4) $|Q'_1| = 4^{\frac{(p-1)(t+1)}{2}} = |Q'_2|$;
(5) $Q_1 = Q'_1 + < j(x) >$ and $Q_2 = Q'_2 + < j(x) >$;
(6) $Q_1^{\perp} = Q'_2$ and $Q_2^{\perp} = Q'_1$ and $Q'_1 \subseteq Q'^{\perp}_2$, $Q'_2 \subseteq Q'^{\perp}_1$;
(7) $Q'_1 \cap Q'_2 =< 0 >$ and $Q'_1 + Q'_2 =< 1 - j(x) >$.

Proof. (1) It is clear that the cyclic codes D_1 and C_1 are equivalent to the cyclic codes D_2 and C_2 over $\mathbb{Z}_4$, respectively. Then Q_1 and Q_1' are equivalent to Q_2 and Q_2', respectively.
(2) By Theorem 2.7, $Q_1 \cap Q_2 =< p_1(x)q_1(x) >=< a_1(x)b_1(x) >=< j(x) >$ and $Q_1 + Q_2 =< p_1(x) + q_1(x) - p_1(x)q_1(x) >=< a_1(x) + b_1(x) - a_1(x)b_1(x) >=< \mathbf{1}_R >=< (1, 1, ..., 1) >$.
(3) Since $|D_i| = 4^{\frac{p+1}{2}}$, with $i = 1, 2$, then $|Q_1| = |D_1||D_2|...|D_2| = 4^{\frac{(p+1)(t+1)}{2}}$. Similarly, $|Q_2| = 4^{\frac{(p+1)(t+1)}{2}}$.
(4) We can prove in a similar way to the one which was used in (3).
(5) Let $Q_1 = u_0D_1 \oplus u_1D_2 \oplus u_2D_1 \oplus ... \oplus u_tD_2$. Since $D_1 = C_1 + < j(x) >$ and $D_2 = C_2 + < j(x) >$, we have $Q_1 = Q_1' + < j(x) >$. Similarly, $Q_2 = Q_2' + < j(x) >$
(6) By Theorem 2.2,

$$Q_1^{\perp} = u_0D_1^{\perp} \oplus u_1D_2^{\perp} \oplus u_2D_1^{\perp} \oplus ... \oplus u_tD_2^{\perp} \text{ and } Q_2^{\perp} = u_0D_2^{\perp} \oplus u_1D_1^{\perp} \oplus u_2D_2^{\perp} \oplus ... \oplus u_tD_1^{\perp}.$$

Note that $D_1^{\perp} = C_2$ and $D_2^{\perp} = C_1$. It follows that $Q_1^{\perp} = Q_2'$ and $Q_2^{\perp} = Q_1'$. To prove the last claim, we can use (5) and the equations $Q_1^{\perp} = Q_2'$ and $Q_2^{\perp} = Q_1'$.
(7) By Theorem 2.7, $Q_1' \cap Q_2' =< p_2(x)q_2(x) >=< a_2(x)b_2(x) >=< 0 >$ and
$Q_1' + Q_2' =< p_2(x) + q_2(x) - p_2(x)q_2(x) >=< a_2(x) + b_2(x) - a_2(x)b_2(x) >=$
$< 1 - j(x) >$. So the proof is complete. □

3.**3**.

Case III. If $p + 1 = 8r$ and r is odd, then two QR-codes of type $4^{\frac{p+1}{2}}$ and two QR-codes of type $4^{\frac{p-1}{2}}$ over $\mathbb{Z}_4$, have generating idempotents $e_1(x) + 2e_2(x)$, $2e_1(x) + e_2(x)$ and $1 + 2e_1(x) + 3e_2(x)$, $1 + 3e_1(x) + 2e_2(x)$, respectively.

3.**4**.

Case VI. If $p + 1 = 8r$ and r is even, then two QR-codes of type $4^{\frac{p+1}{2}}$ and the two QR-codes of type $4^{\frac{p-1}{2}}$ over $\mathbb{Z}_4$, have generating idempotents $3e_1(x)$, $3e_2(x)$ and $1 + e_2(x)$, $1 + e_1(x)$, respectively.

