J. Indones. Math. Soc.
Vol. 30, No. 02 (2024), pp. 139–159.

ON QUANTUM CODES CONSTRUCTION FROM CONSTACYCLIC CODES OVER THE RING $\mathfrak{J}_q[\mathfrak{u},\mathfrak{v}]/\langle \mathfrak{u}^2-\alpha^2,\ \mathfrak{v}^2-\alpha^2,\ \mathfrak{uv}-\mathfrak{vu}\rangle$

Shakir Ali[1], Pushpendra Sharma[2,*]

[1]**Department of Mathematics, Aligarh Muslim University, Aligarh, India, shakir.ali.mm@amu.ac.in**
[2]**Department of Mathematics, Aligarh Muslim University, Aligarh, India, sharmapushpendra52@gmail.com**

Abstract. This paper focuses on studying the properties of constacyclic codes and quantum error-correcting codes. The code is studied over a specific mathematical structure called the ring $\mathfrak{S}$, which is defined as $\mathfrak{S}=\mathfrak{J}_q[\mathfrak{u},\mathfrak{v}]/\langle \mathfrak{u}^2-\alpha^2,\ \mathfrak{v}^2-\alpha^2,\ \mathfrak{uv}-\mathfrak{vu}\rangle$, where $\mathfrak{J}_q$ is a finite field of q elements, α be the nonzero elements of the field $\mathfrak{J}_q$, and q is a power of an odd prime p such that $q=p^m$, for $m\geq 1$. The paper also introduces a Gray map and use it to decompose constacyclic codes over the ring $\mathfrak{S}$ into a direct sum of constacyclic codes over $\mathfrak{J}_q$. We construct new and better quantum error-correcting codes over the ring $\mathfrak{S}$ (cf.; Table 1 and Table 2). Moreover, we also obtain best known linear codes as well as best dimension linear codes (cf.; Table 4).

Key words: Constacyclic code, Quantum code, Gray map, Dual code

1. Introduction

Quantum codes, like conventional linear codes, aid in securing quantum information while it is being transmitted across a quantum channel. These codes are widely employed in quantum computation, which provides faster solutions to difficult problems than classical computation. For instance, in quantum computation, Shor's Algorithm [1] takes polynomial time to determine the prime factors of a big number, whereas in classical computation, it takes sub-exponential time. By Shor [2], quantum codes were first introduced. Later, Calderbank et al. [3] formalized

2020 Mathematics Subject Classification: 94B05, 94B15, 94B60
Received: 27-11-2023, accepted: 30-04-2024.

the challenge of constructing quantum codes from classical codes. A q-ary quantum code with the parameters $[[n,k,d]]_q$ is a type of quantum error-correcting code used in quantum computing. The parameters of the code indicate the length of the code, the number of quantum bits (qubits) it can encode, and the minimum distance among codewords. The quantum singleton bound is a mathematical limit that determines the maximum error that can be corrected by the code, and it is given by the formula $n-k+2 \geq d$. If a code achieves this bound then it is known as Maximum Distance Separable (MDS), which means that it can correct the maximum possible number of errors for its length and dimension.

"One of the primary goals of Coding Theory is to investigate linear codes with large code rates and minimum distances. As a result, this leads to the following inquiries: What is the maximum rate of a code with a given length and distance? What is the maximum distance of a code with a given length and rate? To address these challenges, numerous theoretical bounds on $[n,k,d]$ have been proposed [4], including the Singleton bound, Plotkin bound, Hamming bound, and Griesmer bound, among others. A code $[n,k,d]$ that achieves any of these bounds is referred to as optimal under that bound. Some online databases exist that compile the parameters of optimal and best-known codes (e.g., best known linear codes and best dimension linear codes). The database [5] is a popular platform containing parameters for various types of linear codes over finite fields of size up to 9."

Cyclic codes over $\mathfrak{I}_4+\mathfrak{u}\mathfrak{I}_4$ with $\mathfrak{u}^2=0$ were previously utilized by Kai and Zhu to determine quantum codes over $\mathfrak{I}_4$. Similarly, Qian [6] employed cyclic codes over $\mathfrak{I}_2+v\mathfrak{I}_2$ with $\mathfrak{u}^2=0$ to construct binary quantum codes. The research on cyclic codes over finite commutative rings has had a significant impact on quantum codes, as evident in works such as [7], [8], [9], and [10]. Constacyclic codes, as a generalized type of cyclic codes, have also proven to be essential in quantum code construction ([11], [12]). Notably, the study of constacyclic codes over $\mathfrak{I}_p+\mathfrak{v}\mathfrak{I}_p+v^2\mathfrak{I}_p$, where $\mathfrak{v}^3=\mathfrak{v}$, by Ma et al. [13] and $\mathfrak{u}$-constacyclic codes over $\mathfrak{I}_p+\mathfrak{u}\mathfrak{I}_p$, with $\mathfrak{u}^2=1$, by Gao and Wang [14] in 2018 have led to the development of non-binary quantum codes. Building upon the work of Alkenani et al. [15], who explored constacyclic codes over a finite non-chain ring for constructing quantum codes, this article focuses on quantum codes over the field $\mathfrak{I}_q$. To achieve this, we utilize constacyclic codes over the ring $\mathfrak{S}=\mathfrak{I}_q[\mathfrak{u},\mathfrak{v}]/\langle \mathfrak{u}^2-\alpha^2, \mathfrak{v}^2-\alpha^2, \mathfrak{u}\mathfrak{v}-\mathfrak{v}\mathfrak{u}\rangle$. A key aspect of our investigation is the exploitation of the self-orthogonal property of these constacyclic codes. This approach holds great promise in the construction of efficient quantum codes. In 2019, Islam and Prakash [16] obtained quantum codes over the ring $\mathfrak{I}[\mathfrak{v},\mathfrak{w}]/\langle \mathfrak{v}^2-1, \mathfrak{w}^2-1, \mathfrak{v}\mathfrak{w}-\mathfrak{w}\mathfrak{v}\rangle$. In this article, we describe the properties of constacyclic codes over the ring $\mathfrak{S}$. We define a Gray map and with the help of Gray may we obtain better quantum codes over $\mathfrak{S}$ than the old quantum codes presented in [17, 18, 7, 8, 19, 20, 21, 16, 22] (and references therein).

Three contributions of this article are as follows:

(i) The article offered better quantum codes from the old quantum codes presented in recent references [17, 18, 7, 8, 19, 20, 21, 16, 22], see Tables 1 and 2.
(ii) The article provides some new quantum codes, see Tables 1 and 2
(iii) The article examines some Best Known Linear Codes (BKLC) as well as best dimension linear codes over the ring $\mathfrak{S}$, see Table 4.

2. Some Background

This section provides a review of fundamental definitions in coding theory. We start by considering a linear code $\mathfrak{L}$, which is a subset of $\mathfrak{I}_q^n$. If $x = (x_0, x_1, \ldots, x_{n-1})$ is a codeword in $\mathfrak{L}$, then its $\mathfrak{y}$-constacyclic version, denoted as $\sigma_{\mathfrak{y}}(x)$, is defined as $(\mathfrak{y}x_{n-1}, x_0, \ldots, x_{n-2})$, and this transformed codeword also belongs to $\mathfrak{L}$. When $\mathfrak{y} = 1$ or $\mathfrak{y} = -1$, we refer to $\mathfrak{L}$ as a cyclic code or a negacyclic code, respectively. The dual of a $\mathfrak{y}$-constacyclic code is a $\mathfrak{y}^{-1}$-constacyclic code. We focus on finding quantum codes over the ring $\mathfrak{S} = \mathfrak{I}_q[\mathfrak{u},\mathfrak{v}]/\langle \mathfrak{u}^2-\alpha^2, \mathfrak{v}^2-\alpha^2, \mathfrak{uv}-\mathfrak{vu}\rangle$, for q be an odd prime power. The ring $\mathfrak{S}$ can be written as $\mathfrak{S} = \mathfrak{I}_q+\mathfrak{u}\mathfrak{I}_q+\mathfrak{v}\mathfrak{I}_q+\mathfrak{uv}\mathfrak{I}_q$, satisfying $\mathfrak{u}^2 = \alpha^2$, $\mathfrak{v}^2 = \alpha^2$, $\mathfrak{uv} = \mathfrak{vu}$. Each element in $\mathfrak{S}$ takes the form $a_1 + a_2\mathfrak{u} + a_3\mathfrak{v} + a_4\mathfrak{uv}$, where $a_i \in \mathfrak{I}_q$ for $1 \leq i \leq 4$. Now, let's proceed with the following definitions:

(i) The Hamming distance, denoted by $d(\mathbf{x}, \mathbf{y})$, measures the number of differing components between two codewords $\mathbf{x} = x_1x_2\ldots x_n$ and $\mathbf{y} = y_1y_2\ldots y_n$.
(ii) The Hamming weight of a codeword $\mathbf{x} = x_1x_2\ldots x_n$ is represented as $wt_H(\mathbf{x})$ and counts the number of non-zero components x_i.
(iii) The Euclidean inner product of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathfrak{I}_q^n$ is given by $\mathbf{x}\cdot\mathbf{y} = x_0y_0 + x_1y_1 + \ldots + x_{n-1}y_{n-1}$.
(iv) A linear code is a non-empty subset $\mathfrak{L}$ of the ring $\mathfrak{S}$. It is an $\mathfrak{S}$-submodule of $\mathfrak{S}^n$, and its elements are called codewords.
(v) A code $\mathfrak{L}$ is self-orthogonal if $\mathfrak{L} \subseteq \mathfrak{L}^{\perp}$, self-dual if $\mathfrak{L} = \mathfrak{L}^{\perp}$, and dual-containing if $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$.
(vi) A linear code $\mathfrak{L}$ of length n over $\mathfrak{S}$ is cyclic if every cyclic shift of a codeword c in $\mathfrak{L}$ is also a codeword in $\mathfrak{L}$. The cyclic shift operator is denoted as $\mathfrak{J}$, and the shift of a codeword $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1})$ is given by $\sigma(\mathbf{c}) = (c_{n-1}, c_0, \ldots, c_{n-2})$.
(vii) A linear code C is referred to as a Linear Complementary Dual (LCD) code if it satisfies the condition:

$$\mathfrak{L} \cap \mathfrak{L}^{\perp} = \{\mathbf{0}\}.$$

One of the most crucial parameters associated with a code is its minimum distance. For a linear code $[n, k, d]_q$, the Singleton bound provides an upper limit on its minimum distance: $d(\mathfrak{L}) \leq n - k + 1$.

A linear code $[n, k, d]_q$ that attains this upper bound is known as a Maximum Distance Separable (MDS) code. Furthermore, a linear code C with parameters

$[n, k, d]_q$ is termed an "almost MDS" code if its minimum distance satisfies: $d(\mathfrak{L}) = n - k$.

A code is considered "optimal" if it achieves the highest possible minimum distance for its given length and dimension. Consequently, an MDS code is, by definition, an optimal code.

