Quantum Information and Computation, Vol. 22, No. 5&6 (2022) 0427–0439
© Rinton Press

m-ADIC RESIDUE CODES OVER THE RING $\mathbb{F}_q[v]/(v^s - v)$ AND THEIR APPLICATIONS TO QUANTUM CODES

FERHAT KÜRÜZ [a]
Department of Computer Engineering, Istanbul Gelisim University
Avcılar 34310, Istanbul-Turkey

MUSTAFA SARI [b]
Department of Mathematics, Yildiz Technical University
Esenler 34220, Istanbul-Turkey

MEHMET E. KÖROĜLU [c]
Department of Mathematics, Yildiz Technical University
Esenler 34220, Istanbul-Turkey

Received June 18, 2021
Revised February 17, 2022

Due to their rich algebraic structure, cyclic codes have a great deal of significance amongst linear codes. Duadic codes are the generalization of the quadratic residue codes, a special case of cyclic codes. The m-adic residue codes are the generalization of the duadic codes. The aim of this paper is to study the structure of the m-adic residue codes over the quotient ring $\frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$. We determine the idempotent generators of the m-adic residue codes over $\frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$. We obtain some parameters of optimal m-adic residue codes over $\frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$ with respect to Griesmer bound for rings. Furthermore, we derive a condition for m-adic residue codes over $\frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$ to contain their dual. By making use of a preserving-orthogonality Gray map, we construct a family of quantum error correcting codes from the Gray images of dual-containing m-adic residue codes over $\frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$ and give some examples to illustrate our findings.

Keywords: m-adic residue codes, Cyclic codes, Quadratic residue codes, CSS construction, Quantum codes

1 Introduction

Because of their strong algebraic properties, the class of cyclic codes have a great deal of significance amongst linear codes. As a special case of cyclic codes, the class of quadratic residue codes plays an important role in cyclic codes for theoretical and practical reasons and they have been studied over finite fields for many years. The class of duadic codes is the generalization of the quadratic residue codes. Recently, many researchers have studied the structure of generalization of quadratic residue codes over some special rings (see [1, 2, 3, 4, 5] for instance). The m-adic residue codes are the generalization of the duadic codes ([6]). The

[a] fkuruz@gelisim.edu.tr (F. Kürüz)
[b] musari@yildiz.edu.tr (M. Sarı)
[c] mkoroglu@yildiz.edu.tr (M. E. Köroğlu)

m-adic residue codes are investigated and are found to have many of the strong properties of the quadratic residue codes. For the first time in literature, Brualdi and Pless generalized the quadratic residue codes, which they called polyadic codes, by defining the m-adic residue codes (see [1]). Pless studied the idempotent generators of the polyadic codes in [4]. In [6], by virtue of generator polynomials over finite fields, Job defined m-adic residue codes. In [7], Ling and Xing extended the definition of polyadic cyclic codes to include noncyclic abelian codes, and obtained necessary and sufficient conditions for the existence of non-degenerate polyadic codes. Chen et al. studied the structure of polyadic constacyclic codes and gave a necessary and sufficient condition for the existence of Type-I m-adic λ-constacyclic codes [8]. In [9], Goyal and Raka studied the structure of $(1-2u^3)$-constacyclic codes over the quotient ring $\frac{\mathbb{F}_p[u]}{\langle u^4-u\rangle}$. Then, as a continuation of this paper ([9]) they extended their results to the ring $\frac{\mathbb{F}_p[u]}{\langle u^m-u\rangle}$ and studied quadratic residue codes and their extensions [10]. Kuruz et al. studied the structure of m-adic residue codes over the non-chain ring $\frac{\mathbb{F}_q[v]}{\langle v^2-v\rangle}$ and investigated the relation between the generators of these codes and the reversible DNA codes [11].

On the other hand, there have been many studies on constructing quantum error correcting codes from the codes over the rings, some of which are [12, 13, 14, 15, 16, 17, 18, 19]. In [14], Kai and Zhu studied the linear and cyclic codes over the ring $\mathbb{F}_4 + u\mathbb{F}_4$, where $u^2 = 0$, and determined the parameters of quantum codes obtained by transforming the cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$ onto $\mathbb{F}_4$ via an orthogonality-preserving Gray map. In [19], the authors defined a Gray map from $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ to $\mathbb{F}_2^3$ that preserves the orthogonality, and derived a family of quantum codes from dual-containing cyclic codes over this ring. As a generalization of the study [19], in [17], Sarı and Siap gave a construction for orthogonality-preserving Gray map from the ring $\frac{\mathbb{F}_2[u]}{\langle u^s\rangle}$, $u^s = 0$ to $\mathbb{F}_2^s$, and obtained an existence-condition for dual-containing cyclic codes over the ring $\frac{\mathbb{F}_2[u]}{\langle u^s\rangle}$. They also gave the parameters of quantum codes obtained from the cyclic codes over the ring $\frac{\mathbb{F}_2[u]}{\langle u^s\rangle}$. In [15], Qian studied the quantum codes obtained from cyclic codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$. In [12], the authors considered quantum codes as the Gray images of the cyclic codes over the ring $\mathbb{F}_3 + v\mathbb{F}_3$, $v^3 = v$. In [16], Sarı and Siap extended the results obtained in [15] over a class of nonchain rings $\frac{\mathbb{F}_p[v]}{\langle v^p-v\rangle}$. More recently, in [13], Bag *et al.* obtained new nonbinary quantum codes from the codes over the ring $\frac{\mathbb{F}_p[u]}{\langle u^3-u\rangle}$. In [18], Tang *et al.* utilized $(1+u)$-constacyclic codes over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ to construct quantum codes.

In this work, inspired by the above works, as a generalization of the paper [11], we study the structure of the m-adic residue codes over the quotient ring $\mathcal{R}_{q,s} = \frac{\mathbb{F}_q[v]}{\langle v^s-v\rangle}$. First, we determine the idempotent generators of the m-adic residue codes over $\mathcal{R}_{q,s}$ and give an algebraic characterization for these codes. Then, we obtain some parameters of optimal m-adic residue codes over $\mathcal{R}_{q,s}$ with respect to Griesmer bound for rings. Furthermore, via CSS construction for quantum error correcting codes and the orthogonality-preserving Gray map defined in [20], we apply m-adic residue codes over $\mathcal{R}_{q,s}$ to obtain quantum codes and illustrate the finding by giving some examples.

The rest of this paper is organized as follows. In Section 2, we present some definitions

and basic results of linear codes, cyclic codes and m-adic residue codes. In Section 3, we study the idempotent generators of m-adic residue codes over $\mathcal{R}_{q,s}$ and characterize these codes by determining their algebraic structures. Further, we obtain some parameters of optimal m-adic residue codes over $\mathcal{R}_{q,s}$, with respect to Griesmer bound for rings. In Section 4, we determine the duals of m-adic residue codes over $\mathcal{R}_{q,s}$ and give a condition for these codes to contain their dual. By carrying dual-containing m-adic residue codes over $\mathcal{R}_{q,s}$ via the Gray map given in [20] and using CSS code construction, we derive a family of quantum codes. Moreover, we illustrate our finding by giving some examples. Section 5 is reserved for conclusion and future remarks.

2 Preliminaries

In this section, we give some basic definitions and results about linear codes, cyclic codes and m-adic residue codes and we introduce the structure of the ring $\mathcal{R}_{q,s} = \frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$. For further information about linear codes, cyclic codes and m-adic residue codes the readers may consult the references [6, 21, 22].

