Bull. Korean Math. Soc. **59** (2022), No. 2, pp. 265–276
https://doi.org/10.4134/BKMS.b200214
pISSN: 1015-8634 / eISSN: 2234-3016

# DUADIC CODES OVER FINITE LOCAL RINGS

Arezoo Soufi Karbaski and Karim Samei

Abstract. In this paper, we introduce duadic codes over finite local rings and concentrate on quadratic residue codes. We study their properties and give the comprehensive method for the computing the unique idempotent generator of quadratic residue codes.

## 1. Introduction

Duadic codes over finite fields form an important class of cyclic codes. These codes were first introduced by Leon et al. and they became a widely popular research field in coding theory [3]. Duadic codes generalize quadratic residue codes to composite lengths. In continuation of researches on the quadratic residue codes over $\mathbb{Z}_4$, $\mathbb{Z}_8$ and $\mathbb{Z}_9$ (see [1], [6] and [8]), we study the construction of duadic codes over finite local rings. By using the extended quadratic residue codes over a local ring $R$ with residue field $\mathbb{F}_q$ and a Gray map that preserves self-duality, we can obtain self-dual codes over $\mathbb{F}_q$ which can not be obtaind from the extended quadratic residue codes over $\mathbb{F}_q$.

In Section 2, we state some preliminaries of cyclic codes over finite local rings. In Section 3, we define duadic codes and specially quadratic residue codes over finite local rings. We also study the structure of the extended quadratic residue codes and obtain a method for the computing the unique idempotent generator of quadratic residue codes over finite local rings. In Section 4, we present the examples of quadratic residue codes over finite local rings.

## 2. Preliminaries

Throughout this paper $R$ is a finite local ring with maximal ideal $M$, the residue field $\mathbb{F}_q = \frac{R}{M}$ and $\mu$ is the natural projection $R[x] \to \mathbb{F}_q[x]$. A polynomial $e(x)$ in $R[x]$ is an *idempotent* if $e^2(x) = e(x)$. A linear code $C$ over ring $R$ of length $n$ is a $R$-submodule of $R^n$. A *generator matrix* for a linear code $C$ is a matrix $G$ whose rows generate $C$. The *Hamming weight* of a codeword is the number of non-zero components.

Received March 6, 2020; Revised November 26, 2020; Accepted December 6, 2021.
2020 *Mathematics Subject Classification.* 94B05, 94B15, 11T71.
*Key words and phrases.* Finite local ring, duadic code, quadratic residue code.

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be two elements of $R^n$. The Euclidean inner product of vectors $\mathbf{x}, \mathbf{y}$ is $[\mathbf{x}, \mathbf{y}] = \sum_{i=1}^{n} x_i y_i$. The dual code $C^\perp$ of $C$ with respect to the Euclidean inner product is defined as

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

A code $C$ is *self-orthogonal* provided $C \subseteq C^\perp$, *self-dual* provided $C = C^\perp$, and *complementary-dual* (LCD) provided $C \cap C^\perp = \{0\}$. Note that, if $C$ is a code of length $n$ over $R$, then a *complement* of $C$ is a code $D$ such that $C + D = R^n$ and $C \cap D = \{0\}$. A linear code $C$ of length $n$ over $R$ is said to be *cyclic* if for any codeword $\mathbf{c} \in C$, we have:

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

Such a code can be represented as an ideal of the quotient ring $R_n = \frac{R[x]}{\langle x^n - 1 \rangle}$. Also the map $\mu$ can be extended to the map $\overline{\mu}$ from $\frac{R[x]}{\langle x^n - 1 \rangle}$ to $\frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$. Inasmuch as $\overline{\mu}$ is an epimorphism, we have $C^e = \overline{\mu}(C)$.

Let $a$ be an integer such that $\gcd(a, n) = 1$. The function $\mu_a$ defined on $\{0, 1, 2, \ldots, n-1\}$ by $\mu_a(i) \equiv ai \pmod{n}$ is a permutation of the coordinate positions $\{0, 1, 2, \ldots, n-1\}$ of a cyclic code of length $n$ and is called a *multiplier.* A multiplier takes a cyclic code into an equivalent cyclic code.

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 $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ in $R^n$ is even-like provided that $\sum_{i=0}^{n-1} x_i = 0$).

$x^n - 1$ has no repeated factors in $\mathbb{F}_q[x]$ if and only if $\gcd(n, q) = 1$, an assumption we make throughout this paper. The following theorem is well known, see [4, Theorem XIII.4].

**Proposition 2.1** (Hensel' Lemma). *Let $F(x)$ be in $R[x]$ and $\mu(F(x)) = g_1(x) \cdots g_t(x)$, where $g_1(x), \ldots, g_t(x)$ are pair-wise coprime. Then there exist $G_1(x), \ldots, G_t(x)$ in $R[x]$ such that*

(1) *$G_1(x), \ldots, G_t(x)$ are pair-wise coprime*;

(2) *$\mu(G_i(x)) = g_i(x)$, $1 \leq i \leq t$;*

(3) *$F(x) = G_1(x) \cdots G_t(x)$.*

Now we have the following definition, see [5].

