Advances and Applications in Mathematical Sciences
Volume 22, Issue 2, December 2022, Pages 615-626

QUANTUM CODES OVER $\mathbb{Z}_\rho + \tilde{\xi}\mathbb{Z}_\rho$

SWATI KHARUB[1], SONIKA AHLAWAT[2] and DALIP SINGH[3]

[1,2,3]Department of Mathematics
Maharshi Dayanand University
Rohtak, Haryana 124001, India
E-mail: sahlawat1495@gmail.com
dsmdur@gmail.com

Abstract

This paper gives the construction of quantum codes by using $(\rho - 1 + 2\tilde{\xi})$-constacyclic codes over $\mathbb{Z}_\rho + \tilde{\xi}\mathbb{Z}_\rho$ with $\tilde{\xi}^2 = \tilde{\xi}$ with the help of a well defined gray map. A family of quantum error-correcting codes obtained from Calderbank-Shor-Steane (CSS) construction is applied to $(\rho - 1 + 2\tilde{\xi})$-constacyclic codes over $\mathbb{Z}_\rho + \tilde{\xi}\mathbb{Z}_\rho$. Finally, the parameters of associated quantum error-correcting codes are derived. Some examples of quantum codes of arbitrary length are also obtained as an application of obtained results.

1. Introduction

Quantum error-correction plays a crucial role in quantum computation and communication. The most efficient way to control decoherence is by using quantum error-correcting codes. Rapid development has been observed in recent years in the field of quantum error-correction. In [7], Ashraf and Mohammad designed a method to obtain the self-orthogonal codes over the field F_3 by constructing a Gray map of linear and cyclic codes over a finite semi-local non-chain ring $F_3 + vF_3$ with $v^2 = 1$. The necessary and sufficient condition is also provided for the cyclic codes over the ring considered ring that contains its dual. This work was further extended over the commutative

2020 Mathematics Subject Classification: 94B05, 94B15, 94B35, 94B60.
Keywords: Cyclic codes, gray map, constacyclic codes, quantum codes.
[1]Corresponding author; E-mail: swatikharb0001@gmail.com
Received: January 28, 2022; Accepted April 15-2022

non-chain ring $F_p + vF_p$ with $v^2 = v$ in [6] and some main results are described on the linear and cyclic codes which are used to obtain the quantum codes over this ring. L_i and X_u [9], studied the construction of q-ary quantum maximal distance separable (MDS) codes having parameters $[n, n-4, 3]_q$ with $4 \leq n \leq q^2 + 1$ by using Hermitian self-orthogonal codes over the field F_{q^2}. In [1], Steane presented a method for finding the good quantum error-correcting codes. Classical codes are used to get the codes for up to 16 information qubits with the correction of small number of errors. Kai and Zhu [13], considered the self-orthogonal codes over the finite field F_4 which are used to derive the quantum codes. A method to obtain the Hermitian selforthogonal is also provided over F_4 as the gray map of linear codes over $F_4 + uF_4$. In [11], the authors introduced the concept of Gray images from $F_p + vF_p$ to F_{p^2} and obtained the $(1-2v)$-constacyclic codes of length n and determines their dual codes. BCH codes that contains dual 1 codes are used to derive the quantum stabilizer codes in [10]. Further, it has been proved that a BCH code of length n contain its dual only if its designed distance is $o(\sqrt{n})$ and the convex is derived in case of narrow-sense codes. Results are provided to make it possible to detemine the parameters of quantum BCH codes in terms of their design parameters. In [2], Calderbank, et al. transformed the problem of obtaining the quantum error-correcting codes onto the problem of deriving the additive codes over the field $GF(4)$ which are self-orthogonal with respect to a certain trace inner product. A table of lower and upper bounds on these codes is provided of length up to 30 qubits. Qian et al. in [5] described a new method of finding the self-orthogonal codes over the finite field F_2 and on the basis of this method, quantum error-correcting codes are constructed from the cyclic codes over $F_2 + uF_2$. In [4], a new method is used to construct the quantum error-correcting codes from the cyclic codes over the ring $F_2 + vF_2$. Moreover, in [3] construction of some non-binary quantum codes from u-constacyclic codes over $F_p + uF_p$ is given by Gao and Wang. Recently, Ashraf and Mohammad gave the construction of quantum codes using cyclic codes over the ring

$F_p[u, v]$ where $u^2 = 1, v^3 = v, uv = vu$ in [8]. Using classical cyclic codes many good quantum codes are being constructed.

