Journal of Computer and Communications, 2016, 4, 50-62
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Duadic Codes over the Ring $\mathbb{F}_q[u]/\langle u^m - u\rangle$ and Their Gray Images

Mokshi Goyal, Madhu Raka

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

How to cite this paper: Goyal, M. and Raka, M. (2016) Duadic Codes over the Ring $\mathbb{F}_q[u]/\langle u^m - u\rangle$ and Their Gray Images. *Journal of Computer and Communications*, **4**, 50-62.
http://dx.doi.org/10.4236/jcc.2016.412003

Received: August 10, 2016
Accepted: October 24, 2016
Published: October 27, 2016

Copyright © 2016 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

Let $m \geq 2$ be any natural number and let $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{m-1}\mathbb{F}_q$ be a finite non-chain ring, where $u^m = u$ and q is a prime power congruent to 1 modulo $(m-1)$. In this paper we study duadic codes over the ring $\mathcal{R}$ and their extensions. A Gray map from $\mathcal{R}$ to $\mathbb{F}_q^m$ is defined which preserves self duality of linear codes. As a consequence self-dual, formally self-dual and self-orthogonal codes over $\mathbb{F}_q$ are constructed. Some examples are also given to illustrate this.

Keywords

Quadratic Residue Codes, Duadic Codes, Extended Duadic-Codes, Gray Map, Self-Dual, Self-Orthogonal Codes, Formally Self-Dual Codes

1. Introduction

Duadic codes form a class of cyclic codes that generalizes quadratic residue codes from prime to composite lengths. While initially quadratic residue codes were studied within the confines of finite fields, there have been recent developments on quadratic residue codes over some special rings. Pless and Qian [1] studied quadratic residue codes over $\mathbb{Z}_4$, Chiu *et al.* [2] extended the ideas to the ring $\mathbb{Z}_8$ and Taeri [3] considered QR-codes over $\mathbb{Z}_9$. Kaya *et al.* [4] and Zhang *et al.* [5] studied quadratic residue codes over $\mathbb{F}_p + u\mathbb{F}_p$ where p is an odd prime. Kaya *et al.* [6] studied quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ whereas Liu *et al.* [7] 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. The authors [8] along with Kathuria 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 $p \equiv 1 \pmod 3$. In [9] the authors 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 $u^m = u$ and p is a prime satisfying $p \equiv 1 \pmod{(m-1)}$ generalizing all the previous results.

There are duadic codes which are not quadratic residue codes, but they have properties similar to those of quadratic residue codes. In this paper we extend our results of [9] to duadic codes over the ring $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{m-1}\mathbb{F}_q$, where $u^m = u$, q is a prime power congruent to 1 modulo $(m-1)$. The Gray map defined in [9] is also extended from $\mathcal{R}^n \to \mathbb{F}_q^{mn}$ which preserves linearity and in some special cases preserves self duality. The Gray images of extensions of duadic codes over the ring $\mathcal{R}$ lead to construction of self-dual, formally self-dual and self-orthogonal codes. We give some examples of duadic but non quadratic residue codes which give rise to a [40,20,6] self-dual code over $\mathbb{F}_{13}$, a [27,12,6] self orthogonal code over $\mathbb{F}_7$, a [30,12,8] self-orthogonal code over $\mathbb{F}_{11}$ and a formally self-dual [24,12,6] code over $\mathbb{F}_4$.

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

2. Duadic Codes over $\mathbb{F}_q$ and Their Properties

In this section we give the definition of duadic codes and state some of their properties. Before that we need some preliminary notations and results.

A cyclic code $\mathbb{C}$ 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 idempotent generator $e(x)$.

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

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 $\mathbb{C}$ is called even like (odd like) if all its codewords are even like (odd like). For $(a, n) = 1$, $\mu_a : \mathbb{Z}_n \to \mathbb{Z}_n$ defined as $\mu_a(i) = ai \pmod{n}$ is called a multiplier where $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$. It is extended on $\mathbb{S}_n$ by defining $\mu_a\left(\sum_i f_i x^i\right) = \sum_i f_i x^{\mu_a(i)}$.

Suppose n is odd, $(n, q) = 1$ and $\mathbb{Z}_n = S_1 \cup S_2 \cup 0$, where

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

(ii) $S_1 \cap S_2 = \phi$

(iii) There exists a multiplier μ_b, $(b, n) = 1$ such that $\mu_b(S_1) = S_2$ and $\mu_b(S_2) = S_1$.

Then codes $\mathbb{D}_1$ and $\mathbb{D}_2$ having S_1 and S_2 as defining sets 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.

There is an equivalent definition of duadic codes in terms of idempotents. (For details see Huffman and Pless [10], Chapter 6).

Let $e_1(x)$ and $e_2(x)$ be two even like idempotents with $\mathbb{C}_1 = \langle e_1(x) \rangle$ and $\mathbb{C}_2 = \langle e_2(x) \rangle$. The codes $\mathbb{C}_1$ and $\mathbb{C}_2$ form a pair of even like duadic codes if and only if

(1) the idempotents satisfy

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

(2) There is a multiplier μ_b such that

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

i.e. $\mu_b(\mathbb{C}_1) = \mathbb{C}_2$ and $\mu_b(\mathbb{C}_2) = \mathbb{C}_1$

Associated to $\mathbb{C}_1$ and $\mathbb{C}_2$ there is a pair of odd like duadic codes $\mathbb{D}_1$ and $\mathbb{D}_2$ generated by idempotents $d_1(x)$ and $d_2(x)$ respectively, where $d_1(x) = 1 - e_2(x)$, $d_2(x) = 1 - e_1(x)$

If (1) and (2) hold we say that μ_b gives a splitting for even like duadic codes $\mathbb{C}_1$ and $\mathbb{C}_2$ or for the odd like duadic codes $\mathbb{D}_1$ and $\mathbb{D}_2$.

Lemma 1: 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 $\mathbb{F}_q$. 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. Then:

(i) $e_1 e_2 = 0$,

(ii) $\mathbb{C}_1 \cap \mathbb{C}_2 = \{0\}$ and $\mathbb{C}_1 + \mathbb{C}_2 = \mathcal{E}_n$,

(iii) $\mathbb{C}_i$ is even like subcode of $\mathbb{D}_i$ for $i = 1, 2$,

(iv) $\mathbb{D}_1 \cap \mathbb{D}_2 = \langle \bar{j}(x) \rangle$ and $\mathbb{D}_1 + \mathbb{D}_2 = \mathbb{S}_n$, and

(v) $\mathbb{D}_i = \mathbb{C}_i + \langle \bar{j}(x) \rangle = \langle \bar{j}(x) + e_i(x) \rangle$ for $i = 1, 2$.