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. An $[n,k]_q$ linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are of the form $(c_0, c_1, \ldots, c_{n-1})$ and are called codewords. The Hamming weight of any $c \in \mathcal{C}$ is the number of nonzero coordinates of c and is denoted by $w(c)$. The minimum distance of $\mathcal{C}$ is defined as $d = \min\{w(c) | \mathbf{0} \neq c \in \mathcal{C}\}$. The usual inner product $\langle c, d\rangle$ of two vectors $c = (c_0, c_1, \ldots, c_{n-1})$ and $d = (d_0, d_1, \ldots, d_{n-1})$ in $\mathbb{F}_q^n$ is defined to be $\langle c, d\rangle = \sum_{i=0}^{n-1} c_i d_i$ in $\mathbb{F}_q$. The dual $\mathcal{C}^\perp$ of the code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is the set $\mathcal{C}^\perp = \left\{d \in \mathbb{F}_q^n : \langle c, d\rangle = 0, \forall c \in \mathcal{C}\right\}$. Note that $\mathcal{C}^\perp$ is an $[n, n-k]_q$ linear code if $\mathcal{C}$ is an $[n,k]_q$ linear code.

A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is said to be cyclic if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ we have that $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. A cyclic code of length n over $\mathbb{F}_q$ corresponds to a principal ideal $\langle g(x)\rangle$ of the quotient ring $\frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$ where $g(x) | x^n - 1$. and $g(x)$ is called the generator polynomial of the cyclic code $\mathcal{C}$ if $g(x)$ is monic. If $(n,q) = 1$, there exits a primitive n^{th} root of unity β over some extension of $\mathbb{F}_q$. In this case, the defining set for a cyclic code $\mathcal{C} = \langle g(x)\rangle$ is the set $Z = \left\{i \in \{0, 1, \ldots, n-1\} : g\left(\beta^i\right) = 0\right\}$. A polynomial $e(x) \in \mathbb{F}_q[x]$ satisfying $e^2(x) = e(x)$ is called an idempotent polynomial. Recall that for any cyclic code $\mathcal{C}$ over $\mathbb{F}_q$, there exists unique idempotent generator $e(x)$ such that $\mathcal{C} = \langle e(x)\rangle$. The dual $\mathcal{C}^\perp$ is a cyclic code generated by $h^R(x)$ of length n over $\mathbb{F}_q$ if $\mathcal{C}$ is a cyclic code generated by $g(x)$ of length n over $\mathbb{F}_q$, where $g(x)h(x) = x^n - 1$ and the polynomial $h^R(x)$ is defined to be $h^R(x) = x^{\deg h(x)} h\left(x^{-1}\right)$ and is called the reciprocal polynomial of $h(x)$. Note that a cyclic code $\mathcal{C}$ generated by $g(x)$ of length n is of $n-k$ dimensional and in this case its dual $\mathcal{C}^\perp$ is of k dimensional.

In the following series of the definitions and examples we remind the structure of the m-adic residue codes over finite fields.

Definition 1: [6] Let p be a prime and b be a primitive element of $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. The set of nonzero m-adic residues modulo p is defined as $Q_0 = \left\{a^m : a \in \mathbb{Z}_p^*\right\}$ where $m \geqslant 2$, $m \in \mathbb{Z}$ and $m | (p-1)$. Moreover, set $Q_i = b^i Q_0$ for $0 \leq i \leq m-1$.

Example 1: Let $p = 13$. Then 2 is a primitive element of $\mathbb{Z}_{13}^*$. Since $3|13-1$ we can take $m = 3$. Whence, we have $Q_0 = \{1,5,8,12\}$, $Q_1 = \{2,3,10,11\}$, $Q_2 = \{4,6,7,9\}$.

Definition 2: [6] Let p be a prime and q be a prime power such that p and q are coprime. Let b be a primitive element of $\mathbb{Z}_p^*$ and γ be a primitive p^{th} root of unity in some field extension of $\mathbb{F}_q$. Let Q_0 be the set of nonzero m-adic residues modulo p and $Q_i = b^i Q_0$. If q is an m-adic residue modulo p, then the codes generated by polynomials $g_i(x) = \frac{x^p-1}{\prod_{k\in Q_i}(x-\gamma^k)}$ $(i = 0,1,\ldots,m-1)$ are called even-like families of m-adic residue codes of class I of length p over $\mathbb{F}_q$.

The other families of m-adic residue codes can be defined by derivations of even-like family of m-adic residue codes of class I.

Definition 3: [6]

1. The codes generated by the polynomials $\widehat{g_i}(x) = \prod_{k\in Q_i}(x-\gamma^k)$, where $(i = 0,1,\ldots,m-1)$, are called odd-like class-I m-adic residue codes of length p over $\mathbb{F}_q$ and the code generated by $\widehat{g_i}(x)$ is the complement of the code generated by $g_i(x)$.

2. The codes generated by the polynomials $h_i(x) = (x-1)\widehat{g_i}(x)$, where $(i = 0,1,\ldots,m-1)$, are called even-like class II m-adic residue codes of length p over $\mathbb{F}_q$ and the code generated by $h_i(x)$ is the complementary code of the code generated by $g_i(x)$.

3. The codes generated by the polynomials $\widehat{h_i}(x) = \frac{g_i(x)}{x-1}$, where $(i = 0,1,\ldots,m-1)$, are called odd-like class II m-adic residue codes of length p over $\mathbb{F}_q$ and these codes are the complement of the codes generated by $h_i(x)$.

In the following example, we list all even-like class-I, 6-adic residue codes of length 19 over $\mathbb{F}_7$.

Example 2: Even-like class I, 6-adic residue codes of length 19 over $\mathbb{F}_7$ are

$$\mathcal{C}_0 = \langle 1+4x+6x^2+6x^3+3x^4+4x^6+5x^7+x^8+2x^{10}+2x^{11}+2x^{12}+4x^{13}+5x^{14}+3x^{15}+x^{16}\rangle,$$

$$\mathcal{C}_1 = \langle 1+3x+x^2+x^3+5x^4+x^5+6x^6+x^7+5x^8+6x^9+6x^{11}+3x^{12}+3x^{13}+5x^{14}+x^{15}+x^{16}\rangle,$$

$$\mathcal{C}_2 = \langle 1+5x^2+x^3+4x^4+3x^5+5x^7+3x^8+4x^9+6x^{10}+2x^{11}+6x^{12}+2x^{13}+4x^{14}+2x^{15}+x^{16}\rangle,$$

$$\mathcal{C}_3 = \langle 1+3x+5x^2+4x^3+2x^4+2x^5+2x^6+x^8+5x^9+4x^{10}+3x^{12}+6x^{13}+6x^{14}+4x^{15}+x^{16}\rangle,$$

$$\mathcal{C}_4 = \langle 1+x+5x^2+3x^3+3x^4+6x^5+6x^7+5x^8+x^9+6x^{10}+x^{11}+5x^{12}+x^{13}+x^{14}+3x^{15}+x^{16}\rangle,$$

and

$$\mathcal{C}_5 = \langle 1+2x+4x^2+2x^3+6x^4+2x^5+6x^6+4x^7+3x^8+5x^9+3x^{11}+4x^{12}+x^{13}+5x^{14}+x^{16}\rangle.$$

The minimum distance of all these codes is 15. Hence, all these codes are optimal.

Let $s > 1$ be a natural number and q be a prime such that $q \equiv 1(mod(s-1))$. Then we define the commutative ring $\mathcal{R}_{q,s}$ as the quotient ring $\frac{\mathbb{F}_q[v]}{\langle v^s - v\rangle}$. It is easy to see that $\mathcal{R}_{q,s} \cong \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{s-1}\mathbb{F}_q$.