In this paper, quantum codes obtained through $(\rho - 1 + 2\tilde{\xi})$-constacyclic codes over $\mathbb{Z}_\rho + \tilde{\xi}\mathbb{Z}_\rho$. Section 1, describes the preliminaries consists of fundamental properties. Section 2, incorporates Gray map from $\mathbb{Z}_\rho + \zeta\mathbb{Z}_\rho$ to $\mathbb{Z}_\rho^2$ and the development of said codes are presented in Section 3, which is illustrated using examples in Section 4.

2. Preliminaries

The ring

$$R = \mathbb{Z}_\rho + \tilde{\xi}\mathbb{Z}_\rho = \{0, 1, \ldots, \rho - 1, \tilde{\xi}, 2\tilde{\xi}, \ldots, (\rho - 1)\tilde{\xi},$$

$$1 + \tilde{\xi}, 1 + 2\tilde{\xi}, 2 + \tilde{\xi}, \ldots, \rho - 1 + (\rho - 1)\tilde{\xi}\},$$

where ρ is an odd prime and $\tilde{\xi}^2 = \tilde{\xi}$ is semi-local, commutative, non-chain ring consisting of ρ^2 elements, characteristic ρ, where $(\rho-1)+2\tilde{\xi}$ is a unit of R.

The two maximal ideals of the ring are precisely

$$\langle\tilde{\xi}\rangle,$$

and

$$\langle 1 - \tilde{\xi}\rangle.$$

It is discernible that $R/\langle\tilde{\xi}\rangle, R/\langle 1 - \tilde{\xi}\rangle$ are isomorphic with $\mathbb{Z}_\rho$. Chinese Remainder Theorem allows us to express R as $R \cong \langle\tilde{\xi}\rangle \oplus \langle 1 - \tilde{\xi}\rangle \cong \mathbb{Z}_\rho \oplus \mathbb{Z}_\rho$.

Also, every element $\alpha + \tilde{\xi}\beta$ of this ring can be uniquely expressed as $\alpha + \tilde{\xi}\beta = (\alpha + \beta)(\tilde{\xi}) + (\alpha)(1 - \tilde{\xi})$ for all $\alpha, \beta \in \mathbb{Z}_\rho$.

A nonempty subset $\mathcal{K}$ of R^m is a linear code over R of length m. If $\mathcal{K}$ is an

R-submodule of R^m and the elements of $\mathcal{K}$ are codewords. Let $\mathcal{K}$ be a code over R of length m and its polynomial representation be $T(\mathcal{K})$, that is,

$$T(\mathcal{K}) = \left\{ \sum_{i=0}^{m-1} \chi_i \dagger^i \mid (\chi_0, \chi_1, \ldots, \chi_{m-1}) \in \mathcal{K} \right\}$$

Let Υ, Λ and $\mho$ are the maps from R^m to R^m defined as

$$\Upsilon(\chi_0, \chi_1, \ldots, \chi_{m-1}) = (\chi_{m-1}, \chi_0, \ldots, \chi_{m-2}),$$

$$\Lambda(\chi_0, \chi_1, \ldots, \chi_{m-1}) = (-\chi_{m-1}, \chi_0, \ldots, \chi_{m-2}),$$

$$\mho(\chi_0, \chi_1, \ldots, \chi_{m-1}) = (\vartheta\chi_{m-1}, \chi_0, \ldots, \chi_{m-2}),$$

respectively. Then $\mathcal{K}$ is a cyclic, negacyclic and ϑ-constacyclic if $\Upsilon(\mathcal{K}) = \mathcal{K}, \Lambda(\mathcal{K})$ and $\mho(\mathcal{K}) = \mathcal{K}$ respectively. A code $\mathcal{K}$ over R of length m is cyclic, negacyclic and ϑ-constacyclicif and only if $T(\mathcal{K})$ is an ideal of $R[y]/\langle \dagger^m - 1\rangle$, $R[y]/\langle \dagger^m + 1\rangle$ and $R[y]/\langle \dagger^m - \vartheta\rangle$ respectively.

For the arbitrary elements $\chi = (\chi_0, \chi_1, \ldots, \chi_{m-1})$ and $\nu = (\nu_0, \nu_1, \ldots, \nu_{m-1})$ of R, the inner product is defined as

$$\chi \cdot \nu = (\chi_0\nu_0 + \chi_1\nu_1 + \ldots + \chi_{m-1}\nu_{m-1}).$$

If $\chi \cdot \nu = 0$, then χ and ϑ are orthogonal. If $\mathcal{K}$ is a linear code over R of length m, then the dual code of $\mathcal{K}$ is defined as

$$\mathcal{K}^{\perp} = \{\chi \in R^m : \chi \cdot \nu = 0 \text{ for all } \nu \in \mathcal{K}\}.$$

which is also a linear code over the ring R of length m. A code $\mathcal{K}$ is said to be self orthogonal if $\mathcal{K} \subseteq \mathcal{K}^{\perp}$ and said to be self dual if $\mathcal{K} = \mathcal{K}^{\perp}$.