**Definition 2.2** (Hensel lift of a cyclic code). Let $g(x) \in \mathbb{F}_q[x]$ be a monic polynomial and $g(x) \mid x^n - 1$. The cyclic code $\langle G(x) \rangle$ such that $G(x)$ is the *Hensel* lift of $g(x)$ is called the *Hensel* lift of the cyclic code $\langle g(x) \rangle$ and is denoted by $C^l$.

Thus the Hensel lift of the cyclic code is a cyclic code with a monic generator polynomial. With the notation as in Definition 2.2, the following lemma holds.

**Lemma 2.3.** *Let $C$ be a cyclic code of length $n$ over $\mathbb{F}_q$ with generator polynomial $g(x)$. Then ${C^l}^\perp = {C^\perp}^l$.*

*Proof.* Let $C$ be a cyclic code of length $n$ over $\mathbb{F}_q$ with generator polynomial $g(x)$ such that $x^n - 1 = g(x)h(x)$ in $\mathbb{F}_q[x]$. Then ${C^l}^{\perp} = \langle H^*(x) \rangle$ such that $x^n - 1 = G(x)H(x)$ in $R[x]$ and $\overline{\mu}(G(x)) = g(x)$ and $\overline{\mu}(H(x)) = h(x)$. Also we have ${C^{\perp}}^l = \langle H^*(x) \rangle$. Thus ${C^l}^{\perp} = {C^{\perp}}^l$. □

**Proposition 2.4** ([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 $C^{\perp}$.*

**Proposition 2.5** ([8])**.** *Let $R$ be a finite commutative ring with identity and let $t_1(x)$, $t_2(x)$ be idempotents of $R$. If $C_1 = \langle t_1(x) \rangle$, $C_2 = \langle t_2(x) \rangle$ are cyclic codes over $R$, then $C_1 \cap C_2$ and $C_1 + C_2$ have idempotent generators $t_1(x)t_2(x)$ and $t_1(x) + t_2(x) - t_1(x)t_2(x)$, respectively.*

The proof of the following theorem is similar to [1, Theorem 2.0.1], so we omit the proof here.

**Proposition 2.6.** *Let $G(x)$ be a monic polynomial divisor of $x^n - 1$ in $R$ and $C = \langle G(x) \rangle$. Then the code $C$ of $R$ has a unique idempotent generator.*

**Lemma 2.7.** *Let $e(x)$ be an idempotent polynomial in $\frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$. If $E(x)$ and $E'(x)$ are two idempotent polynomials in $R_n$ such that $\overline{\mu}(E(x)) = \overline{\mu}(E'(x)) = e(x)$, then $E(x) = E'(x)$.*

*Proof.* If $\overline{\mu}(E(x)) = \overline{\mu}(E'(x)) = e(x)$, then $\overline{\mu}(E'(x)E(x) - E'(x)) = 0$. Hence $x^n - 1 \mid \mu(E'(x)E(x) - E'(x))$ and there exists $H(x) \in R[x]$ such that

$$\mu(E'(x)E(x) - E'(x) - H(x)(x^n - 1)) = 0.$$

This equation implies that there exists $m \in \mathbb{N}$ such that

$$(E'(x)E(x) - E'(x) - H(x)(x^n - 1))^m = 0,$$

see [4, Theorem XIII.2]. Hence $E'(x)E(x) - E'(x)$ is nilpotent. On the other hand, $(E'(x)E(x) - E'(x))^2 = -(E'(x)E(x) - E'(x))$. This implies that $E'(x)E(x) = E'(x)$. Similarly, $E'(x)E(x) = E(x)$. Thus $E(x) = E'(x)$. □

Note that if $C$ is a cyclic code over $R$ with idempotent generator $E(x)$, then $C$ is a self-orthogonal code if and only if $C \cap C^{\perp} = C$, this is the case if and only if $E(x)(1 - \mu_{-1}(E(x))) = E(x)$ by Propositions 2.4 and 2.5. Also $C$ is a self-dual code over $R$ if and only if $E(x) = 1 - \mu_{-1}(E(x))$. Now we have the following theorem.

**Proposition 2.8.** *Let $C$ be a cyclic code of length $n$ over $\mathbb{F}_q$ with idempotent generator $e(x)$. Then the following statements hold.*

(1) *$C$ is self-orthogonal code over $\mathbb{F}_q$ if and only if $C^l$ is a self-orthogonal code over $R$;*

(2) *$C$ is self-dual code over $\mathbb{F}_q$ if and only if $C^l$ is a self-dual code over $R$.*

*Proof.* Let $E(x)$ be the idempotent generator of $C^l$. It is sufficient to show that $E(x)(1-\mu_{-1}(E(x))) = E(x)$ if and only if $e(x)(1-\mu_{-1}(e(x))) = e(x)$. If $e(x)(1-\mu_{-1}(e(x))) = e(x)$, then $\overline{\mu}(E(x)(1-\mu_{-1}(E(x)))) = \overline{\mu}(E(x))$ which means that $E(x)(1-\mu_{-1}(E(x))) = E(x)$ by Lemma 2.7. On the other hand if $E(x)(1-\mu_{-1}(E(x))) = E(x)$, then $e(x)(1-\mu_{-1}(e(x))) = \overline{\mu}(E(x)(1-\mu_{-1}(E(x)))) = \overline{\mu}(E(x)) = e(x)$. Therefore part (1) was proved. Similarly, $E(x) = 1-\mu_{-1}(E(x))$ if and only if $e(x) = 1-\mu_{-1}(e(x))$. Then the proof is complete. □