3. Gray map and linear codes over the ring $\mathfrak{S}$

In addition to introducing the Gray map $\mathscr{S}$ over the ring $\mathfrak{S}$ formed by the matrix A, this section will also look at the structure and characteristics of linear codes with length n over $\mathfrak{S}$. We analyze several characteristics of linear codes using this Gray map, which is a key tool in the study of coding theory and its applications. By using this Gray map, we find a class of constacyclic codes over the ring $\mathfrak{S}$. In this paper, we take the ring $\mathfrak{S} = \mathfrak{I}_q[\mathfrak{u}, \mathfrak{v}]/\langle \mathfrak{u}^2 - \alpha^2,\ \mathfrak{v}^2 - \alpha^2,\ \mathfrak{u}\mathfrak{v} - \mathfrak{v}\mathfrak{u}\rangle = \mathfrak{I}_q + \mathfrak{u}\mathfrak{I}_q + v\mathfrak{I}_q + \mathfrak{u}\mathfrak{v}\mathfrak{I}_q$, and the set $B = \{1,\ \mathfrak{u},\ \mathfrak{v},\ \mathfrak{u}\mathfrak{v}\}$ is a set of basis of $\mathfrak{S}$. We represent the basis elements like as $\mathfrak{S}$ as $\zeta_1 = 1$, $\zeta_2 = \mathfrak{u}$, $\zeta_3 = \mathfrak{v}$, $\zeta_4 = \mathfrak{u}\mathfrak{v}$. On the other hand, we have

$$\begin{aligned}
\mathfrak{P}_1 &= \frac{(\alpha + \mathfrak{u})(\alpha + \mathfrak{v})}{4\alpha^2},\\
\mathfrak{P}_2 &= \frac{(\alpha + \mathfrak{u})(\alpha - \mathfrak{v})}{4\alpha^2},\\
\mathfrak{P}_3 &= \frac{(\alpha - \mathfrak{u})(\alpha + \mathfrak{v})}{4\alpha^2},\\
\mathfrak{P}_4 &= \frac{(\alpha - \mathfrak{u})(\alpha - \mathfrak{v})}{4\alpha^2}.
\end{aligned}$$

We can easily seen that $\mathfrak{P}_i^2 = \mathfrak{P}_i$ and $\mathfrak{P}_i\mathfrak{P}_j = 0$, where $i \neq j$ for $1 \leq i, j \leq 4$. It is easy to see that $\sum_{i=1}^{4} \mathfrak{P}_i = 1$ for $1 \leq i, j \leq 4$. Thus $\{\mathfrak{P}_i \mid 1 \leq i \leq 4\}$ can also be regarded as a set of basis of $\mathfrak{S}$. Now, we give the relationship between ζ_i and $\mathfrak{P}_i$ for $1 \leq i \leq 4$ on $\mathfrak{S}$. We have $\zeta_1 = 1$, $\zeta_2 = \mathfrak{u}$, $\zeta_3 = \mathfrak{v}$, $\zeta_4 = \mathfrak{u}\mathfrak{v}$ and $\mathfrak{P}_1 = \frac{(\alpha + \mathfrak{u})(\alpha + \mathfrak{v})}{4\alpha^2}$, $\mathfrak{P}_2 = \frac{(\alpha + \mathfrak{u})(\alpha - \mathfrak{v})}{4\alpha^2}$, $\mathfrak{P}_3 = \frac{(\alpha - \mathfrak{u})(\alpha + \mathfrak{v})}{4\alpha^2}$ and $\mathfrak{P}_4 = \frac{(\alpha - \mathfrak{u})(\alpha - \mathfrak{v})}{4\alpha^2}$. We write the connection of two type of bases in the form,

$$(\mathfrak{P}_1,\ \mathfrak{P}_2,\ \mathfrak{P}_3,\ \mathfrak{P}_4) = (\zeta_1,\ \zeta_2,\ \zeta_3,\ \zeta_4)A,$$

where

$$A = \begin{bmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4\alpha} & \frac{1}{4\alpha} & \frac{-1}{4\alpha} & \frac{-1}{4\alpha} \\ \frac{1}{4\alpha} & \frac{-1}{4\alpha} & \frac{1}{4\alpha} & \frac{-1}{4\alpha} \\ \frac{1}{4\alpha^2} & \frac{-1}{4\alpha^2} & \frac{-1}{4\alpha^2} & \frac{1}{4\alpha^2} \end{bmatrix}.$$

Henceforward, we see that $(A^{-1})^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha & -\alpha & -\alpha \\ \alpha & -\alpha & \alpha & -\alpha \\ \alpha^2 & -\alpha^2 & -\alpha^2 & \alpha^2 \end{bmatrix}$ and $(A^{-1}) = \begin{bmatrix} 1 & \alpha & \alpha & \alpha^2 \\ 1 & \alpha & -\alpha & -\alpha^2 \\ 1 & -\alpha & \alpha & -\alpha^2 \\ 1 & -\alpha & -\alpha & \alpha^2 \end{bmatrix}$. We take that $A^{-1} = N$ and $(A^{-1})^T = N^T$. By using Chinese Remainder Theorem, we write $\mathfrak{S} = \mathfrak{S}\mathfrak{P}_1 \oplus \mathfrak{S}\mathfrak{P}_2 \oplus \mathfrak{S}\mathfrak{P}_3 \oplus \mathfrak{S}\mathfrak{P}_4 = \mathfrak{I}_q\mathfrak{P}_1 \oplus \mathfrak{I}_q\mathfrak{P}_2 \oplus \mathfrak{I}_q\mathfrak{P}_3 \oplus \mathfrak{I}_q\mathfrak{P}_4$. Therefore, $\mathfrak{S}$ is semi-local, commutative, and nonchain ring and each $r \in \mathfrak{S}$ can be represented as $r = \sum_{i=1}^{4} a_i\zeta_i = \sum_{i=1}^{4} \nu_i\mathfrak{P}_i$, where a_i, $\nu_i \in \mathfrak{I}_q$, for $1 \leq i \leq 4$.

With the help of matrix A, we give more intuitive Gray map

$$\mathscr{S} : \mathfrak{S} \longrightarrow \mathfrak{I}_q^4$$

by $\mathscr{S}(\nu_1\mathfrak{P}_1 + \nu_2\mathfrak{P}_2 + \nu_3\mathfrak{P}_3 + \nu_4\mathfrak{P}_4) = (\nu_1, \nu_2, \nu_3, \nu_4)N^T$, where N^T denotes the transpose of N and $N^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha & -\alpha & -\alpha \\ \alpha & -\alpha & \alpha & -\alpha \\ \alpha^2 & -\alpha^2 & -\alpha^2 & \alpha^2 \end{bmatrix}$.

In the matrix N, we choose those nonzero α from the finite field $\mathfrak{I}_q$ such that $NN^T = 4I_4$, where I_4 is the identity matrix of order 4 over $\mathfrak{I}_q$. It is evident that $\mathscr{S}$ is a bijective, linear map that is extendable component-wise over $\mathfrak{S}^{\mathbf{n}}$. We describe Gray weight of $c \in \mathfrak{S}$ such that $w_G(c) = w_H(\mathscr{S}(c))$, where w_H is the Hamming weight in $\mathfrak{I}_q$. The Gray weight $\mathbf{c} \in \mathfrak{S}^n$ is $w_G(\mathbf{c}) = \sum_{i=0}^{n} w_G(c_i)$ and Gray distance between $\mathbf{c}^{'}$ and $\mathbf{c}^{''}$ is $d_G(\mathbf{c}^{'}, \mathbf{c}^{''}) = w_G(\mathbf{c}^{'}, \mathbf{c}^{''})$. Further, the Gray distance for a linear code $\mathfrak{L}$ is given by $d_G(\mathfrak{L}) = \{w_G(c) \mid 0 \neq c \in \mathfrak{L}\}$.

For a linear code $\mathfrak{L}$ of length n over $\mathfrak{S}$, we define four linear codes $\mathfrak{L}_j$ for $1 \leq j \leq 4$ over $\mathfrak{I}_q$ as follows:

$$\mathfrak{L}_j = \{x_j \in \mathfrak{I}_q^n \mid \sum_{i=1}^{4} \mathfrak{P}_i x_i \in \mathfrak{L} \text{ for some } x_i \in \mathfrak{I}_q^n,\ i \neq j, \text{ and } 1 \leq i \leq 4\}.$$

Each $\mathfrak{L}_j$ is a linear code of length n over $\mathfrak{I}_q$, and we denote the linear code $\mathfrak{L}_j$ as $\mathfrak{A}_j$ for $1 \leq j \leq 4$.

Next, we define the sum and product of linear codes:

$$\mathfrak{A}_1 \oplus \mathfrak{A}_2 \oplus \mathfrak{A}_3 \oplus \mathfrak{A}_4 = \{\theta_1 + \theta_2 + \theta_3 + \theta_4 \mid \theta_i \in \mathfrak{A}_i,\ 1 \leq i \leq 4\},$$

and

$$\mathfrak{A}_1 \otimes \mathfrak{A}_2 \otimes \mathfrak{A}_3 \otimes \mathfrak{A}_4 = \{\theta_1,\ \theta_2,\ \theta_3,\ \theta_4 \mid \theta_i \in \mathfrak{A}_i,\ 1 \leq i \leq 4\}.$$

Thus, a linear code $\mathfrak{L}$ having length n over $\mathfrak{S}$ can be uniquely expressed as:

$$\mathfrak{L} = \mathfrak{P}_1\mathfrak{L}_1 \oplus \mathfrak{P}_2\mathfrak{L}_2 \oplus \mathfrak{P}_3\mathfrak{L}_3 \oplus \mathfrak{P}_4\mathfrak{L}_4.$$

In the case where the rows of a matrix generate the code $\mathfrak{L}$, that matrix is referred to as the generator matrix for the code $\mathfrak{L}$. Specifically, let $\mathfrak{G}_i$ be the generator matrix of the code $\mathfrak{L}_i$ for $i = 1, 2, 3, 4$. Then, a generator matrix of the code $\mathfrak{L}$ is

$$\mathfrak{G} = \begin{bmatrix} \mathfrak{P}_1\mathfrak{G}_1 \\ \mathfrak{P}_2\mathfrak{G}_2 \\ \mathfrak{P}_3\mathfrak{G}_3 \\ \mathfrak{P}_4\mathfrak{G}_4 \end{bmatrix}$$

and a generator of $\mathscr{S}(\mathfrak{L})$ is

$$\mathscr{S}(\mathfrak{G}) = \begin{bmatrix} \mathscr{S}(\mathfrak{P}_1\mathfrak{G}_1) \\ \mathscr{S}(\mathfrak{P}_2\mathfrak{G}_2) \\ \mathscr{S}(\mathfrak{P}_3\mathfrak{G}_3) \\ \mathscr{S}(\mathfrak{P}_4\mathfrak{G}_4) \end{bmatrix}.$$

Proposition 3.1. *The Gray map $\mathscr{S}$ is linear and distance preserving map from $(\mathfrak{S}^n,\ d_L)$ to $(\mathfrak{I}_q^{4n},\ d_H)$, where $d_L = d_H$.*

Proof. Let $\mathbf{x_1}, \mathbf{x_2} \in \mathfrak{S}^n$

$$\begin{aligned} \mathbf{x_1} &= \nu_1\mathfrak{P}_1 + \nu_2\mathfrak{P}_2 + \nu_3\mathfrak{P}_3 + \nu_4\mathfrak{P}_4 \\ \mathbf{x_2} &= \nu_1'\mathfrak{P}_1 + \nu_2'\mathfrak{P}_2 + \nu_3'\mathfrak{P}_3 + \nu_4'\mathfrak{P}_4 \end{aligned}$$

where $a_i,\ b_i \in \mathfrak{I}_q$ and $1 \leq i \leq 4$. Then, we have

$$\begin{aligned} \mathbf{x_1} + \mathbf{x_2} &= (\nu_1 + \nu_1')\mathfrak{P}_1 + (\nu_2 + \nu_2')\mathfrak{P}_2 + (\nu_3 + \nu_3')\mathfrak{P}_3 + (\nu_4 + \nu_4')\mathfrak{P}_4 \\ \mathscr{S}(\mathbf{x_1} + \mathbf{x_2}) &= (\nu_1 + \nu_1' + \nu_2 + \nu_2' + \nu_3 + \nu_3' + \nu_4 + \nu_4')(N)^T \\ &= (\nu_1,\ \nu_2,\ \nu_3,\ \nu_4)(N)^T + (\nu_1',\ \nu_2',\ \nu_3',\ \nu_4')(N)^T \\ &= \mathscr{S}(\mathbf{x_1}) + \mathscr{S}(\mathbf{x_2}) \end{aligned}$$

and

$$\begin{aligned}\mathscr{S}(\gamma\mathfrak{L}_1) &= \mathscr{S}(\nu_1\mathfrak{P}_1+\nu_2\mathfrak{P}_2+\nu_3\mathfrak{P}_3+\nu_4\mathfrak{P}_4)\\ &= (\gamma\nu_1,\ \gamma\nu_2,\ \gamma\nu_3,\ \gamma\nu_4)(N)^T\\ &= \gamma(\nu_1,\ \nu_2,\ \nu_3,\ \nu_4)(N)^T\\ &= \gamma\mathscr{S}(\mathbf{x_1}).\end{aligned}$$

So, $\mathscr{S}$ is an $\mathfrak{I}_q$-linear map.