Theorem 3.2. *Let the situation be as in Definition* 3.1. *If* $p \equiv -1$ (*mod* 8), *then the following hold:*
(1) Q_1 and Q_1' are equivalent to Q_2 and Q_2', respectively;
(2) $Q_1 \cap Q_2 =< 3j(x) >$ and $Q_1 + Q_2 = R_p$;
(3) $|Q_1| = 4^{\frac{(p+1)(t+1)}{2}} = |Q_2|$;
(4) $|Q_1'| = 4^{\frac{(p-1)(t+1)}{2}} = |Q_2'|$;
(5) $Q_1 = Q_1' + < 3j(x) >$ and $Q_2 = Q_2' + < 3j(x) >$;
(6) Q_1' and Q_2' are self-orthogonal and $Q_1^{\perp} = Q_1'$ and $Q_2^{\perp} = Q_2'$;
(7) $Q_1' \cap Q_2' =< 0 >$ and $Q_1' + Q_2' =< 1 + j(x) >$.

Proof. The proof of the theorem is similar to that for the cases I and II of this section. □

Corollary 3.1. *If* $p \equiv \pm 1$ (*mod* 8), *there are no Euclidean self-dual QR-codes of length* p *over* R.

Proof. Since D_i and C_i are not Euclidean self-dual codes over $\mathbb{Z}_4$, then by theorem 2.2, there are no Euclidean self-dual QR-codes of length p over R. □

Remark 3.1. *Let* D_i *be the quadratic residue code of length* p *over* $\mathbb{Z}_4$ *with* $i = 1, 2$. *There exist different QR-extended codes over* $\mathbb{Z}_4$ *as follows:*
(1) $\overline{D_i} = \{(c_0, c_1, ..., c_{p-1}, -\Sigma_{i=0}^{p-1} c_i) |\ \ (c_0, c_1, ..., c_{p-1}) \in D_i\}$;
(2) $\hat{D}_i = \{(c_0, c_1, ..., c_{p-1}, \Sigma_{i=0}^{p-1} c_i) |\ \ (c_0, c_1, ..., c_{p-1}) \in D_i\}$.

We can consider extending quadratic residue codes over R in such a way that extensions are self-dual or dual to each other.

Definition 3.2. *The extended codes $\overline{Q_i}$ and $\hat{Q}_i$ over R are formed by adding the same columns that are used to extend codes over $\mathbb{Z}_4$.*

Theorem 3.3. *If $p \equiv \pm 1$ (mod 8), then*

$$\overline{Q_i} = u_0\overline{D}_1 \oplus u_1\overline{D}_2 \oplus ... \oplus u_t\overline{D}_2.$$

If $p \equiv 1$ (mod 8), then

$$\hat{Q}_i = u_0\hat{D}_1 \oplus u_1\hat{D}_2 \oplus ... \oplus u_t\hat{D}_2,$$

where $i = 1, 2$.

Proof. The proof is obvious from the definition of the extended codes over R. □

Theorem 3.4. *If $p \equiv 1$ (mod 8), then the dual of $\overline{Q_1}$ and $\overline{Q_2}$ are $\hat{Q}_2$ and $\hat{Q}_1$, respectively. If $p \equiv -1$ (mod 8), then $\overline{Q_i}$ is self-dual code, with $i = 1, 2$.*

Proof. By [[18], Proposition 11.13], if $p \equiv 1$ (mod 8), then the dual of $\overline{D_1}$ and $\overline{D_2}$ are $\hat{D}_2$ and $\hat{D}_1$, respectively and if $p \equiv -1$ (mod 8), then $\overline{D_i}$ is self-dual code, with $i = 1, 2$. So if $p \equiv 1$ (mod 8), then

$$\overline{Q}_1{}^{\perp} = u_0\overline{D}_1{}^{\perp} \oplus u_1\overline{D}_2{}^{\perp} \oplus ... \oplus u_t\overline{D}_2{}^{\perp} = u_0\hat{D}_2 \oplus u_1\hat{D}_1 \oplus ... \oplus u_t\hat{D}_1 = \hat{Q}_2.$$

We can prove the last statment in a very similar way to the one which was used above.