An element $\eta \in \mathcal{R}_{q,s}$ is called idempotent if $\eta^2 = \eta$ and two idempotents η_1, η_2 are said to be orthogonal if $\eta_1\eta_2 = 0$. An idempotent of $\mathcal{R}_{q,s}$ is said to be primitive if it is non-zero

and it can not be written as sum of orthogonal idempotents. A collection $\{\eta_0, \eta_1, \ldots, \eta_{s-1}\}$ of idempotents of $\mathcal{R}_{q,s}$ is complete if $\eta_0 + \eta_1 + \ldots + \eta_{s-1} = 1$. Any complete collection of idempotents in $\mathcal{R}_{q,s}$ is a basis of the $\mathbb{F}_q$-vector space $\mathcal{R}_{q,s}$. Hence, any element $r \in \mathcal{R}_{q,s}$ can be uniquely represented as $r = r_0\eta_0 + r_1\eta_1 + \ldots + r_{s-1}\eta_{s-1}$, where $r_i \in \mathcal{R}_{q,s}$.

If α is a primitive element of $\mathbb{F}_q^*$, then $\zeta = \alpha^{\frac{q-1}{s-1}}$ is a primitive $(s-1)^{th}$ root of unity and $1 + \zeta + \zeta^2 + \cdots + \zeta^{s-2} = 0$. Let $\eta_0, \eta_1, \ldots, \eta_{s-1}$ denote the following elements of $\mathcal{R}_{q,s}$.

$$\begin{aligned}
\eta_0 &= 1 - v^{s-1} \\
\eta_1 &= (s-1)^{-1}(v + v^2 + \cdots + v^{s-2} + v^{s-1}) \\
\eta_2 &= (s-1)^{-1}(\zeta v + \zeta^2 v^2 + \cdots + \zeta^{s-2} v^{s-2} + v^{s-1}) \\
\eta_3 &= (s-1)^{-1}((\zeta^2)v + (\zeta^2)^2 v^2 + \cdots + (\zeta^2)^{s-2} v^{s-2} + v^{s-1}) \\
&\vdots \\
\eta_{s-1} &= (s-1)^{-1}((\zeta^{s-2})v + (\zeta^{s-2})^2 v^2 + \cdots + (\zeta^{s-2})^{s-2} v^{s-2} + v^{s-1}).
\end{aligned}$$

It can be easily seen that $\eta_i^2 = \eta_i$, $\eta_i\eta_j = 0$ for all i and j such that $0 \leq i, j \leq s-1$, $i \neq j$. Further, $\sum_{i=0}^{s-1} \eta_i = 1$. By the decomposition theorem of ring theory, we can decompose $\mathcal{R}_{q,s}$ as $\mathcal{R}_{q,s} = \eta_0\mathcal{R}_{q,s} \oplus \eta_1\mathcal{R}_{q,s} \oplus \cdots \oplus \eta_{s-1}\mathcal{R}_{q,s}$. See that $\langle \eta_i \rangle = \{\lambda\eta_i : \lambda \in \mathbb{F}_q\}$. Hence, $\mathcal{R}_{q,s} = \eta_0\mathbb{F}_q \oplus \eta_1\mathbb{F}_q \oplus \cdots \oplus \eta_{s-1}\mathbb{F}_q$, which implies that every element r of the ring $\mathcal{R}_{q,s}$ is written uniquely as the sum $r = \lambda_0\eta_0 + \lambda_1\eta_1 + \cdots + \lambda_{s-1}\eta_{s-1}$ for some $\lambda_0, \lambda_1, \ldots, \lambda_{s-1} \in \mathbb{F}_q$.

Let $\mathcal{R}_{q,s}^n$ be the set of n-tuples over $\mathcal{R}_{q,s}$. Then, $\mathcal{R}_{q,s}^n$ is an $\mathcal{R}_{q,s}$-module. A nonempty subset of $\mathcal{R}_{q,s}^n$ is a code over $\mathcal{R}_{q,s}$ of length n. An $\mathcal{R}_{q,s}$-submodule of $\mathcal{R}_{q,s}^n$ is a linear code over $\mathcal{R}_{q,s}$ of length n. For a code C over $\mathcal{R}_{q,s}$ of length n, its dual $C^\perp$ is the set $C^\perp = \left\{y \in \mathcal{R}_{q,s}^n : \langle x, y \rangle = 0, \forall x \in C\right\}$. Note that if C is a linear code over $\mathcal{R}_{q,s}$ of length n, then its dual is also linear code over $\mathcal{R}_{q,s}$ of length n.

3 m-adic residue codes over $\mathcal{R}_{q,s}$

In [4], Pless introduced m-adic residue codes in terms of idempotent generators and gave relation between these idempotent generators. Kuruz et al. studied m-adic residue codes over the ring $\mathcal{R}_{q,2} = \frac{\mathbb{F}_q[v]}{\langle v^2 - v \rangle}$ (see [11]) and identified the idempotent generators of these codes. Also, they gave some conditions for the generator polynomials to be palindromic.

In this section we generalize idempotent generators of the m-adic residue codes to the ring $\mathcal{R}_{q,s}$ and we identify the idempotent generators of all classes of the m-adic residue codes. Furthermore, we determine the algebraic structure for each class of m-adic residue codes over $\mathcal{R}_{q,s}$.

Proposition 1: Let p be a prime and q be a prime power. Let m be a positive integer dividing $p-1$. Let q be an m-adic residue modulo p, i.e., $q \in Q_0$. If, for each $0 \leqslant i \leqslant s-1$, f_i is idempotent in $\frac{\mathbb{F}_q[x]}{\langle x^p - 1 \rangle}$, then $\sum_{i=0}^{s-1} \eta_i f_i$ is idempotent in $\frac{\mathcal{R}_{q,s}[x]}{\langle x^p - 1 \rangle}$.

Proof: Since $\eta_i^2 = \eta_i$ and $\eta_i\eta_j = 0$ for all $0 \leq i, j \leq s-1$ where $i \neq j$, we have $(\sum_{i=0}^{s-1} \eta_i f_i)^2 =$

$\sum_{i=0}^{s-1} (\eta_i f_i)^2 = \sum_{i=0}^{s-1} \eta_i f_i \square$.

It follows from Proposition 1 that $E = \sum_{i=0}^{s-1} \eta_i e_i$ is idempotent when e_i is idempotent generator of an even-like class-I m-adic residue code over $\mathbb{F}_q$ and so we give the following definition of even-like class-I m-adic residue codes of length p over $\mathcal{R}_{q,s}$ with respect to their idempotent generators.

Definition 4: For each $0 \leq i \leq s-1$, let e_i be the idempotent generator of an even-like class-I m-adic residue code of length p over $\mathbb{F}_q$. A code over $\mathcal{R}_{q,s}$ generated by $E = \sum_{i=0}^{s-1} \eta_i e_i$ is called an even-like class-I m-adic residue code of length p over $\mathcal{R}_{q,s}$.

We give the following characterization for even-like class-I m-adic residue codes of length p over $\mathcal{R}_{q,s}$.

Theorem 1: For any even-like class-I m-adic residue code $\mathcal{C}$ of length p over $\mathcal{R}_{q,s}$, there exists even-like class-I m-adic residue codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ of length p over $\mathbb{F}_q$ with generator polynomials $g_0(x), g_1(x), \ldots, g_{s-1}(x)$ such that $\mathcal{C} = \langle g(x) \rangle = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$ where $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1} g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$.