## 3. Duadic codes

Let $C_1$, $C_2$ and $D_1$, $D_2$ be even-like and odd-like duadic codes over $\mathbb{F}_q$, respectively, such that $e_1(x)$ and $e_2(x)$ are the idempotent generators of $[n, \frac{n-1}{2}]$ duadic codes over $\mathbb{F}_q$ and $1-e_2(x)$ and $1-e_1(x)$ are the idempotent generators of $[n, \frac{n+1}{2}]$ duadic codes over $\mathbb{F}_q$ such that

$$e_1(x) + e_2(x) = 1 - \overline{j}(x)$$

and there is a multiplier $\mu_a$ such that

$$\mu_a(e_1(x)) = e_2(x) \text{ and } \mu_a(e_2(x)) = e_1(x).$$

We note that $\overline{j}(x) = \frac{1}{p}(1 + x + x^2 + \cdots + x^{p-1})$ in $\frac{\mathbb{F}_q[x]}{\langle x^p - 1\rangle}$ is the idempotent generator of repetition code of length $p$, see [2, Ch. 6]. We define duadic codes over finite local rings in term of their idempotents.

**Definition 3.1.** Duadic codes over $R$ come in two pairs, one even-like pair, which we usually denote $C'_1$ and $C'_2$, and one odd-like pair, usually denoted $D'_1$ and $D'_2$ such that $C'_i$ and $D'_i$ are Hensel lifts of duadic codes over $\mathbb{F}_q$ for $i = 1, 2$.

Note that $\overline{j'}(x) = \frac{1}{p}(1 + x + x^2 + \cdots + x^{p-1})$ is an idempotent in $R_p$.

**Theorem 3.2.** *Let $C'_1$ and $C'_2$ be a pair of even-like duadic codes over $R$ with idempotent generators $E_1(x)$ and $E_2(x)$, respectively. Then*

(1) $E_1(x) + E_2(x) = 1 - \overline{j'}(x)$ *and*

(2) *there is a multiplier $\mu_a$ such that $\mu_a(C'_1) = C'_2$ and $\mu_a(C'_2) = C'_1$.*

*Proof.* Let $C_1$ and $C_2$ be even-like duadic codes over $\mathbb{F}_q$ with idempotent generators $e_1(x)$ and $e_2(x)$, respectively. To prove the first part it is sufficient to prove that $E_1(x)E_2(x) = 0$. Since $\overline{\mu}(E_1(x)E_2(x)) = e_1(x)e_2(x) = 0 = \overline{\mu}(0)$, then by Lemma 2.7, $E_1(x)E_2(x) = 0$. It follows that $E_1(x) + E_2(x)$ is an idempotent. By Lemma 2.7, $E_1(x) + E_2(x) = 1 - \overline{j'}(x)$, because $\overline{\mu}(1 - \overline{j'}(x)) = 1 - \overline{j}(x) = e_1(x) + e_2(x) = \overline{\mu}(E_1(x) + E_2(x))$. Therefore part (1) was proved. Since $C_1$ and $C_2$ are even-like duadic codes over $\mathbb{F}_q$, then there is a multiplier $\mu_a$ such that $\mu_a(e_1(x)) = e_2(x)$ and $\mu_a(e_2(x)) = e_1(x)$. Inasmuch as $\overline{\mu}(\mu_a(E_1(x))) = e_2(x)$ and $\overline{\mu}(\mu_a(E_2(x))) = e_1(x)$, hence $\mu_a(E_1(x)) = E_2(x)$ and $\mu_a(E_2(x)) = E_1(x)$. □

By Definition 3.1 and [2, Corollary 6.3.2], we have the following theorem.

**Theorem 3.3.** *Duadic codes of length $n$ over $R$ exist if and only if $q$ is a square modulo $n$.*

**Corollary 3.4.** *Let $C_1'$ and $C_2'$ be even-like duadic codes over $R$ with idempotent generators $E_1(x)$ and $E_2(x)$. Then $1 - E_2(x)$ and $1 - E_1(x)$ are the idempotent generators of odd-like duadic codes over $R$.*

*Proof.* Let $E_1'(x)$ and $E_2'(x)$ be the idempotent generators of $D_1'$ and $D_2'$ over $R$. Since $\langle \overline{\mu}(E_1'(x)) \rangle = \overline{\mu}(D_1') = D_1 = \langle 1 - e_2(x) \rangle$ and $\overline{\mu}(E_1'(x))$ is idempotent polynomial, then $\overline{\mu}(E_1'(x)) = 1 - e_2(x)$. From Lemma 2.7, $E_1'(x) = 1 - E_2(x)$. Similarly, $E_2'(x) = 1 - E_1(x)$. □

It is obvious that $C_1'$ and $D_1'$ are equivalent to $C_2'$ and $D_2'$, respectively. Also it is easy to see that $C_1' \subseteq D_1'$ and $C_2' \subseteq D_2'$.