Moreover, we have

$$\begin{aligned}d_L(\mathbf{x_1},\ \mathbf{x_2}) &= w_L(\mathbf{x_1}-\mathbf{x_2})\\ &= w_H(\mathscr{S}(\mathbf{x_1}-\mathbf{x_2}))\\ &= w_H(\mathscr{S}(\mathbf{x_1})-\mathscr{S}(\mathbf{x_2}))\\ &= d_H(\mathscr{S}(\mathbf{x_1}),\ \mathscr{S}(\mathbf{x_2})).\end{aligned}$$

Hence, $\mathscr{S}$ is distance a preserving map.

□

Proposition 3.2. *Let $\mathfrak{L}$ be a linear code having length n over $\mathfrak{S}$. Then*

(i) $\mathscr{S}(\mathfrak{L}^\perp)=\mathscr{S}(\mathfrak{L})^\perp$.

(ii) $\mathscr{S}(\mathfrak{L})$ *is a linear code having the parameters* $[4n,\ \sum_{i=1}^{4}k_i,\ d]$ *over* $\mathfrak{I}_q$.

(iii) $\mathfrak{L}$ *is a self-dual code having length* n *if and only if* $\mathscr{S}(\mathfrak{L})$ *is a self-dual linear code of length* $4n$ *over* $\mathfrak{I}_q$.

(iv) $\mathfrak{L}$ *is a self-orthogonal linear code having length* n *over* $\mathfrak{S}$ *if and only if* $\mathscr{S}(\mathfrak{L})$ *is a self-orthogonal linear code of length* $4n$ *over* $\mathfrak{I}_q$.

Proof. (i) Suppose $c=(c_0,c_1,\ldots,c_{n-1})\in\mathfrak{L}^\perp$, where $c_i=\mathfrak{P}_1c_i^1+\mathfrak{P}_2c_i^2+\mathfrak{P}_3c_i^3+\mathfrak{P}_4c_i^4$, for $0\le i\le n-1$. Then, we will show that $\mathscr{S}(c)\in\mathscr{S}(\mathfrak{L}^\perp)$. Next let us consider, $d=(d_0,d_1,\ldots,d_{n-1})\in\mathfrak{L}$, where $d_i=\mathfrak{P}_1d_i^1+\mathfrak{P}_2d_i^2+\mathfrak{P}_3d_i^3+\mathfrak{P}_4d_i^4$ for $0\le i\le n-1$. Hence,

$$\begin{aligned}c\cdot d &= 0\\ \Longrightarrow \sum_{i=0}^{n-1}c_id_i &= 0\\ \Longrightarrow \sum_{i=0}^{n-1}(\mathfrak{P}_1c_i^1d_i^1+\mathfrak{P}_2c_i^2d_i^2+\mathfrak{P}_3c_i^3d_i^3+\mathfrak{P}_4c_i^4d_i^4) &= 0.\end{aligned}$$

From here,

$$\sum_{i=0}^{n-1}c_i^1d_i^1=\sum_{i=0}^{n-1}c_i^2d_i^2=\sum_{i=0}^{n-1}c_i^3d_i^3=\sum_{i=0}^{n-1}c_i^4d_i^4=0.$$

Now again, $\mathscr{S}(d)=[(d_0^1,d_0^2,d_0^3,d_0^4)N,\ldots,(d_{n-1}^1,d_{n-1}^2,d_{n-1}^3,d_{n-1}^4)N]=(y_0N,y_1N,$

$\ldots, y_{n-1}N)$ and $\mathscr{S}(c) = [(c_0^1, c_0^2, c_0^3, c_0^4)N, \ldots, (c_{n-1}^1, c_{n-1}^2, c_{n-1}^3, c_{n-1}^4)N] = (z_0N, z_1N, \ldots, z_{n-1}N)$, where $y_i = (d_i^1, d_i^2, d_i^3, d_i^4)$, $z_i = (c_i^1, c_i^2, c_i^3, c_i^4)$ and $N = ((A^{-1})^T)$ for $0 \leq i \leq n-1$. Then, we have

$$\begin{aligned}
\mathscr{S}(d) \cdot \mathscr{S}(c) &= \mathscr{S}(d)\mathscr{S}(c)^T \\
&= \sum_{i=0}^{n-1} y_i N N^T z_i^T \\
&= 4\sum_{i=0}^{n-1} y_i z_i^T \\
&= 4\sum_{i=0}^{n-1} (c_i^1 d_i^1 + c_i^2 d_i^2 + c_i^3 d_i^3 + c_i^4 d_i^4) = 0.
\end{aligned}$$

From here, $\mathscr{S}(c) \in \mathscr{S}(\mathfrak{L})^\perp$ and so $\mathscr{S}(\mathfrak{L}^\perp) \subseteq \mathscr{S}(\mathfrak{L})^\perp$. But, $\mathscr{S}$ is a bijective map, $|\mathscr{S}(\mathfrak{L}^\perp)| = |\mathscr{S}(\mathfrak{L})^\perp|$. Therefore, $\mathscr{S}(\mathfrak{L}^\perp) = \mathscr{S}(\mathfrak{L})^\perp$.

(*ii*) We know that $\mathscr{S}(\mathfrak{L})$ is a linear map having length $4n$ over $\mathfrak{I}_q$ and also $\mathscr{S}$ is distance preserving map. Therefore, $\mathscr{S}(\mathfrak{L})$ be a linear code having parameters $[4n, \sum_{i=1}^{4} k_i, d]$ over $\mathfrak{I}_q$.

(*iii*) Suppose $\mathfrak{L}$ be a linear code having length n that means $\mathfrak{L} = \mathfrak{L}^\perp$. Hence, $\mathscr{S}(\mathfrak{L}) = \mathscr{S}(\mathfrak{L}^\perp) = \mathscr{S}(\mathfrak{L})^\perp$. From here, $\mathscr{S}(\mathfrak{L})$ is a self-dual linear code having length $4n$ over $\mathfrak{I}_q$.

(*iv*) Proof is similar as part (*iii*).

□

Proposition 3.3. *Let $\mathfrak{L} = \oplus_{i=1}^4 \mathfrak{P}_i\mathfrak{L}_i$ be a linear code of length n over $\mathfrak{S}$. Then*
(*i*) $\mathscr{S}(\mathfrak{L}) = \mathfrak{L}_1 \otimes \mathfrak{L}_2 \otimes \mathfrak{L}_3 \otimes \mathfrak{L}_4$. *and* $|\mathfrak{L}| = |\mathfrak{L}_1||\mathfrak{L}_2||\mathfrak{L}_3||\mathfrak{L}_4|$.
(*ii*) $\mathfrak{L}^\perp = \oplus_{i=1}^4 \mathfrak{P}_i\mathfrak{L}_i^\perp$, *further, $\mathfrak{L}$ is self-orthogonal if and only if $\mathfrak{L}_i$ is self-orthogonal and $\mathfrak{L}$ is self-dual if and only if $\mathfrak{L}_i$ is self-dual, for* $1 \leq i \leq 4$.

Proof. (*i*) Let $s = (\nu_0^1, \nu_1^1, \ldots, \nu_{n-1}^1, \nu_0^2, \nu_1^2, \ldots, \nu_{n-1}^2, \nu_0^3, \nu_1^3, \ldots, \nu_{n-1}^3, \nu_0^4, \nu_1^4, \ldots, \nu_{n-1}^4) \in \mathscr{S}(\mathfrak{L})$ and $t_j = \sum_{i=1}^{4} \nu_j^i \mathfrak{P}_i$, for $1 \leq j \leq n-1$. So $t = (t_0, t_1, \ldots, t_{n-1}) \in \mathfrak{L}$. Since $\mathscr{S}$ is bijective, $(\nu_0^i, \nu_1^i, \ldots, \nu_{n-1}^i) \in \mathfrak{L}_i$ by definition of $\mathfrak{L}_i$ for $1 \leq i \leq 4$, and this implies that $s \in \mathfrak{L}_1 \otimes \mathfrak{L}_2 \otimes \mathfrak{L}_3 \otimes \mathfrak{L}_4$. Hence, $\mathscr{S}(\mathfrak{L}) \subseteq \mathfrak{L}_1 \otimes \mathfrak{L}_2 \otimes \mathfrak{L}_3 \otimes \mathfrak{L}_4$.

Conversely, let $s = (\nu_0^1, \nu_1^1, \ldots, \nu_{n-1}^1, \nu_0^2, \nu_1^2, \ldots, \nu_{n-1}^2, \nu_0^3, \nu_1^3, \ldots, \nu_{n-1}^3, \nu_0^4, \nu_1^4, \ldots, \nu_{n-1}^4) \in \mathfrak{L}_1 \otimes \mathfrak{L}_2 \otimes \mathfrak{L}_3 \otimes \mathfrak{L}_4$, then $(\nu_0^i, \nu_1^i, \ldots, \nu_{n-1}^i) \in \mathfrak{L}_i$ for $1 \leq i \leq 4$. We choose $t_j = \sum_{i=1}^{4} \nu_j^i \mathfrak{P}_i$ for $1 \leq j \leq n-1$, then $t = (t_0, t_1, \ldots, t_{n-1}) \in \mathfrak{L}$ and

$\mathfrak{y}(t) = s$. Hence $s \in \mathscr{S}(\mathfrak{L})$. This implies that $\mathfrak{L}_1 \otimes \mathfrak{L}_2 \otimes \mathfrak{L}_3 \otimes \mathfrak{L}_4 \subseteq \mathscr{S}(\mathfrak{L})$. Moreover, since $\mathscr{S}$ is bijective, $|\mathfrak{L}| = |\mathscr{S}(\mathfrak{L})|$. Therefore, $|\mathfrak{L}| = |\mathfrak{L}_1 \otimes \mathfrak{L}_2 \otimes \mathfrak{L}_3 \otimes \mathfrak{L}_4| = |\mathfrak{L}_1||\mathfrak{L}_2||\mathfrak{L}_3||\mathfrak{L}_4|$.

(*ii*) Let $D_j = \{t_j \in \mathfrak{I}_q^n \mid \sum_{i=1}^{4} \mathfrak{P}_i t_i \in \mathfrak{L}^{\perp}\}$ for some $t_j \in \mathfrak{I}_q^n$, $i \neq j$ and $1 \leq i, j \leq 4$. Then, $\mathfrak{L}^{\perp}$ is uniquely represented as $\mathfrak{L}^{\perp} = \mathfrak{P}_1 D_1 \oplus \mathfrak{P}_2 D_2 \oplus \mathfrak{P}_3 D_3 \oplus \mathfrak{P}_4 D_4$. Since $D_1 = \{t_1 \in \mathfrak{I}_q^n$ such that $\sum_{i=1}^{4} \mathfrak{P}_i t_i \in \mathfrak{L}^{\perp}$, for some $t_i \in \mathfrak{I}_q^n$, $i \neq 1$ and $1 \leq i \leq 4\}$. Clearly $\mathfrak{L}_1 D_1 = 0$, so $D_1 \subseteq \mathfrak{L}^{\perp}$. Let $\mathfrak{L}_1 \in \mathfrak{L}^{\perp}$, then $\mathfrak{L}_1 x_1 = 0$ for any $c = \sum_{i=1}^{4} \mathfrak{P}_i x_i \in \mathfrak{L}$. So $\mathfrak{P}_1 \mathfrak{L}_1 c = \mathfrak{P}_1 \mathfrak{L}_1 x_1 = 0$ and this implies that $\mathfrak{P}_1 \mathfrak{L}_1 \in \mathfrak{L}^{\perp}$. We have, $\mathfrak{L}_1 \in D_1$ by the unique representation of $\mathfrak{L}^{\perp}$, and hence $\mathfrak{L}^{\perp} \subseteq D_1$. Similarly, we can show $\mathfrak{L}_j^{\perp} = \mathscr{D}_j^{\perp}$ for $1 \leq i \leq 4$. Thus, $\mathfrak{L}^{\perp} = \oplus_{i=1}^{4} \mathfrak{P}_i \mathfrak{L}_i^{\perp}$. Moreover, $\mathfrak{L}$ is self-orthogonal if and only if $\mathfrak{L} \subseteq \mathfrak{L}^{\perp}$. This shows that $\mathfrak{P}_1\mathfrak{L}_1 \oplus \mathfrak{P}_2\mathfrak{L}_2 \oplus \mathfrak{P}_3\mathfrak{L}_3 \oplus \mathfrak{P}_4\mathfrak{L}_4 \subseteq \mathfrak{P}_1\mathfrak{L}_1^{\perp} \oplus \mathfrak{P}_2\mathfrak{L}_2^{\perp} \oplus \mathfrak{P}_3\mathfrak{L}_3^{\perp} \oplus \mathfrak{P}_4\mathfrak{L}_4^{\perp}$, for $1 \leq i \leq 4$. Similarly, $\mathfrak{L}$ is self-dual.