This is part of Theorem 6.1.3 of [10].

Lemma 2: Let $\mathbb{C}_1$ and $\mathbb{C}_2$ be a pair of even-like duadic codes over $\mathbb{F}_q$ with $\mathbb{D}_1$ and $\mathbb{D}_2$ the associated pair of odd-like duadic codes.

(i) If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_2$ and $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_1$
then $\mathbb{C}_1^{\perp} = \mathbb{D}_1$ and $\mathbb{C}_2^{\perp} = \mathbb{D}_2$.

(ii) If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_1$ and $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_2$
then $\mathbb{C}_1^{\perp} = \mathbb{D}_2$ and $\mathbb{C}_2^{\perp} = \mathbb{D}_1$

Proof follows from Theorems 6.4.2 and 6.4.3 of [10].

Lemma 3: $d_1 + d_2 = 1 + \bar{j}(x)$, $e_1 + e_2 = 1 - \bar{j}(x)$, $d_1 - e_1 = \bar{j}(x)$, $d_2 - e_2 = \bar{j}(x)$. Further $d_1 d_2 = \bar{j}(x)$ and $e_1 e_2 = 0$.

Proof follows immediately from the definition and Lemma 1.

3. Cyclic Codes over the Ring $\mathcal{R}$ and the Gray Map

Let q be a prime power, $q = p^s$. Throughout the paper, $\mathcal{R}$ denotes the commutative ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{m-1}\mathbb{F}_q$, where $u^m = u$, $m \geq 2$ is a natural number and

$q \equiv 1 \pmod{(m-1)}$. $\mathcal{R}$ is a ring of size q^m and characteristic p. For a primitive element α of $\mathbb{F}_q$, take $\xi = \alpha^{\frac{q-1}{m-1}}$, so that $\xi^{m-1} = 1, \xi \neq 1$ and $\xi^{m-2} + \xi^{m-3} + \cdots + \xi + 1 = 0$. Let $\eta_1, \eta_2, \eta_3, \cdots, \eta_m$ denote the following elements of $\mathcal{R}$:

$$\begin{aligned}
\eta_1 &= 1 - u^{m-1}, \\
\eta_2 &= (m-1)^{-1}\left(u + u^2 + \cdots + u^{m-2} + u^{m-1}\right), \\
\eta_3 &= (m-1)^{-1}\left(\xi u + \xi^2 u^2 + \cdots + \xi^{m-2} u^{m-2} + u^{m-1}\right), \\
\eta_4 &= (m-1)^{-1}\left(\xi^2 u + \left(\xi^2\right)^2 u^2 + \cdots + \left(\xi^2\right)^{m-2} u^{m-2} + u^{m-1}\right), \\
&\vdots \\
\eta_m &= (m-1)^{-1}\left(\xi^{m-2} u + \left(\xi^{m-2}\right)^2 u^2 + \cdots + \left(\xi^{m-2}\right)^{m-2} u^{m-2} + u^{m-1}\right).
\end{aligned} \tag{1}$$

A simple calculation shows that

$$\eta_i^2 = \eta_i, \eta_i \eta_j = 0 \quad \text{for } 1 \le i, j \le m, i \neq j \text{ and } \sum_{i=1}^{m} \eta_i = 1. \tag{2}$$

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

$$\begin{aligned}
\mathcal{C}_1 &= \left\{x_1 \in \mathbb{F}_q^n : \exists\, x_2, x_3, \cdots, x_m \in \mathbb{F}_q^n \text{ such that } \eta_1 x_1 + \eta_2 x_2 + \cdots + \eta_m x_m \in \mathcal{C}\right\}, \\
\mathcal{C}_2 &= \left\{x_2 \in \mathbb{F}_q^n : \exists\, x_1, x_3, \cdots, x_m \in \mathbb{F}_q^n \text{ such that } \eta_1 x_1 + \eta_2 x_2 + \cdots + \eta_m x_m \in \mathcal{C}\right\} \\
&\vdots \\
\mathcal{C}_m &= \left\{x_m \in \mathbb{F}_q^n : \exists\, x_1, x_2, \cdots, x_{m-1} \in \mathbb{F}_q^n \text{ such that } \eta_1 x_1 + \eta_2 x_2 + \cdots + \eta_m x_m \in \mathcal{C}\right\}
\end{aligned}.$$

Then $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_m$ 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 $|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2| \cdots |\mathcal{C}_m|$. For a code $\mathcal{C}$ over $\mathcal{R}$, the dual code $\mathcal{C}^\perp$ is defined as $\mathcal{C}^\perp = \left\{x \in \mathcal{R}^n \mid x \cdot y = 0 \text{ for all } y \in \mathcal{C}\right\}$ 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 formally self-dual if $\mathcal{C}$ and $\mathcal{C}^\perp$ have the same weight distribution.

The following result is a simple generalization of a result of [7].

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 $\mathcal{C}_i, i = 1, 2, \cdots, m$ are cyclic over $\mathbb{F}_q$.

(ii) If $\mathcal{C}_i = \langle g_i(x) \rangle, g_i(x) \in \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$, $g_i(x) \mid (x^n - 1)$, then

$\mathcal{C} = \langle \eta_1 g_1(x), \eta_2 g_2(x), \cdots, \eta_m g_m(x) \rangle = \langle g(x) \rangle$ where

$g(x) = \eta_1 g_1 + \eta_2 g_2 + \cdots + \eta_m g_m$ and $g(x) \mid (x^n - 1)$.

(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

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

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

The following is a well known result :

Lemma 4: (i) Let C be a cyclic code of length n over a finite ring S generated by the idempotent E in $S[x]/\left\langle x^n-1\right\rangle$ then $C^{\perp}$ is generated by the idempotent $1-E\left(x^{-1}\right)$.

(ii) Let C and D be cyclic codes of length n over a finite ring S generated by the idempotents E_1, E_2 in $S[x]/\left\langle x^n-1\right\rangle$ then $C\cap D$ and $C+D$ are generated by the idempotents E_1E_2 and $E_1+E_2-E_1E_2$ respectively.