□

In continue, we study Hermitian self-dual codes over the ring R and give some results about them.

Theorem 3.5. *Let t be an odd number. The following hold:*
(1) If $p \equiv 1$ (mod 8), then

$$Q_1^{\perp_H} = Q_1' \text{ and } Q_2^{\perp_H} = Q_2';$$

(2) If $p \equiv -1$ (mod 8) , then

$$Q_1^{\perp_H} = Q_2' \text{ and } Q_2^{\perp_H} = Q_1'.$$

Proof. (1) If $p \equiv 1$ (mod 8), then $D_1^{\perp} = C_2$ and $D_2^{\perp} = C_1$, then by Theorem 2.4,

$$Q_1^{\perp_H} = u_0D_2^{\perp} \oplus u_1D_1^{\perp} \oplus u_2D_2^{\perp} \oplus ... \oplus u_tD_1^{\perp} = Q_1'$$

and

$$Q_2^{\perp_H} = u_0D_1^{\perp} \oplus u_1D_2^{\perp} \oplus u_2D_1^{\perp} \oplus ... \oplus u_tD_2^{\perp} = Q_2'.$$

(2) If $p \equiv -1$ (mod 8), then $D_1^{\perp} = C_1$ and $D_2^{\perp} = C_2$. We use similar way to the one used in proof of (1). □

We propose using Theorem 3.5 to construct eight Hermitian self-dual codes of length p over the ring R.

Theorem 3.6. *Let t be an odd number. If $p \equiv 1$ (mod 8), there are four Hermitian self-dual codes over R as follows:*
$E_1 = u_0D_1 \oplus u_1C_2 \oplus u_2D_1 \oplus ... \oplus u_tC_2$;
$E_2 = u_0C_2 \oplus u_1D_1 \oplus u_2C_2 \oplus ... \oplus u_tD_1$;
$E_3 = u_0D_2 \oplus u_1C_1 \oplus u_2D_2 \oplus ... \oplus u_tC_1$;
$E_4 = u_0C_1 \oplus u_1D_2 \oplus u_2C_1 \oplus ... \oplus u_tD_2$.

Proof. If $p \equiv 1 \ (mod\ 8)$, $D_1^{\perp} = C_2$ and $D_2^{\perp} = C_1$. So we can prove this theorem in a very similar way to the one which was used in Theorem 3.5. □

There is another construction in QR-codes over R in addition to that introduced in Theorem 3.6, where t is an odd number and $p \equiv -1 \ (mod\ 8)$.

Theorem 3.7. *Let t be an odd number. If $p \equiv -1 \ (mod\ 8)$, there are four Hermitian self-dual codes over R as follows:*
$E_5 = u_0D_1 \oplus u_1C_1 \oplus u_2D_1 \oplus ... \oplus u_tC_1$;
$E_6 = u_0C_1 \oplus u_1D_1 \oplus u_2C_1 \oplus ... \oplus u_tD_1$;
$E_7 = u_0D_2 \oplus u_1C_2 \oplus u_2D_2 \oplus ... \oplus u_tC_2$;
$E_8 = u_0C_2 \oplus u_1D_2 \oplus u_2C_2 \oplus ... \oplus u_tD_2$.

Proof. Since $D_1^{\perp} = C_1$ and $D_2^{\perp} = C_2$, then this follows from Theorem 2.5.

□

Corollary 3.2. *If $p \equiv 1 \ (mod\ 8)$, then E_1 and E_2 are equivalent to E_3 and E_4, respectively and if $p \equiv -1 \ (mod\ 8)$, then E_5 and E_6 are equivalent to E_7 and E_8, respectively.*

Proof. We use similar way to that used in the proof of Theorem 3.1. □

4. Examples of Hermitian self-dual codes over R

In this section, we study an example of Hermitian cyclic self-dual code of length 3 over R, where $t = 1, 2$. We also investigate an example of Hermitian self-dual families of quadratic residue codes of length 17 over $R = \mathbb{Z}_4 + u_1\mathbb{Z}_4$.