3. Gray Map Over R

The hamming weight $w_H(\chi)$ for any codeword $\chi = (\chi_0, \chi_1, \ldots, \chi_{m-1}) \in R^m$ is defined as the number of non-zero components in $\chi = (\chi_0, \chi_1, \ldots, \chi_{m-1})$. The minimum weight of a code $\mathcal{K}$, that is, $w_H(\mathcal{K})$ is the least weight among all of its non zero codewords. The Hamming distance between two codes $\chi = (\chi_0, \chi_1, \ldots, \chi_{m-1})$ and $\hat{\chi} = (\hat{\chi}_0, \hat{\chi}_1, \ldots, \hat{\chi}_{m-1})$ of R^m, denoted by $d_H(\chi, \hat{\chi}) = w_H(\chi - \hat{\chi})$ and is defined as

$$d_H(\chi, \hat{\chi}) = |\{i \mid \chi_i \neq \hat{\chi}_i\}|.$$

Minimum distance of $\mathcal{K}$, denoted by d_H and is given by minimum distance between the different pairs of codewords of the linear code $\mathcal{K}$. For any codeword $\chi = (\chi_0, \chi_1, \ldots, \chi_{m-1}) \in R^m$, the lee weight is defined as $w_L(\chi) = \sum_{i=0}^{m-1} w_L(\chi_i)$ and lee distance of $(\chi - \hat{\chi})$ is given by $d_L(\chi, \hat{\chi}) = w_L(\chi - \hat{\chi}) = \sum_{i=0}^{m-1} w_L(\chi_i - \hat{\chi}_i)$.

Minimum lee distance of $\mathcal{K}$ is denoted by d_L and is given by minimum lee distance of different pairs of codewords of the linear code $\mathcal{K}$.

The map $\psi : R$ to $\mathbb{Z}_\rho^2$ as

$$\psi(\eta_1 + \tilde{\xi}\eta_2) = (\eta_1, \eta_1 + \eta_2),$$

with $\eta_1 + \tilde{\xi}\eta_2 \in R$ is the gray map and can be extended from $R^m \to \mathbb{Z}_\rho^{2m}$ as

$$\psi(\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_{m-1}) = (\eta_1, \eta_1 + \dot{\eta_1}, \eta_2, \eta_2 + \dot{\eta_2}, \ldots \eta_{m-1}, \eta_1 + \dot{\eta}_{m-1}),$$

where $\alpha_i = \eta_i + \tilde{\xi}\eta_i$ for all $0 \leq i \leq m-1$.

Proposition 3.1. *The Gray map ψ is a linear and distance preserving isometry map from (R^m, d_L) to $(\mathbb{Z}_\rho^{2m}, d_H)$.*

Throughout the text, the code $\mathfrak{C}$ is considered to be a linear code of length m over R.

Proposition 3.2. *For a linear self orthogonal code $\mathfrak{C}$ so is $\psi(\mathfrak{C})$.*

Proof. Consider a self orthogonal code $\mathfrak{C}$ and $\eta_1, \eta_2 \in \mathfrak{C}$ with $\eta_1 = \xi_1 + \tilde{\xi}\varpi_1$ and $\eta_2 = \xi_2 + \tilde{\xi}\varpi_2$, where $\xi_1, \xi_2, \varpi_1, \varpi_2 \in \mathbb{Z}_\rho$.

By self orthogonality of η_1, η_2 we have $\eta_1 . \eta_2 = 0$, that is, $\xi_1\xi_2 + \xi(\varpi_1\varpi_2 + \xi_1\varpi_2 + \xi_2\varpi_1) = 0$, it follow that $\xi_1\xi_2 = \varpi_1\varpi_2 + \xi_1\varpi_2 + \xi_2\varpi_1 = 0$. Now, applying ψ on η_1, η_2 we have

$$\psi(\eta_1). \psi(\eta_2) = (\xi_1, \xi_1 + \varpi_1)(\xi_2, \xi_2 + \varpi_2) = (2\xi_1\xi_2 + \xi_1\varpi_2 + \xi_2\varpi_1 + \varpi_1\varpi_2) = 0,$$

which implies $\psi(\mathfrak{C})$ is self orthogonal.

