Duadic and triadic codes over a finite non-chain ring and their Gray images

Mokshi Goyal and Madhu Raka*

Centre for Advanced Study in Mathematics,
Panjab University,
Chandigarh-160014, India
Email: mouliaggarwal701@gmail.com
Email: mraka@pu.ac.in
*Corresponding author

Abstract: Let $f(u)$ be a polynomial of degree m, $m \geq 2$, which splits into distinct linear factors over a finite field $\mathbb{F}_q$. Let $\mathcal{R} = \mathbb{F}_q[u]/\langle f(u)\rangle$ be a finite non-chain ring. In this paper, we study duadic codes, their extensions and triadic codes over the ring $\mathcal{R}$. A Gray map from $\mathcal{R}^n$ to $(\mathbb{F}_q^m)^n$ is defined which preserves self-duality of linear codes. As a consequence, self-dual, isodual, self-orthogonal and complementary dual(LCD) codes over $\mathbb{F}_q$ are constructed. Some examples are also given to illustrate this.

Keywords: quadratic residue codes; duadic codes; extended duadic-codes; triadic codes; Gray map; self-dual and self-orthogonal codes; isodual codes; LCD codes.

Reference to this paper should be made as follows: Goyal, M. and Raka, M. (2018) 'Duadic and triadic codes over a finite non-chain ring and their Gray images', *Int. J. Information and Coding Theory*, Vol. 5, No. 1, pp.36–54.

Biographical notes: Mokshi Goyal obtained her MSc in 2015 from Department of Mathematics, Panjab University, Chandigarh, India and presently pursuing for PhD under the guidance of Professor Madhu Raka.

Madhu Raka received her MSc in 1974 and PhD in 1979 from Panjab University, Chandigarh, India. Presently she is working as a Professor in the same institution. Her research interests are in algebraic coding theory and geometry of numbers.

1 Introduction

Duadic codes form an important class of cyclic codes. They generalise the well known quadratic residue codes of prime length. Triadic codes further generalise duadic codes. While initially duadic codes were studied within the confines of finite fields, there have been recent developments on duadic codes over some special rings. Pless and Qian (1996) studied quadratic residue codes over $\mathbb{Z}_4$, Chiu et al. (2000) extended the ideas to the ring $\mathbb{Z}_8$ and Taeri (2009) considered quadratic residue codes over $\mathbb{Z}_9$. Kaya et al. (2014a) and Zhang and Zhu (2012) studied quadratic residue codes over $\mathbb{F}_p + u\mathbb{F}_p$, where p is an odd prime. Kaya et al. (2014b) studied quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ whereas Liu et al. (2014)

studied them over non-local ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, where $u^3 = u$ and p is an odd prime. Raka et al. (2017) extended their results over the ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p$, where $u^4 = u$ and $p \equiv 1(\mathrm{mod}\ 3)$. Goyal and Raka (2018) studied quadratic residue codes and their extensions over the ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + \cdots + u^{m-1}\mathbb{F}_p$, where $u^m = u$, m any integer greater than 1 and p is a prime satisfying $p \equiv 1(\mathrm{mod}\ (m-1))$. Goyal and Raka (2016) studied duadic codes and their extensions over the ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{m-1}\mathbb{F}_q$, where $u^m = u$ and q is a prime power satisfying $q \equiv 1(\mathrm{mod}\ (m-1))$, generalising all the previous results.

In our previous papers (2016, 2018), the condition that $q \equiv 1(\mathrm{mod}\ (m-1))$ implied that the polynomial $u^m - u$ splits into distinct linear factors over $\mathbb{F}_q$. Here we work on a more general ring. Let $f(u)$ be any polynomial of degree m, $m \geq 2$, which splits into distinct linear factors over $\mathbb{F}_q$. Let $\mathcal{R} = \mathbb{F}_q[u]/\langle f(u)\rangle$ be a finite non-chain ring. In this paper, we study duadic codes and triadic codes over the ring $\mathcal{R}$. A Gray map is defined from $\mathcal{R}^n \rightarrow \mathbb{F}_q^{mn}$ which preserves linearity and in some special cases preserves self-duality. The Gray images of duadic codes and their extensions over the ring $\mathcal{R}$ lead to the construction of self-dual, isodual and self-orthogonal codes. The Gray images of triadic codes over the ring $\mathcal{R}$ lead to construction of complementary dual (LCD) codes over $\mathbb{F}_q$. In another paper, we will discuss duadic negacyclic codes over the ring $\mathcal{R}$.

The paper is organised as follows: In Section 2, we recall duadic and triadic codes of length n over $\mathbb{F}_q$ and give some of their properties. In Section 3, we study the ring $\mathcal{R} = \mathbb{F}_q[u]/\langle f(u)\rangle$, cyclic codes over the ring $\mathcal{R}$ and define the Gray map $\Phi : \mathcal{R}^n \rightarrow \mathbb{F}_q^{mn}$. In Section 4, we study duadic codes over $\mathcal{R}$, their extensions and their Gray images. In Section 5, we study triadic codes over $\mathcal{R}$ and their Gray images. We also give some examples to illustrate our results.

2 Preliminaries

A cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be regarded as an ideal of the ring $\mathbb{S}_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. It has a unique generating polynomial $g(x)$ and a unique idempotent generator $e(x)$. The set $\{i : \alpha^i$ is a zero of $g(x)\}$, where α is a primitive nth root of unity in some extension field of $\mathbb{F}_q$, is called the defining set of $\mathcal{C}$.

Let $\bar{j}(x) = \frac{1}{n}(1 + x + x^2 + \cdots + x^{n-1})$. The even weight $[n, n-1, 2]$ cyclic code $\mathbb{E}_n$ has generating idempotent $1 - \bar{j}(x)$, its dual is the repetition code with generating idempotent $\bar{j}(x)$.

A polynomial $a(x) = \sum_i a_i x^i \in \mathbb{S}_n$ is called even-like if $a(1) = 0$ otherwise it is called odd-like. A code $\mathcal{C}$ with generator polynomial $g(x)$ is called even-like if $g(1) = 0$ and odd-like if $g(1) \neq 0$.

For $(a, n) = 1$, $\mu_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ defined as $\mu_a(i) = ai(\mathrm{mod}\ n)$ is called a multiplier, where $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. It is extended on $\mathbb{S}_n$ by defining $\mu_a(\sum_i f_i x^i) = \sum_i f_i x^{\mu_a(i)}$.

For a linear code $\mathcal{C}$ over $\mathbb{F}_q$, the dual code $\mathcal{C}^\perp$ is defined as $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in \mathcal{C}\}$, where $x \cdot y$ denotes the usual Euclidean inner product. $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$ and self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$. A code $\mathcal{C}$ is called isodual if it is equivalent to its dual $\mathcal{C}^\perp$ and is called formally self-dual if $\mathcal{C}$ and $\mathcal{C}^\perp$ have the same weight distribution. An isodual code is clearly formally self-dual. A linear code $\mathcal{C}$ whose dual $\mathcal{C}^\perp$ satisfies $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$ is called a complementary dual (LCD) code.

The following is a well-known result:

Lemma 1:

i *Let $\mathcal{C}$ be a cyclic code of length n over a finite field $\mathbb{F}_q$ with defining set T. Then the defining set of $\mu_a(\mathcal{C})$ is $\mu_{a^{-1}}(T)$ and that of $\mathcal{C}^{\perp}$ is $\mathbb{Z}_n - \mu_{-1}(T)$.*

ii *Let $\mathcal{C}$ and $\mathcal{D}$ be cyclic codes of length n over a finite field $\mathbb{F}_q$ with defining sets T_1 and T_2 respectively. Then $\mathcal{C} \cap \mathcal{D}$ and $\mathcal{C} + \mathcal{D}$ are cyclic codes with defining sets $T_1 \cup T_2$ and $T_1 \cap T_2$ respectively.*

iii *Let $\mathcal{C}$ and $\mathcal{D}$ be cyclic codes of length n over $\mathbb{F}_q$ generated by the idempotents E_1, E_2 in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, then $\mathcal{C} \cap \mathcal{D}$ and $\mathcal{C} + \mathcal{D}$ are generated by the idempotents E_1E_2 and $E_1 + E_2 - E_1E_2$ respectively.*

iv *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ generated by the idempotent E, then $\mu_a(\mathcal{C})$ is generated by $\mu_a(E)$ and $\mathcal{C}^{\perp}$ is generated by the idempotent $1 - E(x^{-1})$.*

Remark 1: Dual of a linear code over a finite ring is defined in the same way and results in Lemma 1 (iii) and (iv) also hold true over any finite commutative ring.

2.1 Duadic codes over $\mathbb{F}_q$

In this subsection, we give the definition of duadic codes and state some of their properties. Let n be odd, $(n, q) = 1$ and suppose

$$\mathbb{Z}_n = \{0\} \cup S_1 \cup S_2, \text{ where}$$

i S_1, S_2 are union of q-cyclotomic cosets mod n

ii $S_1 \cap S_2 = \emptyset$

iii There exists a multiplier μ_a, $(a, n) = 1$ such that $\mu_a(S_1) = S_2$ and $\mu_a(S_2) = S_1$.

The triplet (μ_a, S_1, S_2) is called a splitting modulo n. The codes $\mathbb{D}_1$ and $\mathbb{D}_2$ having S_1 and S_2 as their defining sets respectively are called a pair of odd-like duadic codes and codes $\mathbb{C}_1$ and $\mathbb{C}_2$ having $S_1 \cup \{0\}$ and $S_2 \cup \{0\}$ as defining sets are called a pair of even-like duadic codes.

It is known that duadic codes exist if and only if q is a square mod n.

The next lemma investigates when does a splitting by μ_{-1} exist and when it does not. For reference, see Guenda and Yildiz (2015) and Smid (1987).

Lemma 2: *Let $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ be the prime factorisation of the odd integer n and q be a square mod n.*

i *If $p_i \equiv 3 (\bmod 4)$, for all $i, 1 \le i \le k$, then all splittings mod n are given by μ_{-1}.*

ii *If at least one $p_i \equiv 1 (\bmod 4)$, $1 \le i \le k$, then there is a splitting mod n which is not given by μ_{-1}.*

The following Lemmas 3 and 4 state various properties of duadic codes. For reference, see Theorems 6.1.3, 6.4.2, 6.4.3 and 6.4.12 of Huffman and Pless (2003).