□

4. $\mathfrak{y}$-Constacyclic codes over $\mathfrak{S}$

In this section, we investigate $\mathfrak{y}$-constacyclic codes and their generators over $\mathfrak{S}$. Moreover, this $\mathfrak{y}$-constacyclic codes help to obtain quantum codes that are better quantum codes (see Table **??** and Table 2). We also obtain Best Known Linear Codes (BKLC), and Best Dimension Linear Codes (BDLC), i.e., optimal codes in Table 4.

Let $\mathfrak{y} \in \mathfrak{S}$ such that $\mathfrak{y} = \sum_{i=1}^{4} \mathfrak{y}_i \zeta_i$, where $\mathfrak{y}_i \in \mathfrak{I}_q$ for $1 \leq i \leq 4$. Let $\mathfrak{y} \in R$ such that $\mathfrak{y} = \mathfrak{y}_1 + \mathfrak{y}_2\mathfrak{u} + \mathfrak{y}_3\mathfrak{v} + \mathfrak{y}_4\mathfrak{u}\mathfrak{v}$, where $\mathfrak{y}_i \in \mathfrak{I}_q$ for $1 \leq i \leq 4$.

$$\mathfrak{y} = (\mathfrak{y}_1,\ \mathfrak{y}_2,\ \mathfrak{y}_3,\ \mathfrak{y}_4)N^T \begin{bmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \\ \mathfrak{P}_3 \\ \mathfrak{P}_4 \end{bmatrix} = (\ell_1,\ \ell_2,\ \ell_3,\ \ell_4) \begin{bmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \\ \mathfrak{P}_3 \\ \mathfrak{P}_4 \end{bmatrix}.$$

This implies that

$$\begin{aligned} (\ell_1,\ \ell_2,\ \ell_3,\ \ell_4) &= (\mathfrak{y}_1,\ \mathfrak{y}_2,\ \mathfrak{y}_3,\ \mathfrak{y}_4)N^T \\ (\ell_1,\ \ell_2,\ \ell_3,\ \ell_4) &= (\mathfrak{y}_1,\ \mathfrak{y}_2,\ \mathfrak{y}_3,\ \mathfrak{y}_4) \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha & -\alpha & -\alpha \\ \alpha & -\alpha & \alpha & -\alpha \\ \alpha^2 & -\alpha^2 & -\alpha^2 & \alpha^2 \end{bmatrix} \end{aligned}$$

and hence

$$\begin{aligned}\ell_1 &= \mathfrak{y}_1+\alpha\mathfrak{y}_2+\alpha\mathfrak{y}_3+\alpha^2\mathfrak{y}_4\\ \ell_2 &= \mathfrak{y}_1+\alpha\mathfrak{y}_2-\alpha\mathfrak{y}_3-\alpha^2\mathfrak{y}_4\\ \ell_3 &= \mathfrak{y}_1-\alpha\mathfrak{y}_2+\alpha\mathfrak{y}_3-\alpha^2\mathfrak{y}_4\\ \ell_4 &= \mathfrak{y}_1-\alpha\mathfrak{y}_2-\alpha\mathfrak{y}_3+\alpha^2\mathfrak{y}_4.\end{aligned}$$

Proposition 4.1. *Suppose* $\mathfrak{y} = \sum_{i=1}^{4}\mathfrak{y}_i\zeta_i$ *is an element of* $\mathfrak{S}$ *and* $(\ell_1,\ \ell_2,\ \ell_3,\ \ell_4) = (\mathfrak{y}_1,\ \mathfrak{y}_2,\ \mathfrak{y}_3,\ \mathfrak{y}_4)N^T$. *Then* $\mathfrak{y}$ *is a unit in* $\mathfrak{S} \iff \ell_i$ *are units in* $\mathfrak{I}_q$ *for* $1 \le i \le 4$.

Proof. We know that $\mathfrak{y} = \sum_{i=1}^{4}\ell_i\mathfrak{P}_i$ (where $\ell_i's$ are mentioned above). Therefore, $\mathfrak{y}$ is unit in $\mathfrak{S}$ if and only if there exists an element $\nu = \sum_{i=1}^{4}\beta_i\mathfrak{P}_i$ in $\mathfrak{S}$ such that

$$1 = \mathfrak{y}\nu = \left(\sum_{i=1}^{4}\ell_i\mathfrak{P}_i\right)\left(\sum_{i=1}^{4}\beta_i\mathfrak{P}_i\right) = \sum_{i=1}^{4}\ell_i\beta_i\mathfrak{P}_i.$$

Here, $\mathfrak{P}_i$ for $1 \le i \le 4$ are $\mathfrak{I}_q$ linear independent and $\sum_{i=1}^{4}\mathfrak{P}_i = 1$. Therefore, $\mathfrak{y}$ is unit if and only if $\ell_i\beta_i = 1$ for $1 \le i \le 4$. □

Theorem 4.2. *Suppose* $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$ *is a linear code having length* n *over the ring* $\mathfrak{S}$, *for* $\mathfrak{y} \in U(\mathfrak{S})$. *Then,* $\mathfrak{L}$ *is a* $\mathfrak{y}$*-constacyclic codes having length* n *over* $\mathfrak{S} \iff \mathfrak{L}_i$ *are* ℓ_i*-constacyclic codes having length* n *over* $\mathfrak{I}_q$ *for* $1 \le i \le 4$.

Proof. Let $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$ represent a linear code with length n over $\mathfrak{S}$. For every codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathfrak{L}$, where $c_j = \sum_{i=1}^{4} c_j^i\mathfrak{P}_i$, $c_j^i \in \mathfrak{I}_q$ for $1 \le i \le 4$ and $j = 0, 1, 2, \ldots, n-1$, we have

$$\begin{aligned}x_1 &= (c_0^1,\ c_1^1,\ c_2^1,\ \ldots,\ c_{n-1}^1),\\ x_2 &= (c_0^2,\ c_1^2,\ c_2^2,\ \ldots,\ c_{n-1}^2),\\ x_3 &= (c_0^3,\ c_1^3,\ c_2^3,\ \ldots,\ c_{n-1}^3)\end{aligned}$$

and

$$x_4 = (c_0^4,\ c_1^4,\ c_2^4,\ \ldots,\ c_{n-1}^4).$$

It is important that $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic code having length n over $\mathfrak{S} \iff \sigma_{\mathfrak{y}}(c) = (\mathfrak{y}c_{n-1},\ c_0,\ c_1,\ \ldots\ , c_{n-2}) \in \mathfrak{L}$ for any $c = (c_0,\ c_1,\ c_2,\ \ldots\ , c_{n-1}) \in \mathfrak{L}$.

$$\begin{aligned}\mathfrak{y}c_{n-1} &= \mathfrak{y}\sum_{i=1}^{4}c_{n-1}^i\mathfrak{P}_i\\ &= \sum_{i=1}^{4}\mathfrak{y}c_{n-1}^i\mathfrak{P}_i\\ &= \sum_{i=1}^{4}\ell_i c_{n-1}^i\mathfrak{P}_i.\end{aligned}$$

Consequently, $\sigma_{\mathfrak{y}}(c) = (\mathfrak{y}c_{n-1},\ c_0,\ c_1,\dots,c_{n-2}) = \sum_{i=1}^{4}(\ell_i c_{n-1}^i,\ c_0^i,\ c_1^i,\dots,c_{n-2}^i)\mathfrak{P}_i$. Thus, $\sigma_{\mathfrak{y}}(c) \in \mathfrak{L}$ if and only if $\sigma_{\mathfrak{y}}(x_i) = (\ell_i c_{n-1}^i,\ c_0^i,\ c_1^i,\dots,c_{n-2}^i) \in \mathfrak{L}_i$ for $1 \le i \le 4$. Hence, $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic codes of length n over $\mathfrak{S}$ if and only if each $\mathfrak{L}_i$ is ℓ_i-constacyclic codes of length n over $\mathfrak{I}_q$ for $1 \le i \le 4$.

□

The following theorem related to generators of $\mathfrak{y}$-constacyclic code having length n over $\mathfrak{S}$.

Theorem 4.3. *Let $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$ be a $\mathfrak{y}$-constacyclic code with length n over $\mathfrak{S}$, for $\mathfrak{y} \in U(\mathfrak{S})$ and $l_i(\vartheta)$ is the generator polynomial of a ℓ_i-constacyclic code $\mathfrak{L}_i$, which divide $\vartheta^n - \ell_i$ for $1 \le i \le 4$.*

(i) $\mathfrak{L} = \langle l_1(\vartheta)\mathfrak{P}_1,\ l_2(\vartheta)\mathfrak{P}_2,\ l_3(\vartheta)\mathfrak{P}_3,\ l_4(\vartheta)\mathfrak{P}_4\rangle$ and $|\mathfrak{L}| = q^{4n-\sum_{i=1}^{4} deg(l_i(\vartheta))}$.

(ii) $f(\vartheta) = \sum_{i=1}^{4} l_i(\vartheta)\mathfrak{P}_i$ is a divisor of $\vartheta^n - \mathfrak{y}$ such that $\mathfrak{L} = \langle f(\vartheta)\rangle$.

Proof. *(i)* In view of Theorem 4.2, $\mathfrak{L}_i^{'}s$ are ℓ_i-constacyclic codes of length n over $\mathfrak{I}_q$ for $1 \le i \le 4$. Since $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$ is a $\mathfrak{y}$-constacyclic code of length n over $\mathfrak{S}$. Here $l_i(\vartheta)$ is the monic generator polynomial of $\mathfrak{L}_i$, we get $\mathfrak{L}_i = \langle l_i(\vartheta)\rangle \subseteq \mathfrak{I}_q[\vartheta]/\langle \vartheta^n - 1\rangle$ for $1 \le i \le 4$. Therefore, $\mathfrak{L} = \langle l_1(\vartheta)\mathfrak{P}_1,\ l_2(\vartheta)\mathfrak{P}_2,\ l_3(\vartheta)\mathfrak{P}_3,\ l_4(\vartheta)\mathfrak{P}_4\rangle$. Since the Gray map $\mathscr{S}$ is bijective, we have $|\mathscr{S}(\mathfrak{L})| = |\mathfrak{L}|$. From Proposition 3.3, we get

$$\begin{aligned} |\mathfrak{L}| &= |\mathfrak{L}_1||\mathfrak{L}_2||\mathfrak{L}_3||\mathfrak{L}_4| \\ &= q^{n-degl_1(\vartheta)} \cdot q^{n-degl_2(\vartheta)} \cdot q^{n-degl_3(\vartheta)} \cdot q^{n-degl_4(\vartheta)} \\ &= q^{4n-\sum_{i=1}^{4} degl_i(\vartheta)}. \end{aligned}$$