4. Quantum Codes Through $(\rho - 1 + 2\widetilde{\xi})$-Constacyclic Codes Over *R*

For a linear code $\mathfrak{C}$,

$$\mathfrak{C}_1 = \{a \in \mathbb{Z}_\rho^m \mid \text{for some } b \in \mathbb{Z}_\rho^m \text{ such that } (a + b\widetilde{\xi}) \in \mathfrak{C}\},$$

and

$$\mathfrak{C}_2 = \{a + b \in \mathbb{Z}_\rho^m \mid \text{such that } (a + b\widetilde{\xi}) \in \mathfrak{C}\},$$

are σ-ary codes such that

$$(1 - \widetilde{\xi})\mathfrak{C}_1 = \mathfrak{C}, \bmod(\widetilde{\xi}),$$

and

$$(\widetilde{\xi})\mathfrak{C}_2 = \mathfrak{C}, \bmod(1 - \widetilde{\xi}).$$

Therefore, $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are the linear $[m, k_1, d_1]$ and $[m, k_2, d_2]$ codes over $\mathbb{Z}_\rho$ respectively. Moreover,

$$\mathfrak{C} = (1 - \widetilde{\xi})\mathfrak{C}_1 \oplus (\widetilde{\xi})\mathfrak{C}_2,$$

and

$$|\mathfrak{C}| = |\mathfrak{C}_1||\mathfrak{C}_2|.$$

Further, $\psi(\mathfrak{C})$ is a σ-ary linear $[2m, k_1 + k_2, \min(d_1, d_2)]$ code.

Theorem 4.1. *The code* $\mathfrak{C}$ is $(\rho - 1 + 2\widetilde{\xi})$*-constacyclic if and only if* $\mathfrak{C}_1$ *is negacyclic and* $\mathfrak{C}_2$ *is cyclic over* $\mathbb{Z}_\rho$.

Proof. For any $\dot{a} = (\dot{a}_0, \dot{a}_1, \dots \dot{a}_{m-1}) \in \mathfrak{C}_1$, and $\dot{b} = (\dot{b}_0, \dot{b}_1, \dots \dot{b}_{m-1}) \in \mathfrak{C}_2$. For an arbitrary element $\zeta_i = (1 - \tilde{\xi})\dot{a}_i + (\tilde{\xi})\dot{b}_i$, where $\dot{a}_i, \dot{b}_i \in \mathbb{Z}_\rho$ for $i = 0, 1, \dots, m-1$.

Let $\zeta = (\zeta_0, \zeta_1, \dots \zeta_{m-1}) \in \mathfrak{C}$.

For $(\rho - 1 + 2\tilde{\xi})$-constacyclic code $\mathfrak{C}$,

$\mho(\zeta) = (\rho - 1 + 2\tilde{\xi})\zeta_{m-1}, \zeta_{0, \dots}\zeta_{m-2})$

$= ((\rho - 1 + 2\tilde{\xi})a_{m-1} + \tilde{\xi}(\rho - 1)b_{m-1} + 2\tilde{\xi}(1 - \tilde{\xi})a_{m-1} + 2\tilde{\xi}b_{m-1}, (1 - \tilde{\xi})\dot{\alpha}_0$

$+ \tilde{\xi}\dot{b}_0, \dots, (1 - \tilde{\xi})a_{\dot{m}-2} + \tilde{\xi}b_{m-2})$

$= (1 - \tilde{\xi})\Lambda(\dot{a}) + \tilde{\xi}\Upsilon(\dot{b}),$

which is in $\mathfrak{C}$. Therefore, $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are negacyclic and cyclic codes over $\mathbb{Z}_\rho$ respectively with length m. Again, if $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are negacyclic and cyclic code over $\mathbb{Z}_\rho$, respectively, with length m, then for any $\zeta = (\zeta_0, \zeta_1, \dots, \zeta_{m-1}) \in \mathfrak{C}$ where $\zeta_i = (1 - \tilde{\xi})\dot{a}_i + \tilde{\xi}\dot{b}_i$, and $\dot{a}_i, \dot{b}_i \in \mathbb{Z}_\rho$ for $i = 0, 1, \dots, m-1$.

If $\mathfrak{C}_1$ is a negacyclic code and $\mathfrak{C}_2$ is a cyclic code over the ring $\mathbb{Z}_\rho$ of length m, then $\Lambda(\dot{a}) \in \mathfrak{C}_1$, $\Upsilon(\dot{b}) \in \mathfrak{C}_2$.

So, $(1 - \tilde{\xi})\Lambda(\dot{a}) + \tilde{\xi}\Upsilon(\dot{b}) \in \mathfrak{C}$, where $\mho(\zeta) = (1 - \tilde{\xi})\Lambda(\dot{a}) + (\tilde{\xi})\Upsilon(\dot{b})$. Thus, $\mho(\zeta) \in \mathfrak{C}$. Hence, $\mathfrak{C}$ is a $(\rho - 1 + 2\tilde{\xi})$-constacyclic code.