Lemma 3: *Let* $\mathbb{C}_1=\langle e_1(x)\rangle$ *and* $\mathbb{C}_2=\langle e_2(x)\rangle$ *be a pair of even-like duadic codes of length* n *over* $\mathbb{F}_q$ *with idempotent generators* $e_1(x)$ *and* $e_2(x)$. *Suppose* μ_a *gives the splitting for* $\mathbb{C}_1$ *and* $\mathbb{C}_2$. *Let* $\mathbb{D}_1$ *and* $\mathbb{D}_2$ *be the associated odd-like duadic codes with idempotent generators* $d_1(x)$ *and* $d_2(x)$. *Then:*

- *i* $e_1e_2 = 0$ *and* $d_1d_2 = \overline{j}(x)$
- *ii* $e_1 + e_2 = 1 - \overline{j}(x)$ *and* $d_1 + d_2 = 1 + \overline{j}(x)$
- *iii* $d_1 - e_1 = \overline{j}(x)$, $d_2 - e_2 = \overline{j}(x)$
- *iv* $\mathbb{C}_1 \cap \mathbb{C}_2 = \{0\}$ $\mathbb{C}_1 + \mathbb{C}_2 = \mathbb{E}_n$
- *v* $\mathbb{C}_i$ *is even-like subcode of* $\mathbb{D}_i$ *for* $i = 1, 2$
- *vi* $\mathbb{D}_1 \cap \mathbb{D}_2 = \langle\overline{j}(x)\rangle$ *and* $\mathbb{D}_1 + \mathbb{D}_2 = \mathbb{S}_n$
- *vii* $\mathbb{D}_i = \mathbb{C}_i + \langle\overline{j}(x)\rangle = \langle\overline{j}(x) + e_i(x)\rangle$ *for* $i = 1, 2$
- *viii* $\mathbb{C}_1$ *is equivalent to* $\mathbb{C}_2$, $\mathbb{D}_1$ *is equivalent to* $\mathbb{D}_2$
- *ix* *If* μ_{-1} *gives the splitting mod* n, *then* $\mathbb{C}_1^{\perp} = \mathbb{D}_1$ *and* $\mathbb{C}_2^{\perp} = \mathbb{D}_2$
- *x* *If* $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_1$ *and* $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_2$, *i.e., if* μ_{-1} *does not give the splitting, then* $\mathbb{C}_1^{\perp} = \mathbb{D}_2$ *and* $\mathbb{C}_2^{\perp} = \mathbb{D}_1$.

Lemma 4: *Let* $\mathbb{D}_1$ *and* $\mathbb{D}_2$ *be a pair of odd-like duadic codes of length* n *over* $\mathbb{F}_q$. *Suppose* $1 + \gamma^2 n = 0$ *has a solution* γ *in* $\mathbb{F}_q$. *Let* $\overline{\mathbb{D}}_i$ *be the extension of* $\mathbb{D}_i$, *for* $i = 1, 2$, *defined by*

$$\overline{\mathbb{D}}_i = \{(c_0, c_1, \ldots, c_{n-1}, c_\infty) \ : \ c_\infty = \gamma \sum_{j=0}^{n-1} c_j, \ (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{D}_i\}.$$

Then the following hold:

- *i* *If* μ_{-1} *gives the splitting of* $\mathbb{D}_1$ *and* $\mathbb{D}_2$, *then* $\overline{\mathbb{D}}_1$ *and* $\overline{\mathbb{D}}_2$ *are self-dual.*
- *ii* *If* $\mu_{-1}(\mathbb{D}_1) = \mathbb{D}_1$, *i.e., if the splitting is not given by* μ_{-1}, *then* $\overline{\mathbb{D}}_1$ *and* $\overline{\mathbb{D}}_2$ *are duals of each other and hence* $\overline{\mathbb{D}}_1$ *and* $\overline{\mathbb{D}}_2$ *are isodual.*

2.2 Triadic codes over $\mathbb{F}_q$

In this subsection, we give the definition of triadic codes and study some of their properties. For reference see Sharma et al. (2007) and Pless and Rushanan (1988). Let $(n, q) = 1$ and suppose

$$\mathbb{Z}_n = S_1 \cup S_2 \cup S_3 \cup X_\infty, \text{ where}$$

- i S_1, S_2, S_3 and X_∞ are union of q-cyclotomic cosets mod n
- ii S_1, S_2, S_3 and X_∞ are pairwise disjoint
- iii There exists a multiplier μ_a, $(a, n) = 1$ such that $\mu_a(S_1) = S_2$, $\mu_a(S_2) = S_3$, $\mu_a(S_3) = S_1$ and $\mu_a(X_\infty) = X_\infty$.

It is clear that $0 \in X_\infty$ always. Let $X'_\infty = X_\infty - \{0\}$. Note that here the multiplier μ_a cannot be μ_{-1}.

Then the codes, for $i = 1, 2, 3$, having $S_i \cup X'_\infty$ or $(S_i \cup X_\infty)^c$ as their defining sets are called odd-like triadic codes and the codes having $(S_i \cup X'_\infty)^c$ or $S_i \cup X_\infty$ as their defining sets are the associated even-like triadic codes. Let $\mathbb{D}_i$ denote the odd-like codes having $S_i \cup X'_\infty$ as their defining sets; $\mathbb{D}'_i$ denote the odd-like codes having $(S_i \cup X_\infty)^c$ as their defining sets; $\mathbb{C}_i$ denote the even-like codes having $(S_i \cup X'_\infty)^c$ as their defining sets and $\mathbb{C}'_i$ denote the even-like codes having $S_i \cup X_\infty$ as their defining sets.

Clearly $\mathbb{D}_1$, $\mathbb{D}_2$, $\mathbb{D}_3$ are equivalent codes; $\mathbb{D}'_1$, $\mathbb{D}'_2$, $\mathbb{D}'_3$ are equivalent; $\mathbb{C}_1$, $\mathbb{C}_2$, $\mathbb{C}_3$ are equivalent and $\mathbb{C}'_1$, $\mathbb{C}'_2$, $\mathbb{C}'_3$ are equivalent codes.

For $i = 1, 2, 3$, let $e_i(x)$ and $e'_i(x)$ be the even-like idempotent generators of even-like triadic codes $\mathbb{C}_i$ and $\mathbb{C}'_i$ respectively, $d_i(x)$ and $d'_i(x)$ be the odd-like idempotent generators of odd-like triadic codes $\mathbb{D}_i$ and $\mathbb{D}'_i$ respectively.

As the defining set of $\mathbb{C}_1$ is $S_2 \cup S_3 \cup \{0\}$, the defining set of $\mu_a(\mathbb{C}_1)$ is $\mu_{a^{-1}}(S_2 \cup S_3 \cup \{0\}) = S_1 \cup S_2 \cup \{0\}$. Therefore $\mu_a(\mathbb{C}_1) = \mathbb{C}_3$ and hence $\mu_a(e_1) = e_3$. Similarly $\mu_a(e_2) = e_1$, $\mu_a(e_3) = e_2$ and $\mu_a(d_1) = d_3$, $\mu_a(d_2) = d_1$, $\mu_a(d_3) = d_2$. Similar results hold for e'_i and d'_i.

Triadic codes over $\mathbb{F}_q$ of prime length p exist if and only if q is a cubic residue mod p. When length n is a prime power, the conditions for the existence of triadic codes over $\mathbb{F}_q$ are given by Sharma et al. (2007) and for general n, see Bakshi et al. (2007).

Similar to the properties of duadic codes, we have following results for triadic codes.

Proposition 1: *We have*

i $\quad \mathbb{C}_1 \cap \mathbb{C}_2 \cap \mathbb{C}_3 = \mathbb{C}_1 \cap \mathbb{C}_2 = \mathbb{C}_1 \cap \mathbb{C}_3 = \mathbb{C}_2 \cap \mathbb{C}_3$

ii $\quad \mathbb{C}_1 + \mathbb{C}_2 + \mathbb{C}_3 = \mathbb{E}_n = \langle x - 1 \rangle = \langle 1 - \bar{j}(x) \rangle$

iii $\quad \mathbb{D}_1 + \mathbb{D}_2 + \mathbb{D}_3 = \mathbb{D}_1 + \mathbb{D}_2 = \mathbb{D}_2 + \mathbb{D}_3 = \mathbb{D}_1 + \mathbb{D}_3$

iv $\quad \mathbb{D}_1 \cap \mathbb{D}_2 \cap \mathbb{D}_3 = \langle \bar{j}(x) \rangle$

v $\quad \mathbb{C}_i + \mathbb{D}_i = \mathbb{S}_n$, $\mathbb{C}_i \cap \mathbb{D}_i = \{0\}$ for $i = 1, 2, 3$

vi $\quad e_1(x)e_2(x)e_3(x) = e_1(x)e_2(x) = e_1(x)e_3(x) = e_2(x)e_3(x)$

vii $\quad e_1(x) + e_2(x) + e_3(x) - 2e_1(x)e_2(x)e_3(x) = 1 - \bar{j}(x)$

viii $\quad d_1(x)d_2(x)d_3(x) = \bar{j}(x)$

ix $\quad d_1 + d_2 + d_3 - d_1d_2 - d_2d_3 - d_3d_1 + d_1d_2d_3 = d_1 + d_2 - d_1d_2$
$\qquad = d_2 + d_3 - d_2d_3 = d_1 + d_3 - d_3d_1$

x $\quad d_i(x) = 1 - e_i(x),\ e_i(x)d_i(x) = 0$ for $i = 1, 2, 3$.

Proof: By Lemma 1 (ii), the defining set of each of $\mathbb{C}_1 \cap \mathbb{C}_2 \cap \mathbb{C}_3$, $\mathbb{C}_1 \cap \mathbb{C}_2$, $\mathbb{C}_2 \cap \mathbb{C}_3$ and $\mathbb{C}_3 \cap \mathbb{C}_1$ is $S_1 \cup S_2 \cup S_3 \cup \{0\}$, hence they are equal. The defining set of $\mathbb{C}_1 + \mathbb{C}_2 + \mathbb{C}_3$ is $\{0\}$, which is the defining set of even weight code $\mathbb{E}_n$ whose generating idempotent is $1 - \bar{j}(x)$. Again by Lemma 1(ii), the defining set of each of $\mathbb{D}_1 + \mathbb{D}_2 + \mathbb{D}_3$, $\mathbb{D}_1 + \mathbb{D}_2$, $\mathbb{D}_2 + \mathbb{D}_3$ and $\mathbb{D}_3 + \mathbb{D}_1$ is X'_∞, hence they are all equal. The defining set of $\mathbb{D}_1 \cap \mathbb{D}_2 \cap \mathbb{D}_3$ is $S_1 \cup S_2 \cup S_3 \cup X'_\infty = \mathbb{Z}_n - \{0\}$, which is the defining set of the repetition code whose generating idempotent is $\bar{j}(x)$. The defining set of $\mathbb{C}_i \cap \mathbb{D}_i$ is whole of $\mathbb{Z}_n$, hence it is $\{0\}$

in the ring $\mathbb{S}_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$; whereas defining set of $\mathbb{C}_i + \mathbb{D}_i$ is $\emptyset$, so $\mathbb{C}_i + \mathbb{D}_i$ is equal to $\mathbb{S}_n$. The other results follow by Lemma 1(iii). □