Let the Gray map $\Phi:\mathcal{R}\to\mathbb{F}_q^m$ be given by

$$r(u)=a_0+a_1u+a_2u^2+\cdots+a_{m-1}u^{m-1}\mapsto\left(r(0),r(1),r(\xi),\cdots,r\left(\xi^{m-2}\right)\right)V$$

$$=\left(a_0,a_1,a_2,\cdots,a_{m-1}\right)\begin{pmatrix}1&1&1&1&\cdots&1\\0&1&\xi&\xi^2&\cdots&\xi^{m-2}\\0&1&\xi^2&\left(\xi^2\right)^2&\cdots&\left(\xi^2\right)^{m-2}\\0&1&\xi^3&\left(\xi^3\right)^2&\cdots&\left(\xi^3\right)^{m-2}\\\vdots&\vdots&\vdots&\vdots&\cdots&\vdots\\0&1&\xi^{m-2}&\left(\xi^{m-2}\right)^2&\cdots&\left(\xi^{m-2}\right)^{m-2}\\0&1&1&1&\cdots&1\end{pmatrix}V$$

$$=\left(a_0,a_1,a_2,\cdots,a_{m-1}\right)MV$$

where M is an $m\times m$ nonsingular matrix of Vandermonde determinant $\prod_{1\le i<j\le m-1}\left(\xi^j-\xi^i\right)$ and V is any nonsingular matrix over $\mathbb{F}_q$ of order $m\times m$. This map can be extended from $\mathcal{R}^n$ to $\mathbb{F}_q^{mn}$ component wise.

Let the Gray weight of an element $r\in\mathcal{R}$ be $w_G(r)=w_H\left(\Phi(r)\right)$, the Hamming weight of $\Phi(r)$. The Gray weight of a codeword $c=\left(c_0,c_1,\cdots,c_{n-1}\right)\in\mathcal{R}^n$ is defined as $w_G(c)=\sum_{i=0}^{n-1}w_G(c_i)=\sum_{i=0}^{n-1}w_H\left(\Phi(c_i)\right)=w_H\left(\Phi(c)\right)$. For any two elements $c_1,c_2\in\mathcal{R}^n$, the Gray distance d_G is given by $d_G(c_1,c_2)=w_G(c_1-c_2)=w_H\left(\Phi(c_1)-\Phi(c_2)\right)$.

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). Further if the matrix V satisfies $VV^{\mathrm{T}}=\lambda I_m$, $\lambda\in\mathbb{F}_q^*$, 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 $\mathbb{F}_q^{mn}$.

The proof follows exactly on the same lines as the proof of Theorem 2 of [9]. The only difference is that here q is an arbitrary prime power and not just an odd prime. For the sake of completeness of the result we reproduce the proof here.

Proof. The first two assertions hold as MV is an invertible matrix over $\mathbb{F}_q$.

Let now $V=(v_{ij})$, $1\le i, j\le m$, satisfying $VV^{\mathrm{T}}=\lambda I_m$. So that

$$\sum_{k=1}^{m} v_{jk}^2=\lambda \text{ for all } j, 1\le j\le m \text{ and } \sum_{k=1}^{m} v_{jk}v_{\ell k}=0 \text{ for } j\ne \ell. \tag{3}$$

Let $\mathcal{C}$ be a self-dual code over $\mathcal{R}$. Let $r=(r_0,r_1,\cdots,r_{n-1}), s=(s_0,s_1,\cdots,s_{n-1})\in\mathcal{C}$ where $r_i=a_{i0}+a_{i1}u+\cdots+a_{im-1}u^{m-1}$ and $s_i=b_{i0}+b_{i1}u+\cdots+b_{im-1}u^{m-1}$. Then

$$0=r\cdot s=\sum_{i=0}^{n-1} r_i s_i=\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\sum_{\ell=0}^{m-1} a_{ij}b_{i\ell}u^{j+\ell}$$

implies that (comparing the coefficients of u^r on both sides)

$$\sum_{i=0}^{n-1} a_{i0}b_{i0}=0 \tag{4}$$

$$\sum_{i=0}^{n-1}\left(a_{i0}b_{ir}+a_{i1}b_{i,r-1}+\cdots+a_{ir}b_{i0}+a_{ir}b_{i,m-1}+a_{i,r+1}b_{i,m-2}+\cdots+a_{i,m-1}b_{i0}\right)=0, \tag{5}$$

for each r, $1\le r\le m-1$.

For convenience we call $\left(r_i(0), r_i(1), r_i(\xi),\cdots, r_i(\xi^{m-2})\right)=(\alpha_{i1},\alpha_{i2},\cdots,\alpha_{im})$ and $\left(s_i(0), s_i(1), s_i(\xi),\cdots, s_i(\xi^{m-2})\right)=(\beta_{i1},\beta_{i2},\cdots,\beta_{im})$. Then

$$\Phi(r_i)=(\alpha_{i1},\alpha_{i2},\cdots,\alpha_{im})V=\left(\sum_{j=1}^{m}\alpha_{ij}v_{j1},\sum_{j=1}^{m}\alpha_{ij}v_{j2},\cdots,\sum_{j=1}^{m}\alpha_{ij}v_{jm}\right)$$

Similarly

$$\Phi(s_i)=\left(\sum_{\ell=1}^{m}\beta_{i\ell}v_{\ell 1},\sum_{\ell=1}^{m}\beta_{i\ell}v_{\ell 2},\cdots,\sum_{\ell=1}^{m}\beta_{i\ell}v_{\ell m}\right).$$

Using (2), we find that

$$\begin{aligned}\Phi(r_i)\cdot\Phi(s_i)&=\sum_{k=1}^{m}\sum_{j=1}^{m}\sum_{\ell=1}^{m}\alpha_{ij}\beta_{i\ell}v_{jk}v_{\ell k}\\&=\sum_{j=1,\ell=j}^{m}\alpha_{ij}\beta_{ij}\left(\sum_{k=1}^{m}v_{jk}^2\right)+\sum_{j=1}^{m}\sum_{\ell=1,\ell\ne j}^{m}\alpha_{ij}\beta_{i\ell}\left(\sum_{k=1}^{m}v_{jk}v_{\ell k}\right)=\lambda\sum_{j=1}^{m}\alpha_{ij}\beta_{ij}.\end{aligned}$$