Lemma 4.2. *For a* $(\rho - 1 + 2\tilde{\xi})$*-constacyclic code* $\mathfrak{C}$

$$\mathfrak{C} = \langle (1 - \tilde{\xi})g_1(\dagger), \tilde{g}_2(\dagger) \rangle = \langle (1 - \tilde{\xi})g_1(\dagger) + \tilde{\xi}g_2(\dagger) \rangle,$$

with $|\mathfrak{C}| = p^{2m - \deg(g_1(\dagger)) - \deg(g_2(\dagger))}$, *where polynomials* $g_i(\dagger)$ *generates* $\mathfrak{C}_i$, $i = 1, 2$.

Proof. Since $\mathfrak{C}_1$ is negacyclic and $\mathfrak{C}_2$ is cyclic code over $\mathbb{Z}_\rho$ with length m, so

$$\mathfrak{C}_1 = \langle g_1(\dagger)\rangle \subseteq \mathbb{Z}_\rho/\langle \dagger^m + 1\rangle,$$

$$\mathfrak{C}_2 = \langle g_2(\dagger)\rangle \subseteq \mathbb{Z}_\rho/\langle \dagger^m - 1\rangle.$$

Further, $\mathfrak{C} = (1-\widetilde{\xi})\mathfrak{C}_1 \oplus \widetilde{\xi}\ \mathfrak{C}_2$. Thus, $\mathfrak{C} = \{g(\dagger) \mid g(\dagger) = (1-\widetilde{\xi})f_1(\dagger) + \widetilde{\xi}f_2(\dagger)\}$, where $f_1(\dagger) \in \mathfrak{C}_1$, $f_2(\dagger) \in \mathfrak{C}_2$. Therefore,

$$\begin{aligned}\mathfrak{C} &\subseteq \langle (1-\widetilde{\xi})g_1(\dagger) + \widetilde{\xi}g_2(\dagger)\rangle \\ &= \langle (1-\widetilde{\xi})g_1(\dagger), \widetilde{\xi}g_2(\dagger)\rangle \\ &= R[\dagger]/\langle \dagger^m - (\rho - 1 + 2\widetilde{\xi})\rangle.\end{aligned}$$

Conversely, for any $(1-\widetilde{\xi})h_1(\dagger)g_1(\dagger) + \widetilde{\xi}h_2(\dagger)g_2(\dagger) \in \langle (1-\widetilde{\xi})g_1(\dagger) + \widetilde{\xi}g_2(\dagger)\rangle$, implies $(1-\widetilde{\xi})h_1(\dagger)g_1(\dagger) + \widetilde{\xi}h_2(\dagger)g_2(\dagger) \subseteq R[\dagger]/\langle \dagger^m - (\rho - 1 + 2\widetilde{\xi})\rangle$, where $g_1(\dagger)$, $g_2(\dagger) \in R[\dagger]/\langle \dagger^m - (\rho - 1 + 2\widetilde{\xi})\rangle$, there exists $r_1(\dagger), r_2(\dagger) \in \mathbb{Z}_\rho[\dagger]$ such that

$$(1-\widetilde{\xi})g_1(\dagger) = (1-\widetilde{\xi})r_1(\dagger),$$

$$\widetilde{\xi}g_2(\dagger) = \widetilde{\xi}r_2(\dagger).$$

So, $\langle (1-\widetilde{\xi})g_1(\dagger) + \widetilde{\xi}g_2(\dagger)\rangle = \langle (1-\widetilde{\xi})g_1(\dagger)\widetilde{\xi}g_2(\dagger)\rangle \subseteq \mathfrak{C}$, and hence $\mathfrak{C} = \langle (1-\widetilde{\xi})g_1(\dagger) + \widetilde{\xi}g_2(\dagger)\rangle = \langle (1-\widetilde{\xi})g_1(\dagger)\widetilde{\xi}g_2(\dagger)\rangle$. Since, $|\mathfrak{C}| = |\mathfrak{C}_1||\mathfrak{C}_2|$, so $|\mathfrak{C}| = p^{2m-(\deg(g_1(\dagger)) - \deg(g_2(\dagger)))}$.

Theorem 4.3. *Dual of* $(\rho - 1 + 2\widetilde{\xi})$*-constacyclic code is of similar length* $(\rho - 1 + 2\widetilde{\xi})$*-constacyclic code.*

Proof. The proof hold trivially because $(\rho - 1 + 2\widetilde{\xi})$ is a self unit element, that is,

$$(\rho - 1 + 2\widetilde{\xi})^{-1} = \rho - 1 + 2\widetilde{\xi},$$

and dual code is $(\rho - 1 + 2\widetilde{\xi})$-constacyclic code.