Proposition 2: *We have*

i $\mathbb{C}'_1 \cap \mathbb{C}'_2 \cap \mathbb{C}'_3 = \{0\}$

ii $\mathbb{C}'_1 + \mathbb{C}'_2 + \mathbb{C}'_3 = \mathbb{C}'_1 + \mathbb{C}'_2 = \mathbb{C}'_1 + \mathbb{C}'_3 = \mathbb{C}'_2 + \mathbb{C}'_3$

iii $\mathbb{D}'_1 \cap \mathbb{D}'_2 \cap \mathbb{D}'_3 = \mathbb{D}'_1 \cap \mathbb{D}'_2 = \mathbb{D}'_2 \cap \mathbb{D}'_3 = \mathbb{D}'_1 \cap \mathbb{D}'_3$

iv $\mathbb{D}'_1 + \mathbb{D}'_2 + \mathbb{D}'_3 = \mathbb{S}_n = \langle 1\rangle,$

v $\mathbb{C}'_i + \mathbb{D}'_i = \mathbb{S}_n,\ \mathbb{C}'_i \cap \mathbb{D}'_i = \{0\}$

vi $d'_1(x)d'_2(x)d'_3(x) = d'_1(x)d'_2(x) = d'_1(x)d'_3(x) = d'_2(x)d'_3(x)$

vii $d'_1(x) + d'_2(x) + d'_3(x) - 2d'_1(x)d'_2(x)d'_3(x) = 1$

viii $e'_1(x)e'_2(x)e'_3(x) = 0$

ix $e'_1 + e'_2 + e'_3 - e'_1e'_2 - e'_2e'_3 - e'_3e'_1 + e'_1e'_2e'_3 = e'_1 + e'_2 - e'_1e'_2$
$= e'_2 + e'_3 - e'_2e'_3 = e'_1 + e'_3 - e'_3e'_1$

x $d'_i(x) = 1 - e'_i(x),\ e'_i(x)d'_i(x) = 0$

xi $\mathbb{C}_i + \langle\bar{j}(x)\rangle = \mathbb{D}'_i,\ \mathbb{C}_i \cap \langle\bar{j}(x)\rangle = \{0\}$

xii $\mathbb{C}'_i + \langle\bar{j}(x)\rangle = \mathbb{D}_i,\ \mathbb{C}'_i \cap \langle\bar{j}(x)\rangle = \{0\}$

xiii $\mathbb{C}_i \cap \mathbb{C}'_i = \{0\}, \mathbb{C}_i + \mathbb{C}'_i = \langle 1 - \bar{j}(x)\rangle,$

xiv $\mathbb{D}_i \cap \mathbb{D}'_i = \langle\bar{j}(x)\rangle, , \mathbb{D}_i + \mathbb{D}'_i = \mathbb{S}_n$

xv $e_i + \bar{j}(x) = d'_i,\ e'_i + \bar{j}(x) = d_i,\ e_i\bar{j}(x) = 0,\ e'_i\bar{j}(x) = 0$ *and*

xvi $e_ie'_i = 0, e_i + e'_i = 1 - \bar{j}(x), d_id'_i = \bar{j}(x), d_i + d'_i = 1 + \bar{j}(x).$

Proof: Statements (i)–(x) are similar to that of (i) to (x) of Proposition 1. For (xi), we note that the defining set of the repetition code $\langle\bar{j}(x)\rangle$ is $\mathbb{Z}_n - \{0\}$. Therefore the defining set of $\mathbb{C}_i \cap \langle\bar{j}(x)\rangle$ is $\mathbb{Z}_n$ and defining set of $\mathbb{C}_i + \langle\bar{j}(x)\rangle$ is same as that of $\mathbb{D}'_i$. Similarly, we have (xii). The defining set of $\mathbb{C}_i \cap \mathbb{C}'_i$ is $\mathbb{Z}_n$ and that of $\mathbb{C}_i + \mathbb{C}'_i$ is $\{0\}$. The defining set of $\mathbb{D}_i \cap \mathbb{D}'_i$ is $\mathbb{Z}_n - \{0\}$ and that of $\mathbb{D}_i + \mathbb{D}'_i$ is $\emptyset$. Now (xv) and (xvi) follow by Lemma 1(iii). □

Proposition 3: *Suppose X'_∞ is empty, then we have the following additional results:*

i $\mathbb{C}_1 \cap \mathbb{C}_2 \cap \mathbb{C}_3 = \mathbb{C}_1 \cap \mathbb{C}_2 = \mathbb{C}_1 \cap \mathbb{C}_3 = \mathbb{C}_2 \cap \mathbb{C}_3 = \{0\}$

ii $\mathbb{D}_1 + \mathbb{D}_2 + \mathbb{D}_3 = \mathbb{D}_1 + \mathbb{D}_2 = \mathbb{D}_2 + \mathbb{D}_3 = \mathbb{D}_1 + \mathbb{D}_3 = \mathbb{S}_n$

iii $\mathbb{D}'_1 \cap \mathbb{D}'_2 \cap \mathbb{D}'_3 = \mathbb{D}'_1 \cap \mathbb{D}'_2 = \mathbb{D}'_2 \cap \mathbb{D}'_3 = \mathbb{D}'_1 \cap \mathbb{D}'_3 = \langle\bar{j}(x)\rangle$

iv $\mathbb{C}'_1 + \mathbb{C}'_2 + \mathbb{C}'_3 = \mathbb{C}'_1 + \mathbb{C}'_2 = \mathbb{C}'_1 + \mathbb{C}'_3 = \mathbb{C}'_2 + \mathbb{C}'_3 = \mathbb{E}_n = \langle 1 - \bar{j}(x)\rangle$

v $e_1(x)e_2(x)e_3(x) = e_1(x)e_2(x) = e_1(x)e_3(x) = e_2(x)e_3(x) = 0$

vi $d'_1(x)d'_2(x)d'_3(x) = d'_1(x)d'_2(x) = d'_1(x)d'_3(x) = d'_2(x)d'_3(x) = \bar{j}(x)$

vii $d_1+d_2+d_3-d_1d_2-d_2d_3-d_3d_1+d_1d_2d_3=d_1+d_2-d_1d_2$
$=d_2+d_3-d_2d_3=d_1+d_3-d_3d_1=1$

viii $e'_1+e'_2+e'_3-e'_1e'_2-e'_2e'_3-e'_3e'_1+e'_1e'_2e'_3=e'_1+e'_2-e'_1e'_2$
$=e'_2+e'_3-e'_2e'_3=e'_1+e'_3-e'_3e'_1=1-\overline{j}(x).$

Proof follows immediately from Propositions 1 and 2, using Lemma 1.

Proposition 4: *Let $\mathbb{C}_i$, $\mathbb{C}'_i$, for $i=1,2,3$, be two pairs of even-like triadic codes over $\mathbb{F}_q$ with $\mathbb{D}_i$, $\mathbb{D}'_i$ the associated pairs of odd-like triadic codes. Then*

$$\mathbb{C}_i^{\perp}=\mu_{-1}(\mathbb{D}_i) \text{ and } \mathbb{C}_i'^{\perp}=\mu_{-1}(\mathbb{D}'_i).$$

Further, if $\mu_{-1}(\mathbb{D}_i)=\mathbb{D}_i$, then

$$\mathbb{C}_i^{\perp}=\mathbb{D}_i, \mathbb{C}_i'^{\perp}=\mathbb{D}'_i \text{ and so } \mathbb{C}_i \text{ and } \mathbb{C}'_i \text{ are LCD codes .}$$

Proof: As the defining set of $\mathbb{C}_1$ is $(S_1\cup X'_\infty)^c=\{0\}\cup S_2\cup S_3$, the defining set of $\mathbb{C}_1^{\perp}$, by Lemma 1(i) is

$$\begin{aligned}
&=\mathbb{Z}_n-\mu_{-1}(\{0\}\cup S_2\cup S_3)\\
&=\mu_{-1}(\mathbb{Z}_n)-\mu_{-1}(\{0\}\cup S_2\cup S_3)\\
&=\mu_{-1}(S_1\cup S_2\cup S_3\cup X_\infty)-\mu_{-1}(\{0\}\cup S_2\cup S_3)\\
&=\mu_{-1}(S_1\cup X'_\infty)\\
&=\mu_{-1}(\text{defining set of } \mathbb{D}_1).
\end{aligned}$$

This proves that $\mathbb{C}_1^{\perp}=\mu_{-1}(\mathbb{D}_1)$. Similar is the proof of others.

When $\mu_{-1}(\mathbb{D}_i)=\mathbb{D}_i$, i.e., the defining set of $\mathbb{D}_i$ is mapped to itself by μ_{-1}, we see that the defining set of $\mathbb{D}'_i$ also goes to itself by μ_{-1} and so $\mu_{-1}(\mathbb{D}'_i)=\mathbb{D}'_i$. Therefore $\mathbb{C}_i^{\perp}=\mu_{-1}(\mathbb{D}_i)=\mathbb{D}_i$, $\mathbb{C}_i'^{\perp}=\mu_{-1}(\mathbb{D}'_i)=\mathbb{D}'_i$.
Further in case $\mu_{-1}(\mathbb{D}_i)=\mathbb{D}_i$, we get, from Propositions 1(v) and 2(v), that $\mathbb{C}_i\cap\mathbb{C}_i^{\perp}=\mathbb{C}_i\cap\mathbb{D}_i=\{0\}$ and $\mathbb{C}'_i\cap\mathbb{C}_i'^{\perp}=\mathbb{C}'_i\cap\mathbb{D}'_i=\{0\}$; proving that $\mathbb{C}_i$ and $\mathbb{C}'_i$ are LCD codes.