Proof: By the definition, we take an even-like class-I m-adic residue code $\mathcal{C}$ over $\mathcal{R}_{q,s}$ as a code generated by $E = \sum_{i=0}^{s-1} \eta_i e_i$. Define the set $J = \langle \eta_0 e_0, \eta_1 e_1, \ldots, \eta_{s-1} e_{s-1} \rangle$. Then, clearly $\mathcal{C} \subseteq J$. Conversely, for all $0 \leq i \neq j \leq s-1$, it follows from $\eta_i \eta_j = 0$ and $\eta_i \eta_i = \eta_i$ that $\eta_i (\eta_0 e_0 + \cdots + \eta_i e_i + \cdots + \eta_{s-1} e_{s-1}) = \eta_i e_i$ and so $J \subseteq \mathcal{C}$. Hence, $J = \mathcal{C}$. The last equality implies that $\mathcal{C} = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$ where $\mathcal{C}_i$ is an even-like class-I m-adic residue code over $\mathbb{F}_q$ with idempotent generator e_i. Letting $g_i(x)$ to be generator polynomial for $\mathcal{C}_i$, one gets that $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1} g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)} \square$.

We have from [1] that $1 - e$ is idempotent generator of an odd-like class-I m-adic residue code over $\mathbb{F}_q$ when e is idempotent generator of an even-like class-I m-adic residue code over $\mathbb{F}_q$. Then, Proposition 1 implies that $E' = \sum_{i=0}^{s-1} \eta_i (1 - e_i) = 1 - E$ is idempotent if e_i is idempotent generator of an even-like class-I m-adic residue code over $\mathbb{F}_q$. Hence, we consider the odd-like class-I m-adic residue codes of length p over $\mathcal{R}_{q,s}$ with respect to their idempotent generators.

Definition 5: Let $E = \sum_{i=0}^{s-1} \eta_i e_i$ where for $0 \leq i \leq s-1$, e_i is the idempotent generator of an even-like class-I m-adic residue code of length p over $\mathbb{F}_q$. A code over $\mathcal{R}_{q,s}$ generated by $E' = 1 - E = \sum_{i=0}^{s-1} \eta_i (1 - e_i)$ is called an odd-like class-I m-adic residue code of length p over $\mathcal{R}_{q,s}$.

Similar to the characterization for even-like class-I m-adic residue codes, we characterize odd-like class-I m-adic residue codes of length p over $\mathcal{R}_{q,s}$ in the following theorem.

Theorem 2: For any odd-like class-I m-adic residue code $\mathcal{C}$ of length p over $\mathcal{R}_{q,s}$, there exists odd-like class-I m-adic residue codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ of length p over $\mathbb{F}_q$ with generator polynomials $g_0(x), g_1(x), \ldots, g_{s-1}(x)$ such that $\mathcal{C} = \langle g(x) \rangle = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$

where $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1} g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$.

Proof: Let $\mathcal{C}$ be an odd-like class-I m-adic residue code $\mathcal{C}$ of length p over $\mathcal{R}_{q,s}$. By the definition for odd-like class-I m-adic residue codes over $\mathcal{R}_{q,s}$, $\mathcal{C} = \langle 1 - E \rangle$. See that $1 - E = \sum_{i=0}^{s-1} \eta_i - \sum_{i=0}^{s-1} \eta_i e_i = \sum_{i=0}^{s-1} \eta_i (1 - e_i)$ and define the set

$$J = \langle \eta_0 (1 - e_0), \eta_1 (1 - e_1), \ldots, \eta_{s-1} (1 - e_{s-1}) \rangle .$$

Then, it is clear that $\mathcal{C} \subseteq J$. Moreover, for each $0 \leqslant i \leqslant s-1$, $\eta_i \sum_{i=0}^{s-1} \eta_i (1 - e_i) = \eta_i^2 (1 - e_i) = \eta_i (1 - e_i) \in \mathcal{C}$, we get $J \subseteq \mathcal{C}$ and so $J = \mathcal{C}$. Note that $1 - e_i$ is an idempotent generator for an odd-like class-I m-adic residue code over $\mathbb{F}_q$ whenever e_i is an idempotent generator for an even-like class-I m-adic residue code over $\mathbb{F}_q$. Hence, the equality $J = \mathcal{C}$ implies that $\mathcal{C} = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$ where $\mathcal{C}$ is an odd-like class-I m-adic residue code over $\mathbb{F}_q$ with idempotent generator $1 - e_i$. Taking $g_i(x)$ as a generator polynomial of $\mathcal{C}_i$, one obtains that $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1} g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$ $\square$.

Let $h(x) = x + x^2 + \ldots + x^{p-1}$. Note that $1 - \frac{1}{p} h - e$ is idempotent generator of an even-like class-II m-adic residue code of length p over $\mathbb{F}_q$ when e is idempotent generator of an even-like class-II m-adic residue code of length p over $\mathbb{F}_q$ [1]. In this case, from Proposition 1, we get that $D = \sum_{i=0}^{s-1} \eta_i \left(1 - \frac{1}{p} h - e_i\right) = 1 - \frac{1}{p} h - E$ is idempotent if e_i is idempotent generator of an even-like class-I m-adic residue code over $\mathbb{F}_q$. Hence, we consider the even-like class-II m-adic residue codes of length p over $\mathcal{R}_{q,s}$ with respect to their idempotent generators.

Definition 6: Let $E = \sum_{i=0}^{s-1} \eta_i e_i$ where for $0 \leq i \leq s-1$, e_i is the idempotent generator of an even-like class-I m-adic residue code of length p over $\mathbb{F}_q$. A code over $\mathcal{R}_{q,s}$ generated by $D = 1 - \frac{1}{p} h - E = \sum_{i=0}^{s-1} \eta_i \left(1 - \frac{1}{p} h - e_i\right)$ is called an even-like class-II m-adic residue code of length p over $\mathcal{R}_{q,s}$.

The following is the exact structure of even-like class-II m-adic residue codes of length p over $\mathcal{R}_{q,s}$.

Theorem 3: Let $\mathcal{C}$ be an even-like class-II m-adic residue code of length p over $\mathcal{R}_{q,s}$. Then, for some even-like class-II m-adic residue codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ of length p over $\mathbb{F}_q$ with generator polynomials $g_0(x), g_1(x), \ldots, g_{s-1}(x)$, $\mathcal{C} = \langle g(x) \rangle = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$ where $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1} g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$.

Proof: Let $\mathcal{C}$ be an even-like class-II m-adic residue code of length p over $\mathcal{R}_{q,s}$. By the definition for an even-like class-II m-adic residue codes over $\mathcal{R}_{q,s}$, $\mathcal{C} = \left\langle 1 - \frac{1}{p} h - E \right\rangle$. See that $1 - \frac{1}{p} h - E = \sum_{i=0}^{s-1} \eta_i \left(1 - \frac{1}{p} h\right) - \sum_{i=0}^{s-1} \eta_i e_i = \sum_{i=0}^{s-1} \eta_i \left(1 - \frac{1}{p} h - e_i\right)$ and define the set $J = \left\langle \eta_0 \left(1 - \frac{1}{p} h - e_0\right), \eta_1 \left(1 - \frac{1}{p} h - e_1\right), \ldots, \eta_{s-1} \left(1 - \frac{1}{p} h - e_{s-1}\right) \right\rangle$. Then, it is clear that $\mathcal{C} \subseteq J$. Also, since $\eta_i \sum_{i=0}^{s-1} \eta_i \left(1 - \frac{1}{p} h - e_i\right) = \eta_i^2 \left(1 - \frac{1}{p} h - e_i\right) = \eta_i \left(1 - \frac{1}{p} h - e_i\right) \in \mathcal{C}$ for each $0 \leqslant$

$i \leqslant s-1$, we get $J \subseteq \mathcal{C}$, and so $J = \mathcal{C}$. Note that $1 - \frac{1}{p}h - e_i$ is idempotent generator for an even-like class-II m-adic residue code over $\mathbb{F}_q$ whenever e_i is idempotent generator for an even-like class-I m-adic residue code over $\mathbb{F}_q$. Hence, it follows from $J = \mathcal{C}$ that $\mathcal{C} = \eta_0\mathcal{C}_0 \oplus \eta_1\mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1}\mathcal{C}_{s-1}$ where $\mathcal{C}_i$ is an even-like class-II m-adic residue code over $\mathbb{F}_q$ with idempotent generator $1 - \frac{1}{p}h - e_i$. Let $g_i(x)$ to be generator polynomial for $\mathcal{C}_i$. Then, it is easy to see that $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1}g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$ $\square$.