Now

$$\begin{aligned}\Phi(r)\cdot\Phi(s)&=\sum_{i=0}^{n-1}\Phi(r_i)\cdot\Phi(s_i)=\lambda\sum_{i=0}^{n-1}\sum_{j=1}^{m}\alpha_{ij}\beta_{ij}\\&=\sum_{i=0}^{n-1}\left(\alpha_{i1}\beta_{i1}+\sum_{j=2}^{m}\alpha_{ij}\beta_{ij}\right)\\&=\sum_{i=0}^{n-1}a_{i0}b_{i0}+\sum_{i=0}^{n-1}\sum_{j=2}^{m}r_i\left(\xi^{j-2}\right)s_i\left(\xi^{j-2}\right)\\&=\sum_{i=0}^{n-1}\sum_{k=0}^{m-2}r_i\left(\xi^{k}\right)s_i\left(\xi^{k}\right)\\&=\sum_{i=0}^{n-1}\sum_{k=0}^{m-2}\left(\sum_{j=0}^{m-1}a_{ik}\xi^{kj}\right)\left(\sum_{\ell=0}^{m-1}b_{i\ell}\xi^{k\ell}\right)\\&=\sum_{i=0}^{n-1}\sum_{k=0}^{m-2}\sum_{j=0}^{m-1}\sum_{\ell=0}^{m-1}a_{ik}b_{i\ell}\xi^{k(j+\ell)}\\&=A_0+A_1\xi+A_2\xi^2+\cdots+A_{m-2}\xi^{m-2}\quad\text{say.}\end{aligned}$$

Using (3) and (4), one can check that each A_i is zero, which proves the result.

4. Duadic Codes over the Ring $\mathcal{R}$

We now define duadic codes over the ring $\mathcal{R}$ in terms of their idempotent generators. Let $\mathcal{R}_n$ denote the ring $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$. Using the properties (2) of idempotents η_i, we have

Lemma 5: Let $q \equiv 1(\bmod(m-1))$ and $\eta_i, 1 \le i \le m$ be idempotents as defined in (1). Then for $i_1, i_2, \cdots, i_m \in \{1,2\}$ and for any tuple $(d_{i_1}, d_{i_2}, \cdots, d_{i_m})$ of odd-like idempotents not all equal and for any tuple $(e_{i_1}, e_{i_2}, \cdots, e_{i_m})$ 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 $\mathcal{R}_n = \frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$.

Throughout the paper we assume that q is a square mod n so that duadic codes of length n over $\mathbb{F}_q$ exist. The construction and the properties of duadic codes over the ring $\mathcal{R}$ is similar to that of quadratic residue codes over the ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + \cdots + u^{m-1}\mathbb{F}_p$, where $u^m = u$ given in [9]. We denote the set $\{1,2,\cdots,m\}$ by $\mathbb{A}$. For each $i \in \mathbb{A}$, let $D_{\{i\}}$ denote the odd-like idempotent of the ring $\mathcal{R}_n$ in which d_1 occurs at the ith place and d_2 occurs at the remaining $1,2,\cdots,i-1,i+1,\cdots,m$ places *i.e.*

$$D_{\{i\}} = \eta_1 d_2 + \eta_2 d_2 + \cdots + \eta_{i-1} d_2 + \eta_i d_1 + \eta_{i+1} d_2 + \cdots + \eta_m d_2 = \eta_i d_1 + (1-\eta_i) d_2. \tag{6}$$

For $i_1, i_2 \in \mathbb{A}$, $i_1 \ne i_2$ let $D_{\{i_1,i_2\}}$ denote the odd-like idempotent in which d_1 occurs at the i_1th and i_2th places and d_2 occurs at the remaining $1,2,\cdots,i_1-1,i_1+1,\cdots,i_2-1,i_2+1,\cdots,m$ places *i.e.*

$$\begin{aligned} D_{\{i_1,i_2\}} &= \eta_1 d_2 + \eta_2 d_2 + \cdots + \eta_{i_1-1} d_2 + \eta_{i_1} d_1 + \eta_{i_1+1} d_2 + \cdots \\ &\quad + \eta_{i_2-1} d_2 + \eta_{i_2} d_1 + \eta_{i_2+1} d_2 + \cdots + \eta_m d_2 \\ &= (\eta_{i_1} + \eta_{i_2}) d_1 + (1-\eta_{i_1} - \eta_{i_2}) d_2. \end{aligned} \tag{7}$$

In the same way, for $i_1, i_2, \cdots, i_k \in \mathbb{A}$, $i_r \ne i_s, 1 \le r, s \le k$ let $D_{\{i_1,i_2,\cdots,i_k\}}$ denote the odd-like idempotent

$$D_{\{i_1,i_2,\cdots,i_k\}} = (\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_k}) d_1 + (1-\eta_{i_1} - \eta_{i_2} - \cdots - \eta_{i_k}) d_2. \tag{8}$$

For $i \in \mathbb{A}$, $i_1, i_2, \cdots, i_k \in \mathbb{A}$, where $i_r \ne i_s, 1 \le r, s \le k$ let the corresponding odd-like idempotents be

$$D'_{\{i\}} = \eta_i d_2 + (1-\eta_i) d_1. \tag{9}$$

$$D'_{\{i_1,i_2,\cdots,i_k\}} = (\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_k}) d_2 + (1-\eta_{i_1} - \eta_{i_1} - \cdots - \eta_{i_k}) d_1. \tag{10}$$

Similarly we define even-like idempotents for $i \in \mathbb{A}$ and $i_1, i_2, \cdots, i_k \in \mathbb{A}$, $i_r \ne i_s, 1 \le r, s \le k$,

$$E_{\{i\}} = \eta_i e_1 + (1-\eta_i) e_2. \tag{11}$$

$$E'_{\{i\}} = \eta_i e_2 + (1-\eta_i) e_1. \tag{12}$$

$$E_{\{i_1,i_2,\cdots,i_k\}} = (\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_k}) e_1 + (1-\eta_{i_1} - \eta_{i_2} - \cdots - \eta_{i_k}) e_2. \tag{13}$$

$$E'_{\{i_1,i_2,\cdots,i_k\}} = (\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_k}) e_2 + (1-\eta_{i_1} - \eta_{i_2} - \cdots - \eta_{i_k}) e_1. \tag{14}$$