3 Cyclic codes over the ring $\mathcal{R}$ and The Gray map

3.1 Cyclic codes over the ring $\mathcal{R}$

Let q be a prime power, $q=p^s$. Throughout the paper, $\mathcal{R}$ denotes the commutative ring $\mathbb{F}_q[u]/\langle f(u)\rangle$, where $f(u)$ is any polynomial of degree $m\geq 2$, which splits into distinct linear factors over $\mathbb{F}_q$. Let $f(u)=(u-\alpha_1)(u-\alpha_2)...(u-\alpha_m)$, with $\alpha_i\in\mathbb{F}_q$, $\alpha_i\neq\alpha_j$. $\mathcal{R}$ is a non-chain ring of size q^m and characteristic p. The ideals $\langle\frac{f(u)}{u-\alpha_i}\rangle$ for $i=1,2,...,m$

are all the maximal ideals of $\mathcal{R}$. Let $\eta_i,\ i=1,2,\ldots,m$ denote the following elements of $\mathcal{R}$:

$$\begin{aligned}
\eta_1 &= \tfrac{(u-\alpha_2)(u-\alpha_3)\cdots(u-\alpha_{m-1})(u-\alpha_m)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots(\alpha_1-\alpha_{m-1})(\alpha_1-\alpha_m)},\\
\eta_2 &= \tfrac{(u-\alpha_1)(u-\alpha_3)\cdots(u-\alpha_{m-1})(u-\alpha_m)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\cdots(\alpha_2-\alpha_{m-1})(\alpha_2-\alpha_m)},\\
\cdots & \quad \cdots \quad \cdots \quad \cdots\\
\eta_i &= \tfrac{(u-\alpha_1)(u-\alpha_2)\cdots(u-\alpha_{i-1})(u-\alpha_{i+1})\cdots(u-\alpha_m)}{(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_m)},\\
\cdots & \quad \cdots \quad \cdots \quad \cdots\\
\eta_m &= \tfrac{(u-\alpha_1)(u-\alpha_2)\cdots(u-\alpha_{m-2})(u-\alpha_{m-1})}{(\alpha_m-\alpha_1)(\alpha_m-\alpha_2)\cdots(\alpha_m-\alpha_{m-2})(\alpha_m-\alpha_{m-1})}.
\end{aligned} \tag{1}$$

Lemma 5: *We have* $\eta_i^2=\eta_i,\ \eta_i\eta_j=0$ for $1\le i,j\le m,\ i\neq j$ and $\sum_{i=1}^m \eta_i=1$ *in* $\mathcal{R}$.

Proof: It is clear that $\eta_i\eta_j\equiv 0 \pmod{f(u)}$ for $1\le i,j\le m,\ i\neq j$. To prove $\eta_i^2=\eta_i$ it is enough to prove that $\eta_i(\eta_i-1)=0$ in $\mathcal{R}$, so it is sufficient to prove that $(u-\alpha_j)|\,\eta_i(\eta_i-1)$ for each j. By definition of η_i, it is clear that $(u-\alpha_j)|\,\eta_i$ for all $j\neq i$. Also $\eta_i(\alpha_i)=1$, so $(u-\alpha_i)|\,(\eta_i-1)$ for all i. Therefore $f(u)|\,\eta_i(\eta_i-1)$ and hence $\eta_i^2=\eta_i$ in $\mathcal{R}$. Now to prove $\sum_{i=1}^m\eta_i=1$ in $\mathcal{R}$, it is sufficient to prove $\sum_{i=1}^m\eta_i\equiv 1 \pmod{f(u)}$. As $\eta_1(\alpha_i)+\eta_2(\alpha_i)+\cdots+\eta_m(\alpha_i)=1$ for all i, we find that $(u-\alpha_i)|\,(\eta_1+\eta_2+\cdots+\eta_m-1)$ for all i and the result follows. □

The decomposition theorem of ring theory tells us that
$\mathcal{R}=\eta_1\mathcal{R}\oplus\eta_2\mathcal{R}\oplus\cdots\oplus\eta_m\mathcal{R}$.

For a linear code $\mathcal{C}$ of length n over the ring $\mathcal{R}$, let

$\mathcal{C}_1=\{x_1\in\mathbb{F}_q^n : \exists\, x_2,x_3,\ldots,x_m\in\mathbb{F}_q^n$ such that $\eta_1x_1+\eta_2x_2+\cdots+\eta_mx_m\in\mathcal{C}\}$,
$\mathcal{C}_2=\{x_2\in\mathbb{F}_q^n : \exists\, x_1,x_3,\ldots,x_m\in\mathbb{F}_q^n$ such that $\eta_1x_1+\eta_2x_2+\cdots+\eta_mx_m\in\mathcal{C}\}$,
$\cdots \quad \cdots \quad \cdots \quad \cdots$
$\mathcal{C}_m=\{x_m\in\mathbb{F}_q^n : \exists\, x_1,x_2,\ldots,x_{m-1}\in\mathbb{F}_q^n$ such that $\eta_1x_1+\cdots+\eta_mx_m\in\mathcal{C}\}$.

Then $\mathcal{C}_1,\mathcal{C}_2,\ldots,\mathcal{C}_m$ are linear codes of length n over $\mathbb{F}_q$, $\mathcal{C}=\eta_1\mathcal{C}_1\oplus\eta_2\mathcal{C}_2\oplus\cdots\oplus\eta_m\mathcal{C}_m$ and $|\mathcal{C}|=|\mathcal{C}_1|\,|\mathcal{C}_2|\,\cdots\,|\mathcal{C}_m|$.

The following is a result of Goyal and Raka (2016).

Theorem 1: *Let* $\mathcal{C}=\eta_1\mathcal{C}_1\oplus\eta_2\mathcal{C}_2\oplus\cdots\oplus\eta_m\mathcal{C}_m$ *be a linear code of length* n *over* $\mathcal{R}$. *Then*

- *i* $\mathcal{C}$ *is cyclic over* $\mathcal{R}$ *if and only if* $\mathcal{C}_i,\ i=1,2,\ldots,m$ *are cyclic over* $\mathbb{F}_q$.
- *ii* *If* $\mathcal{C}_i=\langle g_i(x)\rangle,\ g_i(x)\in\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle},\ g_i(x)|(x^n-1)$, *then* $\mathcal{C}=\langle\eta_1g_1(x),\eta_2g_2(x),\ldots,\eta_mg_m(x)\rangle=\langle g(x)\rangle$ *where* $g(x)=\eta_1g_1+\eta_2g_2+\cdots+\eta_mg_m$ *and* $g(x)|(x^n-1)$.
- *iii* *Further* $|\mathcal{C}|=q^{mn-\sum_{i=1}^m deg(g_i)}$.
- *iv* *Suppose that* $g_i(x)h_i(x)=x^n-1,\ 1\le i\le m$. *Let* $h(x)=\eta_1h_1(x)+\eta_2h_2(x)+\cdots+\eta_mh_m(x)$, *then* $g(x)h(x)=x^n-1$.
- *v* $\mathcal{C}^\perp=\eta_1\mathcal{C}_1^\perp\oplus\eta_2\mathcal{C}_2^\perp\oplus\cdots\oplus\eta_m\mathcal{C}_m^\perp$.

vi $\mathcal{C}^{\perp} = \langle h^{\perp}(x)\rangle$, $h^{\perp}(x) = \eta_1 h_1^{\perp}(x) + \eta_2 h_2^{\perp}(x) + \cdots + \eta_m h_m^{\perp}(x)$, *where* $h_i^{\perp}(x)$ *is the reciprocal polynomial of* $h_i(x)$, $1 \leq i \leq m$.

vii $|\mathcal{C}^{\perp}| = q^{\sum_{i=1}^{m} deg(g_i)}$.

3.2 The Gray map

Every element $r(u)$ of the ring $\mathcal{R} = \mathbb{F}_q[u]/\langle f(u)\rangle$ can be uniquely expressed as

$$r(u) = r_0 + r_1 u + r_2 u^2 + \cdots + r_{m-1}u^{m-1} = \eta_1 a_1 + \eta_2 a_2 + \cdots + \eta_m a_m,$$

where $a_i = r(\alpha_i)$ for $i = 1, 2, ..., m$. This is so because, by (1), $\eta_i(\alpha_i) = 1$ and $\eta_i(\alpha_j) = 0$ for all $j \neq i, 1 \leq i, j \leq m$.

Define a Gray map $\Phi : \mathcal{R} \to \mathbb{F}_q^m$ by

$$r(u) = \eta_1 a_1 + \eta_2 a_2 + \cdots + \eta_m a_m \longmapsto (a_1, a_2, \ldots, a_m)V,$$

where V is any nonsingular matrix over $\mathbb{F}_q$ of order $m \times m$. This map can be extended from $\mathcal{R}^n$ to $(\mathbb{F}_q^m)^n$ component-wise.

For an element $r \in \mathcal{R}$, let the Gray weight be defined as $w_G(r) = w_H(\Phi(r))$, the Hamming weight of $\Phi(r)$. The Gray weight of an element in $\mathcal{R}^n$ and Gray distance d_G of two elements in $\mathcal{R}^n$ are defined in the natural way.

Theorem 2: *The Gray map Φ is an $\mathbb{F}_q$ - linear, one to one and onto map. It is also distance preserving map from ($\mathcal{R}^n$, Gray distance d_G) to ($\mathbb{F}_q^{mn}$, Hamming distance d_H). Further if the matrix V satisfies $VV^T = \lambda I_m$, $\lambda \in \mathbb{F}_q^*$, where V^T denotes the transpose of the matrix V, then the Gray image $\Phi(\mathcal{C})$ of a self-dual code $\mathcal{C}$ over $\mathcal{R}$ is a self-dual code in $\mathbb{F}_q^{mn}$.*

Proof: The first two assertions hold as V is an invertible matrix over $\mathbb{F}_q$.
Let now $V = (v_{ij})$, $1 \leq i, j \leq m$, satisfying $VV^T = \lambda I_m$. So that

$$\sum_{k=1}^{m} v_{jk}^2 = \lambda \text{ for all } j, 1 \leq j \leq m \text{ and } \sum_{k=1}^{m} v_{jk}v_{\ell k} = 0 \text{ for } j \neq \ell. \tag{2}$$

Let $\mathcal{C}$ be a self-dual code over $\mathcal{R}$. Let $r = (r_0, r_1, \ldots, r_{n-1}), s = (s_0, s_1, \ldots, s_{n-1}) \in \mathcal{C}$, where $r_i = \eta_1 a_{i1} + \eta_2 a_{i2} + \cdots + \eta_m a_{im}$ and $s_i = \eta_1 b_{i1} + \eta_2 b_{i2} + \cdots + \eta_m b_{im}$. Using the properties of η_i's from Lemma 5, we get

$$r_i s_i = \eta_1 a_{i1} b_{i1} + \eta_2 a_{i2} b_{i2} + \cdots + \eta_m a_{im} b_{im}.$$

Then

$$0 = r \cdot s = \sum_{i=0}^{n-1} r_i s_i = \sum_{i=0}^{n-1} \sum_{j=1}^{m} \eta_j\, a_{ij}\, b_{ij} = \sum_{j=1}^{m} \eta_j \Big(\sum_{i=0}^{n-1} a_{ij}\, b_{ij} \Big)$$

implies that

$$\sum_{i=0}^{n-1} a_{ij} b_{ij} = 0, \quad \text{for all } j = 1, 2, \ldots, m. \tag{3}$$

Now

$$\Phi(r_i) = (a_{i1}, a_{i2}, \ldots, a_{im})V = \big(\sum_{j=1}^{m} a_{ij}v_{j1}, \sum_{j=1}^{m} a_{ij}v_{j2}\ , \ldots, \sum_{j=1}^{m} a_{ij}v_{jm}\big)$$

Similarly

$$\Phi(s_i) = \big(\sum_{\ell=1}^{m} b_{i\ell}\, v_{\ell 1}, \sum_{\ell=1}^{m} b_{i\ell}\, v_{\ell 2}\ , \ldots, \sum_{\ell=1}^{m} b_{i\ell}\, v_{\ell m}\big).$$