We have from [1] that $\frac{1}{p}h + e$ is idempotent generator of an odd-like class-II m-adic residue code over $\mathbb{F}_q$ when e is idempotent generator of an even-like class-I m-adic residue code over $\mathbb{F}_q$. Then, from Proposition 1, we have that $D' = \sum_{i=0}^{s-1} \eta_i \left(\frac{1}{p}h + e_i\right) = 1 - D = \frac{1}{p}h + E$ is idempotent if e_i is idempotent generator of an even-like class-I m-adic residue code over $\mathbb{F}_q$. Hence, we consider the odd-like class-II m-adic residue codes of length p over $\mathcal{R}_{q,s}$ with respect to their idempotent generators.

Definition 7: Let $E = \sum_{i=0}^{s-1} \eta_i e_i$ where for $0 \leq i \leq s-1$, e_i is the idempotent generator of an even-like class-I m-adic residue code of length p over $\mathbb{F}_q$. A code over $\mathcal{R}_{q,s}$ generated by $D' = 1 - D = \frac{1}{p}h + E = \sum_{i=0}^{s-1} \eta_i \left(\frac{1}{p}h + e_i\right)$ is called an odd-like class-II m-adic residue code of length p over $\mathcal{R}_{q,s}$.

In the following, we give the exact structure for odd-like class-II m-adic residue codes of length p over $\mathcal{R}_{q,s}$.

Theorem 4: Let $\mathcal{C}$ be an odd-like class-II m-adic residue code of length p over $\mathcal{R}_{q,s}$. Then, for some odd-like class-II m-adic residue codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ of length p over $\mathbb{F}_q$ with generator polynomials $g_0(x), g_1(x), \ldots, g_{s-1}(x)$, $\mathcal{C} = \langle g(x) \rangle = \eta_0\mathcal{C}_0 \oplus \eta_1\mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1}\mathcal{C}_{s-1}$ where $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1}g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$.

Proof: Let $\mathcal{C}$ be an odd-like class-II m-adic residue code of length p over $\mathcal{R}_{q,s}$. By the definition for an odd-like class-II m-adic residue codes over $\mathcal{R}_{q,s}$, $\mathcal{C} = \left\langle \frac{1}{p}h + E \right\rangle$. See that $\frac{1}{p}h + E = \sum_{i=0}^{s-1} \eta_i \frac{1}{p}h + \sum_{i=0}^{s-1} \eta_i e_i = \sum_{i=0}^{s-1} \eta_i \left(\frac{1}{p}h + e_i\right)$ and define the set

$$J = \left\langle \eta_0 \left(\frac{1}{p}h + e_0\right), \eta_1 \left(\frac{1}{p}h + e_1\right), \ldots, \eta_{s-1} \left(\frac{1}{p}h + e_{s-1}\right) \right\rangle.$$

Then, it is clear that $\mathcal{C} \subseteq J$. Also, since $\eta_i \sum_{i=0}^{s-1} \eta_i \left(\frac{1}{p}h + e_i\right) = \eta_i^2 \left(\frac{1}{p}h + e_i\right) = \eta_i \left(\frac{1}{p}h + e_i\right) \in \mathcal{C}$ for each $0 \leq i \leq s-1$, we get $J \subseteq \mathcal{C}$, and so $J = \mathcal{C}$. Note that $\frac{1}{p}h + e_i$ is idempotent generator for an odd-like class-II m-adic residue code over $\mathbb{F}_q$ whenever e_i is idempotent generator for an even-like class-I m-adic residue code over $\mathbb{F}_q$. Hence, it follows from $J = \mathcal{C}$ that $\mathcal{C} = \eta_0\mathcal{C}_0 \oplus \eta_1\mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1}\mathcal{C}_{s-1}$ where $\mathcal{C}_i$ is an odd-like class-II m-adic residue code over $\mathbb{F}_q$ with idempotent generator $\frac{1}{p}h + e_i$. Let $g_i(x)$ be the generator polynomial of $\mathcal{C}_i$. Then, it is easy to see that $g(x) = \eta_0 g_0(x) + \eta_1 g_1(x) + \cdots + \eta_{s-1}g_{s-1}(x)$ and $|\mathcal{C}| = q^{ps - \sum_{i=0}^{s-1} \deg g_i(x)}$ $\square$.

In the following example, we list some of even-like class-I 4-adic residue codes of length 13 over $\mathcal{R}_{3,3}$.

Example 3: The idempotent generators of even-like class-I 4-adic residue codes of length 13 over $\mathbb{F}_3$ are $e_0 = l_0 + 2l_2 + 2l_3$, $e_1 = 2l_1 + 2l_2 + l_3$, $e_2 = 2l_0 + 2l_1 + l_2$ and $e_3 = 2l_0 + l_1 + 2l_3$, where $l_0 = x + x^3 + x^9$, $l_1 = x^2 + x^5 + x^6$, $l_2 = x^4 + x^{10} + x^{12}$, $l_3 = x^7 + x^8 + x^{11}$. Let $E_0 = \eta_0 e_0 + \eta_1 e_1 + \eta_2 e_2$, $E_1 = \eta_0 e_3 + \eta_1 e_0 + \eta_2 e_1$, $E_2 = \eta_0 e_2 + \eta_1 e_3 + \eta_2 e_0$, $E_3 = \eta_0 e_1 + \eta_1 e_2 + \eta_2 e_3$, where $\eta_0 = 1 - v^2$, $\eta_1 = 2v + 2v^2$ and $\eta_2 = v + 2v^2$.
Let $g_i(x)$ be the generator polynomial of even-like class-I 4-adic residue code of length 13 over $\mathcal{R}_{3,3}$ with idempotent generator E_i, then
$g_0(x) = 1 + (2v+1)x + (2v+2v^2)x^2 + (2v^2+v+1)x^3 + (v^2+2v+1)x^4 + (2v^2+2v+1)x^5 + 2vx^6 + (v+2)x^7 + vx^8 + (v^2+2v+2)x^9 + x^{10}$,
$g_1(x) = 1 + 2vx + (2v+1)x^2 + (v+1)x^3 + (2v+1)x^4 + (2v+2)x^5 + (2v+2)x^6 + vx^7 + (v+1)x^8 + (2v+2)x^9 + x^{10}$,
$g_2(x) = g_3(x) = 1 + x + 2x^2 + 2x^3 + 2x^5 + 2x^8 + x^9$.
The parameters of the codes generated by $g_0(x), g_1(x), g_2(x)$ and $g_3(x)$ are $[13,3,9]$, $[13,3,6]$, $[13,4,6]$, and $[13,4,6]$ respectively. The code generated by $g_0(x)$ attains the Griesmer bound given in [23]. The other codes are nearly optimal with respect to Griesmer bound for rings.