(ii) By part *(i)*, $\mathfrak{L} = \langle l_1(\vartheta)\mathfrak{P}_1,\ l_2(\vartheta)\mathfrak{P}_2,\ l_3(\vartheta)\mathfrak{P}_3,\ l_4(\vartheta)\mathfrak{P}_4\rangle$. Suppose $\mathscr{D} = \langle l_1(\vartheta)\mathfrak{P}_1 + l_2(\vartheta)\mathfrak{P}_2 + l_3(\vartheta)\mathfrak{P}_3 + l_4(\vartheta)\mathfrak{P}_4\rangle$. Then it is obvious that $\mathscr{D} \subseteq \mathfrak{L}$. Since $\mathfrak{P}_i^2 = \mathfrak{P}_i$ and $\mathfrak{P}_i\mathfrak{P}_j = 0$, where $i \ne j$ for $i,\ 1 \le j \le 4$. Hence, $l_i\mathfrak{P}_i = (l_1(\vartheta)\mathfrak{P}_1 + l_2(\vartheta)\mathfrak{P}_2 + l_3(\vartheta)\mathfrak{P}_3 + l_4(\vartheta)\mathfrak{P}_4)$. This implies that $\mathfrak{L} \subseteq \mathscr{D}$. Therefore, $\mathfrak{L} = \mathscr{D} = \langle f(\vartheta)\rangle$, where $f(\vartheta) = \sum_{i=1}^{4} l_i(\vartheta)\mathfrak{P}_i$, for $1 \le i \le 4$. Here, $l_i(\vartheta)$ is the monic generator polynomials of $\mathfrak{L}_i$ for $1 \le i \le 4$. Hence, $l_i(\vartheta)$ divides $\vartheta^n - \ell_i$ such that $\vartheta^n - \ell_i = h_i(\vartheta)l_i(\vartheta)$, which

implies that $(\vartheta^n - \ell_i)\mathfrak{P}_i = h_i(\vartheta)l_i(\vartheta)\mathfrak{P}_i$ for $1 \leq i \leq 4$. Then, we have

$$\begin{aligned}
\vartheta^n - \mathfrak{y} &= \vartheta^n \left(\sum_{i=1}^{4} \mathfrak{P}_i\right) - \left(\sum_{i=1}^{4} \ell_i\right) \\
&= \sum_{i=1}^{4} (\vartheta^n - \ell_i)\mathfrak{P}_i \\
&= \sum_{i=1}^{4} h_i(\vartheta)l_i(\vartheta)\mathfrak{P}_i \\
&= \left(\sum_{i=1}^{4} h_i(\vartheta)\mathfrak{P}_i\right)\left(\sum_{i=1}^{4} l_i(\vartheta)\mathfrak{P}_i\right) \\
\vartheta^n - \mathfrak{y} &= \sum_{i=1}^{4} (h_i(\vartheta)\mathfrak{P}_i)f(\vartheta).
\end{aligned}$$

Hence, $f(\vartheta)$ divides $\vartheta^n - \mathfrak{y}$. □

Consider $\mathfrak{L}$ as a linear code of length n over $\mathfrak{S}$, given by $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$. According to Proposition 3.3, the dual code $\mathfrak{L}^{\perp} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i^{\perp}$ is also a linear code of length n over $\mathfrak{S}$. It is worth noting that the dual of a $\mathfrak{y}$-constacyclic code of length n over $\mathfrak{S}$ corresponds to a $\mathfrak{y}^{-1}$-constacyclic code of the same length and over the same ring $\mathfrak{S}$. Exploiting this duality property, we present the following insightful results regarding the dual $\mathfrak{y}$-constacyclic codes.

Corollary 4.4. *Let $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$ be a $\mathfrak{y}$-constacyclic code of length n over $\mathfrak{S}$ such that $\mathfrak{y} = \sum_{i=1}^{4} \ell_i\mathfrak{P}_i \in \mathfrak{S}$ is a unit. We have*
(i) The dual $\mathfrak{L}^{\perp} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i^{\perp}$ is a $\mathfrak{y}^{-1}$-constacyclic code of length n over $\mathfrak{S}$ and $\mathfrak{L}_i^{\perp}$ are γ_i^{-1}-constacyclic codes with length n over $\mathfrak{I}_q$, where $1 \leq i \leq 4$ respectively.
(ii) Let $l_i(\vartheta)$ is the monic generator polynomials of ℓ_i-constacyclic code $\mathfrak{L}_i$ which divides $\vartheta^n - \ell_i$ for $1 \leq i \leq 4$. Then,

(a) $\mathfrak{L}^{\perp} = \langle l_1^*(\vartheta)\mathfrak{P}_1,\ l_2^*(\vartheta)\mathfrak{P}_2,\ l_3^*(\vartheta)\mathfrak{P}_3,\ l_4^*(\vartheta)\mathfrak{P}_4\rangle$ and $|\mathfrak{L}^{\perp}| = p^{\sum_{i=1}^{4} degl_i(\vartheta)}$.
(b) $\mathfrak{L}^{\perp} = \langle h^{'}(\vartheta)\rangle$, where $h^{'}(\vartheta) = \sum_{i=1}^{4} h_i^*(\vartheta)\mathfrak{P}_i$.
Here $\vartheta^n - \ell_i = h_i(\vartheta)l_i(\vartheta)$ for some $h_i(\vartheta) \in \mathfrak{I}_q[\vartheta]$ and $h_i(\vartheta) = \beta_0 + \beta_1\vartheta + \cdots + \beta_{n-r}\vartheta^{n-r}$. Then $h_i^*(\vartheta) = \beta_{n-r} + \beta_{n-r-1}\vartheta + \cdots + \beta_0\vartheta^{n-r}$ and $h_i^*(\vartheta)$ generates the dual ℓ_i^{-1}-constacyclic code $\mathfrak{L}^{\perp}$.

Consider $\mathfrak{L}$ as a linear code of length n over $\mathfrak{S}$, given by $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$. Let $\mathfrak{y}$ be a unit, represented as $\mathfrak{y} = \sum_{i=1}^{4} \mathfrak{y}_i\zeta_i = \sum_{i=1}^{4} \ell_i\mathfrak{P}_i$. Based on Proposition 3.3, we find that $\mathfrak{L}$ is self-dual if and only if each $\mathfrak{L}_i$ is self-dual. Furthermore, in view of Proposition 4.1 and Corollary 4.4, we can deduce that $\mathfrak{L}$ can possess self-duality if

ℓ_i takes values of ± 1 for $1 \leq i \leq 4$.

Proposition 4.5. *Let $\mathfrak{L} = \oplus_{i=1}^{4} \mathfrak{P}_i \mathfrak{L}_i$ be a $\mathfrak{y}$-constacyclic code of length n over $\mathfrak{S}$. Then*
(i) $\mathfrak{L}$ is cyclic code of length n over $\mathfrak{S}$ if and only if each $\mathfrak{L}_i$ is cyclic code of length n over $\mathfrak{I}_q$ for $1 \leq i \leq 4$.
(ii) $\mathfrak{L}$ is negacyclic code of length n over $\mathfrak{S}$ if and only if each $\mathfrak{L}_i$ is negacyclic code of length n over $\mathfrak{I}_q$ for $1 \leq i \leq 4$.

Proof. (i) Let $\mathfrak{L}$ be a cyclic code of length n over $\mathfrak{S}$. Let $p \in \mathfrak{L}_1,\ q \in \mathfrak{L}_2,\ r \in \mathfrak{L}_3,\ s \in \mathfrak{L}_4$ such that

$$\begin{aligned} p &= (p_0,\ p_1,\ p_2, \ldots, p_{n-1}), \\ q &= (q_0,\ q_1,\ q_2, \ldots, q_{n-1}), \\ r &= (r_0,\ r_1,\ r_2, \ldots, r_{n-1}), \end{aligned}$$

and

$$s = (s_0,\ s_1,\ s_2, \ldots, s_{n-1}).$$

Now again, $c = (c_0,\ c_1,\ \ldots,\ c_{n-1}) \in \mathfrak{L}$. By definition $\sigma(c) \in \mathfrak{L}$. Since $\nu_1\sigma(p) + \nu_2\sigma(q) + \nu_3\sigma(r) + \nu_4\sigma(s) = \sigma(c)$, we have $\nu_1\sigma(p) + \nu_2\sigma(q) + \nu_3\sigma(r) + \nu_4\sigma(s) \in \mathfrak{L}$. Thus, $\sigma(p) \in \mathfrak{L}_1,\ \sigma(q) \in \mathfrak{L}_2,\ \sigma(r) \in \mathfrak{L}_3,\ \sigma(s) \in \mathfrak{L}_4$. This implies that $\mathfrak{L}_1,\ \mathfrak{L}_2,\ \mathfrak{L}_3$ and $\mathfrak{L}_4$ are cyclic codes of length n over $\mathfrak{I}_q$.

Conversely, for any $c = (c_0,\ c_1,\ \ldots,\ c_{n-1}) \in \mathfrak{L}$, we have write its components as $c_i = \nu_1 p_i + \nu_2 q_i + \nu_3 r_i + \nu_4 s_i$, where $p_i,\ q_i,\ r_i,\ s_i \in \mathfrak{I}_q$ for $0 \leq i \leq n-1$. Consider $p = (p_0,\ p_1,\ p_2, \ldots, p_{n-1})$, $q = (q_0,\ q_1,\ q_2, \ldots, q_{n-1})$, $r = (r_0,\ r_1,\ r_2, \ldots, r_{n-1})$ and $s = (s_0,\ s_1,\ s_2, \ldots, s_{n-1})$. Then $p \in \mathfrak{L}_1,\ q \in \mathfrak{L}_2,\ r \in \mathfrak{L}_3,\ s \in \mathfrak{L}_4$. Now suppose that $\mathfrak{L}_1,\ \mathfrak{L}_2,\ \mathfrak{L}_3,\ \mathfrak{L}_4$ are cyclic codes over $\mathfrak{I}_q$. That is,

$$\begin{aligned} \sigma(p) &= (p_{n-1},\ p_0,\ \ldots\ p_{n-2}) \in \mathfrak{L}_1, \\ \sigma(q) &= (q_{n-1},\ q_0,\ \ldots\ q_{n-2}) \in \mathfrak{L}_2, \\ \sigma(r) &= (r_{n-1},\ r_0,\ \ldots\ r_{n-2}) \in \mathfrak{L}_3, \end{aligned}$$

and

$$\sigma(s) = (s_{n-1},\ s_0,\ \ldots\ s_{n-2}) \in \mathfrak{L}_4.$$

Thus, $\nu_1\sigma(p) + \nu_2\sigma(q) + \nu_3\sigma(r) + \nu_4\sigma(s) \in \mathfrak{L}$. It can be easily seen that $\nu_1\sigma(p) + \nu_2\sigma(q) + \nu_3\sigma(r) + \nu_4\sigma(s) \in \mathfrak{L} = \sigma(c)$. Hence, $\sigma(c) \in \mathfrak{L}$. Therefore, $\mathfrak{L}$ is cyclic code over $\mathfrak{S}$.

Proof of (ii) is similar as (i). □

We have established that $\mathfrak{L}$ can be self-dual if $\ell_i = \pm 1$ for $1 \leq i \leq 4$. Consequently, the corresponding values of $\mathfrak{y}$ have exactly $2^4 = 16$ different possibilities. We now provide findings for certain conditions of $\mathfrak{y}$ on $\mathfrak{y}$-constacyclic codes with length n over $\mathfrak{S}$.

Proposition 4.6. *Consider the $\mathfrak{y}$-constacyclic code $\mathfrak{L} = \oplus_{i=1}^{4}\mathfrak{P}_i\mathfrak{L}_i$ of length n over $\mathfrak{S}$. Then, the following results provide conditions under which $\mathfrak{L}$ satisfies the properties of a $\mathfrak{y}$-constacyclic code:*

(i) If $\mathfrak{y} = 1$, then $\mathfrak{L}$ is a cyclic code $\iff$ $\mathfrak{L}_1, \mathfrak{L}_2, \mathfrak{L}_3$, and $\mathfrak{L}_4$ are cyclic codes.

(ii) If $\mathfrak{y} = -1$, then $\mathfrak{L}$ is a negacyclic code $\iff$ $\mathfrak{L}_1, \mathfrak{L}_2, \mathfrak{L}_3$, and $\mathfrak{L}_4$ are negacyclic codes.