**Theorem 3.5.** *If $\mu_a$ gives the splitting for $C_1'$ and $C_2'$, then the following statements hold.*

(1) $E_1(x)E_2(x) = 0$;

(2) $C_1' \cap C_2' = \{0\}$ *and* $C_1' + C_2' = \langle 1 - \overline{j}'(x) \rangle$;

(3) $|C_i'| = |R|^{\frac{n-1}{2}}$ *and* $|D_i'| = |R|^{\frac{n+1}{2}}$;

(4) $D_1'$ *is the cyclic complement of* $C_2'$ *and* $D_2'$ *is the cyclic complement of* $C_1'$;

(5) $\mu_a(D_1') = D_2'$ *and* $\mu_a(D_2') = D_1'$;

(6) $D_1' \cap D_2' = \langle \overline{j}'(x) \rangle$ *and* $D_1' + D_2' = R_n$;

(7) $D_i' = C_i' + \langle \overline{j}'(x) \rangle = \langle \overline{j}'(x) + E_i(x) \rangle$, *where* $i = 1, 2$.

*Proof.* (1) See the proof of Theorem 3.2.

(2) By Proposition 2.5 and part (1) above, $C_1' \cap C_2' = \langle E_1(x)E_2(x) \rangle = \{0\}$ and $C_1' + C_2' = \langle E_1(x) + E_2(x) - E_1(x)E_2(x) \rangle = \langle 1 - \overline{j}'(x) \rangle$.

(3) Since $\dim(C_i) = \frac{n-1}{2}$ and $\dim(D_i) = \frac{n+1}{2}$, we conclude part (3) from Definition 3.1.

(4) To prove this part, we can use Proposition 2.5 and Corollary 3.4.

(5) This part is obtained from the following equations

$$\mu_a(D_1') = \langle \mu_a(1 - E_2(x)) \rangle = \langle 1 - E_1(x) \rangle = D_2'$$

and

$$\mu_a(D_2') = \langle \mu_a(1 - E_1(x)) \rangle = \langle 1 - E_2(x) \rangle = D_1'.$$

(6) By Proposition 2.5,

$$D_1' \cap D_2' = \langle (1 - E_2(x))(1 - E_1(x)) \rangle = \langle 1 - E_1(x) - E_2(x) \rangle = \langle \overline{j}'(x) \rangle$$

and

$$D_1' + D_2' = \langle (1 - E_2(x)) + (1 - E_1(x)) - \overline{j}'(x) \rangle = \langle 1 \rangle = R_n.$$

(7) Inasmuch as $E_i(x)\overline{j}'(x) = E_i(x)(1 - E_1(x) - E_2(x)) = 0$ for $i = 1, 2$, hence

$$D_1' = \langle 1 - E_2(x) \rangle = \langle \overline{j}'(x) + E_1(x) \rangle = C_1' + \langle \overline{j}'(x) \rangle$$

and

$$D'_2 = \langle 1 - E_1(x)\rangle = \langle \overline{j'}(x) + E_2(x)\rangle = C'_2 + \langle \overline{j'}(x)\rangle.$$

Then the proof is complete. □

Note that if $C$ is a cyclic code of length $n$ over $R$, then $C$ is an even-like code over $R$ if and only if $\overline{\mu}(C)$ is an even-like code over $\mathbb{F}_q$. In particular, $C$ is an odd-like code over $R$ if and only if $\overline{\mu}(C)$ is an odd-like code over $\mathbb{F}_q$. Also if $C$ is any $[n, \frac{n-1}{2}]$ cyclic code over $\mathbb{F}_q$, then $C$ is self-orthogonal if and only if $C$ is an even-like duadic code whose splitting is given by $\mu_{-1}$, see [2, Theorem 6.4.1]. Thus we have the following corollary.

**Corollary 3.6.** *Let $C$ be any $[n, \frac{n-1}{2}]$ cyclic code over $\mathbb{F}_q$. Then $C'$ is self-orthogonal if and only if $C'$ is an even-like duadic code whose splitting is given by $\mu_{-1}$.*

**Theorem 3.7.** *Let $C'_1$, $C'_2$ and $D'_1$, $D'_2$ be even-like and odd-like duadic codes over $R$, respectively. Then the following statements are equivalent.*
(1) $C'^{\perp}_1 = D'_1$;
(2) $C'^{\perp}_2 = D'_2$;
(3) $\mu_{-1}(C'_1) = C'_2$;
(4) $\mu_{-1}(C'_2) = C'_1$.

*Proof.* By [2, Theorem 6.4.2], $C_1^{\perp} = D_1$ if and only if $C_2^{\perp} = D_2$. Hence $C_1^{{\perp}^{l'}} = D'_1$ if and only if $C_2^{{\perp}^{l'}} = D'_2$. By Lemma 2.3, parts (1) and (2) are equivalent. Since $\mu_{-1}^{-1} = \mu_{-1}$, parts (3) and (4) are equivalent. If $C'^{\perp}_1 = D'_1$, then $C'_1$ is self-orthogonal. We conclude part (3) from Corollary 3.6. Conversely, if part (3) holds, by Proposition 2.4 we have $C'^{\perp}_1 = D'_1$. □

**Theorem 3.8.** *Let $C'_1$, $C'_2$ and $D'_1$, $D'_2$ be even-like and odd-like duadic codes over $R$, respectively. Then the following statement are equivalent.*
(1) $C'^{\perp}_1 = D'_2$;
(2) $C'^{\perp}_2 = D'_1$;
(3) $\mu_{-1}(C'_1) = C'_1$;
(4) $\mu_{-1}(C'_2) = C'_2$.