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

$$Q_{\{i\}} = \langle D_{\{i\}} \rangle, \quad Q'_{\{i\}} = \langle D'_{\{i\}} \rangle, \quad S_{\{i\}} = \langle E_{\{i\}} \rangle, \quad S'_{\{i\}} = \langle E'_{\{i\}} \rangle,$$

$$Q_{\{i_1,i_2,\cdots,i_k\}} = \langle D_{\{i_1,i_2,\cdots,i_k\}} \rangle, \quad Q'_{\{i_1,i_2,\cdots,i_k\}} = \langle D'_{\{i_1,i_2,\cdots,i_k\}} \rangle,$$

$$S_{\{i_1,i_2,\cdots,i_k\}} = \langle E_{\{i_1,i_2,\cdots,i_k\}} \rangle, \quad S'_{\{i_1,i_2,\cdots,i_k\}} = \langle E'_{\{i_1,i_2,\cdots,i_k\}} \rangle.$$

Theorem 3: Let $q \equiv 1 \pmod{(m-1)}$, Then for $i \in \mathbb{A}$, $Q_{\{i\}}$ is equivalent to $Q'_{\{i\}}$ and $S_{\{i\}}$ is equivalent to $S'_{\{i\}}$. For $i_1, i_2, \cdots, i_k \in \mathbb{A}$, $i_r \neq i_s, 1 \leq r, s \leq k$, $Q_{\{i_1,i_2,\cdots,i_k\}}$ is equivalent to $Q'_{\{i_1,i_2,\cdots,i_k\}}$, and $S_{\{i_1,i_2,\cdots,i_k\}}$ is equivalent to $S'_{\{i_1,i_2,\cdots,i_k\}}$. 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 $\mathcal{R}$.

Proof: Let the multiplier μ_b give splitting of $\mathbb{C}_1$ and $\mathbb{C}_2$ or of $\mathbb{D}_1$ and $\mathbb{D}_2$. Then $\mu_b(d_1) = d_2$, $\mu_b(d_2) = d_1$, $\mu_b(e_1) = e_2$, $\mu_b(e_2) = e_1$ and so $\mu_b(\eta_i d_1 + (1-\eta_i) d_2) = \eta_i d_2 + (1-\eta_i) d_1$, $\mu_b(\eta_i e_1 + (1-\eta_i) e_2) = \eta_i e_2 + (1-\eta_i) e_1$, $\mu_b(D_{\{i_1,i_2,\cdots,i_k\}}) = D'_{\{i_1,i_2,\cdots,i_k\}}$, $\mu_b(E_{\{i_1,i_2,\cdots,i_k\}}) = E'_{\{i_1,i_2,\cdots,i_k\}}$. This proves that $Q_i \sim Q'_i$ $S_i \sim S'_i$, $Q_{\{i_1,i_2,\cdots,i_k\}} \sim Q'_{\{i_1,i_2,\cdots,i_k\}}$, and $S_{\{i_1,i_2,\cdots,i_k\}} \sim S'_{\{i_1,i_2,\cdots,i_k\}}$.

Note that $D_{\mathbb{A}-\{i\}} = D'_{\{i\}}$, $E_{\mathbb{A}-\{i\}} = E'_{\{i\}}$, $D_{\mathbb{A}-\{i_1,i_2,\cdots,i_k\}} = D'_{\{i_1,i_2,\cdots,i_k\}}$, $E_{\mathbb{A}-\{i_1,i_2,\cdots,i_k\}} = E'_{\{i_1,i_2,\cdots,i_k\}}$. Therefore

$$Q_{\mathbb{A}-\{i\}} \sim Q'_{\{i\}} \sim Q_{\{i\}}, \; S_{\mathbb{A}-\{i\}} \sim S'_{\{i\}} \sim S_{\{i\}}, \tag{15}$$

$$Q_{\mathbb{A}-\{i_1,i_2,\cdots,i_k\}} \sim Q_{\{i_1,i_2,\cdots,i_k\}}, \; S_{\mathbb{A}-\{i_1,i_2,\cdots,i_k\}} \sim S_{\{i_1,i_2,\cdots,i_k\}}. \tag{16}$$

For a given positive integer *k*, the number of choices of the subsets $\{i_1, i_2, \cdots, i_k\}$ of $\mathbb{A}$ is $\binom{m}{k}$.

Let *m* be even first. Then $\left|\{i_1, i_2, \cdots, i_{m/2}\}\right| = \left|\mathbb{A} - \{i_1, i_2, \cdots, i_{m/2}\}\right| = \frac{m}{2}$. Using (15) and (16), we find that the number of inequivalent odd-like or even-like duadic-codes is $\binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{(m/2)-1} + \frac{1}{2}\binom{m}{m/2} = 2^{m-1} - 1$. If *m* is odd the number of inequivalent odd-like or even-like duadic codes is $\binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{(m-1)/2} = 2^{m-1} - 1$.

Let $[x]$ denote the greatest integer $\le x$. we have $\left[\frac{m}{2}\right]=\frac{m}{2}$ when m is even and $\left[\frac{m}{2}\right]=\frac{m-1}{2}$ when m is odd.

Theorem 4: If $q\equiv 1(\bmod(m-1))$, then for subsets $\{i_1,i_2,\cdots,i_k\}$ of $\mathbb{A}$ with cardinality k, $1\le k\le\left[\frac{m}{2}\right]$, the following assertions hold for duadic codes over $\mathcal{R}$.

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

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

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

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

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

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

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

Proof: From the relations (2),(6)-(14) we see that $D_{\{i_1,i_2,\cdots,i_k\}}+D'_{\{i_1,i_2,\cdots,i_k\}}=d_1+d_2$, $E_{\{i_1,i_2,\cdots,i_k\}}+E'_{\{i_1,i_2,\cdots,i_k\}}=e_1+e_2$, $D_{\{i_1,i_2,\cdots,i_k\}}D'_{\{i_1,i_2,\cdots,i_k\}}=d_1d_2$ and $E_{\{i_1,i_2,\cdots,i_k\}}E'_{\{i_1,i_2,\cdots,i_k\}}=e_1e_2$. Therefore by Lemmas 1 and 4, $Q_{\{i_1,i_2,\cdots,i_k\}}\cap Q'_{\{i_1,i_2,\cdots,i_k\}}=\left\langle D_{\{i_1,i_2,\cdots,i_k\}}D'_{\{i_1,i_2,\cdots,i_k\}}\right\rangle=\langle\bar{j}(x)\rangle$, and