(iii) If $\mathfrak{y} = \alpha\mathfrak{u}$, then $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic code $\iff$ $\mathfrak{L}_1$ and $\mathfrak{L}_2$ are cyclic codes, while $\mathfrak{L}_3$ and $\mathfrak{L}_4$ are negacyclic codes.

(iv) If $\mathfrak{y} = \alpha\mathfrak{v}$, then $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic code $\iff$ $\mathfrak{L}_1$ and $\mathfrak{L}_3$ are cyclic codes, while $\mathfrak{L}_2$ and $\mathfrak{L}_4$ are negacyclic codes.

(v) If $\mathfrak{y} = \alpha\mathfrak{u}\mathfrak{v}$, then $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic code $\iff$ $\mathfrak{L}_1$ and $\mathfrak{L}_4$ are cyclic codes, while $\mathfrak{L}_2$ and $\mathfrak{L}_3$ are negacyclic codes.

(vi) If $\mathfrak{y} = \frac{1}{2} + \frac{\alpha\mathfrak{u}}{2} + \frac{\alpha\mathfrak{v}}{2} - \frac{\mathfrak{u}\mathfrak{v}}{2}$, then $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic code $\iff$ $\mathfrak{L}_1$, $\mathfrak{L}_2$, and $\mathfrak{L}_3$ are cyclic codes, while $\mathfrak{L}_4$ is a negacyclic code.

(vii) If $\mathfrak{y} = -\frac{1}{2} - \frac{\alpha\mathfrak{u}}{2} - \frac{\alpha\mathfrak{v}}{2} + \frac{\mathfrak{u}\mathfrak{v}}{2}$, then $\mathfrak{L}$ is a $\mathfrak{y}$-constacyclic code $\iff$ $\mathfrak{L}_1$, $\mathfrak{L}_2$, and $\mathfrak{L}_3$ are negacyclic codes, while $\mathfrak{L}_4$ is a cyclic code.

5. Quantum codes from $\mathfrak{y}$-constacyclic code over $\mathfrak{S}$

In this part, using the reliable Calderbank-Shor-Steane (CSS) construction described in the reference [26], we set out to explore the fascinating field of quantum codes. The CSS construction recognised for its effectiveness, allowing the use of dual-containing constacyclic codes to construct quantum codes with extraordinary properties. With the help of CSS construction, we are able to outperform the capabilities of current codes and obtain quantum codes with better dimensions and minimum distances. "We apply a necessary and sufficient condition over finite fields to define the requirements to for constacyclic codes to contain their duals. It is important to note that the set of n-fold tensor product $(\mathbf{C}^q)^{\otimes n} = \mathbf{C}^q \otimes \mathbf{C}^q \otimes \cdots \otimes \mathbf{C}^q$ (n-times) represents a Hilbert space of dimension q^n, where $\mathbf{C}^q$ denotes a Hilbert space of dimension q over the complex field $\mathbf{C}$. A quantum code appears in this setting as a subspace of the Hilbert space $(\mathbf{C}^q)^{\otimes n}$. In the finite field $\mathfrak{I}_q$, where q is a power of prime, we identify a quantum code of length n as $[[n, k, d]]_q$, where d is the minimum distance and k is the dimension. It is interesting to notice that the singleton bound $n-k+2 \geq 2d$, holds for all quantum codes. If a quantum code fulfils the equality $n-k+2 = 2d$, it is said to be MDS (Maximum Distance Separable) code."

Another focus of this study is on two key requirements to obtain quantum codes that are more sophisticated than their predecessors:

Higher Dimension (k): To make a quantum code better, we can make it bigger, represented by the letter "k". This means we can store more special instructions or pieces of information in the code. By creating a larger code than what's already out there, we can save more data using the same number of quantum bits, giving us more storage space and making our quantum computer more powerful.

Larger Minimum Distance (d): A quantum code's capacity to correct errors is greatly influenced by its minimum distance, abbreviated as "d". With a larger

minimum distance, error detection and correction capabilities are improved. "A quantum code $[[n,k,d]]_q$ is better to another quantum code $[[n^{'},k^{'},d^{'}]]_q$ if either or both the following conditions hold:

(i) $\frac{k}{n} > \frac{k^{'}}{n^{'}}$, where $d = d^{'}$ (Larger code rate with the same distance).

(ii) $d > d^{'}$ where $\frac{k}{n} = \frac{k^{'}}{n^{'}}$ (Larger distance with the same code rate)."

We may generate quantum codes which are better to the ones that we already have for these codes. CSS construction is given in the following lemma.

Lemma 5.1. [26] *"(CSS Construction) If $\mathfrak{L}$ is an $[n,k,d]$ linear code with $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$ over $\mathfrak{I}_q$, then there exists a quantum error correcting code with parameters $[[n,2k-n,d]]_q$ over $\mathfrak{I}_q$."*

The dual containing property, denoted as $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$, holds significant importance in the construction of quantum error correcting codes derived from linear codes. This pivotal property plays a crucial role in ensuring the effectiveness and reliability of quantum error correction.

Lemma 5.2. [3] *"Let $\mathfrak{L}$ be a $\mathfrak{y}$-constacyclic code with generator polynomial with $l(\vartheta)$ over $\mathfrak{I}_q$. Then $\mathfrak{L}$ contains its dual if and only if*

$$\vartheta^n - \mathfrak{y} \equiv 0 \pmod{(l(\vartheta)l^*(\vartheta))},$$

where $l^*(\vartheta)$ is the reciprocal polynomial of $l(\vartheta)$ and $\mathfrak{y} = \pm 1$."

Theorem 5.3. *Let $\mathfrak{L} = \oplus \sum_{i=1}^{4} \mathfrak{P}_i\mathfrak{L}_i$ be a $\mathfrak{y}$-constacyclic code of length n over $\mathfrak{S}$ such that $\mathfrak{y} = \sum_{i=1}^{4} \ell_i\mathfrak{P}_i$ with $\ell_i = \pm 1$. Then $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$ if and only if*

$$\vartheta^n - \ell_i \equiv 0 \pmod{(l_i(\vartheta)l_i^*(\vartheta))},$$

where $l_i^*(\vartheta)$ is the reciprocal polynomial of $l_i(\vartheta)$, for $1 \leq i \leq 4$.

Proof. Let $\mathfrak{L} = \oplus \sum_{i=1}^{4} \mathfrak{P}_i\mathfrak{L}_i$ be a $\mathfrak{y}$-constacyclic code of length n over $\mathfrak{S}$, where $\mathfrak{L}_1 = \langle l_1(\vartheta)\rangle,\ \mathfrak{L}_2 = \langle l_2(\vartheta)\rangle,\ \mathfrak{L}_3 = \langle l_3(\vartheta)\rangle,\ \mathfrak{L}_4 = \langle l_4(\vartheta)\rangle$. Now

$$\vartheta^n - \ell_i \equiv 0 \pmod{(l_i(\vartheta)l_i^*(\vartheta))},$$

then $\mathfrak{L}_i^{\perp} \subseteq \mathfrak{L}_i$ for $1 \leq i \leq 4$. This implies that $\mathfrak{P}_i\mathfrak{L}_i^{\perp} \subseteq \mathfrak{P}_i\mathfrak{L}_i$ for $1 \leq i \leq 4$. Hence, $\mathfrak{P}_1\mathfrak{L}_1^{\perp} \oplus \mathfrak{P}_2\mathfrak{L}_2^{\perp} \oplus \mathfrak{P}_3\mathfrak{L}_3^{\perp} \oplus \mathfrak{P}_4\mathfrak{L}_4^{\perp} \subseteq \mathfrak{P}_1\mathfrak{L}_1^{\perp} \oplus \mathfrak{P}_2\mathfrak{L}_2^{\perp} \oplus \mathfrak{P}_3\mathfrak{L}_3^{\perp} \oplus \mathfrak{P}_4\mathfrak{L}_4^{\perp}$, that is $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$. Conversely, if $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$, then $\mathfrak{P}_1\mathfrak{L}_1^{\perp} \oplus \mathfrak{P}_2\mathfrak{L}_2^{\perp} \oplus \mathfrak{P}_3\mathfrak{L}_3^{\perp} \oplus \mathfrak{P}_4\mathfrak{L}_4^{\perp} \subseteq \mathfrak{P}_1\mathfrak{L}_1^{\perp} \oplus \mathfrak{P}_2\mathfrak{L}_2^{\perp} \oplus \mathfrak{P}_3\mathfrak{L}_3^{\perp} \oplus \mathfrak{P}_4\mathfrak{L}_4^{\perp}$. Since $\mathfrak{L}_i$ are the q-ary codes such that $\mathfrak{P}_i\mathfrak{L}_i$ are the q-ary codes such that $\mathfrak{P}_i\mathfrak{L}_i$ is equal to $\mathfrak{L} \pmod{}P_j$ for $i,j = 1,2,3,4$ and $i \neq j$. It follows that $\mathfrak{L}_i^{\perp} \subseteq \mathfrak{L}_i$ for $1 \leq i \leq 4$. Therefore,

$$\vartheta^n - \ell_i \ \equiv\ 0 \pmod{(l_i(\vartheta)l_i^*(\vartheta))}.$$

□

Corollary 5.4. *Let* $\mathfrak{L} = \oplus \sum_{i=1}^{4} \mathfrak{P}_i\mathfrak{L}_i$ *be a* $\mathfrak{y}$*-constacyclic code of length* n *over* $\mathfrak{S}$ *such that* $\mathfrak{y} = \sum_{i=1}^{4} \ell_i\mathfrak{P}_i$ *with* $\ell_i = \pm 1$*. Then* $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$ *if and only if* $\mathfrak{L}_i^{\perp} \subseteq \mathfrak{L}_i$ *for* $1 \leq i \leq 4$.

Theorem 5.5. *Let* $\mathfrak{L} = \oplus \sum_{i=1}^{4} \mathfrak{P}_i\mathfrak{L}_i$ *be a* $\mathfrak{y}$*-constacyclic code of length* n *over* $\mathfrak{S}$*, where* $\mathfrak{L}_i = \langle l_i(\vartheta)\rangle$ *for* $i = 1, 2, 3, 4$ *and* $\mathscr{S}(\mathfrak{L})$ *has the parameters* $[4n, \sum_{i=1}^{4} k_i, d_H]$.

(i) If $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$*, then there exists a quantum code* $[[4n, \sum_{i=1}^{4} k_i - 4n, d_H]]_q$ *over* $\mathfrak{I}_q$.

(ii) If $\vartheta^n - \ell_i \equiv 0 \pmod{l_i(\vartheta)l_i^*(\vartheta)}$*, where* $l_i^*(\vartheta)$ *is the reciprocal polynomial of* $l_i(\vartheta)$*, and* $i = 1, 2, 3, 4$*, then there exists a quantum code* $[[4n, 2\sum_{i=1}^{4} k_i - 4n, d_H]]_q$ *over* $\mathfrak{I}_q$.

Proof. (i) First, let us consider that $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$. By Proposition 3.2, $\mathscr{S}(\mathfrak{L}^{\perp}) = \mathscr{S}(\mathfrak{L})^{\perp}$, $\mathscr{S}(\mathfrak{L})^{\perp} \subseteq \mathscr{S}(\mathfrak{L})$. Hence, $\mathscr{S}(\mathfrak{L})$ is a dual containing linear code over $\mathfrak{I}_q$. By Lemma 5.1, there exists a quantum code $[[4n, 2\sum_{i=1}^{4} k_i - 4n, d_H]]_q$ over $\mathfrak{I}_q$.