Using (2) and (3), we find that

$$\begin{aligned}\Phi(r) \cdot \Phi(s) &= \sum_{i=0}^{n-1}\Phi(r_i) \cdot \Phi(s_i) = \sum_{i=0}^{n-1}\sum_{k=1}^{m}\sum_{j=1}^{m}\sum_{\ell=1}^{m} a_{ij}\, b_{i\ell}\, v_{jk}\, v_{\ell k} \\ &= \sum_{i=0}^{n-1}\sum_{j=1,\ell=j}^{m} a_{ij}\, b_{ij}\Big(\sum_{k=1}^{m} v_{jk}^2\Big) + \sum_{i=0}^{n-1}\sum_{j=1}^{m}\sum_{\ell=1,\ell\neq j}^{m} a_{ij}\, b_{i\ell}\Big(\sum_{k=1}^{m} v_{jk}\, v_{\ell k}\Big) \\ &= \lambda\sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij}\, b_{ij} \\ &= \lambda\sum_{j=1}^{m}\Big(\sum_{i=0}^{n-1} a_{ij}\, b_{ij}\Big) = 0,\end{aligned}$$

which proves the result. □

4 Duadic Codes over the ring $\mathcal{R}$

In this Section, we study duadic codes over the ring $\mathcal{R} = \mathbb{F}_q[u]/\langle f(u)\rangle$ in terms of their idempotent generators, the extensions of duadic codes and their Gray images. Let $\mathcal{R}_n$ denote the ring $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$. The definitions, results for duadic codes over $\mathcal{R}$ and their proofs are similar to those obtained by the authors (2016), where $f(u)$ was taken as $u^m - u$, a special polynomial. Here $f(u)$ being a general polynomial, the ring $\mathcal{R}$ gives us more flexibility for obtaining the Gray images which lead to the construction of many new self-dual, isodual and self-orthogonal codes. Moreover, we need not restrict to the condition that $q \equiv 1(\mathrm{mod}(m-1))$ taken by the authors (2016). We omit the proofs of the results as these are similar to those given by the authors (2016).
Using the properties (Lemma 5) of idempotents η_i, we have

Lemma 6: *Let $\eta_i,\ 1 \leq i \leq m$ be the idempotents as defined in equation (1). Then for $i_1, i_2, \ldots, i_m \in \{1, 2\}$ and for any tuple $(d_{i_1}, d_{i_2}, \ldots, d_{i_m})$ of odd-like idempotents not all equal and for any tuple $(e_{i_1}, e_{i_2}, \ldots, e_{i_m})$ of even-like idempotents not all equal, $\eta_1 d_{i_1} + \eta_2 d_{i_2} + \cdots + \eta_m d_{i_m}$ and $\eta_1 e_{i_1} + \eta_2 e_{i_2} + \cdots + \eta_m e_{i_m}$ are respectively odd-like and even-like idempotents in the ring $\mathcal{R}_n = \frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$.*

We assume that q is a square mod n so that duadic codes of length n over $\mathbb{F}_q$ exist. We denote the set $\{1,2,\ldots,m\}$ by $\mathbb{A}$.

For a proper subset $\{i_1,i_2,\ldots,i_k\}\subset\mathbb{A}, i_r\neq i_s,\ 1\leq r,s\leq k$, let $D_{\{i_1,i_2,\ldots,i_k\}}$ denote the odd-like idempotent

$$D_{\{i_1,i_2,\ldots,i_k\}}=(\eta_{i_1}+\eta_{i_2}+\cdots+\eta_{i_k})d_1+(1-\eta_{i_1}-\eta_{i_2}-\cdots-\eta_{i_k})d_2. \tag{4}$$

$$D'_{\{i_1,i_2,\ldots,i_k\}}=(\eta_{i_1}+\eta_{i_2}+\cdots+\eta_{i_k})d_2+(1-\eta_{i_1}-\eta_{i_2}-\cdots-\eta_{i_k})d_1. \tag{5}$$

Similarly, we define even-like idempotents

$$E_{\{i_1,i_2,\ldots,i_k\}}=(\eta_{i_1}+\eta_{i_2}+\cdots+\eta_{i_k})e_1+(1-\eta_{i_1}-\eta_{i_2}-\cdots-\eta_{i_k})e_2. \tag{6}$$

$$E'_{\{i_1,i_2,\ldots,i_k\}}=(\eta_{i_1}+\eta_{i_2}+\cdots+\eta_{i_k})e_2+(1-\eta_{i_1}-\eta_{i_2}-\cdots-\eta_{i_k})e_1. \tag{7}$$

Let $Q_{\{i_1,i_2,\ldots,i_k\}},\ Q'_{\{i_1,i_2,\ldots,i_k\}}$ denote the odd-like duadic codes and $S_{\{i_1,i_2,\ldots,i_k\}}$, $S'_{\{i_1,i_2,\ldots,i_k\}}$ denote the even-like duadic codes over $\mathcal{R}$ generated by the corresponding idempotents, i.e.,

$Q_{\{i_1,i_2,\ldots,i_k\}}=\langle D_{\{i_1,i_2,\ldots,i_k\}}\rangle,\ \ Q'_{\{i_1,i_2,\ldots,i_k\}}=\langle D'_{\{i_1,i_2,\ldots,i_k\}}\rangle,$
$S_{\{i_1,i_2,\ldots,i_k\}}=\langle E_{\{i_1,i_2,\ldots,i_k\}}\rangle,\ \ S'_{\{i_1,i_2,\ldots,i_k\}}=\langle E'_{\{i_1,i_2,\ldots,i_k\}}\rangle.$

Theorem 3: *For $i_1,i_2,\ldots,i_k\in\mathbb{A},\ i_r\neq i_s,\ 1\leq r,s\leq k,\ Q_{\{i_1,i_2,\ldots,i_k\}}$ is equivalent to $Q'_{\{i_1,i_2,\ldots,i_k\}}$ and $S_{\{i_1,i_2,\ldots,i_k\}}$ is equivalent to $S'_{\{i_1,i_2,\ldots,i_k\}}$. Further there are $2^{m-1}-1$ inequivalent odd-like duadic codes and $2^{m-1}-1$ inequivalent even-like duadic codes over the ring $\mathcal{R}$.*

Theorem 4: *For subsets $\{i_1,i_2,\ldots,i_k\}$ of $\mathbb{A}$, the following assertions hold for duadic codes over $\mathcal{R}$.*

i $Q_{\{i_1,i_2,\ldots,i_k\}}\cap Q'_{\{i_1,i_2,\ldots,i_k\}}=\langle\bar{j}(x)\rangle$

ii $Q_{\{i_1,i_2,\ldots,i_k\}}+Q'_{\{i_1,i_2,\ldots,i_k\}}=\mathcal{R}_n$

iii $S_{\{i_1,i_2,\ldots,i_k\}}\cap S'_{\{i_1,i_2,\ldots,i_k\}}=\{0\}$

iv $S_{\{i_1,i_2,\ldots,i_k\}}+S'_{\{i_1,i_2,\ldots,i_k\}}=\langle 1-\bar{j}(x)\rangle$

v $S_{\{i_1,i_2,\ldots,i_k\}}\cap\langle\bar{j}(x)\rangle=\{0\},\ S'_{\{i_1,i_2,\ldots,i_k\}}\cap\langle\bar{j}(x)\rangle=\{0\}$

vi $S_{\{i_1,i_2,\ldots,i_k\}}+\langle\bar{j}(x)\rangle=Q_{\{i_1,i_2,\ldots,i_k\}},\ S'_{\{i_1,i_2,\ldots,i_k\}}+\langle\bar{j}(x)\rangle=Q'_{\{i_1,i_2,\ldots,i_k\}},$

vii $|Q_{\{i_1,i_2,\ldots,i_k\}}|=q^{\frac{m(n+1)}{2}},|S_{\{i_1,i_2,\ldots,i_k\}}|=q^{\frac{m(n-1)}{2}}.$

Theorem 5: *If $\mu_{-1}(\mathbb{C}_1)=\mathbb{C}_2,\ \ \mu_{-1}(\mathbb{C}_2)=\mathbb{C}_1$, then for each possible tuple $\{i_1,i_2,\ldots,i_k\}\in\mathbb{A}$, the following assertions hold for duadic codes over $\mathcal{R}$.*

i $Q^{\perp}_{\{i_1,i_2,\ldots,i_k\}}=S_{\{i_1,i_2,\ldots,i_k\}}$

ii $S_{\{i_1,i_2,\ldots,i_k\}}$ *is self orthogonal.*

Theorem 6: *If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_1$, $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_2$, then for all possible choices of $\{i_1, i_2, \ldots, i_k\} \in \mathbb{A}$, the following assertions hold for duadic codes over $\mathcal{R}$.*

i $Q^{\perp}_{\{i_1,i_2,\ldots,i_k\}} = S'_{\{i_1,i_2,\ldots,i_k\}}$,

ii $Q'^{\perp}_{\{i_1,i_2,\ldots,i_k\}} = S_{\{i_1,i_2,\ldots,i_k\}}$.

Consider the equation

$$1 + \gamma^2 n = 0. \tag{8}$$

This equation has a solution γ in $\mathbb{F}_q$ if and only if n and -1 are both squares or both non-squares in $\mathbb{F}_q$ (see [Huffman and Pless (2003), Chapter 6]). Extended duadic codes over the ring $\mathcal{R}$ are defined in a similar way as defined over the field $\mathbb{F}_q$ (see Lemma 4).

Theorem 7: *Suppose there exists a γ in $\mathbb{F}_q$ satisfying equation (8). If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_2$, $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_1$, then for all possible choices of $\{i_1, i_2, \ldots, i_k\} \in \mathbb{A}$, the extended duadic codes $\overline{Q_{\{i_1,i_2,\ldots,i_k\}}}$ of length $n+1$ are self-dual.*

Theorem 8: *Suppose there exists a γ in $\mathbb{F}_q$ satisfying equation (8). If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_1$, $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_2$, then for all possible choices of $\{i_1, i_2, \ldots, i_k\} \in \mathbb{A}$, the extended duadic codes satisfy $\overline{Q_{\{i_1,i_2,\ldots,i_k\}}}^{\perp} = \overline{Q'_{\{i_1,i_2,\ldots,i_k\}}}$ and hence are isodual.*

Corollary 1: *Let the matrix V taken in the definition of the Gray map Φ satisfy $VV^T = \lambda I_m$, $\lambda \in \mathbb{F}_q^*$. If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_2$, then for all possible choices of $\{i_1, i_2, \ldots, i_k\} \in \mathbb{A}$, the Gray images of extended duadic codes $\overline{Q_{\{i_1,i_2,\ldots,i_k\}}}$, i.e., $\Phi(\overline{Q_{\{i_1,i_2,\ldots,i_k\}}})$ are self-dual codes of length $m(n+1)$ over $\mathbb{F}_q$ and the Gray images of the even-like duadic codes $S_{\{i_1,i_2,\ldots,i_k\}}$, i.e., $\Phi(S_{\{i_1,i_2,\ldots,i_k\}})$ are self-orthogonal codes of length mn over $\mathbb{F}_q$. If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_1$, then $\Phi(\overline{Q_{\{i_1,i_2,\ldots,i_k\}}})$ are isodual codes of length $m(n+1)$ over $\mathbb{F}_q$.*

Example 1 illustrates our theory for duadic codes. Some other examples when $q = 5, 7, 9, 11, 13$ are given in Table 1. The minimum distances of all these codes have been computed by the Magma Computational Algebra System.