4 Quantum Codes from m-adic Residue Codes over $\mathcal{R}_{q,s}$

In this section, as an application of m-adic residue codes over the ring $R_{q,s}$, we are going to derive some families of quantum error correcting codes. Before giving the well-known quantum code construction, called CSS construction, from linear codes over finite fields, we here give a brief introduction for quantum codes.

An $[\![n,k,d]\!]_q$ quantum code is a q^k-dimensional subspace of q^n-dimensional complex vector space $\mathbb{C}^{\otimes q^n}$, where $\otimes$ denotes the tensor product and, n, k and d are said to be the parameters of the quantum code. Such a quantum code encodes k qudits to n qudits and corrects up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. There exists an analogue between the linear codes over finite fields and quantum codes as follows:

Theorem 5:[CSS Code Construction] [24] Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear codes over the finite field $\mathbb{F}_q$ having the parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ such that $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1$. Then, there exists an $[\![n,k_1+k_2-n,d]\!]_q$ quantum error correcting code where

$$d = \min\left\{ w(c) : c \in \left(\mathcal{C}_1 - \mathcal{C}_2^{\perp}\right) \cup \left(\mathcal{C}_2 - \mathcal{C}_1^{\perp}\right) \right\}.$$

In particular, if $\mathcal{C}_1^{\perp} \subseteq \mathcal{C}_1$, then there exits an $[\![n,2k_1-n,d_1]\!]_q$ quantum error correcting code.

We determine the structure of the duals for each class of m-adic residue codes over $\mathcal{R}_{q,s}$.

Theorem 6: Let $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ be m-adic residue codes of length p over $\mathbb{F}_q$ with the generator polynomials $g_0(x), g_1(x), \ldots, g_{s-1}(x)$, respectively and let $\mathcal{C} = \eta_0\mathcal{C}_0 \oplus \eta_1\mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1}\mathcal{C}_{s-1}$ be an m-adic residue code of length p over $\mathcal{R}_{q,s}$. Then, the dual code of $\mathcal{C}$ is $\mathcal{C}^{\perp} = \langle g^{\perp}(x) \rangle = \eta_0\mathcal{C}_0^{\perp} \oplus \eta_1\mathcal{C}_1^{\perp} \oplus \cdots \oplus \eta_{s-1}\mathcal{C}_{s-1}^{\perp}$ where $\mathcal{C}_i^{\perp}$'s are the duals of $\mathcal{C}_i$'s over $\mathbb{F}_q$, $g^{\perp}(x) = \eta_0 h_0^R(x) + \eta_1 h_1^R(x) + \cdots + \eta_{s-1} h_{s-1}^R$ and $x^p - 1 = g_i(x)\, h_i(x)$ over $\mathbb{F}_q$ for each i.

Proof: Define the ideal $J = \langle \eta_0 h_0^R(x), \eta_1 h_1^R(x), \ldots, \eta_{s-1} h_{s-1}^R \rangle$. Since $\eta_i g_i(x)\, \eta_j h_j(x) = 0$ for all $0 \leqslant i,j \leqslant s-1$, $J \subseteq \mathcal{C}^{\perp}$. It follows from comparing the cardinalities of J and $\mathcal{C}^{\perp}$

that $J = \mathcal{C}^{\perp}$. Then, it is not difficult to see that $\mathcal{C}^{\perp}$ is a code generated by the polynomial $g^{\perp}(x) = \eta_0 h_0^R(x) + \eta_1 h_1^R(x) + \cdots + \eta_{s-1} h_{s-1}^R \square$.

Now, we derive a condition for m-adic residue codes over $R_{q,s}$ to contain their duals.

Proposition 2: Let $\mathcal{C} = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$ be an m-adic residue code of length p over $\mathcal{R}_{q,s}$. Then, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ if and only if $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$ for each i.

Proof: It is clear that if, for each i, $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$, then $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Suppose that $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Then, for each $0 \leqslant i \leqslant s-1$, we get

$$\mathcal{C}^{\perp} \bmod (\eta_0, \eta_1, \ldots, \eta_{i-1}, \eta_{i+1}, \ldots, \eta_{s-1}) \subseteq \mathcal{C} \bmod (\eta_0, \eta_1, \ldots, \eta_{i-1}, \eta_{i+1}, \ldots, \eta_{s-1})$$

It follows that $\eta_i \mathcal{C}_i^{\perp} \subseteq \eta_i \mathcal{C}_i$ and $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i \square$.

Recall that for a cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ with defining set Z, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ if and only if $-Z \cap Z = \emptyset$ [24]. Then, for an odd-like class-I m-adic residue code with defining set $Z = Q_i$, the condition to contain its dual reduces $-Q_i \cap Q_i = \emptyset$, which is only possible when $-1 \notin Q_i$. The following explores when the case $-1 \notin Q_i$ is satisfied.

Proposition 3: Let p be a prime and b be a primitive element of $\mathbb{Z}_p^*$. Let Q_0 be the set of nonzero m-adic residues modulo p with $m \geqslant 2$, $m \in \mathbb{Z}$ and $m|(p-1)$. Let $Q_i = b^i Q_0$. In this case, if m does not divide $(p-1)/2$, then $-Q_0 \neq Q_0$ and so $-Q_i \neq Q_i$ for each $0 \leqslant i \leqslant m-1$.

Proof: Suppose that $m \nmid (p-1)/2$ and $-Q_0 = Q_0$. Then, clearly, $-1 \notin Q_0$. Since $b^{(p-1)/2} = -1$, for some $1 \leqslant j \leqslant p-2$, we get $b^{jm} = b^{(p-1)/2}$. This gives the congruence $jm - (p-1)/2 \equiv 0 \,(\bmod\, (p-1))$, where $m|p-1$ and $1 \leqslant j \leqslant p-2$. However, this is a contradiction because the last congruence has no solution since $m|(p-1)$ and $m \nmid (p-1)/2$. To complete the proof, suppose that $-Q_0 \neq Q_0$ but $-Q_i = Q_i$. Then, $-b^i \in Q_i$ implies that $-1 \in Q_0$, which is a contradiction$\square$.

As a result of Proposition 3, we rearrange Proposition 2 as following:

Proposition 4: Let $\mathcal{C} = \eta_0 \mathcal{C}_0 \oplus \eta_1 \mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1} \mathcal{C}_{s-1}$ be an odd-like class-I m-adic residue code of length p over $\mathcal{R}_{q,s}$, where $\mathcal{C}_i$ is an odd-like class-I m-adic residue code of length p over $\mathbb{F}_q$ with the defining set Q_i. Then, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ if and only if $-Q_i \neq Q_i$ for each $0 \leqslant i \leqslant s-1$.

To get quantum error correcting codes by using CSS code construction, we need to carry the codes over the ring $\mathcal{R}_{q,s}$ onto the finite field $\mathbb{F}_q$ via a Gray map preserving the orthogonality from $\mathcal{R}_{q,s}^n$ to $\mathbb{F}_q^{sn}$. We here state such a Gray map defined in [20] and recall its some properties.

Definition 8: [20] Let ζ be $(s-1)^{th}$ primitive root of unity over $\mathbb{F}_q$, where $(s-1) \mid (q-1)$. A Gray map $\Phi : \mathcal{R}_{q,s} \to \mathbb{F}_q^s$ is defined by

$$a_0 + a_1 v + \cdots + a_{s-1} v^{s-1} \to (a_0, a_1, \ldots, a_{s-1})\, MV,$$

where V is any $s \times s$ nonsingular matrix over $\mathbb{F}_q$ and M is $s \times s$ nonsingular matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \zeta & \zeta^2 & \cdots & \zeta^{s-2} \\ 0 & 1 & \zeta^2 & \left(\zeta^2\right)^2 & \cdots & \left(\zeta^2\right)^{s-2} \\ 0 & 1 & \zeta^3 & \left(\zeta^3\right)^2 & \cdots & \left(\zeta^3\right)^{s-2} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 1 & \zeta^{s-2} & \left(\zeta^{s-2}\right)^2 & \cdots & \left(\zeta^{s-2}\right)^{s-2} \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The Gray map from $\mathcal{R}_{q,s}^n$ to $\mathbb{F}_q^{sn}$ is the componentwise extension of the Gray map Φ.