Lemma 4. 4. *For a* $(\rho - 1 + 2\widetilde{\xi})$*-constacyclic code, the dual code*

1. $\mathfrak{C}^{\perp} = (1-\tilde{\xi})\mathfrak{C}_1^{\perp} \oplus \tilde{\xi}\mathfrak{C}_2^{\perp}$

2. $\mathfrak{C}^{\perp} = \langle (1-\tilde{\xi})g_1^*(\dagger), \tilde{\xi}g_2^*(\dagger)\rangle = \langle (1-\tilde{\xi})g_1^*(\dagger) + \tilde{\xi}g_1^*(\dagger)\rangle$

3. $|\mathfrak{C}^{\perp}| = p^{\deg(g_1(\dagger))+\deg(g_2)(\dagger)}$

where polynomials $g_1^*(\dagger)$ and $g_2^*(\dagger)$ are reciprocal of $\frac{(\dagger^m + 1)}{g_1(\dagger)}$ and $\frac{(\dagger^m - 1)}{g_2(\dagger)}$ respectively.

Lemma 4.5 [2]. *If $\mathfrak{C}$ is a cyclic or negacyclic code over the ring $\mathbb{Z}_\rho$ with generator polynomial $g(\dagger)$. Then, $\mathfrak{C}$ contains its dual if and only if $x^n - T \equiv 0 \bmod (g(\dagger)g^*(\dagger))$, where $T = \pm 1$.*

Theorem 4.6. *For a $(\rho - 1 + 2\tilde{\xi})$-constacyclic codes $\mathfrak{C} = \langle (1-\tilde{\xi})g_1(\dagger), \tilde{\xi}g_2(\dagger)\rangle$, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ if and only if $\dagger^m + 1 \equiv 0 \bmod (g_1(\dagger)g_1^*(\dagger))$ for $\mathfrak{C}_1$ and $\dagger^m - 1 \equiv 0 \bmod (g_2(\dagger)g_2^*(\dagger))$* for $\mathfrak{C}_2$.

Proof. First consider $\dagger^m + 1 \equiv 0 \bmod (g_1(\dagger)g_1^*(\dagger))$ for $\mathfrak{C}_1$, and $\dagger^m - 1 \equiv 0 \bmod (g_2(\dagger)g_2^*(\dagger))$ for $\mathfrak{C}_2$. Then by lemma 4.5, $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1$ and $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_2$ and therefore $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1$ and $\tilde{\xi}\mathfrak{C}_2^{\perp} \subseteq \tilde{\xi}\mathfrak{C}_2$ which implies that $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \oplus \tilde{\xi}\mathfrak{C}_2^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1 \oplus \tilde{\xi}\mathfrak{C}_2$. Thus, $\langle (1-\tilde{\xi})g_1^*(\dagger) + \tilde{\xi}g_2^*(\dagger)\rangle \subseteq \langle (1-\tilde{\xi})g_1(\dagger) + \tilde{\xi}g_2(\dagger)\rangle$ and hence, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$.

Conversely, consider $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$, then $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \oplus \tilde{\xi}\mathfrak{C}_1^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1 \oplus \tilde{\xi}\mathfrak{C}_2$, that implies $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1$ and $\tilde{\xi}\mathfrak{C}_2^{\perp} \subseteq \tilde{\xi}\mathfrak{C}_2$. Hence $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1$ and $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_2$, and by Theorem 4.3, we have $\dagger^m + 1 \equiv 0 \bmod (g_1(\dagger)g_1^*(\dagger))$ for $\mathfrak{C}_1$ and $\dagger^m + 1 \equiv 0 \bmod (g_2(\dagger)g_2^*(\dagger))$ for $\mathfrak{C}_2$. □

Corollary 4.7. *For a $(\rho - 1 + 2\tilde{\xi})$-constacyclic code $\mathfrak{C} = (1-\tilde{\xi})\mathfrak{C}_1 \oplus \tilde{\xi}\mathfrak{C}_2$ where $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are linear codes. Then $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ if and only if $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1$ and $\mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_2$.*

Proof. As $\mathfrak{C}^{\perp} = (1-\tilde{\xi})\mathfrak{C}_1^{\perp} \oplus \tilde{\xi}\mathfrak{C}_1^{\perp}$, so, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ implies $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \oplus \tilde{\xi}\mathfrak{C}_1^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1 \oplus (\tilde{\xi})\mathfrak{C}_2$ and hence $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1$, $(\tilde{\xi})\mathfrak{C}_2^{\perp} \subseteq (\tilde{\xi})\mathfrak{C}_2$ which implies, $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1$, $\mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_2$.