Example 1: Let $m = 2$, $q = 7$, $n = 3$, $f(u) = (u-1)(u+3)$ and $V = \begin{pmatrix} 4 & 1 \\ 1 & -4 \end{pmatrix}$ be a matrix over $\mathbb{F}_7$ satisfying $VV^T = 3I$. The even-like idempotent generators of duadic codes of length 3 over $\mathbb{F}_7$ are $e_1 = 6x^2 + 3x + 5$, $e_2 = 3x^2 + 6x + 5$. The Gray image of even-like duadic code $S_{\{1\}}$ is self-orthogonal and MDS [6,2,5] code over $\mathbb{F}_7$ and the Gray image $\Phi(\overline{Q}_{\{1\}})$ is [8,4,4] self-dual and nearly MDS code over $\mathbb{F}_7$.

Table 1 Gray images of duadic codes

q	n	m	$f(u)$	V	$\Phi(S_{\{1\}})$	$\Phi(\overline{Q}_{\{1\}})$
5	11	3	$(u-2)(u-3)(u-4)$	2,3,1 1,2,2 2,1,3	[33,15,10] self-orthogonal	[36,18,9] self-dual
7	3	2	$(u-1)(u+3)$	4,1 1,–4	[6,2,5] self-orthogonal MDS	[8,4,4] self-dual nearly MDS
7	3	4	$(u-2)(u-3)$ $(u+1)(u+3)$	2,–2,1,1 –1,1,2,2 2,2,1,–1 1,1,–2,2	[12,4,6] self-orthogonal	[16,8,4] self-dual
9*	5	2	$(u-\alpha^2)(u-\alpha^6)$	1,α α,–1	[10,4,4] LCD	[12,6,4] isodual
9*	5	3	$(u-\alpha^2)(u-\alpha^4)(u-\alpha^6)$	1,0,0 0,1,0 0,0,1	[15,6,4] LCD	[18,9,4] isodual
11	5	3	$(u-3)(u-4)(u-9)$	4,4,–2 –2,4,4 4,–2,4	[15,6,8] LCD	[18,9,6] isodual
11†	5	4	$(u-3)(u-4)$ $(u-5)(u-9)$	2,–2,1,1 –1,1,2,2 2,2,1,–1 1,1,–2,2	[20,8,8] LCD	[24,12,6] isodual
13	3	2	$(u+1)(u-5)$	2,1 1,–2	[6,2,4] self-orthogonal nearly MDS	[8,4,4] self-dual nearly MDS
13	3	4	$u(u+1)(u-5)(u-8)$	2,–2,1,1 –1,1,2,2 2,2,1,–1 1,1,–2,2	[12,4,6] self-orthogonal	[16,8,4] self-dual

*Here α is a primitive element of $\mathbb{F}_9$.

† Note that, here, one does not have $q \equiv 1(\bmod\ (m-1))$.

5 Triadic codes over the ring $\mathcal{R}$

We now define triadic codes of length n over the ring $\mathcal{R}$ in terms of their idempotent generators with the assumption that the conditions on n and q for the existence of triadic codes over the field $\mathbb{F}_q$ are satisfied. Let $\eta_i,\ 1 \le i \le m$ be the idempotents as defined in equation (1). Let the set of suffixes $\{1, 2, \ldots, m\}$ be divided into three disjoint non-empty sets

$$\{1, 2, \ldots, m\} = \{i_1, i_2, \ldots, i_r\} \cup \{j_1, j_2, \ldots, j_s\} \cup \{k_1, k_2, \ldots, k_t\},$$

where $r + s + t = m$ and r, s, t vary from 1 to $m - 2$. Denote

$$\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_r} = \theta_{i_r},\ \eta_{j_1} + \eta_{j_2} + \cdots + \eta_{j_s} = \theta_{j_s}, \eta_{k_1} + \eta_{k_2} + \cdots + \eta_{k_t} = \theta_{k_t}.$$

Using Lemma 5, we find that

$$\theta_{i_r} + \theta_{j_s} + \theta_{k_t} = 1, \tag{9}$$

and that $\theta_{i_r}, \theta_{j_s}, \theta_{k_t}$ are mutually orthogonal idempotents in the ring $\mathcal{R}$, i.e.

$$\theta_{i_r}^2 = \theta_{i_r},\ \theta_{j_s}^2 = \theta_{j_s},\ \theta_{k_t}^2 = \theta_{k_t} \text{ and } \theta_{i_r}\theta_{j_s} = \theta_{j_s}\theta_{k_t} = \theta_{k_t}\theta_{i_r} = 0. \tag{10}$$

For $i = 1, 2, 3$, let $e_i,\ e_i',\ d_i,\ d_i'$ be the idempotent generators of triadic codes over $\mathbb{F}_q$ as defined in Section 2.2. Let μ_a be the corresponding multiplier. For any tuple (r, s, t), let

$$\begin{aligned}
E_1 = E_1^{(r,s,t)} &= \theta_{i_r}e_1 + \theta_{j_s}e_2 + \theta_{k_t}e_3,\\
E_2 = \mu_a(E_1) &= \theta_{i_r}\mu_a(e_1) + \theta_{j_s}\mu_a(e_2) + \theta_{k_t}\mu_a(e_3)\\
&= \theta_{i_r}e_3 + \theta_{j_s}e_1 + \theta_{k_t}e_2,\\
E_3 = \mu_a(E_2) &= \theta_{i_r}e_2 + \theta_{j_s}e_3 + \theta_{k_t}e_1,\\
E_1' = E_1'^{(r,s,t)} &= \theta_{i_r}e_1' + \theta_{j_s}e_2' + \theta_{k_t}e_3',\\
E_2' = \mu_a(E_1') &= \theta_{i_r}e_3' + \theta_{j_s}e_1' + \theta_{k_t}e_2' \text{ and}\\
E_3' = \mu_a(E_2') &= \theta_{i_r}e_2' + \theta_{j_s}e_3' + \theta_{k_t}e_1'
\end{aligned} \tag{11}$$

be even-like idempotents in the ring $\mathcal{R}[x]/\langle x^n - 1\rangle$. Similarly, let

$$\begin{aligned}
D_1 = D_1^{(r,s,t)} &= \theta_{i_r}d_1 + \theta_{j_s}d_2 + \theta_{k_t}d_3,\\
D_2 = \mu_a(D_1) &= \theta_{i_r}d_3 + \theta_{j_s}d_1 + \theta_{k_t}d_2,\\
D_3 = \mu_a(D_2) &= \theta_{i_r}d_2 + \theta_{j_s}d_3 + \theta_{k_t}d_1,\\
D_1' = D_1'^{(r,s,t)} &= \theta_{i_r}d_1' + \theta_{j_s}d_2' + \theta_{k_t}d_3',\\
D_2' = \mu_a(D_1') &= \theta_{i_r}d_3' + \theta_{j_s}d_1' + \theta_{k_t}d_2' \text{ and}\\
D_3' = \mu_a(D_2') &= \theta_{i_r}d_2' + \theta_{j_s}d_3' + \theta_{k_t}d_1'
\end{aligned} \tag{12}$$

be odd-like idempotents in the ring $\mathcal{R}[x]/\langle x^n - 1\rangle$.

For each tuple (r, s, t), $1 \le r, s, t \le m-2$ and for each i, $1 \le i \le 3$, let $T_i^{(r,s,t)}, T_i'^{(r,s,t)}$ denote the odd-like triadic codes and $P_i^{(r,s,t)}$, $P_i'^{(r,s,t)}$ denote the even-like triadic codes over $\mathcal{R}$ generated by the corresponding idempotents, i.e.

$$\begin{aligned}
T_i^{(r,s,t)} &= \langle D_i^{(r,s,t)}\rangle,\ \ T_i'^{(r,s,t)} = \langle D_i'^{(r,s,t)}\rangle,\\
P_i^{(r,s,t)} &= \langle E_i^{(r,s,t)}\rangle,\ \ P_i'^{(r,s,t)} = \langle E_i'^{(r,s,t)}\rangle.
\end{aligned} \tag{13}$$

Theorem 9: *For any tuple (r, s, t), $1 \le r, s, t \le m-2$, $T_1^{(r,s,t)}$, $T_2^{(r,s,t)}$ and $T_3^{(r,s,t)}$ are equivalent; $T_1'^{(r,s,t)}$, $T_2'^{(r,s,t)}$ and $T_3'^{(r,s,t)}$ are equivalent; $P_1^{(r,s,t)}$, $P_2^{(r,s,t)}$ and $P_3^{(r,s,t)}$ are equivalent; $P_1'^{(r,s,t)}$, $P_2'^{(r,s,t)}$ and $P_3'^{(r,s,t)}$ are equivalent. Further there are $\frac{2}{3}\sum_{r=1}^{m-2}\sum_{s=1}^{m-r-1}\binom{m}{r}\binom{m-r}{s}$ inequivalent odd-like triadic codes and the same number of inequivalent even-like triadic codes over the ring $\mathcal{R}$.*

Proof: The first statement is clear. Out of m idempotents $\eta_i, 1 \le i \le m, \theta_{i_r}$ can be chosen in $\binom{m}{r}$ ways; out of the remaining $m-r$ idempotents η_i's, θ_{j_s} can be chosen in $\binom{m-r}{s}$ ways. As θ_{k_t} must have at least one η_i, the number of choices of idempotents $\theta_{i_r}d_1 + \theta_{j_s}d_2 + \theta_{k_t}d_3$ is $\sum_{r=1}^{m-2}\sum_{s=1}^{m-r-1}\binom{m}{r}\binom{m-r}{s}$. Since $\mu_a(D_1) = D_2, \mu_a(D_2) = D_3, \mu_a(D_3) = D_1$, the inequivalent odd-like idempotents $D_i^{(r,s,t)}$'s are $\frac{1}{3}\sum_{r=1}^{m-2}\sum_{s=1}^{m-r-1}\binom{m}{r}\binom{m-r}{s}$. The other $D_i'^{(r,s,t)}$'s contribute an equal number of inequivalent odd-like idempotents. Hence the result. $\square$

We drop the superscript (r, s, t), when there is no confusion with the idempotents or the corresponding triadic codes.