Example 4.1. *Let $t = 1$ and $R = \mathbb{Z}_4 + u_1\mathbb{Z}_4$. Over $\mathbb{Z}_4$, we have*

$$x^3 - 1 = (3 + x)(1 + x + x^2) = g_1(x)g_2(x).$$

There are nine Hermitian cyclic self-dual codes of length 3 over R. For example the code $C =< 2u_0g_1 + u_1(2 + g_2) >$ is Hermitian cyclic self-dual code of length 3 and type $4^1 2^4$ over R and its Gray image corresponds to a $(6, 64, 2)$ linear code over $\mathbb{Z}_4$ and $[12, 6, 2]$ linear code over $\mathbb{F}_2$. So the Gray image $\overline{C}$ corresponds to a $(8, 64, 4)$ linear code over $\mathbb{Z}_4$ and $[16, 6, 4]$ linear code over $\mathbb{F}_2$. Let $t = 2$ and $R' = u_0\mathbb{Z}_4 + u_1\mathbb{Z}_4 + u_2\mathbb{Z}_4$. There are nine Hermitian cyclic self-dual codes of length 3 over R'. To obtain these codes we can simply add $2u_2$ to the generators of the Hermitian cyclic self-dual codes over R. There is only one Euclidean cyclic self-dual code of length 3 over R. It is $C =< 2 >$.

Example 4.2. *Let $R = \mathbb{Z}_4 + u_1\mathbb{Z}_4$ and $p = 17$. Let $e_1(x) = x + x^2 + x^4 + x^8 + x^9 + x^{13} + x^{15} + x^{16}$ and $e_2(x) = x^3 + x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{12} + x^{14}$. Then QR-codes Q_1 and Q_1' are generated by $p_1(x) = u_0(1 + e_1(x)) + u_1(1 + e_2(x))$ and $p_2(x) = u_0(3e_2(x)) + u_1(3e_1(x))$ in $\frac{R[X]}{<X^{17}-1>}$, respectively. By Theorem 3.6, E_i is a Hermitian self-dual code of length 17 over R, with $1 \leq i \leq 4$. So its Gray image corresponds to a $(34, 4^{17}, 5)$ linear code over $\mathbb{Z}_4$ and $(68, 2^{34}, 5)$ non-linear code over $\mathbb{F}_2$ and $d_E(E_i) = d_L(E_i) = 7$. The Lee and Euclidean and Hamming weight distribution of E_i are given as follows:*
$W_L(z) = 1 + 136z^7 + 476z^8 + 578z^9 + 2788z^{10} + 4760z^{11} + 13328z^{12} + 14008z^{13} + 30804z^{14} + 50864z^{15} + 102510z^{16} + 245856z^{17} + 636497z^{18} + ...$
$W_E(z) = 1 + 136z^7 + 340z^8 + 170z^9 + 544z^{10} + 544z^{11} + 1258z^{12} + 1768z^{13} + 4760z^{14} + 28152z^{15} + 38148z^{16} + 53756z^{17} + 105400z^{18} + ...$
$W_H(z) = 1 + 34z^5 + 136z^6 + 748z^7 + 3502z^8 + 8449z^9 + 21760z^{10} + 45220z^{11} + 67524z^{12} +$

$153102z^{13} + 356320z^{14} + 1453568z^{15} + 5404589z^{16} + 17024568z^{17} + 49412064z^{18} + ...$

5. Quantum codes from quadratic residue codes over R

Let q be a prime power. A q-ary quantum code of length n ia a subspace of $\mathbb{C}^{q^n}$. The following theorem gives a condition on the existence of quantum codes over $\mathbb{F}_{q^k}$ which obtain from linear codes over finite chain ring with residue field $\mathbb{F}_{q^k}$.