$Q_{\{i_1,i_2,\cdots,i_k\}}+Q'_{\{i_1,i_2,\cdots,i_k\}}=\left\langle D_{\{i_1,i_2,\cdots,i_k\}}+D'_{\{i_1,i_2,\cdots,i_k\}}-D_{\{i_1,i_2,\cdots,i_k\}}D'_{\{i_1,i_2,\cdots,i_k\}}\right\rangle=\langle d_1+d_2-d_1d_2\rangle=\mathcal{R}_n$;

$S_{\{i_1,i_2,\cdots,i_k\}}\cap S'_{\{i_1,i_2,\cdots,i_k\}}=\left\langle E_{\{i_1,i_2,\cdots,i_k\}}E'_{\{i_1,i_2,\cdots,i_k\}}\right\rangle=\langle 0\rangle$, and

$S_{\{i_1,i_2,\cdots,i_k\}}+S'_{\{i_1,i_2,\cdots,i_k\}}=\left\langle E_{\{i_1,i_2,\cdots,i_k\}}+E'_{\{i_1,i_2,\cdots,i_k\}}-E_{\{i_1,i_2,\cdots,i_k\}}E'_{\{i_1,i_2,\cdots,i_k\}}\right\rangle$. This proves (i)-(iv).
$=\langle e_1+e_2-e_1e_2\rangle=\langle 1-\bar{j}(x)\rangle$

Using that $\bar{j}(x)=(1-e_1-e_2)$ and $e_1e_2=0$ from Lemma 3 and noting that $e_1^2=e_1, e_2^2=e_2$ we find that $E_{\{i_1,i_2,\cdots,i_k\}}(\bar{j}(x))=0$.

Similarly using $(e_1+\bar{j}(x))=d_1$ and $(e_2+\bar{j}(x))=d_2$ from Lemma 3, we see that $E_{\{i_1,i_2,\cdots,i_k\}}+(\bar{j}(x))=D_{\{i_1,i_2,\cdots,i_k\}}$.

Therefore $S_{\{i_1,i_2,\cdots,i_k\}}\cap\langle\bar{j}(x)\rangle=\left\langle E_{\{i_1,i_2,\cdots,i_k\}}(\bar{j}(x))\right\rangle=\{0\}$, and

$S_{\{i_1,i_2,\cdots,i_k\}}+\langle\bar{j}(x)\rangle=\left\langle E_{\{i_1,i_2,\cdots,i_k\}}+\bar{j}(x)-E_{\{i_1,i_2,\cdots,i_k\}}\bar{j}(x)\right\rangle=\left\langle D_{\{i_1,i_2,\cdots,i_k\}}\right\rangle=Q_{\{i_1,i_2,\cdots,i_k\}}$. This proves (v) and (vi).

Finally for $1\le k\le\left[\frac{m}{2}\right]$, we have

$$\left|Q_{\{i_1,i_2,\cdots,i_k\}}\cap Q'_{\{i_1,i_2,\cdots,i_k\}}\right|=\left|\langle\bar{j}(x)\rangle\right|=q^m,$$

it being a repetition code over $\mathcal{R}$. Therefore

$$q^{mn} = |\mathcal{R}_n| = \left|Q_{\{i_1,i_2,\cdots,i_k\}} + Q'_{\{i_1,i_2,\cdots,i_k\}}\right| = \frac{\left|Q_{\{i_1,i_2,\cdots,i_k\}}\right|\left|Q'_{\{i_1,i_2,\cdots,i_k\}}\right|}{\left|Q_{\{i_1,i_2,\cdots,i_k\}} \cap Q'_{\{i_1,i_2,\cdots,i_k\}}\right|} = \frac{\left|Q_{\{i_1,i_2,\cdots,i_k\}}\right|^2}{q^m}.$$

This gives $\left|Q_{\{i_1,i_2,\cdots,i_k\}}\right| = q^{\frac{m(n+1)}{2}}$. Now we find that

$$q^{\frac{m(n+1)}{2}} = \left|Q_{\{i_1,i_2,\cdots,i_k\}}\right| = \left|S_{\{i_1,i_2,\cdots,i_k\}} + \left\langle \overline{j}(x)\right\rangle\right| = \left|S_{\{i_1,i_2,\cdots,i_k\}}\right|\left|\left\langle \overline{j}(x)\right\rangle\right| = \left|S_{\{i_1,i_2,\cdots,i_k\}}\right| q^m.$$

since $\left|S_{\{i_1,i_2,\cdots,i_k\}} \cap \left\langle \overline{j}(x)\right\rangle\right| = |\langle 0\rangle| = 1$. This gives $\left|S_{\{i_1,i_2,\cdots,i_k\}}\right| = q^{\frac{m(n-1)}{2}}$.

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

(i) $Q^{\perp}_{\{i_1,i_2,\cdots,i_k\}} = S_{\{i_1,i_2,\cdots,i_k\}}$,

(ii) $S_{\{i_1,i_2,\cdots,i_k\}}$ is self orthogonal.

Proof: By using Lemma 2 and Lemma 4, we have $\mathbb{C}_1 = \mathbb{D}_1^{\perp} = \left\langle 1 - \mu_{-1}(d_1(x))\right\rangle$ so $d_1(x^{-1}) = 1 - e_1(x)$. Similarly $d_2(x^{-1}) = 1 - e_2(x)$. For

$$D_{\{i_1,i_2,\cdots,i_k\}}(x) = (\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_k}) d_1(x) + (1 - \eta_{i_1} - \eta_{i_2} - \cdots - \eta_{i_k}) d_2(x),$$

$$1 - D_{\{i_1,i_2,\cdots,i_k\}}(x^{-1}) = 1 - (\eta_{i_1} + \eta_{i_2} + \cdots + \eta_{i_k})(1 - e_1(x)) - (1 - \eta_{i_1} - \eta_{i_2} - \cdots - \eta_{i_k})(1 - e_2(x))$$

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

Now result (i) follows from Lemma 4. Using (vi) of Theorem 4, we have $S_{\{i_1,i_2,\cdots,i_k\}} \subseteq Q_{\{i_1,i_2,\cdots,i_k\}} = S^{\perp}_{\{i_1,i_2,\cdots,i_k\}}$. Therefore $S_{\{i_1,i_2,\cdots,i_k\}}$ is self orthogonal.