Theorem 10: *The following assertions hold for triadic codes over $\mathcal{R}$.*

i $T_1 \cap T_2 \cap T_3 = \langle \bar{j}(x) \rangle =$ the repetition code over $\mathcal{R}$

ii $T_1 + T_2 + T_3 = T_1 + T_2 = T_2 + T_3 = T_1 + T_3$

iii $P_1 \cap P_2 \cap P_3 = P_1 \cap P_2 = P_2 \cap P_3 = P_1 \cap P_3$

iv $P_1 + P_2 + P_3 = \langle 1 - \bar{j}(x) \rangle =$ the even weight code over $\mathcal{R}$

v $P_i \cap \langle \bar{j}(x) \rangle = \{0\},\ T_i \cap \langle \bar{j}(x) \rangle = \langle \bar{j}(x) \rangle$ and

vi $P_i + T_i = \mathcal{R}[x]/\langle x^n - 1 \rangle,\ P_i \cap T_i = \{0\}$.

Proof: From the definitions and relations (9)–(12), we see that

$$\begin{aligned}
&E_1 + E_2 + E_3 = e_1 + e_2 + e_3,\ D_1 + D_2 + D_3 = d_1 + d_2 + d_3,\\
&D_1 D_2 D_3 = d_1 d_2 d_3,\ E_1 E_2 E_3 = e_1 e_2 e_3,\\
&D_1 D_2 + D_2 D_3 + D_3 D_1 = d_1 d_2 + d_2 d_3 + d_3 d_1,\\
&E_1 E_2 + E_2 E_3 + E_3 E_1 = e_1 e_2 + e_2 e_3 + e_3 e_1.
\end{aligned}$$

Therefore by Lemma 1(iii) and Proposition 1(viii), $T_1 \cap T_2 \cap T_3 = \langle D_1 D_2 D_3 \rangle = \langle \bar{j}(x) \rangle$. This proves (i).

To prove (ii), we find that $T_1 + T_2 + T_3 = \langle D_1 + D_2 + D_3 - D_1 D_2 - D_2 D_3 - D_3 D_1 + D_1 D_2 D_3 \rangle$, $T_1 + T_2 = \langle D_1 + D_2 - D_1 D_2 \rangle$. Now by Proposition 1(ix),

$$\begin{aligned}
D_1 + D_2 - D_1 D_2 &= \theta_{i_r}(d_1 + d_3 - d_1 d_3) + \theta_{j_s}(d_2 + d_1 - d_2 d_1) + \theta_{k_t}(d_2 + d_3 - d_2 d_3)\\
&= d_1 + d_2 + d_3 - d_1 d_2 - d_2 d_3 - d_1 d_3 + d_1 d_2 d_3\\
&= D_1 + D_2 + D_3 - D_1 D_2 - D_2 D_3 - D_3 D_1 + D_1 D_2 D_3.
\end{aligned}$$

Hence $T_1 + T_2 + T_3 = T_1 + T_2$. Similarly $T_2 + T_3 = T_1 + T_2 + T_3 = T_1 + T_3$.

Again by Proposition 1(vi),

$$\begin{aligned}
E_1 E_2 &= \theta_{i_r}(e_1 e_3) + \theta_{j_s}(e_2 e_1) + \theta_{k_t}(e_2 e_3)\\
&= (\theta_{i_r} + \theta_{j_s} + \theta_{k_t})(e_1 e_2 e_3)\\
&= e_1 e_2 e_3 = E_1 E_2 E_3 = E_2 E_3 = E_3 E_1.
\end{aligned}$$

Therefore $P_1 \cap P_2 \cap P_3 = P_1 \cap P_2 = P_2 \cap P_3 = P_1 \cap P_3$. Similarly

$$\begin{aligned}
&E_1 + E_2 + E_3 - E_1 E_2 - E_2 E_3 - E_3 E_1 + E_1 E_2 E_3\\
&= e_1 + e_2 + e_3 - e_1 e_2 - e_2 e_3 - e_1 e_3 + e_1 e_2 e_3\\
&= e_1 + e_2 + e_3 - 2 e_1 e_2 e_3 = 1 - \bar{j}(x).
\end{aligned}$$

Hence $P_1 + P_2 + P_3 = \langle 1 - \bar{j}(x) \rangle$. This proves (iii) and (iv).
Since $e_i(\bar{j}(x)) = 0$ by Proposition 2(xv), we get $E_i(\bar{j}(x)) = 0$ and so $P_i \cap \langle \bar{j}(x) \rangle = \{0\}$. As $d_i = 1 - e_i$, we get $D_i = 1 - E_i$, so we have $D_i(\bar{j}(x)) = \bar{j}(x) - E_i(\bar{j}(x)) = \bar{j}(x)$. Therefore $T_i \cap \langle \bar{j}(x) \rangle = \langle \bar{j}(x) \rangle$. This proves (v).
Finally to prove (vi), we note that $E_1 D_1 = \theta_{i_r}(e_1 d_1) + \theta_{j_s}(e_2 d_2) + \theta_{k_t}(e_3 d_3)$ and $E_1 +$

$D_1 = \theta_{i_r}(e_1 + d_1) + \theta_{j_s}(e_2 + d_2) + \theta_{k_t}(e_3 + d_3)$, which are equal to 0 and 1 respectively by Proposition 1(x). Therefore $P_1 \cap T_1 = \langle E_1 D_1 \rangle = \{0\}$ and $P_1 + T_1 = \langle E_1 + D_1 - E_1 D_1 \rangle = \langle 1 \rangle$. In the same way $P_i \cap T_i = \{0\}$ and $P_i + T_i = \langle 1 \rangle$ for $i = 2, 3$. □

Similarly, we have

Theorem 11:

i $T'_1 \cap T'_2 \cap T'_3 = T'_1 \cap T'_2 = T'_2 \cap T'_3 = T'_1 \cap T'_3$

ii $T'_1 + T'_2 + T'_3 = \langle 1 \rangle = \mathcal{R}[x]/\langle x^n - 1 \rangle$

iii $P'_1 \cap P'_2 \cap P'_3 = \{0\}$

iv $P'_1 + P'_2 + P'_3 = P'_1 + P'_2 = P'_2 + P'_3 = P'_1 + P'_3$

v $P'_i \cap \langle \bar{j}(x) \rangle = \{0\},\ T'_i \cap \langle \bar{j}(x) \rangle = \langle \bar{j}(x) \rangle$

vi $P'_i + T'_i = \mathcal{R}[x]/\langle x^n - 1 \rangle,\ P'_i \cap T'_i = \{0\}$

vii $P_i + \langle \bar{j}(x) \rangle = T'_i,\ P'_i + \langle \bar{j}(x) \rangle = T_i$

viii $P_i + P'_i = \langle 1 - \bar{j}(x) \rangle,\ P_i \cap P'_i = \{0\}$ and

ix $T_i + T'_i = \mathcal{R}[x]/\langle x^n - 1 \rangle,\ T_i \cap T'_i = \langle \bar{j}(x) \rangle.$

Proof: The proof of statements (i) to (vi) is similar to that of (i) to (vi) of Theorem 10. To prove (vii), we note that

$$\begin{aligned}
&E_1 + \bar{j}(x) - E_1(\bar{j}(x)) = E_1 + \bar{j}(x) \\
&= \theta_{i_r} e_1 + \theta_{j_s} e_2 + \theta_{k_t} e_3 + \bar{j}(x)(\theta_{i_r} + \theta_{j_s} + \theta_{k_t}) \\
&= \theta_{i_r}(e_1 + (\bar{j}(x)) + \theta_{j_s}(e_2 + (\bar{j}(x)) + \theta_{k_t}(e_3 + (\bar{j}(x)) \\
&= \theta_{i_r} d'_1 + \theta_{j_s} d'_2 + \theta_{k_t} d'_3 = D'_1, \quad \text{by Proposition 2(xv).}
\end{aligned}$$

Hence $P_1 + \langle \bar{j}(x) \rangle = T'_1$. Similarly others. The remaining statements (viii) and (ix) follow from the definition and Proposition 2(xvi). □

Theorem 12: *Let P_i, P'_i, for $i = 1, 2, 3$, be two pairs of even-like triadic codes over the ring with T_i, T'_i the associated pairs of odd-like triadic codes. Then*

$P_i^{\perp} = \mu_{-1}(T_i)$ *and* $P_i'^{\perp} = \mu_{-1}(T'_i)$.

Further if $\mu_{-1}(d_i) = d_i$ for $i = 1, 2, 3$, then

$P_i^{\perp} = T_i$, $P_i'^{\perp} = T'_i$ *and P_i, P'_i are LCD codes over $\mathcal{R}$.*

Proof: By Proposition 1(x), $e_i + d_i = 1$. So $\mu_{-1}(e_i) + \mu_{-1}(d_i) = \mu_{-1}(1) = 1$. Therefore

$$\begin{aligned}
1 - \mu_{-1}(E_1) &= \theta_{i_r} + \theta_{j_s} + \theta_{k_t} - \mu_{-1}(\theta_{i_r} e_1 + \theta_{j_s} e_2 + \theta_{k_t} e_3) \\
&= \theta_{i_r}(1 - \mu_{-1}(e_1)) + \theta_{j_s}(1 - \mu_{-1}(e_2)) + \theta_{k_t}(1 - \mu_{-1}(e_3)) \\
&= \theta_{i_r} \mu_{-1}(d_1) + \theta_{j_s} \mu_{-1}(d_2) + \theta_{k_t} \mu_{-1}(d_3) \\
&= \mu_{-1}(\theta_{i_r} d_1 + \theta_{j_s} d_2 + \theta_{k_t} d_3) = \mu_{-1}(D_1).
\end{aligned}$$

Hence $P_1^{\perp} = \langle 1 - \mu_{-1}(E_1) \rangle = \langle \mu_{-1}(D_1) \rangle = \mu_{-1}(\langle D_1 \rangle) = \mu_{-1}(T_1)$. Similarly, we get the others.

Further if $\mu_{-1}(d_i) = d_i$ for $i = 1, 2, 3$, and so $\mu_{-1}(d'_i) = d'_i$, then by Theorem 10(vi) and

Theorem 11(vi), we see that

$$P_i \cap P_i^{\perp} = P_i \cap T_i = \{0\},\ P_i' \cap P_i'^{\perp} = P_i' \cap T_i' = \{0\}$$

proving thereby that P_i and P_i' are LCD codes over $\mathcal{R}$. $\square$

Theorem 13: *If X'_∞ is empty, then we have the following additional results:*

i $|P_i| = q^{\frac{m(n-1)}{3}}, |T_i'| = q^{\frac{m(n+2)}{3}}$ and

ii $|P_i'| = q^{\frac{2m(n-1)}{3}}, |T_i| = q^{\frac{m(2n+1)}{3}}$.