*Proof.* By [2, Theorem 6.4.3], $C_1^{\perp} = D_2$ if and only if $C_2^{\perp} = D_1$. Hence it is easy to see that parts (1) and (2) are equivalent. By Proposition 2.4, parts (1) and (3) are equivalent. Simiralry, parts (2) and (4) are equivalent. □

### 3.1. Quadratic residue codes

Quadratic residue codes over finite fields are cyclic codes which can be defined in terms of their idempotent generators. In this section, we assume that $Q_p$ and $N_p$ are the sets of non-zero quadratic residue and quadratic non-residue modulo $p$, respectively. Also we let $q_1(x) = \sum_{i\in Q_p} x^i$ and $q_2(x) = \sum_{i\in N_p} x^i$. We note that the quadratic residue codes over finite local rings are special cases of duadic codes.

**Definition 3.9.** The quadratic residue codes over $R$ are duadic codes of odd prime length $p$.

By Theorem 3.3, we have the following corollary.

**Corollary 3.10.** *Quadratic residue codes of odd prime length $p$ exist over $R$ if and only if $q$ is a square modulo $p$.*

**Theorem 3.11.** *Let $C$ be a quadratic residue code over $R$ with idempotent generator $E(x)$. Then $\mu_a(E(x)) = E(x)$ for all $a \in Q_p$.*

*Proof.* If $C$ is a quadratic residue code over $R$, then $\overline{\mu}(C)$ is a quadratic residue code over $\mathbb{F}_q$ with idempotent generator $\overline{\mu}(E(x)) = e(x)$. Hence by [2, Theorem 6.6.3], we have $\mu_a(e(x)) = e(x)$ for all $a \in Q_p$. It is sufficient to show that $\mu_a(e(x)) = e(x)$ if and only if $\mu_a(E(x)) = E(x)$ for every $a$. If $\mu_a(e(x)) = e(x)$, then $\overline{\mu}(\mu_a(E(x))) = e(x)$. Thus by Lemma 2.7, we conclude that $\mu_a(E(x)) = E(x)$. It follows that if $\mu_a(e(x)) = e(x)$, then $\mu_a(E(x)) = E(x)$ for all $a$. Also the converse statment is true. Now, the proof is complete. □

By [2, Theorem 6.6.4], for any $b \in N_p$, $\mu_b$ is a multiplier such that $\mu_b(C_1) = C_2$ and $\mu_b(C_2) = C_1$. Thus we have the following theorem.

**Theorem 3.12.** *Let $C_1'$ be an even-like quadratic residue code of odd prime length $p$ over $R$ with idempotent generator $E_1(x)$. Therefore four quadratic residue codes over $R$ have idempotent generators $E_1(x)$, $\mu_b(E_1(x))$, $E_1(x) + \overline{j'}(x)$, and $\mu_b(E_1(x)) + \overline{j'}(x)$ for any $b \in N_p$.*

*Proof.* By Definition 3.1 and Corollary 3.4, $E_1(x)$, $E_2(x) = \mu_b(E_1(x))$, $1 - E_2(x) = E_1(x) + \overline{j}(x)$ and $1 - E_1(x) = E_2(x) + \overline{j}(x) = \mu_b(E_1(x)) + \overline{j}(x)$ are idempotent generators of four quadratic residue codes over $R$, for any $b \in N_p$. □

The results of Theorem 3.12 show that $\mu_a(C_1') = C_2'$, $\mu_a(C_2') = C_1'$, $\mu_a(D_1') = D_2'$ and $\mu_a(D_2') = D_1'$ for any $b \in N_p$.

**Theorem 3.13.** *Let $C_1'$, $C_2'$ and $D_1'$, $D_2'$ be even-like and odd-like duadic codes over $R$, respectively. Then the following statements hold.*

(1) *If $p \equiv -1 \pmod 4$, then $C_1'$ and $C_2'$ are self-orthogonal and $C_1'^{\perp} = D_1'$ and $C_2'^{\perp} = D_2'$;*

(2) *If $p \equiv 1 \pmod 4$, then $C_1'^{\perp} = D_2'$ and $C_2'^{\perp} = D_1'$.*

*Proof.* (1) If $p \equiv -1 \pmod 4$, then $-1 \in N_p$. Hence by Theorem 3.12, $\mu_{-1}(C_1') = C_2'$ and $\mu_{-1}(C_2') = C_1'$. Then by Theorem 3.7, we have ${C_1'}^{\perp} = D_1'$ and ${C_2'}^{\perp} = D_2'$.

(2) By Theorem 3.11, if $p \equiv 1 \pmod 4$, we conclude that $\mu_{-1}(C_i') = C_i'$ for $i = 1, 2$. It follows ${C_1'}^{\perp} = D_2'$ and ${C_2'}^{\perp} = D_1'$ from Theorem 3.8. □

**Theorem 3.14.** *If $p \equiv 1 \pmod 4$, then $D_1'$ and $D_2'$ are LCD codes over $R$.*

*Proof.* If $p \equiv 1 \pmod 4$, by Theorem 3.13, we have ${C_1'}^{\perp} = D_2'$ and ${C_2'}^{\perp} = D_1'$. Hence by Proposition 2.5, $D_i' \cap {D_i'}^{\perp} = \langle (1 - E_i(x))E_i(x) \rangle = \{0\}$ for $i = 1, 2$. □

### 3.2. Extending quadratic residue codes

In this section, we are ready to define the extended quadratic residue codes over a finite local ring. We can also consider extending odd-like quadratic residue codes in such a way that the extensions are self-dual or dual to each other.