(ii) Let us consider that $\vartheta^n - 1 \equiv 0 \pmod{l_i(\vartheta)l_i^*(\vartheta)}$ for $i = 1, 2, 3, 4$, where l_i^* denotes the reciprocal polynomial of $l_i(\vartheta)$. By Theorem 5.3, $\mathfrak{L}^{\perp} \subseteq \mathfrak{L}$. Hence, by using part (i), there exists a quantum code $[[4n, 2\sum_{i=1}^{4} k_i - 4n, d_H]]_q$ over $\mathfrak{I}_q$. □

6. Some Examples

In this section, we give examples of better and new quantum error correcting codes from cyclic codes, $\alpha\mathfrak{u}$-constacyclic codes and $\frac{1}{2} + \frac{\alpha\mathfrak{u}}{2} + \frac{\alpha\mathfrak{v}}{2} - \frac{\mathfrak{u}\mathfrak{v}}{2}$-constacyclic codes by Proposition 4.6, where $\mathfrak{L}_1, \mathfrak{L}_2, \mathfrak{L}_3, \mathfrak{L}_4$ are cyclic codes in part (i), $\mathfrak{L}_1, \mathfrak{L}_2$ are cyclic codes, $\mathfrak{L}_3, \mathfrak{L}_4$ are negacyclic codes in part (iii), and $\mathfrak{L}_1, \mathfrak{L}_2, \mathfrak{L}_3$ are cyclic codes, $\mathfrak{L}_4$ is negacyclic code in part (vi), respectively. Here, we also obtain best known linear codes as well as best dimension linear codes. All the calculations in these examples were done using the Magma computation system [23].

Example 6.1. *Let* $\mathfrak{S} = \mathfrak{I}_3[\mathfrak{u}, \mathfrak{v}]/\langle \mathfrak{u}^2 - \alpha^2, \mathfrak{v}^2 - \alpha^2, \mathfrak{u}\mathfrak{v} - \mathfrak{v}\mathfrak{u}\rangle$ *be a finite commutative ring,* $n = 9, q = 3$ *and* $\mathfrak{y} = 1$*. Then,*

$$\vartheta^9 - 1 = (\vartheta + 2)^9 \in \mathfrak{I}_3[\vartheta].$$

Take

$$\begin{aligned} l_1(\vartheta) &= (\vartheta + 2)^4 \\ l_2(\vartheta) &= (\vartheta + 2) \\ l_3(\vartheta) &= (\vartheta + 2) \\ l_4(\vartheta) &= 1. \end{aligned}$$

Then, the cyclic code $\mathfrak{C}$ is of length 9 over $\mathfrak{S}$ and its Gray image is of length 36, dimension 30, and distance 3 over $\mathfrak{I}_3$, i.e., $[36,30,3]_3$. Moreover

$$t^9-1\equiv\ 0\pmod{l_i(\vartheta)l_i^*(\vartheta)},$$

for $1\leq i\leq 4$. Thus, $\mathfrak{L}^{\perp}\subseteq\mathfrak{L}$ by Theorem 5.3. In view of Theorem 5.5, we conclude that there exists a quantum code $[[36,24,3]]_3$. This quantum code is better than the known quantum code $[[36,22,3]]_3$ obtained in [17].

Example 6.2. *$n=30, q=5$, and take $\mathfrak{y}=\frac{1}{2}+\frac{\alpha\mathfrak{u}}{2}+\frac{\alpha\mathfrak{v}}{2}-\frac{\mathfrak{uv}}{2}$. $\mathfrak{S}\ =\ \mathfrak{I}_5[\mathfrak{u},\mathfrak{v}]/\langle\mathfrak{u}^2-\alpha^2,\mathfrak{v}^2-\alpha^2,\mathfrak{uv}-\mathfrak{vu}\rangle$*

$$\vartheta^{30}-1=(\vartheta+1)^5(\vartheta+4)^5(\vartheta^2+\vartheta+1)^5(\vartheta^2+4\vartheta+1)^5\in\mathfrak{I}_5[\vartheta]$$

$$\vartheta^{30}+1=(\vartheta+2)^5(\vartheta+3)^5(\vartheta^2+2\vartheta+4)^5(\vartheta^2+3\vartheta+4)^5\in\mathfrak{I}_5[\vartheta])$$

$l_1(\vartheta)=(\vartheta+1)^2(\vartheta^2+\vartheta+1)$, $l_2(\vartheta)=(\vartheta+1)$, $l_3(\vartheta)=1$, and $l_4(\vartheta)=(\vartheta+2)^2(\vartheta^2+2\vartheta+4)$. Hence $\mathfrak{L}_1,\mathfrak{L}_2,\mathfrak{L}_3$ are the cyclic codes with the parameters $[90,85,3]$ over $\mathfrak{I}_5$ and $\mathfrak{L}_4$ are the negacyclic codes with the parameters $[30,26,3]$ over $\mathfrak{I}_5$. Then Gray image of $\mathfrak{L}$ having the parameters $[120,111,3]_5$ by Preposition 3.2. Since $l_i(\vartheta)l_i^*(\vartheta)$ divides $\vartheta^{30}-1$ and $l_j(\vartheta)l_j^*(\vartheta)$ divides $\vartheta^{30}+1$, where $i=1,2,3$ and $j=4$. Then using by Theorem 5.3, $\mathfrak{L}^{\perp}\subseteq\mathfrak{L}$. Hence, there exists a quantum error correcting code having the parameters $[[120,102,3]]_5$ by Theorem 5.5. This quantum code is better than the known quantum code $[[120,96,3]]_5$ obtained in [18].

Example 6.3. *$n=35, q=5$, $\mathfrak{y}=\alpha\mathfrak{u}$, and $\mathfrak{S}=\mathfrak{I}_5[\mathfrak{u},\mathfrak{v}]/\langle\mathfrak{u}^2-\alpha^2,\mathfrak{v}^2-\alpha^2,\mathfrak{uv}-\mathfrak{vu}\rangle$*

$$\vartheta^{35}-1=(\vartheta+4)^5(\vartheta^6+\vartheta^5+\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1)^5\in\mathfrak{I}_5[\vartheta]$$

$$\vartheta^{35}+1=(\vartheta+1)^5(\vartheta^6+4\vartheta^5+\vartheta^4+4\vartheta^3+\vartheta^2+4\vartheta+1)^5\in\mathfrak{I}_5[\vartheta])$$

$l_1(\vartheta)=l_2(\vartheta)=(\vartheta+4)^2(\vartheta^6+\vartheta^5+\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1)$, $l_3(\vartheta)=l_4(\vartheta)=(\vartheta+1)^2(\vartheta^6+4\vartheta^5+\vartheta^4+4\vartheta^3+\vartheta^2+4\vartheta+1)$. Hence $\mathfrak{L}_1,\mathfrak{L}_2$ are the cyclic codes with the parameters $[35,27,4]_5$ over $\mathfrak{I}_5$ and $\mathfrak{L}_3,\mathfrak{L}_4$ are the negacyclic codes with the parameters $[35,27,4]$ over $\mathfrak{I}_5$. Then Gray image of $\mathfrak{L}$ having the parameters $[140,108,4]_5$ by Preposition 3.2. Since $l_i(\vartheta)l_i^*(\vartheta)$ divides $\vartheta^{35}-1$ and $l_j(\vartheta)l_j^*(\vartheta)$ divides $\vartheta^{35}+1$, where $i=1,2$ and $j=3,4$. Then using by Theorem 5.3, $\mathfrak{L}^{\perp}\subseteq\mathfrak{L}$. Therefore, by Theorem 5.5, there exists a quantum error correcting code having the parameters $[[140,76,4]]_5$.

Example 6.4. *Let $\mathfrak{S}\ =\ \mathfrak{I}_3[\mathfrak{u},\mathfrak{v}]/\langle\mathfrak{u}^2-\alpha^2,\ \mathfrak{v}^2-\alpha^2,\ \mathfrak{uv}-\mathfrak{vu}\rangle$ be a finite commutative ring, $n=3, q=3$, and $\mathfrak{y}=1$. Then,*

$$\vartheta^3-1=(\vartheta+2)^3\in\mathfrak{I}_3[\vartheta].$$

Take

$$l_1(\vartheta)=(\vartheta+1)^2$$
$$l_2(\vartheta)=(\vartheta+2)$$
$$l_3(\vartheta)=(\vartheta+2)$$
$$l_4(\vartheta)=1.$$

Then, the Gray image $\mathscr{S}(\mathfrak{L})$ is also a Best Known Linear Code (BKLC) with the parameters $[12,8,3]_3$ over $\mathfrak{I}_3$. This is also an optimal code according to the database [5].

Example 6.5. *Let* $\mathfrak{S} = \mathfrak{I}_3[\mathfrak{u},\mathfrak{v}]/\langle \mathfrak{u}^2-\alpha^2,\ \mathfrak{v}^2-\alpha^2,\ \mathfrak{u}\mathfrak{v}-\mathfrak{v}\mathfrak{u}\rangle$ *be a finite commutative ring,* $n = 3, q = 3$, *and* $\mathfrak{y} = 1$. *Then,*

$$\vartheta^3 - 1 \ = \ (\vartheta+2)^3 \in \mathfrak{I}_3[\vartheta].$$

Take

$$\begin{aligned} l_1(\vartheta) &= (\vartheta+1)^3 \\ l_2(\vartheta) &= \ (\vartheta+2) \\ l_3(\vartheta) &= \ (\vartheta+2) \\ l_4(\vartheta) &= \ 1. \end{aligned}$$

Then, the Gray image $\mathscr{S}(\mathfrak{L})$ *is also a Best Dimension Linear Code (BDLC) with the parameters* $[12,7,3]_3$ *over* $\mathfrak{I}_3$. *This is also an optimal code according to the database* [5].

TABLE 1. Quantum Codes from Cyclic Codes Over $\mathfrak{S}$ Over $\mathfrak{S}$

n	$l_1(\vartheta)$	$l_2(\vartheta)$	$l_3(\vartheta)$	$l_4(\vartheta)$	$\phi(\mathfrak{L})$	$[[n,\ k,\ d]]_q$	$[[n^{'},\ k^{'},\ d^{'}]]_q$
9	$(\vartheta+2)^4$	$\vartheta+2$	$\vartheta+2$	1	[36, 30, 3]	$[[36, 24, 3]]_3$	$[[36, 22, 3]]_3$[17]
10	$(\vartheta+1)^2(\vartheta+4)$	$\vartheta+1$	$\vartheta+1$	1	40, 35, 3	$[[40, 30, 3]]_5$	$[[40, 24, 3]]_5$[22]
15	$(\vartheta+4)^2(\vartheta^2+\vartheta+1)$	$\vartheta+4$	$\vartheta+1$	1	$[[60, 54, 3]]_5$	$[[60, 48, 3]]_5$	$[[60, 48, 2]]_5$[8]
20	$(\vartheta+1)^2(\vartheta+2)$	$\vartheta+1$	$\vartheta+1$	1	[80, 75, 3]	$[[80, 70, 3]]_5$	$[[80, 56, 3]]_5$[17]
25	$(\vartheta+1)^6$	$\vartheta+4$	$\vartheta+4$	1	[100, 92, 3]	$[[100, 84, 3]]_5$	$[[100, 70, 3]]_5$[18]
80	$(\vartheta+1)^2(\vartheta^4+3)$	$\vartheta+1$	$\vartheta+1$	1	[320, 312, 3]	$[[320, 304, 3]]_5$	New quantum code
7	$(\vartheta+6)^3$	$\vartheta+6$	$\vartheta+6$	1	[28, 23, 4]	$[[28, 18, 4]]_7$	New quantum code
12	$(\vartheta+2)(\vartheta^2+2)$	$\vartheta+2$	$\vartheta+2$	1	[48, 43, 3]	$[[48, 38, 3]]_7$	$[[48, 36, 2]]_7$[16]
14	$(\vartheta+1)^3(\vartheta+6)$	$\vartheta+1$	$\vartheta+1$	1	[56, 50, 4]	$[[56, 44, 4]]_7$	$[[42, 12, 4]]_7$[20]
21	$(\vartheta+3)^3(\vartheta+5)(\vartheta+6)$	$\vartheta+3$	$\vartheta+3$	1	[84, 77, 4]	$[[84, 70, 4]]_7$	$[[84, 68, 3]]_7$[21]
28	$(\vartheta+1)^3(\vartheta^2+1)$	$\vartheta+1$	$\vartheta+1$	1	[112, 105, 4]	$[[112, 98, 4]]_7$	New quantum code