Similarly we get

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

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

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

The extended duadic codes over $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{m-1}\mathbb{F}_q$ are formed in the same way as the extended duadic codes over $\mathbb{F}_q$ are formed. See Theorem 6.4.12 of [10].

Consider the equation

$$1 + \gamma^2 n = 0. \tag{17}$$

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 [10], Chapter 6).

Theorem 7: Suppose there exist a γ in $\mathbb{F}_q$ satisfying Equation (17). If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_2$, $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_1$ then for all possible choices of $\{i_1, i_2, \cdots, i_k\} \in \mathbb{A}$, the extended duadic codes $\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}$ of length $n+1$ are self-dual.

Proof: As $Q_{\{i_1,i_2,\cdots,i_k\}} = S_{\{i_1,i_2,\cdots,i_k\}} + \left\langle \overline{j}(x)\right\rangle$, by Theorem 4, let $\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}$ be the extended duadic code over $\mathcal{R}$ generated by

$$\overline{G_{\{i_1,i_2,\cdots,i_k\}}} = \begin{array}{c} \begin{matrix} \infty & 0 & 1 & 2 & \cdots & n-1 \end{matrix} \\ \begin{pmatrix} 0 & & & & & \\ 0 & & & G_{\{i_1,i_2,\cdots,i_k\}} & & \\ \vdots & & & & & \\ -n\gamma & 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \end{array}$$

where $G_{\{i_1,i_2,\cdots,i_k\}}$ is a generator matrix for the even-like duadic code $S_{\{i_1,i_2,\cdots,i_k\}}$. The row above the matrix shows the column labeling by $\mathbb{Z}_n \cup \infty$. Since the all one vector belongs to $Q_{\{i_1,i_2,\cdots,i_k\}}$ and its dual $Q^{\perp}_{\{i_1,i_2,\cdots,i_k\}}$ is equal to $S_{\{i_1,i_2,\cdots,i_k\}}$, the last row of $\overline{G_{\{i_1,i_2,\cdots,i_k\}}}$ is orthogonal to all the previous rows of $\overline{G_{\{i_1,i_2,\cdots,i_k\}}}$. The last row is orthogonal to itself also as $\gamma^2 n^2 + n = 0$ in $\mathbb{F}_q$. Further as $S_{\{i_1,i_2,\cdots,i_k\}}$ is self orthogonal by Theorem 5, we find that the code $\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}$ is self orthogonal. Now the result follows from the fact that $\left|\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}\right| = q^m \left|S_{\{i_1,i_2,\cdots,i_k\}}\right| = q^{\frac{m(n+1)}{2}} = \left|\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}^{\perp}\right|$.

Theorem 8: Suppose there exists a γ in $\mathbb{F}_q$ satisfying Equation (17). If $\mu_{-1}(\mathbb{C}_1) = \mathbb{C}_1$, $\mu_{-1}(\mathbb{C}_2) = \mathbb{C}_2$ then for all possible choices of $\{i_1, i_2, \cdots, i_k\} \in \mathbb{A}$, the extended duadic codes satisfy $\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}^{\perp} = \overline{Q'_{\{i_1,i_2,\cdots,i_k\}}}$.

Proof: Let $\overline{Q_{\{i_1,i_2,\cdots,i_k\}}}$ and $\overline{Q'_{\{i_1,i_2,\cdots,i_k\}}}$ be the extended duadic codes over $\mathcal{R}$ generated by

$$G_1 = \overline{G_{\{i_1,i_2,\cdots,i_k\}}} = \begin{array}{c} \begin{matrix} \infty & 0 & 1 & 2 & \cdots & n-1 \end{matrix} \\ \begin{pmatrix} 0 & & & & & \\ 0 & & & G_{\{i_1,i_2,\cdots,i_k\}} & & \\ \vdots & & & & & \\ -n\gamma & 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \end{array}$$

and

$$G_2 = \overline{G'_{\{i_1,i_2,\cdots,i_k\}}} = \begin{array}{c} \begin{matrix} \infty & 0 & 1 & 2 & \cdots & n-1 \end{matrix} \\ \begin{pmatrix} 0 & & & & & \\ 0 & & & G'_{\{i_1,i_2,\cdots,i_k\}} & & \\ \vdots & & & & & \\ -n\gamma & 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \end{array}$$

respectively where $G_{\{i_1,i_2,\cdots,i_k\}}$ is a generator matrix for the duadic code $S_{\{i_1,i_2,\cdots,i_k\}}$ and $G'_{\{i_1,i_2,\cdots,i_k\}}$ is a generator matrix for the duadic code $S'_{\{i_1,i_2,\cdots,i_k\}}$. Let v denote the all one vector of length n. As $v \in Q'_{\{i_1,i_2,\cdots,i_k\}}$ and $Q'^{\perp}_{\{i_1,i_2,\cdots,i_k\}} = S_{\{i_1,i_2,\cdots,i_k\}}$, v is orthogonal to all the rows of $G_{\{i_1,i_2,\cdots,i_k\}}$. Also $(-n\gamma, v)\cdot(-n\gamma, v) = 0$. Further rows of $G'_{\{i_1,i_2,\cdots,i_k\}}$ are in $S'_{\{i_1,i_2,\cdots,i_k\}} = Q^{\perp}_{\{i_1,i_2,\cdots,i_k\}}$, so are orthogonal to rows of $G_{\{i_1,i_2,\cdots,i_k\}}$. Therefore all rows of G_2 are orthogonal to all the rows of G_1. Hence $\overline{Q'_{\{i_1,i_2,\cdots,i_k\}}} \subseteq \overline{Q_{\{i_1,i_2,\cdots,i_k\}}}^{\perp}$. Now the result follows from comparing their orders.

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

Next we give some examples to illustrate our theory. The minimum distances of all the examples appearing have been computed by the Magma Computational Algebra System.

Example 1: Let $m=3$, $q=7$, $n=9$ and $V = \begin{pmatrix} 2 & -2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{pmatrix}$ be a matrix over $\mathbb{F}_7$ satisfying $VV^{\mathrm{T}} = 2I$. The even like idempotent generators of duadic codes of length 9 over $\mathbb{F}_7$ are $e_1 = 2x^8 + x^7 + 3x^6 + 2x^5 + x^4 + 2x^2 + x + 2$, $e_2 = x^8 + 2x^7 + x^5 + 2x^4 + 3x^3 + x^2 + 2x + 2$. Here $\mu_{-1}(e_1) = e_2$, $\mu_{-1}(e_2) = e_1$. The Gray image of even like duadic code $S_{\{1\}}$ is a self-orthogonal [27,12,6] code over $\mathbb{F}_7$. Here there is no $\gamma \in \mathbb{F}_7$ satisfying Equation (17).