Theorem 5.1. [[7], Corollary 5.4] Let R be a finite chain ring with maximal ideal $< \gamma >$, nilpotency index e, and residue field $\frac{R}{<\gamma>} = \mathbb{F}_{q^k}$ and let C_1 and C_2 be two linear codes over R of length n such that $C_1 \subset C_2$ with $|C_1| = K_1$ and $|C_2| = K_2$. Then there exists an $((q^{k(e-1)}n, \frac{K_2}{K_1}, d))$ quantum code over $\mathbb{F}_{q^k}$ with minimum distance $d = min\{d_{hom}(C_2 \setminus C_1), d_{hom}(C_1^{\perp})\}$.

Theorem 5.2. *Let $p \equiv -1$ (mod 8). Then there exists an $((2(t+1)p, 2^{2(t+1)}, d))$ quantum code over $\mathbb{F}_2$, with minimum distance $d = min\{d_L(Q_1 \setminus Q_1^{\perp}), d_L(Q_1)\}$. Moreover, there exists an $((2(t+1)p, 1, d_L(Q_1')))$ quantum code over $\mathbb{F}_2$.*

Proof. By Theorem 3.2, if $p \equiv -1$ (mod 8), Q_1' and Q_2' are self-orthogonal and $Q_1'^{\perp} = Q_1$ and $Q_2'^{\perp} = Q_2$. So $Q_i^{\perp} = Q_i' \subseteq Q_i'^{\perp} = Q_i$, where $i = 1, 2$. Then $\phi'(Q_i)^{\perp} = \phi'(Q_i^{\perp}) \subseteq \phi'(Q_i)$. Then by Corollary 5.1, there exists an $((2(t+1)p, 2^{2(t+1)}, d))$ quantum code over $\mathbb{F}_2$, with minimum distance $d = min\{d_L(Q_1 \setminus Q_1^{\perp}), d_L(Q_1)\}$. On the other hand, $\phi'(Q_i')^{\perp} = \phi'(Q_i'^{\perp}) = \phi'(Q_i)$, where $i = 1, 2$. Then by Theorem 5.1, there exists an $((2(t+1)p, 1, d_L(Q_1')))$ over $\mathbb{F}_2$.

□

Theorem 5.3. *Let $p \equiv 1$ (mod 8). Then there exists an $((2(t+1)p, 2^{2(t+1)}, d))$ quantum code over $\mathbb{F}_2$, with minimum distance $d = min\{d_L(Q_1 \setminus Q_2^{\perp}), d_L(Q_2)\}$. Moreover, there exists an $((2(t+1)p, 1, d_L(Q_2')))$ quantum code over $\mathbb{F}_2$.*

Proof. By Theorem 3.1, if $p \equiv 1$ (mod 8), then $Q_i' \subseteq Q_i$ and $Q_1'^{\perp} = Q_2$ and $Q_2'^{\perp} = Q_1$, where $i = 1, 2$. So $Q_1^{\perp} \subseteq Q_2$ and $Q_2^{\perp} \subseteq Q_1$. Then $\phi'(Q_1)^{\perp} = \phi'(Q_1^{\perp}) \subseteq \phi'(Q_2)$ and $\phi'(Q_2)^{\perp} = \phi'(Q_2^{\perp}) \subseteq \phi'(Q_1)$. Then by Theorem 5.1, there exists an $((2(t+1)p, 2^{2(t+1)}, d))$ quantum code over $\mathbb{F}_2$, with minimum distance $d = min\{d_L(Q_1 \setminus Q_2^{\perp}), d_L(Q_2)\}$. On the other hand, since $\phi'(Q_1')^{\perp} = \phi'(Q_1'^{\perp}) = \phi'(Q_2)$ and $\phi'(Q_2')^{\perp} = \phi'(Q_2'^{\perp}) = \phi'(Q_1)$, it follows there exists an $((2(t+1)p, 1, d_L(Q_2')))$ quantum code over $\mathbb{F}_2$. □

Table 1 presents some $((n, K, d))$ quantum codes derived from quadratic residue codes over $\mathbb{Z}_4 + u_1\mathbb{Z}_4$ using Theorems 5.2 and 5.3.