Conversely, for $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1$, $\mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_2$ this $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1$, $(\tilde{\xi})\mathfrak{C}_2^{\perp} \subseteq (\tilde{\xi})\mathfrak{C}_2$ holds. So, $(1-\tilde{\xi})\mathfrak{C}_1^{\perp} \oplus (\tilde{\xi})\mathfrak{C}_2^{\perp} \subseteq (1-\tilde{\xi})\mathfrak{C}_1 \oplus (\tilde{\xi})\mathfrak{C}_2$ and therefore, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. □

Lemma 4.8 [2] (CSS Construction)**.** *Let $\mathfrak{C}$ be a linear code over Z_ρ having parameters $[m, k, d]$. Then, a quantum code with parameters $[m, 2k-m, \geq d]_\rho$ can be obtained if $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$.*

Construction of quantum codes is provided by using Lemma 4.8 and Corollary 4.7 as:

Theorem 4.9. *For a $(\rho - 1 + 2\tilde{\xi})$-constacyclic code $\mathfrak{C}$ there exists a quantum $[2m, 2k-2m, \geq d_L]_\rho$ code with dimension of $\psi(\mathfrak{C})$ is k and d_L is minimum Lee distance of linear code is $\mathfrak{C}$.*

5. Examples

Several examples are discussed in this section to illustrate the codes obtained through $(\rho - 1 + 2\tilde{\xi})$-constacyclic codes.

Example 5.1. In $Z_7(\dagger)$, $\dagger^9 - 1 = (\dagger - 1)(\dagger - 2)(\dagger - 4)(\dagger^3 - 2)(\dagger^3 - 4)$ and $\dagger^9 + 1 = (\dagger + 1)(\dagger + 2)(\dagger + 4)(\dagger^3 - 3)(\dagger^3 - 5)$. For a $\mathfrak{C}$ be a $(6 + 2\tilde{\xi})$-constacyclic codes over the ring R of length 9. Let $h_1(\dagger) = t^3 - 2$ and $h_1(\dagger) = t + 1$ then $h(\dagger) = (1-\tilde{\xi})(\dagger^3 - 2)) + \tilde{\xi}(\dagger + 1)$ is generator polynomial of $\mathfrak{C}$. Since $h_1(\dagger)h_1^*(\dagger) \mid \dagger^9 - 1$ and $h_2(\dagger)h_2^*(\dagger) \mid \dagger^9 + 1$, hen due to Theorem 4.6 $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. Further $\psi(\mathfrak{C})$ is a $[18, 14, 3]$ linear code. Theorem 4.9, implies that parameters of quantum code are $[18, 10, \geq 3]_7$.

Example 5.2. In $Z_7(\dagger)$, $\dagger^{20} - 1 = (\dagger - 1)(\dagger + 6)(\dagger^2 + 1)(\dagger^4 + \dagger^3 + \dagger^2 + \dagger + 1)$ $(\dagger^4 + 3\dagger^3 + 4\dagger^2 + 4\dagger + 1)(\dagger^4 + 4\dagger^3 + 4\dagger^2 + 3\dagger + 1)(\dagger^4 + 6\dagger^3 + \dagger^2 + 6\dagger + 1)\dagger^{20}$ and $+1 = (\dagger^2 + 3\dagger + 1)(\dagger^2 + 4\dagger + 1)(\dagger^4 + \dagger^3 + 6\dagger^2 + 3\dagger + 1)(\dagger^4 + 3\dagger^3 + 6\dagger^2 + \dagger + 1)$ $(\dagger^4 + 4\dagger^3 + 6\dagger^2 + 6\dagger + 1)(\dagger^4 + 6\dagger^3 + 6\dagger^2 + 4\dagger + 1)$. For a $6 + 2\tilde{\xi}$-constacyclic code $\mathfrak{C}$ over R with length 20.

Let $h_1(\dagger) = (\dagger + 6)$ and $h_2(\dagger) = (\dagger^2 + 3\dagger + 1)$, then $g(\dagger) = (1 + \tilde{\xi})(\dagger + 6)$ $(1 + \tilde{\xi})(\dagger^2 + 3\dagger + 1)$ is generator polynomial of $\mathfrak{C}$. Since $h_1(\dagger)h_1^*(\dagger) \mid \dagger^{20} - 1$ and $h_2(\dagger)h_2^*(\dagger) \mid \dagger^{20} - 1$, then due to Theorem 4.6, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. Further, $\Psi(\mathfrak{C})$ is a $[40, 37, 3]$ linear code. Theorem 4.9, implies that parameters of quantum code are $[40, 34, \geq 3]_7$.

Example 5.3. In $\mathbb{Z}_{11}(\dagger)$, $\dagger^{18} - 1 = (\dagger + 1)(\dagger + 10)(\dagger^2 + \dagger k + 1)(\dagger^2 + 10\dagger + \dagger 1)$ $(\dagger^6 + \dagger^3 + 1)(\dagger^6 + 10\dagger^3 + 1)$ and $\dagger^{18} + 1 = (\dagger^2 + 1)(\dagger^2 + 5\dagger + 1)(\dagger^2 + 6\dagger + 1)$ $(\dagger^6 + 5\dagger^3 + 1)(\dagger^6 + 6\dagger^3 + 1)$. For a $(10 + 2\tilde{\xi})$-constacyclic code $\mathfrak{C}$ over R with length 20.