**Definition 3.15.** Let $D'_i$ be an odd-like quadratic residue code of length $p$ over a finite local ring $R$, with $i = 1, 2$. Then there exist different extended quadratic residue codes over $R$ as follows:

(1) $\overline{D_i} = \{(c_0, c_1, \ldots, c_{p-1}, c_p) : (c_0, c_1, \ldots, c_{p-1}) \in D_i \text{ with } \sum_{i=0}^{p} c_i = 0\}$;
(2) $\hat{D}_i = \{(c_0, c_1, \ldots, c_{p-1}, \frac{1}{p}\sum_{i=0}^{p-1} c_i) : (c_0, c_1, \ldots, c_{p-1}) \in D_i\}$.

Note that, if $R$ is a finite local ring with characteristic $q^t$ and $p \equiv -1 \pmod{q^t}$, then $\hat{D}'_i = \overline{D'_i}$.

**Theorem 3.16.** *Let $R$ be a finite local ring with characteristic $q^t$. If $p \equiv -1$ $(\mathrm{mod}\ q^t)$ and $p \equiv -1 \pmod 4$, then $\overline{D'_1}$ and $\overline{D'_2}$ are self-dual.*

*Proof.* $\overline{D'_1}$ has the following $\frac{(p+1)}{2} \times (p+1)$ generator matrix:

$$G = \begin{pmatrix} 0 & & & & & \\ 0 & & & & & \\ \cdot & & & G'_1 & & \\ \cdot & & & & & \\ \cdot & & & & & \\ -1 & \frac{1}{p} & \frac{1}{p} & \frac{1}{p} & \cdots & \frac{1}{p} \end{pmatrix},$$

where $G'_1$ is a generator matrix for $C'_1$. Since

$$D'_i = C'_i + \langle \overline{j}'(x) \rangle, \text{ where } i = 1, 2$$

and $C'_1$ is self-orthogonal by Theorem 3.13, the rows of $G'_1$ are orthogonal to each other and clearly also orthogonal to the last row. On the other hand, the last row is orthogonal to itself, then $\overline{D'_1}$ is self-orthogonal. Since $|\overline{D'_1}| = |D'_1| = |R|^{(\frac{p+1}{2})}$ and $|\overline{D'_1}^{\perp}| = \frac{|R|^{p+1}}{|\overline{D'_1}|} = |R|^{(\frac{p+1}{2})}$, we conclude that $\overline{D'_1}$ is self-dual. A similar argument allows us to prove that $\overline{D'_2}$ is self-dual. □

**Theorem 3.17.** *If $p \equiv 1 \pmod 4$, then $\hat{D}'_1$ and $\overline{D'_2}$ are duals of each other.*

*Proof.* We can prove this theorem in a similar way to the one which was used in Theorem 3.16. □

**Corollary 3.18.** *Let $R$ be a finite local ring with characteristic $q^t$. If $p \equiv 1$ $(\mathrm{mod}\ 4)$ and $p \equiv -1 \pmod{q^t}$, then $\overline{D'_i}$ is formally self-dual, where $i = 1, 2$.*

### 3.3. Idempotent generator of a quadratic residue codes over finite local ring

As we know the unique idempotent generator of quadratic residue codes over finite field have been identified. But finding the unique idempotent generator of these codes over finite local rings is not always easy, see [1] and [8]. Then we present a practical method for the computing the unique idempotent generator of quadratic residue codes over finite local rings.

*Remark* 3.19. Let $R$ be a finite local ring with maximal ideal $M$. Then $ker(\bar{\mu}) = \{k(x) + \langle x^n - 1\rangle : k(x) \in M[x]\}$. By [4, Theorem XIII.2], $M[x] = \cap\{P : P \text{ is a prime ideal in } R[x]\}$, then

$$\sqrt{0_{R_n}} = \cap\left\{\frac{P}{\langle x^n - 1\rangle} : P \text{ is a prime ideal in } R[x]\right\} = \frac{M[x]}{\langle x^n - 1\rangle}.$$

So by [7, Lemma 8.21], there exists $k \in \mathbb{N}$ such that $(\sqrt{0_{R_n}})^k = 0$.

Now we can define the nilpotency index of $ker(\bar{\mu})$.

**Definition 3.20.** Define the nilpotency index of $ker(\bar{\mu})$ to be the smallest natural number $k$ such that $L^k(x) = 0$ for every $L(x) \in ker(\bar{\mu})$.

Thus we are ready to obtain the idempotent generator of a quadratic residue code over finite local ring.