TABLE 1. $((n, K, d))_2$ quantum codes derived from quadratic residue codes over $\mathbb{Z}_4 + u_1\mathbb{Z}_4$

Length	$((n, K, d))_2$
7	$((28, 2^4, 4))_2$
7	$((28, 1, 6))_2$
17	$((68, 2^4, 7))_2$
17	$((68, 1, 8))_2$
23	$((92, 2^4, 10))_2$
23	$((92, 1, 12))_2$
31	$((124, 2^4, 11))_2$
31	$((124, 1, 12))_2$

6. Conclusions

We studied the structure of linear, cyclic and, especially, quadratic residue codes over the ring $R = \mathbb{Z}_4 + u_1\mathbb{Z}_4 + ... + u_t\mathbb{Z}_4$, where $t \geq 1$. Moreover, we gave general properties of Euclidean and Hermitian linear self-dual codes over R and obtained a method to construct quantum codes over $\mathbb{F}_2$ from Gray images of quadratic residue codes over the ring R.

REFERENCES

[1] *I. F. Blake*, Codes over certain rings, Inform. control., **20**(1972), No. 4, 396-404.

[2] *I. F. Blake*, Codes over integer residue rings, Inform. Control., **29**(1975), No. 4, 295-300.

[3] *A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane*, Quantum error correction via codes $\mathbb{F}_4$, IEEE Trans. Inform. Theory., **44**(1998), No. 4, 1369-1387.

[4] *M.H. Chiu, S. T. Yau and Y. Yue*, $\mathbb{Z}_8$-cyclic codes and quadratic residue codes, Adv. Appl. Math., **14**(2009), No. 2, 13-20.

[5] *S.T. Dougherty, J.L. Kim and H. Kulosman*, MDS codes over finite principal ideal rings, Des. Codes Cryptogr., **50**(2009), No. 1, 77-92.

[6] *H. Dinh and S.R. López- permouth*, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory., **50**(2004), No. 8, 1728-1744.

[7] *K. Guenda, T. A. Gulliver*, Quantum codes over rings, Int. J. Quantum Inform., **12**(2014), No. 4, 1450020-1450031.

[8] *W.C. Huffman and V. Pless*, Fundamentals of error correcting codes, Cambrigde University press, 2003.

[9] *A. Kaya, B, Yildiz and I, Siap*, Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$ and their Gray images, J. Pure Appl. Algebra., **218**(2014), No. 11, 1999-2011.

[10] *V. Pless and P. Solé*, Cyclic Self-Dual $\mathbb{Z}_4$-codes, Finite Fields Appl., **3**(1997), No. 1, 48-69.

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

[12] *J. Qian*, Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, Int. J. Inform. Comput. Sci., **10**(2013), No. 4, 1715-1722.

[13] *K. Samei and A. Soufi*, Quadratic residue codes over $\mathbb{F}_{p^r} + u_1\mathbb{F}_{p^r} + ... + u_t\mathbb{F}_{p^r}$, Adv. Math. Commun., **11**(2017), No. 4, 791-804.

[14] *M. Shi, Q. Liqin, L. Sok, N. Aydin and P. Solé*, On constacyclic codes over $\frac{\mathbb{Z}_4[u]}{<u^2-1>}$ and their Gray images, Finite Fields Appl., **45**(2017), 86-95.

[15] *M. Shi, P. Solé and B. Wu*, Cyclic codes and the weight enumerators over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$, Appl. Comput. Math., **12**(2013), No. 2, 247-255.

[16] *M. Shi and Y, Zhang*, Quasi-twisted codes with constacyclic constituent codes, Finite Fields Appl., **39**(2016), 159-178.

[17] *B. Taeri*, Quadratic Residue codes over $\mathbb{Z}_9$, J. Korean Math. Soc., **46**(2009), No. 1, 13-33.

[18] *Z. X. Wan*, Quaternary codes, Singapore, World Scientific, 1997.