Available online at http://scik.org
J. Math. Comput. Sci. 11 (2021), No. 3, 2583-2592
https://doi.org/10.28919/jmcs/5593
ISSN: 1927-5307

QUANTUM CODES OBTAINED THROUGH $(1+(p-2)v)$-CONSTACYCLIC CODES OVER Z_p+vZ_p

JAGBIR SINGH[1], PRATEEK MOR[2,*]

[1]Department of Mathematics, Maharshi Dayanand University, Rohtak-124001, India

[2]Department of Mathematics, Government College Matanhail, Jhajjar-124103, India

Abstract. This paper is concerned with, structural properties and construction of quantum codes over Z_p by using $(1+(p-2)v)$-Constacyclic codes over the finite commutative non-chain ring $\Re = Z_p+vZ_p$ where $v^2=v$ and Z_p is field having p elements with characteristic p where p is prime. A Gray map is defined between $\Re$ and Z_p^2. The parameters of quantum codes over Z_p are obtained by decomposing $(1+(p-2)v)$-constacyclic codes into cyclic and negacyclic codes over Z_p. As an application, some examples of quantum codes of arbitrary length, are also obtained.

Keywords: cyclic codes; constacyclic codes; negacyclic; quantum codes.

2010 AMS Subject Classification: 94B05, 94B15.

1. Introduction

There has been an enormous development in the research on quantum codes. As the disclosure that quantum codes secure quantum information similar to classical codes classic information. Quantum information can propagate faster than light under certain conditions, while classical information cannot. Quantum information can't be duplicated but classical information can be. Quantum codes provide the most efficient way to overcome decoherence. The

*Corresponding author

E-mail address: prateekmor1992@gmail.com

Received Feburary 23, 2021

first quantum code was found by Shor [7]. From then on, the construction of quantum codes through classical cyclic codes and their generalizations haRs developed rapidly. Quantum codes attracted world wide attention therefore. Later on, Calderbank et al. [1] gave a technique to build quantum codes through classical codes in 1998. Recently the theory of quantum codes is on the path of everlasting development. In recent years, the theory of quantum code has been developed rapidly (see reference [4, 8, 9]).

A significant development in the construction of quantum codes through cyclic codes over finite chain ring F_2+uF_2 where $u^2=0$ of odd length was made by Qian [2]. Kai and Zhu [10] also gave a method to construct quantum codes through cyclic codes over finite chain ring F_4+uF_4 where $u^2=0$ of odd length. Qian [3] studied quantum codes of arbitrary length through cyclic codes over finite non-chain ring F_2+vF_2 where $v^2=v$. Recently, Ashraf and Mohammad [5] defined the construction of quantum codes through cyclic codes over finite non-chain ring F_3+vF_3 where $v^2=1$. Then in [6] Ashraf and Mohammad studied this topic over the different finite non-chain ring F_q+vF_q where $v^2=v$. In this paper, encouraged by these type of problems, we study quantum codes through $(1+(p-2)v)$-constacyclic codes over finite non-chain ring Z_p+vZ_p where $v^2=v$.

This paper is structured as follows. Section 2 contains preliminaries that deal with some basic properties of the considered ring and some basic definitions. In section 3, Gray Map is defined over the considered ring and the construction of quantum codes through constacyclic codes over the considered ring are given. Some examples are provided to illustrate the main result in section 4. Finally, paper is concluded in section 5.

2. PRELIMINARIES

Let Z_p is a finite filed having p elements for some odd prime p. We first start with a general overview of the ring $\mathfrak{R}=Z_p+vZ_p$ where $v^2=v$, $\mathfrak{R}$ is a finite, commutative and non-chain, semi-local ring with p^2 elements. One of the Unit of $\mathfrak{R}$ is $(1+(p-2)v)$. The considered ring $\mathfrak{R}$ has two maximal ideals which are $<v>$ and $<1-v>$. Since, it is clear that $\mathfrak{R}/<v>$, $\mathfrak{R}/<1-v>$ both are isomorphic to Z_p.

Now by chinese remainder theorem, the considered ring can be expressed as $\mathfrak{R}\cong <v>\oplus<1-v>\cong Z_p\oplus Z_p$. Therefore, an arbitrary element $\alpha+v\ \beta$ of the considered ring can be written as $(\alpha+\beta)\ (\nu)+(\alpha)(1-\nu)$ for all $\alpha,\beta \in Z_p$.