**Proposition 3.21.** *Let $R$ be a finite local ring of characteristic $q^t$ with residue field $\mathbb{F}_q$ and let $k$ be the nilpotency index of $ker(\bar{\mu})$. If $e(x)$ and $E(x)$ are the idempotent generators of quadratic residue codes over $\mathbb{F}_q$ and $R$, respectively, and $F(x)$ is the polynomial in $R[x]$ such that $\bar{\mu}(F(x)) = e(x)$, now we have the following statements.*

(1) *If $k \leq q^t$ and $j$ are the smallest integer number such that $q^t \mid \binom{q^{t+j}}{i}$ for every $1 \leq i \leq k-1$, then $E(x) = (F(x))^{q^{t+j}}$;*

(2) *If $q^t < k$ and $j$ are the smallest integer number such that $q^t \mid \binom{k+j}{i}$ for every $1 \leq i \leq k-1$, then $E(x) = (F(x))^{k+j}$.*

*Furthermore, if $R$ and $\mathbb{F}_q$ have the same characteristic, then $e(x)$ is the idempotent generator of quadratic residue codes over $R$.*

*Proof.* (1) Since $\bar{\mu}(F(x)) = e(x) = \bar{\mu}(E(x))$, then there exists $L(x) \in ker(\bar{\mu})$ such that $F(x) = E(x) + L(x)$. Moreover, if $k \leq q^t$ and $j$ are the smallest integer number such that $q^t \mid \binom{q^{t+j}}{i}$ for every $1 \leq i \leq k-1$, then $(F(x))^{q^{t+j}} = (E(x) + L(x))^{q^{t+j}} = E(x)$. It follows that $(F(x))^{q^{t+j}}$ is the unique idempotent generator of $C$.

(2) We use similar way to that used in the proof of part (1) above.

To prove the claim in the last sentence of the lemma, it is sufficient that we suppose that $F(x) = e(x)$. □

For simplicity, if $R=\mathbb{Z}_{q^t}$, we can suppose that $F(x)=e(x)$ in the above theorem. It should be noted that after obtaining of the idempotent generator of $D_1'$, we can find other three idempotent generators of quadratic residue codes over $R$ by Theorem 3.12. In the next example we obtain idempotent generators of quadratic residue codes of length 5 over $GR(9,2)$ by Proposition 3.21.

**Example 3.22.** Let $R=GR(9,2)=\{a+bw : a,b\in\mathbb{Z}_9 \text{ and } w^2=7w+7\}$ of characteristic 9 with residue field $\mathbb{F}_9=\{\rho^i : \rho=1,\dots,8 \text{ and } \rho^2=\rho+1\}\cup\{0\}$. Then $k=2$ and $j=0$. Since the unique idempotent generator of $C_1$ of length 5 is $\rho^3x^4+\rho x^3+\rho x^2+\rho^3x+1$ and $\bar{\mu}(w)=\rho$, now we can let

$$F(x)=w^3x^4+wx^3+wx^2+w^3x+1\in R.$$

Thus

$$\begin{aligned}(F(x))^9&=(2w+1)x^4+(7w+6)x^3+(7w+6)x^2+(2w+1)x+4\\&=(2w+1)q_1(x)+(7w+6)q_2(x)+4\end{aligned}$$

is the unique idempotent generator of $C_1'$. Similarly, we obtain the unique idempotent generators of $C_2'$, $D_1'$ and $D_2'$ as follows:

$$\begin{aligned}C_2'&=\langle(7w+6)q_1(x)+(2w+1)q_2(x)+4\rangle;\\D_1'&=\langle(2w+3)q_1(x)+(7w+8)q_2(x)+6\rangle;\\D_2'&=\langle(7w+8)q_1(x)+(2w+3)q_2(x)+6\rangle.\end{aligned}$$

In the following example we find the unique idempotent generator of odd-like quadratic residue code of length 11 over $\mathbb{F}_3+u\mathbb{F}_3$, where $u^2=0$.

**Example 3.23.** Let $R=\mathbb{F}_3+u\mathbb{F}_3$, where $u^2=0$. Then $R$ is a finite chain ring with residue field $\mathbb{F}_3$. The unique idempotent generator of odd-like quadratic residue code of length 11 over $\mathbb{F}_3$ is $-(x+x^3+x^4+x^5+x^9)$. Then by Corollary 2.2, the unique idempotent generator of odd-like quadratic residue code of length 11 over $R$ is $-q_1(x)$. Similarly, $C_1'=\langle 1+q_2(x)\rangle$, $C_2'=\langle 1+q_1(x)\rangle$ and $D_2'=\langle -q_2(x)\rangle$.

## 4. Examples of quadratic residue codes over finite chain rings

In this section, we investigate the examples of quadratic residue codes over finite chain rings.

**Example 4.1.** Let $R=GR(4,3)$ be a finite chain ring of characteristic 4 with residue field $\mathbb{F}_8=\{\rho^i : \rho=1,\dots,7 \text{ and } \rho^3=\rho+1\}\cup\{0\}$. Then $R=\{a+bw+cw^2 : a,b,c\in\mathbb{Z}_4 \text{ and } w^3=3w+3\}$. Then the quadratic residue code $D_1'$ of length 7 over $R$ is generated by the monic generator polynomial $(x+3w+2)(x+3w^2)(x+w^2+w)$. Thus $D_1'$ is the $(7,|R|^4,3)$ code and $\overline{D_1'}$ is the $(8,|R|^4,4)$ self-dual code over $R$.

**Example 4.2.** Let $R=GR(9,2)$ and $p=5$. Then $D_1'$ corresponds to a $(5,|R|^3,3)$ MDS and LCD code over $R$. Also its extended corresponds to a $(6,|R|^3,4)$ MDS over $R$.