Proof: Since $e_1e_2e_3 = e_1e_2 = e_2e_3 = e_3e_1 = 0$, we find that $E_1E_2 = (\theta_{i_r}e_1 + \theta_{j_s}e_2 + \theta_{k_t}e_3)(\theta_{i_r}e_3 + \theta_{j_s}e_1 + \theta_{k_t}e_2) = \theta_{i_r}e_1e_3 + \theta_{j_s}e_2e_1 + \theta_{k_t}e_3e_2 = 0$. Similarly $(E_1 + E_2 - E_1E_2)E_3 = 0$. Therefore $P_1 \cap P_2 = \langle E_1E_2\rangle = \{0\}$ and $(P_1 + P_2) \cap P_3 = \langle (E_1 + E_2 - E_1E_2)E_3\rangle = \{0\}$. Hence, by Theorem 10(iv), we have

$$|\langle 1 - \bar{j}(x)\rangle| = |P_1 + P_2 + P_3| = \frac{|P_1 + P_2||P_3|}{|(P_1 + P_2) \cap P_3|}$$
$$= \frac{|P_1||P_2||P_3|}{|P_1 \cap P_2||(P_1 + P_2) \cap P_3|} = |P_1|^3.$$

As $|\langle 1 - \bar{j}(x)\rangle| = (q^m)^{(n-1)}$, we get that $|P_1| = q^{\frac{m(n-1)}{3}} = |P_2| = |P_3|$. Since from Theorems 11(vii) and 10(v), we have $P_i + \langle \bar{j}(x)\rangle = T_i'$ and $P_i \cap \langle \bar{j}(x)\rangle = \{0\}$, we get

$$|T_i'| = |P_i||\langle \bar{j}(x)\rangle| = q^{\frac{m(n-1)}{3}} q^m = q^{\frac{m(n+2)}{3}}.$$

Again from Theorem 11(viii), we see that $|P_i||P_i'| = |\langle 1 - \bar{j}(x)\rangle| = q^{m(n-1)}$, which gives $|P_i'| = q^{\frac{2m(n-1)}{3}}$. Finally, by Theorem 11(v) and (vii), we have $P_i' \oplus \langle \bar{j}(x)\rangle = T_i$ which gives

$$|T_i| = |P_i'||\langle \bar{j}(x)\rangle| = q^{\frac{2m(n-1)}{3}} q^m = q^{\frac{m(2n+1)}{3}}.$$

$\square$

Corollary 2: *Let the matrix V taken in the definition of the Gray map Φ satisfy $VV^T = \lambda I_m$, $\lambda \in \mathbb{F}_q^*$. If $\mu_{-1}(e_i) = e_i$, i.e., if $\mu_{-1}(S_i) = S_i$, for $i = 1, 2, 3$, then for all possible choices of (r, s, t), $1 \le r, s, t \le m - 2$, the Gray images of even-like triadic codes $P_i^{(r,s,t)}$ and $P_i'^{(r,s,t)}$, i.e., $\Phi(P_i^{(r,s,t)})$ and $\Phi(P_i'^{(r,s,t)})$ are linear complementary dual(LCD) codes of length mn over $\mathbb{F}_q$. Also $\Phi(T_i^{(r,s,t)})$ is dual of $\Phi(P_i^{(r,s,t)})$ and $\Phi(T_i'^{(r,s,t)})$ is dual of $\Phi(P_i'^{(r,s,t)})$. Further if X'_∞ is empty, then $\Phi(P_i^{(r,s,t)})$ is of dimension $\frac{m(n-1)}{3}$ and $\Phi(P_i'^{(r,s,t)})$ is of dimension $\frac{2m(n-1)}{3}$.*

The following example illustrates our theory for triadic codes when $m = 4$. Some other examples for $m = 3$ are given in Table 2. The minimum distances of all these codes have been computed by the Magma Computational Algebra System.

Example 2: Let $q = 5$, $n = 13$, $m = 4$, $f(u) = u(u-1)(u-3)(u-4)$ and

$$V = \begin{pmatrix} 1 & 3 & 1 & 9 \\ -3 & 1 & 9 & -1 \\ -1 & -9 & 1 & 3 \\ -9 & 1 & -3 & 1 \end{pmatrix}$$

be a matrix over $\mathbb{F}_5$ satisfying $VV^T = 2I$. Here $S_1 = \{1, 5, 8, 12\}, S_2 = \{2, 3, 10, 11\}, S_3 = \{4, 6, 7, 9\}$ and $X'_\infty = \emptyset$. The even-like idempotent generators of triadic codes of length 13 over $\mathbb{F}_5$ are $e_1 = 4x^{12} + 3x^{11} + 3x^{10} + x^9 + 4x^8 + x^7 + x^6 + 4x^5 + x^4 + 3x^3 + 3x^2 + 4x + 3$, $e_2 = 3x^{12} + x^{11} + x^{10} + 4x^9 + 3x^8 + 4x^7 + 4x^6 + 3x^5 + 4x^4 + x^3 + x^2 + 3x + 3$ and $e_3 = x^{12} + 4x^{11} + 4x^{10} + 3x^9 + x^8 + 3x^7 + 3x^6 + x^5 + 3x^4 + 4x^3 + 4x^2 + x + 3$. Here $\mu_{-1}(e_1) = e_1$, $\mu_{-1}(e_2) = e_2$ and $\mu_{-1}(e_3) = e_3$. The Gray image of triadic codes $P_1^{(2,1,1)}$, $T_1^{(2,1,1)}$, $P_1'^{(2,1,1)}$ and $T_1'^{(2,1,1)}$ with $\theta_{i_2} = \eta_1 + \eta_4, \theta_{j_1} = \eta_2$ and $\theta_{k_1} = \eta_3$ are respectively [52,16,16], [52,36,5], [52,32,6] and [52,20,12] LCD codes over $\mathbb{F}_5$.

Table 2 Gray images of some triadic codes when $m = 3$ and
$$V = \begin{pmatrix} 4 & 4 & -2 \\ -2 & 4 & 4 \\ 4 & -2 & 4 \end{pmatrix}$$

q	n	$f(u)$	$\Phi(P_1^{(1,1,1)})$	$\Phi(T_1^{(1,1,1)})$	$\Phi(P_1'^{(1,1,1)})$	$\Phi(T_1'^{(1,1,1)})$
5	13	$(u-1)(u+1)$ $(u-3)$	[39,12,12] LCD	[39,27,5] LCD dual of $\Phi(P_1)$	[39,24,6] LCD	[39,15,10] LCD dual of $\Phi(P_1')$
5	13^2	$(u-1)(u+1)$ $(u-3)$	[507,480,2] LCD	[507,27,65] LCD dual of $\Phi(P_1)$	[507,24,78] LCD	[507,483,2] LCD dual of $\Phi(P_1')$
7	19	$(u-1)(u-2)$ $(u-4)$	[57,18,18] LCD	[57,39,7] LCD dual of $\Phi(P_1)$	[57,36,8] LCD	[57,21,15] LCD dual of $\Phi(P_1')$
11	19	$(u-8)(u+2)$ $(u+5)$	[57,18,26] LCD	[57,39,8] LCD dual of $\Phi(P_1)$	[57,36] LCD	[57,21,19] LCD dual of $\Phi(P_1')$

6 Conclusion

In this paper, duadic codes, their extensions and triadic codes over a non-chain ring $\mathcal{R} = \mathbb{F}_q[u]/\langle f(u)\rangle$ are studied, where $f(u)$ is a polynomial of degree $m(\geq 2)$ which splits into distinct linear factors over $\mathbb{F}_q$. A Gray map from $\mathcal{R}^n$ to $(\mathbb{F}_q^m)^n$ is defined which preserves self-duality of linear codes. As a consequence, self-dual, isodual, self-orthogonal and complementary dual(LCD) codes over $\mathbb{F}_q$ are constructed. Some examples are also given to illustrate this. Further, in this direction, polyadic codes or duadic constacyclic codes over the ring $\mathcal{R}$ can be explored.

References

Bakshi, G.K.. Raka, M. and Sharma, A. (2007) 'Existence of polyadic codes in terms of Diophantine Equations', *Diophantine Equations (Proceeding of International Conference on Diophantine Equations, 16-20 December, 2005, TIFR, Mumbai)*, pp.33–48.

Batoul, A., Guenda, K., Kaya, A. and Yildiz, B. (2015) 'Cyclic isodual and formally self-dual codes over $\mathbb{F}_p + v\mathbb{F}_p$', *European J. Pure Appl. Maths.*, Vol. 8, pp.64–80.

Chiu, M.H., Yau, S.T. and Yu, Y. (2000) '$\mathbb{Z}_8$-cyclic codes and quadratic residue codes', *Adv. Appl. Math.*, Vol. 25, pp.12–33.

Goyal, M. and Raka, M. (2018) 'Quadratic residue codes over the ring $\mathbb{F}_p[u]/\langle u^m - u\rangle$ and their Gray images', *Cryptography and Communications, 2018*, Vol. 10, No. 2, pp.343–355.

Goyal, M. and Raka, M. (2016) 'Duadic codes over $\mathbb{F}_p[u]/\langle u^m - u\rangle$', *Journal of Computer and Communications*, Vol. 4, pp.50–62.

Huffman, W.C. and Pless, V. (2003) *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, UK.

Kaya, A., Yildiz, B. and Siap, I. (2014a) 'Quadratic residue codes over $\mathbb{F}_p + u\mathbb{F}_p$ and their Gray images', *Journal of Pure and Appl. Alg.*, Vol. 218, pp.1999–2011.

Kaya, A., Yildiz, B. and Siap, I. (2014b) 'New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$', *Finite Fields Appl.*, Vol. 29, pp.160–177.

Liu, Y., Shi, M. and Solé, P. (2014) 'Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$', *WAIFI*, pp.204–211.

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

Pless, V. and Rushanan, J. (1988) 'Triadic codes over a finite field', *Linear Algebra and its Applications*, Vol. 98, pp.415–433.

Raka, M., Kathuria, L. and Goyal, M. (2017) '$(1 - 2u^3)$-constacyclic codes and quadratic residue codes over $\mathbb{F}_p[u]/\langle u^4 - u\rangle$', *Cryptogr. Commun.*, Vol. 9, No. 4, pp.459–473.

Sharma, A., Bakshi, G.K. and Raka, M. (2007) 'Polyadic codes of prime power length', *Finite Fields Appl.*, Vol. 13, pp.1071–1085.

Smid, M.H.M. (1987) 'Duadic codes', *IEEE Trans. Inform. Theory*, Vol. 33, No. 3, pp.432–433.

Taeri, B. (2009) 'Quadratic residue Codes over $\mathbb{Z}_9$', *J. Korean Math. Soc.*, Vol. 46, No. 1, pp.13–30.

Zhang, T. and Zhu, S. (2012) 'Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$', *J. Univ. Sci. Technol.*, Vol. 42, No. 3, pp.208–213.