Example 2: Let $m=4$, $q=13$, $n=9$ and

$$V = \begin{pmatrix} 2 & -2 & 1 & 1 \\ -1 & 1 & 2 & 2 \\ 2 & 2 & 1 & -1 \\ 1 & 1 & -2 & 2 \end{pmatrix}$$

be a matrix over $\mathbb{F}_7$ satisfying $VV^{\mathrm{T}} = 10I$. The even like idempotent generators of duadic codes of length 9 over $\mathbb{F}_{13}$ are $e_1 = x^8 + 9x^7 + 6x^6 + x^5 + 9x^4 + 4x^3 + x^2 + 9x + 12$, $e_2 = 9x^8 + x^7 + 4x^6 + 9x^5 + x^4 + 6x^3 + 9x^2 + x + 12$. Here $\mu_{-1}(e_1) = e_2$, $\mu_{-1}(e_2) = e_1$ and $\gamma = 6$ is a solution of (17). The Gray image $\Phi\left(\overline{Q}_{\{1\}}\right)$ of extended duadic code $\overline{Q}_{\{1\}}$ is a self-dual [40,20,6] code over $\mathbb{F}_{13}$.

Example 3: Let $m=6$, $q=11$, $n=5$ and

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & -3 & 1 & 2 & -3 \\ 1 & -3 & 2 & 1 & -3 & 2 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 2 & -3 & -1 & -2 & 3 \\ 1 & -3 & 2 & -1 & 3 & -2 \end{pmatrix}$$

be a matrix over $\mathbb{F}_{11}$ satisfying $VV^{\mathrm{T}} = 6I$. The even like idempotent generators of duadic codes of length 5 over $\mathbb{F}_{11}$ are $e_1 = 6x^4 + 9x^3 + 4x^2 + 7x + 7$,

$e_2 = 7x^4 + 4x^3 + 9x^2 + 6x + 7$. The Gray image of even like duadic code $S_{\{1\}}$ is a self-orthogonal [30,12,8] code over $\mathbb{F}_{11}$.

Example 4 : Let $m = 4$, $q = 4$, $n = 5$ and let a be the primitive element of $\mathbb{F}_4$

$$V = \begin{pmatrix} a & -a^2 & 1 & 1 \\ -1 & 1 & a & a^2 \\ a^2 & a & -1 & 1 \\ 1 & 1 & a^2 & -a \end{pmatrix}$$

be a matrix over $\mathbb{F}_4$ satisfying $VV^{\mathrm{T}} = I$. The even like idempotent generators of duadic codes of length 5 over $\mathbb{F}_4$ are $e_1 = ax^4 + a^2x^3 + a^2x^2 + ax$, $e_2 = a^2x^4 + ax^3 + ax^2 + a^2x$. Here $\mu_{-1}(e_1) = e_1$, $\mu_{-1}(e_2) = e_2$ and $\gamma = 1$ is a solution of (17). The Gray image $\Phi\left(\overline{Q}_{\{1\}}\right)$ of extended duadic code $\overline{Q}_{\{1\}}$ is a formally self-dual [24,12,6] code over $\mathbb{F}_4$.

References

[1] Pless, V. and Qian, Z. (1996) Cyclic Codes and Quadratic Residue Codes over $\mathbb{Z}_4$. *IEEE Transactions on Information Theory*, **42**, 1594-1600.

[2] Chiu, M.H., Yau, S.T. and Yu, Y. (2000) $\mathbb{Z}_8$-Cyclic Codes and Quadratic Residue Codes. *Advances in Applied Mathematics*, **25**, 12-33. http://dx.doi.org/10.1006/aama.2000.0687

[3] Taeri, B. (2009) Quadratic Residue Codes over $\mathbb{Z}_9$. *The Korean Journal of Mathematics*, **46**, 13-30. http://dx.doi.org/10.4134/JKMS.2009.46.1.013

[4] Kaya, A., Yildiz, B. and Siap, I. (2014) Quadratic Residue Codes over $\mathbb{F}_p + u\mathbb{F}_p$ and Their Gray Images. *ournal of Pure and Applied Algebra*, **218**, 1999-2011. http://dx.doi.org/10.1016/j.jpaa.2014.03.002

[5] Zhang, T. and Zhu, S. (2012) Quadratic Residue Codes over $\mathbb{F}_p + v\mathbb{F}_p$. *Journal of University of Science and Technology of China*, **42**, 208-213.

[6] Kaya, A., Yildiz, B. and Siap, I. (2014) 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 and Their Applications*, **29**, 160-177. http://dx.doi.org/10.1016/j.ffa.2014.04.009

[7] Liu, Y., Shi, M. and Solé, P. (2014) Quadratic Residue Codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. *Arithmetic of Finite Fields* 5*th International Workshop WAIFI* 2014, Gebze, 204-211.

[8] Raka, M., Kathuria, L. and Goyal, M. (2016) $\left(1-2u^3\right)$-Constacyclic Codes and Quadratic Residue Codes over $\mathbb{F}_p[u]/\langle u^4 - u\rangle$. *Cryptography and Communications*, 1-15. http://dx.doi.org/10.1007/s12095-016-0184-7

[9] Goyal, M. and Raka, M. (2016) Quadratic Residue Codes over the Ring $\mathbb{F}_p[u]/\langle u^m - u\rangle$ and Their Gray Images. arXiv: 1609. 07862v1 [math.NT] 2016.

[10] Cary Huffman, W. and Pless, V. (2003) Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge.

Scientific Research Publishing

Submit or recommend next manuscript to SCIRP and we will provide best service for you:

Accepting pre-submission inquiries through Email, Facebook, LinkedIn, Twitter, etc.
A wide selection of journals (inclusive of 9 subjects, more than 200 journals)
Providing 24-hour high-quality service
User-friendly online submission system
Fair and swift peer-review system
Efficient typesetting and proofreading procedure
Display of the result of downloads and visits, as well as the number of cited articles
Maximum dissemination of your research work

Submit your manuscript at: http://papersubmission.scirp.org/
Or contact jcc@scirp.org