Table 1. Quadratic residue codes over $GR(4, s)$, where $s = 2, 3, 4$

| Ring | $(n, K, d)_R$ |
|---|---|
| $R = GR(4, 2)$ | $D_1' = (3, \|R\|^2, 2)^*$ |
| $R = GR(4, 2)$ | $\overline{D'}_1 = (4, \|R\|^2, 3)^*$ self-dual |
| $R = GR(4, 2)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(4, 2)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |
| $R = GR(4, 2)$ | $D_1' = (7, \|R\|^4, 3)$ |
| $R = GR(4, 2)$ | $\overline{D'}_1 = (8, \|R\|^4, 4)$ self-dual |
| $R = GR(4, 2)$ | $D'_1 = (11, \|R\|^6, 5)$ |
| $R = GR(4, 2)$ | $\overline{D'}_1 = (12, \|R\|^6, 6)$ self-dual |
| $R = GR(4, 3)$ | $D_1' = (7, \|R\|^4, 3)$ |
| $R = GR(4, 3)$ | $\overline{D'}_1 = (8, \|R\|^4, 4)$ self-dual |
| $R = GR(4, 4)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(4, 4)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |

Table 2. Quadratic residue codes over $GR(2^s, 2)$, where $s = 3, 4, 5$

| Ring | $(n, K, d)_R$ |
|---|---|
| $R = GR(8, 2)$ | $D_1' = (3, \|R\|^2, 2)^*$ |
| $R = GR(8, 2)$ | $\overline{D'}_1 = (4, \|R\|^2, 3)^*$ |
| $R = GR(8, 2)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(8, 2)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |
| $R = GR(8, 2)$ | $D_1' = (7, \|R\|^4, 3)$ |
| $R = GR(8, 2)$ | $\overline{D'}_1 = (8, \|R\|^4, 4)$ self-dual |
| $R = GR(16, 2)$ | $D_1' = (3, \|R\|^2, 2)^*$ |
| $R = GR(16, 2)$ | $\overline{D'}_1 = (4, \|R\|^2, 3)^*$ |
| $R = GR(16, 2)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(16, 2)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |
| $R = GR(32, 2)$ | $D_1' = (3, \|R\|^2, 2)^*$ |
| $R = GR(32, 2)$ | $\overline{D'}_1 = (4, \|R\|^2, 3)^*$ |
| $R = GR(32, 2)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(32, 2)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |

We finish this section by combining the results in Tables 1, 2 and 3.

In Tables 1, 2 and 3, $*$ denotes that the code is MDS.

**Acknomledgments.** The authors would like to thank the referees for carefully reading the manuscript and for their valuable comments and suggestions which improved the exposition of the paper.

TABLE 3. Quadratic residue codes over $GR(q^k, 2)$, where ($q = 3$ and $k = 2, 3$), ($q = 5, 7$ and $k = 2$)

| Ring | $(n, K, d)_R$ |
|---|---|
| $R = GR(9, 2)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(9, 2)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |
| $R = GR(9, 2)$ | $D_1' = (7, \|R\|^4, 4)^*$ |
| $R = GR(9, 2)$ | $\overline{D'}_1 = (8, \|R\|^4, 5)^*$ |
| $R = GR(27, 2)$ | $D_1' = (5, \|R\|^3, 3)^*$ LCD code |
| $R = GR(27, 2)$ | $\overline{D'}_1 = (6, \|R\|^3, 4)^*$ |
| $R = GR(25, 2)$ | ${D'}_1 = (3, \|R\|^2, 2)^*$ |
| $R = GR(25, 2)$ | $\overline{D'}_1 = (4, \|R\|^2, 3)^*$ |
| $R = GR(49, 2)$ | $D_1' = (3, \|R\|^2, 2)^*$ |
| $R = GR(49, 2)$ | $\overline{D'}_1 = (4, \|R\|^2, 3)^*$ |

## References

[1] M. H. Chiu, S. T. Yau, and Y. Yu, $\mathbb{Z}_8$*-cyclic codes and quadratic residue codes*, Adv. Math. Commun. **11** (2017), no. 1, 99–114.

[2] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. https://doi.org/10.1017/CBO9780511807077

[3] J. S. Leon, J. M. Masley, and V. Pless, *Duadic codes*, IEEE Trans. Inform. Theory **30** (1984), no. 5, 709–714. https://doi.org/10.1109/TIT.1984.1056944

[4] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York, 1974.

[5] G. H. Norton and A. Sălăgean, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 6, 489–506. https://doi.org/10.1007/PL00012382

[6] V. S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $Z_4$, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600. https://doi.org/10.1109/18.532906

[7] R. Y. Sharp, *Steps in Commutative Algebra*, second edition, London Mathematical Society Student Texts, 51, Cambridge University Press, Cambridge, 2000.

[8] B. Taeri, *Quadratic residue codes over* $\mathbb{Z}_9$, J. Korean Math. Soc. **46** (2009), no. 1, 13–30. https://doi.org/10.4134/JKMS.2009.46.1.013

Arezoo Soufi Karbaski
Department of Mathematics
Bu Ali Sina University
Hamedan, Iran
*Email address*: arezoo.sufi@basu.ac.ir

Karim Samei
Department of Mathematics
Bu Ali Sina University
Hamedan, Iran
*Email address*: samei@ipm.ir