TABLE 2. Quantum Codes from $\frac{1}{2}+\frac{\alpha\mathfrak{u}}{2}+\frac{\alpha\mathfrak{v}}{2}-\frac{\mathfrak{u}\mathfrak{v}}{2}$-Constacyclic Code Over $\mathfrak{S}$

n	$l_1(\vartheta)$	$l_2(\vartheta)$	$l_3(\vartheta)$	$l_4(\vartheta)$	$\phi(\mathfrak{L})$	$[[n,\ k,\ d]]_q$	$[[n^{'},\ k^{'},\ d^{'}]]_q$
5	$(\vartheta+4)^2$	$\vartheta+4$	1	$(\vartheta+1)^2$	[20, 15, 3]	$[[20, 10, 3]]_5$	New quantum code
10	$(\vartheta+1)^2(\vartheta+4)$	$\vartheta+1$	1	$(\vartheta+2)(\vartheta+3)$	[40, 34, 3]	$[[40, 28, 3]]_5$	$[[40, 24, 2]]_5$[7]
30	$(\vartheta+1)^2(\vartheta^2+\vartheta+1)$	$\vartheta+1$	1	$(\vartheta+2)^2(\vartheta^2+2\vartheta+4)$	$[[120, 111, 3]]_5$	$[[120, 102, 3]]_5$	$[[120, 96, 3]]_5$[25]
35	$(\vartheta+1)^2$ $(\vartheta^6+\vartheta^5+\vartheta^4+$ $\vartheta^3+\vartheta^2+\vartheta+1)$	$\vartheta+4$	$\vartheta+4$	$\vartheta+4$	[140, 129, 3]	$[[140, 118, 3]]_5$	$[[140, 112, 2]]_5$[7]
40	$(\vartheta+4)^2(\vartheta^2+2)$	$\vartheta+4$	1	ϑ^4+2	[160, 151, 3]	$[[160, 142, 3]]_5$	$[[150, 140, 2]]_5$[19]

TABLE 3. Quantum Codes from $\alpha\mathfrak{u}$-Constacyclic Code Over $\mathfrak{S}$

n	$l_1(\vartheta)=l_2(\vartheta)$	$l_3(\vartheta)=l_4(\vartheta)$	$\phi(\mathfrak{L})$	$[[n,\ k,\ d]]_q$
15	$(\vartheta+4)^2(\vartheta^2+\vartheta+1)$	$(\vartheta+1)^2(\vartheta^2+4\vartheta+1)$	[60, 44, 3]	$[[60, 28, 3]]_5$
21	$(\vartheta+3)^2(\vartheta+5)$	$(\vartheta+1)^2(\vartheta+2)$	[84, 72, 3]	$[[84, 60, 3]]_7$
28	$(\vartheta+1)^3(\vartheta^2+1)$	$(\vartheta^2+3\vartheta+1)^3(\vartheta^2+4\vartheta+1)$	[112, 86, 4]	$[[112, 50, 4]]_7$
22	$(\vartheta+1)^3(\vartheta+10)$	$(\vartheta^2+1)^3$	[88, 68, 4]	$[[88, 48, 4]]_{11}$
33	$(\vartheta+10)^3(\vartheta^2+\vartheta+1)$	$(\vartheta^2+10\vartheta+1)(\vartheta+1)^3$	[132, 112, 4]	$[[132, 92, 4]]_{11}$
17	$(\vartheta+16)^6$	$(\vartheta+1)^6$	[68, 44, 7]	$[[68, 20, 7]]_{17}$

TABLE 4. Gray Images of Cyclic Codes of Length n Over $\mathfrak{S}$

n	$l_1(\vartheta)$	$l_2(\vartheta)$	$l_3(\vartheta)$	$l_4(\vartheta)$	$\phi(\mathfrak{L})$	*optimal*
3	$(\vartheta+2)^2$	$\vartheta+2$	$\vartheta+2$	1	$[12,8,3]_3$	*BKLC*
3	$(\vartheta+2)^3$	$\vartheta+2$	$\vartheta+2$	1	$[12,7,4]_3$	*BDLC*
4	$(\vartheta+1)(\vartheta^2+1)$	$(\vartheta+1)$	$(\vartheta+1)$	1	$[16,11,4]_3$	*BKLC & BDLC*
5	$\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1$	$(\vartheta+2)$	$(\vartheta+2)$	1	$[20,14,4]_3$	*BKLC*
8	$(\vartheta^2+1)(\vartheta^2+2\vartheta+2)$	$(\vartheta+2)$	$(\vartheta+2)$	1	$[32,26,4]_3$	*BKLC*
10	$\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1$	$\vartheta+1$	$\vartheta+1$	$\vartheta+1$	$[40,33,4]_3$	*BKLC*

In Tables 1, 2, and 3, we present better and new quantum error correcting codes obtained from cyclic codes and constacyclic codes $\mathfrak{L} = \langle \oplus \sum_{i=1}^{4} \mathfrak{P}_i l_i(\vartheta)\rangle$ of length n over $\mathfrak{S}$, where $\mathfrak{L}_i = \langle l_i(\vartheta)\rangle$, such that $\vartheta^n - 1 \equiv 0 \pmod{l_i(\vartheta) l_i^*(\vartheta)}$ for $i = 1,2,3,4$. It should be emphasized that our QEC codes $[[n,k,d]]_q$ are better to the old quantum codes $[[n^{'},k^{'},d^{'}]]_q$ gathered from the many reference listed in this article. In Table 4, we obtain BKLC as well as BDLC codes $\mathfrak{L} = \langle \oplus \sum_{i=1}^{4} \mathfrak{P}_i l_i(\vartheta)\rangle$ of length n over $\mathfrak{S}$ for $i = 1,2,3,4$.

7. Conclusion

This paper focuses on the investigation of constacyclic codes over the ring $\mathfrak{S} = \mathfrak{I}_q[\mathfrak{u},\mathfrak{v}]/\langle \mathfrak{u}^2-\alpha^2,\ \mathfrak{v}^2-\alpha^2,\ \mathfrak{uv}-\mathfrak{vu}\rangle$. By leveraging the self-orthogonal property of these constacyclic codes, we explored their potential for generating new and better quantum codes. Moreover, we also study the Best Known Linear Codes (BKLC) as well as Best Dimension Linear Codes (BDLC).

8. Declarations

Author Contributions
All authors have equal contribution.

Data Availability Statement
Data sharing is not applicable to this article as no data sets were generated or analyzed during the current study.

Conflicts of Interest
The authors declare that they have no conflicts of interest.

Acknowledgement
The authors are very thankful to the anonymous referees for their valuable comments and suggestions which have improved the manuscript immensely.

REFERENCES

[1] Shor, P. W.: Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124-134. (1994). https://doi.org/10.1109/sfcs.1994.365700.

[2] Shor, P. W.: Scheme for reducing decoherence in quantum memory. Phys. Rev. A **52**, 2493-2496 (1995).

[3] Calderbank, A. R., Rains, E. M., Shor, P. M., Sloane, N. J. A.: Quantum error-correction via codes over $GF(4)$. IEEE Trans. Inf Theory **44**, 1369-1387 (1998).

[4] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, North-Holland (1977)

[5] Grassl, M.: Code Tables: Bounds on the parameters of various types of codes available at http://www.codetables.de/ accessed on 20/04/2023.

[6] Qian, J.: Quantum codes from cyclic codes over $\mathfrak{J}2 + v\mathfrak{J}2$. J. Inf. Compt. Sci. **10**, 1715-1722 (2013).

[7] Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $\mathfrak{I}_q + u\mathfrak{I}_q + v\mathfrak{I}_q + uv\mathfrak{I}_q$. Quantum Inf. Process. **15**(10), 4089-4098 (2016), , DOI: 10.1007/s11128-016-1379-8.

[8] Ashraf, M., Mohammad, G.: Quantum codes over Fp from cyclic codes over $\mathfrak{I}p[u,v]/\langle u^2-1,\ v^3-v,\ uv-vu\rangle$. Cryptogr. Commun. **11**, 325-335 (2019).

[9] Edel, Y. Some good quantum twisted codes. https://www.mathi.uni-heidelberge.de/ yves/Matritzen/QTBCH/ QTBCHIndex.html.

[10] Gao, Y., Gao, J., Fu, F. W.: Quantum codes from cyclic codes over the ring $\mathfrak{I}_q + v\mathfrak{I}_q + \ldots + v^r\mathfrak{I}_q$ .AAECC **30**, 161-174 (2019).

[11] Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans.Inf. Theory **61**(3), 1474-1484 (2015).

[12] Islam, H., Prakash, O., Bhunia, D.K.: Quantum codes obtained from constacyclic codes. Internat. J. Theoret. phys. **58**(11), 3945-3951(2019).

[13] Ma, F., Gao, J., Fu, F.W.: Constacyclic codes over the ring $\mathfrak{I}_q + v\mathfrak{I}_q + v^2\mathfrak{I}_q$ and their applications of constructing new non-binary quantum codes. Quantum Inf. Proces **17**(6), 4 (2018).

[14] Gao, J., Wang, Y.: u-Constacyclic codes over $\mathfrak{I}_q + u\mathfrak{I}_q$ and their applications of constructing new non-binary quantum codes. Quantum Inf. Process. **17**(1), Art. 4 (2018).

[15] Alkenani, A. N., Ashraf, M., mohammad, G.: Quantum codes from constacyclic codes over the ring $\mathfrak{I}_q[u_1,u_2]/\langle u_1^2-1, u_2^2-1, u_1u_2-u_2u_1\rangle$. Mathematics **8**(5), 781: https://doi.org/10.3390/math8050781 (2020).

[16] Islam, H., Prakash, O., Verma, R. K.: Quantum codes from the cyclic codes over $F_p[v,\ w]/\langle v^2-1,\ w^2-1,\ vw-wv\rangle$. Springer Proc. Math. Stat. **307**. https://doi.org/10.1007/978-981-15-1157-8-6 (2019).

[17] Ali, S., Alali, A. S., Jeelani, M., Kurulay, M., Oztas, E. S., & Sharma, P.: On the construction of quantum and LCD codes from cyclic codes over the finite commutative rings. Axioms **12**(4), 367, (2023).

[18] Ali, S., Alali, A. S., Sharma, P., Wong, K.B., Oztas, E. S., Jeelani, M.: On Optimal and Quantum Code Construction from Cyclic Codes over $\mathbb{F}_qPQ$ with Applications. Entropy **25**(8) 1161, (2023).

[19] Cengellenmis, Y., & Dertli, A.; The Quantum Codes over F_q and Quantum Quasi-cyclic Codes over F_p. Mathematical Sciences and Applications E-Notes, 7(1), 87-93, (2019).

[20] Diao, L., Gao, J., Lu., J.: Some results on -additive cyclic codes. Advances in Mathematics of Communications, , **14**(4): 555-572, 2020. doi: 10.3934/amc.2020029.

[21] Islam, H., & Prakash, O.: New quantum codes from constacyclic and additive constacyclic codes. Quantum Information Processing, 19, 1-17, (2020).

[22] Ma, F., Gao, J., Fu, F.W.: New non-binary quantum codes from constacyclic codes over $\mathfrak{I}_q[u,v]/\langle u^2-1, v^2-v, uv-vu\rangle$. Adv. Math. Commun. **13**(2), 421-434 (2019).

[23] Bosma, W., Cannon, J.: Handbook of magma functions. University of Sydney (1995).

[24] Dertli, A., Cengellenmis, Y., Eren, S.: On quantum codes obtained from cyclic codes over A2. Int. J. Quantum Inf. **13**(3), 1550031 (2015).
[25] Dinh, H. Q., Bag, T., Upadhyay, A. K., Ashraf, M., Mohammad, G., & Chinnakum, W.: Quantum codes from a class of constacyclic codes over finite commutative rings. Journal of Algebra and Its Applications, **19**(12), 2150003, 2020.
[26] Grassl, M., Beth, T.: On optimal quantum codes. Int. J. Quantum Inf. **2**(1), 55-64 (2004).