For an element $r \in \mathcal{R}_{q,s}$, its Gray weight $w_G(r)$ is the Hamming weight of $\Phi(r)$. For a vector $c = (c_0, c_1, \ldots, c_{n-1})$ in $\mathcal{R}_{q,s}^n$, its Gray weight $w_G(c)$ is the sum of the Gray weights of its components. The Gray distance $d_G(c,d)$ between two vectors c and d in $\mathcal{R}_{q,s}^n$ is the Gray weight of their difference $c - d$ [20]. The Gray distance $d_G(\mathcal{C})$ of a code $\mathcal{C}$ is the minimum Gray distance between distinct nonzero codewords in the code $\mathcal{C}$. We also have the following:

Proposition 5: [20] The Gray map Φ is an $\mathbb{F}_q$-linear and distance preserving map from $\mathcal{R}_{q,s}^n$ to $\mathbb{F}_q^{sn}$. Moreover, if $VV^T = \lambda I_n$, where $\lambda \in F_q$, then Φ is a preserving orthogonality map from $\mathcal{R}_{q,s}^n$ to $\mathbb{F}_q^{sn}$.

Combining Theorem 5, Proposition 4 and Proposition 5, we derive a class of quantum error correcting codes by applying CSS codes construction after taking the Φ-Gray images of class-I odd-like m-adic residue codes over the ring $\mathcal{R}_{q,s}$ that contain their duals.

Theorem 7: Let $\mathcal{C} = \eta_0\mathcal{C}_0 \oplus \eta_1\mathcal{C}_1 \oplus \cdots \oplus \eta_{s-1}\mathcal{C}_{s-1}$ be an odd-like class-I m-adic residue code of length p over $\mathcal{R}_{q,s}$, where $\mathcal{C}_i$ is an odd-like class-I m-adic residue code of length p over $\mathbb{F}_q$ with the defining set Q_i and the generator polynomial $g_i(x)$. Then, if $-Q_i \neq Q_i$ for each $0 \leqslant i \leqslant s-1$, then there exists a quantum error correcting code with the parameters $[\![ps, ps-2k, d_G]\!]_q$ where $k = \sum_{i=0}^{s-1} \deg g_i(x)$ and d_G is the Gray distance of the code $\mathcal{C}$.

We are going to present some examples of quantum error correcting codes to illustrate what we find in this chapter.

Example 4: Let $\mathcal{C} = \left(1-v^2\right)\mathcal{C}_0 \oplus \left(2v+2v^2\right)\mathcal{C}_1 \oplus \left(v+2v^2\right)\mathcal{C}_2$ be an odd-like class-I 4-adic residue code of length 13 over the ring $\mathcal{R}_{3,3}$, where $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are odd-like class-I 4-adic residue codes of length 13 over $\mathbb{F}_3$ with the generator polynomials $g_0(x) = 2 + x + x^2 + x^3$, $g_1(x) = 2 + x^2 + x^3$ and $g_2(x) = 2 + 2x + x^3$, respectively. In this case, since the defining sets of $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are $Z_0 = Q_0 = \{1,3,9\}$, $Z_1 = 2Q_0 = \{2,6,5\}$ and $Z_2 = 8Q_0 = \{8,11,7\}$, respectively, it follows from $Z_i \neq -Z_i$ and so $\mathcal{C}_i^\perp \subseteq \mathcal{C}_i$ for $0 \leqslant i \leqslant 2$ that $\mathcal{C}^\perp \subseteq \mathcal{C}$. Taking image of $\mathcal{C}$ under the Gray map $\Phi : \mathcal{R}_{3,3} \to \mathbb{F}_3^3$, $r_0 + r_1v + r_2v^2 \to (r_0, r_0 + r_1 + r_2, r_0 + 2r_1 + r_2)$ and using Theorem 7, we get a $[\![39,21,3]\!]_3$ quantum code.

Example 5: Let $\mathcal{C} = (1-v)\mathcal{C}_0 \oplus v\mathcal{C}_1$ be an odd-like class-I 6-adic residue code of length 19 over the ring $\mathcal{R}_{7,2}$, where $\mathcal{C}_0$ and $\mathcal{C}_1$ are odd-like class-I 6-adic residue codes of length 19 over $\mathbb{F}_7$ with the generator polynomials $g_0(x) = 6 + 4x + 4x^2 + x^3$ and $g_1(x) = 6 + x + 4x^2 + x^3$, respectively. In this case, since the defining sets of $\mathcal{C}_0$ and $\mathcal{C}_1$ are $Z_0 = Q_0 = \{1,7,11\}$ and $Z_1 = 16Q_0 = \{16,17,5\}$, respectively, it follows from $Z_i \neq -Z_i$ and so $\mathcal{C}_i^\perp \subseteq \mathcal{C}_i$ for $0 \leqslant i \leqslant 1$ that $\mathcal{C}^\perp \subseteq \mathcal{C}$. Taking image of $\mathcal{C}$ under the Gray map $\Phi : \mathcal{R}_{7,2} \to \mathbb{F}_7^2$, $r_0 + r_1v \to (r_0, r_0 + r_1)$ and using Theorem 7, we get a $[\![38,26,3]\!]_7$ quantum code.

Example 6: Let $\mathcal{C} = \left(1 - v^2\right)\mathcal{C}_0 \oplus \left(4v + 4v^2\right)\mathcal{C}_1 \oplus \left(3v + 4v^2\right)\mathcal{C}_2$ be an odd-like class-I 6-adic residue code of length 19 over the ring $\mathcal{R}_{7,3}$, where $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are odd-like class-I 6-adic residue codes of length 19 over $\mathbb{F}_7$ with the generator polynomials $g_0(x) = 6 + 3x + 6x^2 + x^3$, $g_1(x) = 6 + 5x^2 + x^3$ and $g_2(x) = 6 + 3x + 3x^2x^3$, respectively. In this case, since the defining sets of $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are $Z_0 = 2Q_0 = \{2, 14, 3\}$, $Z_1 = 4Q_0 = \{4, 9, 6\}$ and $Z_2 = 8Q_0 = \{8, 18, 12\}$, respectively, it follows from $Z_i \neq -Z_i$ and so $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$ for $0 \leqslant i \leqslant 2$ that $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Taking image of $\mathcal{C}$ under the Gray map $\Phi : \mathcal{R}_{7,3} \to \mathbb{F}_7^3$, $r_0 + r_1v + r_2v^2 \to (r_0, r_0 + r_1 + r_2, r_0 + 6r_1 + r_2)$ and using Theorem 7, we get a $[\![57, 39, 3]\!]_7$ quantum code.