Let $h_1(\dagger) = (\dagger^2 + 10\dagger + 1)$ and $h_2(\dagger) = (\dagger^2 + 6\dagger + 1)$, then $g(\dagger) = (1 + \tilde{\xi})(\dagger^2 + 10\dagger + 1) + (1 - \tilde{\xi})(\dagger^2 + 6\dagger + 1)$ is generator polynomial of $\mathfrak{C}$. Since $h_1(\dagger)h_1^*(\dagger) \mid \dagger^{18} - 1$ and $h_2(\dagger)h_2^*(\dagger) \mid \dagger^{18} + 1$, then due to Theorem 4.6, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. Further, $\Psi(\mathfrak{C})$ is a $[36, 32, 3]$ linear code. Theorem 4.9, implies that parameters of quantum code are $[36, 28, \geq 3]_{11}$.

Example 5.4. In $\mathbb{Z}_{11}(\dagger)$, $\dagger^{18} - 1 = (\dagger - 1)(\dagger + 10)(\dagger^2 + \dagger + 1)(\dagger^2 + 10\dagger + 1)$ $(\dagger^2 + \dagger^3 + 1)(\dagger^6 + 10\dagger^3 + 1)$ and $\dagger^{18} + 1 = (\dagger^2 + 1)(\dagger^2 + 5\dagger + 1)(\dagger^2 + 6\dagger + 1)$ $(\dagger^2 + 5\dagger^3 + 1)(\dagger^6 + 6\dagger^3 + 1)$. For a $(10 + 2\tilde{\xi})$-constacyclic code $\mathfrak{C}$ over R with length 20.

Let $h_1(\dagger) = (\dagger^6 + \dagger^3 + 1)$ and $h_2(\dagger) = (\dagger^2 + 1)$, then $g(\dagger) = (1 + \tilde{\xi})(\dagger^6 + \dagger^3 + 1)$ $+ (1 - \tilde{\xi})(\dagger^2 + 1)$ is generator polynomial of $\mathfrak{C}$. Since $h_1(\dagger)h_1^*(\dagger) \mid \dagger^{18} - 1$ and

$h_2(\dagger)h_2^*(\dagger) \mid \dagger^{18}+1$ then due to Theorem 4.6, $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. Further, $\Psi(\mathfrak{C})$ is a $[36, 28, 4]$ linear code. Theorem 4.9, implies that parameters of quantum code are $[36, 20, \geq 4]_{11}$.

References

[1] A. M. Steane, Simple quantum error-correcting codes, Phys. Rev. A 54(6) (1996), 4741.

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

[3] J. Gao and Y. Wang, u-Constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and their applications of constructing new non-binary quantum codes, Quantum Inf. Process 17(122) (2018), 1-19.

[4] J. Qian, Quantum codes from cyclic codes over $F_2 + vF_2$, J. Inf. Comput. Sci. 10(6) (2013), 1715-1722.

[5] J. Qian, W. Ma and W. Guo, Quantum codes from cyclic codes over finite ring, Int. J. Quantum Inf. 7(06) (2009), 1277-1283.

[6] M. Ashraf and G. Mohammad, Construction of quantum codes from cyclic codes over $F_p + vF_p$, Int. J. Inf. Coding Theory 3(2) (2015), 137-144.

[7] M. Ashraf and G. Mohammad, Quantum codes from cyclic codes over $F_3 + vF_3$, Int. J. Quantum Inf. 12(06) (2014), 1450042.

[8] M. Ashraf and G. Mohammad, Quantum codes over F_p from cyclic codes over $F_p[u, v]/\langle u^2 - 1, v^3 - v, uv - vu\rangle$, Cryptogr. Commun. 11 (2019), 325-335.

[9] R. Li and Z. Xu, Construction of $[n, n-4, 3]_q$ quantum codes for odd prime power q, Phys. Rev. A 82(5) (2010), 052316.

[10] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, On quantum and classical BCH codes, IEEE Trans. Inf. Theory 53(3) (2007), 1183-1188.

[11] S. Zhu and L. Wang, A class of constacyclic codes over $F_p + vF_p$, and its Gray image, Discrete Math. 311(23-24) (2011), 2677-2682.

[12] Y. Liu, R. Li, L. Lv et al., A class of constacyclic BCH codes and new quantum codes, Quantum Inf. Process 16(66) (2017).

[13] X. Kai and S. Zhu, Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$, Int. J. Quantum Inf. 9(02) (2011), 689-700.