Example 7: Let $\mathcal{C} = (1 - v)\mathcal{C}_0 \oplus v\mathcal{C}_1$ be an odd-like class-I 4-adic residue code of length 19 over the ring $\mathcal{R}_{7,2}$, where $\mathcal{C}_0$ and $\mathcal{C}_1$ are odd-like class-I 4-adic residue codes of length 29 over $\mathbb{F}_7$ with the generator polynomials $g_0(x) = 6 + 6x + 2x^2 + 4x^3 + 6x^6 + x^7$ and $g_1(x) = 6 + 5x + 2x^2 + 2x^4 + x^5 + 6x^6 + x^7$, respectively. In this case, since the defining sets of $\mathcal{C}_0$ and $\mathcal{C}_1$ are $Z_0 = Q_0 = \{1, 7, 16, 20, 23, 24, 25\}$ and $Z_1 = 2Q_0 = \{2, 3, 11, 14, 17, 19, 21\}$, respectively, it follows from $Z_i \neq -Z_i$ and so $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$ for $0 \leqslant i \leqslant 1$ that $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Taking image of $\mathcal{C}$ under the Gray map $\Phi : \mathcal{R}_{7,2} \to \mathbb{F}_7^2$, $r_0 + r_1v \to (r_0, r_0 + r_1)$ and using Theorem 7, we get a $[\![58, 30, 6]\!]_7$ quantum code.

Example 8: Let $\mathcal{C} = \left(1 - v^2\right)\mathcal{C}_0 \oplus \left(4v + 4v^2\right)\mathcal{C}_1 \oplus \left(3v + 4v^2\right)\mathcal{C}_2$ be an odd-like class-I 4-adic residue code of length 29 over the ring $\mathcal{R}_{7,3}$, where $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are odd-like class-I 4-adic residue codes of length 29 over $\mathbb{F}_7$ with the generator polynomials $g_0(x) = 6 + 5x + 2x^2 + 2x^4 + x^5 + 6x^6 + x^7$, $g_1(x) = 6 + x + 3x^4 + 5x^5 + x^6 + x^7$ and $g_2(x) = 6 + x + 6x^2 + 5x^3 + 5x^5 + 2x^6 + x^7$, respectively. In this case, since the defining sets of $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are $Z_0 = 2Q_0 = \{2, 3, 11, 14, 17, 19, 21\}$, $Z_1 = 4Q_0 = \{4, 5, 6, 9, 13, 22, 28\}$ and $Z_2 = 8Q_0 = \{8, 10, 12, 15, 18, 26, 27\}$, respectively, it follows from $Z_i \neq -Z_i$ and so $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$ for $0 \leqslant i \leqslant 2$ that $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Taking image of $\mathcal{C}$ under the Gray map $\Phi : \mathcal{R}_{7,3} \to \mathbb{F}_7^3$, $r_0 + r_1v + r_2v^2 \to (r_0, r_0 + r_1 + r_2, r_0 + 6r_1 + r_2)$ and using Theorem 7, we get a $[\![87, 45, 6]\!]_7$ quantum code.

5 Conclusion and Future Remarks

In this paper, we generalize results of [11] to the non-chain quotient ring $\mathcal{R}_{q,s}$, where q is a prime power and s is an integer. We study the algebraic structure of m-adic residue codes over $\mathcal{R}_{q,s}$ in spite of the fact that previous papers worked over finite fields. Further, these previous papers have more restrictions on the parameters of the codes they obtained. We achieve to obtain some optimal codes with respect to Griesmer bound for rings (see [23]), which makes this study even more remarkable. We seek a condition for the existence of dual-containing m-adic residue codes over $\mathcal{R}_{q,s}$, and by taking their Gray images, we construct a family of quantum error correcting codes. By giving some examples, we complete the paper.

It can be shown that for some special cases, the generators of the m-adic residue codes over $\mathcal{R}_{q,s}$ are palindromic. Thus, by help of this fact DNA codes can be constructed as a future work.

References

1. R. Brualdi, V. Pless, *Polyadic codes*, Discrete Appl. Math., **25**, 3-71, 1989.
2. X. Dong, L. Wenjie, Z. Yan, *Generating idempotents of cubic and quartic residue codes over field* $\mathbb{F}_2$, Computer Engineering and Applications, **49**, 41-44, 2013.
3. F.J. MacWilliams, *Generalized quadratic residue codes*, IEEE Trans. Inf. Theory, **24**, 730-737, 1978.

4. V. Pless, *Polyadic Codes*, Algebraic Combinatorial Theory, 107-115, 1988.
5. A.J. van Zanten, A. Bojilov, S.M. Dodunekov, *Generalized residue and t-residue codes and their idempotent generators*, Des. Codes Cryptogr., **75**, 315-334, 2015.
6. V.R. Job, *m-adic residue codes*, IEEE Trans. Inf. Theory, **38**, 496-501, 1992.
7. S. Ling and C. Xing, *Polyadic codes revisited*, IEEE Trans. Inf. Theory, **50**, 200-207, 2004.
8. B. Chen, H.Q. Dinh, Y. Fan and S. Ling, *Polyadic constacyclic codes*, IEEE Trans. Inf. Theory, **61**, 4895-4904, 2015.
9. M. Raka, L. Kathuria, M. Goyal, $(1-2u^3)$*-constacyclic codes and quadratic residue codes over* $\mathbb{F}_p[u]/(u^4-u)$, Cryptogr. Commun., **9**, 459-473, 2017.
10. M. Goyal, M. Raka, *Quadratic residue codes over the ring* $\mathbb{F}_p[u]/(u^m-u)$ *and their Gray images*, Cryptogr. Commun., **10**, 343-355, 2018.
11. F. Kuruz, E.S. Oztas and I. Siap, *m-adic codes over* $\mathbb{F}_q[v]/(v^2-v)$ *and DNA codes*, Bull. Korean Math. Soc., **37**, 37-38, 2018.
12. M. Ashraf, G. Mohamed, *Quantum codes from cyclic codes over* $\mathbb{F}_3+v\mathbb{F}_3$, Int. J. Quantum Inf., **12** (6), 1450042, 2014.
13. T. Bag, A.K. Upadhyay, *M. Ashraf, G. Mohammad, Quantum codes from cyclic codes over the ring* $F_p[u]/\langle u^3-u\rangle$, Asian-Eur. J. Math., **12** (07), 2050008, 2019.
14. X. Kai, S. Zhu, *Quaternary construction of quantum codes from cyclic codes over* $\mathbb{F}_4+u\mathbb{F}_4$, Int. J. Quantum Inf., **9** (02), 689-700, 2011.
15. J. Qian, *Quantum codes from cyclic codes over* $\mathbb{F}_2+v\mathbb{F}_2$, J. Inf. Comput. Sci., **10** (6), 1715-1722, 2013.
16. M. Sarı, I. Siap, *On quantum codes from cyclic codes over a class of nonchain rings*, Bull. Korean Math. Soc., **53** (6), 1617-1628, 2016.
17. M. Sarı, I. Siap, *Quantum codes over a class of finite chain rings*, Quantum Inf. Comput., **16** (1-2), 0039-0049, 2016.
18. Y. Tang, T. Yao, S. Zhu, X. Kai, *A family of constacyclic codes over* $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ *and its application to quantum codes*, Chin. J. Electron., **29** (1), 114-120, 2020.
19. Y. Xunru, M. Wenping, *Gray map and quantum codes over the ring* $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 897-899, 2011.
20. M. Goyal, M. Raka, *Duadic codes over the ring* $\mathbb{F}_q[u]/(u^m-u)$ *and their gray images*, J. Comput. Commun., **4** (12), 50-62, 2016.
21. S. Ling and C. Xing, *Coding theory: A first course*, Cambridge University Press, 2004.
22. F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, Elsevier, 1977.
23. K. Shiromoto, L. Storme, *A Griesmer bound for linear codes over finite quasi-Frobenius rings*, Discrete Appl. Math., **128.1**, 263-274, 2003.
24. A. Ketkar, A. Klappenecker, S. Kumar and P.K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory, **52** (11), 4892-4914, 2006.