A nonempty subset $\mathscr{K}$ of $\Re^n$ is a linear code over $\Re$ of length n. If $\mathscr{K}$ is an $\Re$-submodule of $\Re^n$ and the elements of $\mathscr{K}$ are codewords. Let Υ, Λ and $\mho$ are the maps from $\Re^n$ to $\Re^n$ defined as

$$\Upsilon(\chi_0,\chi_1,...,\chi_{n-1}) = (\chi_{n-1},\chi_0,...,\chi_{n-2}),$$

$$\Lambda(\chi_0,\chi_1,...,\chi_{n-1}) = (-\chi_{n-1},\chi_0,...,\chi_{n-2}),$$

$$\mho(\chi_0,\chi_1,...,\chi_{n-1}) = ((1+(p-2)\nu)\chi_{n-1},\chi_0,...,\chi_{n-2}),$$

respectively. Then $\mathscr{K}$ is a cyclic, negacyclic, $(1+(p-2)\nu)$-constacyclic if $\Upsilon(\mathscr{K}) = \mathscr{K}$, $\Lambda(\mathscr{K}) = \mathscr{K}$, $\mho(\mathscr{K}) = \mathscr{K}$ respectively. For the arbitrary elements $\chi = (\chi_0,\chi_1,...,\chi_{n-1})$ and $\psi = (\psi_0,\psi_1,...,\psi_{n-1})$ of $\Re$, the inner product is defined as

$$\chi.\psi = (\chi_0\psi_0+\chi_1\psi_1+...+\chi_{n-1}\psi_{n-1}).$$

If $\chi.\psi = 0$, then χ and ψ are orthogonal. If $\mathscr{K}$ is a linear code over $\Re$ of length n, then the dual code of $\mathscr{K}$ is defined as

$$\mathscr{K}^{\perp} = \{\ \chi\ \in\ \Re^n:\ \chi.\psi = 0\ for\ all\ \psi \in \mathscr{K}\}.$$

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

The hamming weight $w_H(\chi)$ for any codeword $\chi = (\chi_0,\chi_1,...,\chi_{n-1}) \in \Re^n$ is defined as the number of all non-zero components in $\chi = (\chi_0,\chi_1,...,\chi_{n-1})$. The minimum weight of a code $\mathscr{K}$, that is, $w_H(\mathscr{K})$ is the least weight among all of its non zero codewords. The Hamming distance between two codes $\chi = (\chi_0,\chi_1,...,\chi_{n-1})$ and $\psi = (\psi_0,\psi_1,...,\psi_{n-1})$ of $\Re^n$, denoted by $d_H(\chi,\psi) = w_H(\chi-\psi)$ and is defined as

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

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

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

3. Quantum Codes Obtained through $(1+(p-2)\nu)$-Constacyclic Codes over $\mathfrak{R}$

The Gray map φ from $\mathfrak{R}$ to Z_p^2, that is, φ: $\mathfrak{R} \to Z_p^2$ is defined as

$$\varphi(w = w_1 + \nu w_2) = (w_1, w_1 + w_2)$$

This map can be extended to $\mathfrak{R}^n$, that is φ: $\mathfrak{R}^n \to Z_p^{2n}$ as

$$\varphi(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_{n-1}) \ = \ (w_1, w_1 + \dot{w_1}, w_2, w_2 + \dot{w_2}, ..., w_{n-1}, w_{n-1} + \dot{w_{n-1}})$$

where $\alpha_i = w_i + \nu \dot{w_i}$ for all $0 \le i \le n-1$.

It is obvious that, the map φ is linear and distance preserving isometry from $(\mathfrak{R}^n, d_L)$ to (Z_p^{2n}, d_H), where d_L and d_H are the lee distance and hamming distance in $\mathfrak{R}^n$ and Z_p^{2n} respectively.

For a linear code $\mathscr{K}$ of length n over $\mathfrak{R}$, we characterize

$$\mathscr{K}_\infty \ = \ \{a \ \in \ Z_p^n | \ for\ some\ b \ \in \ Z_p^n\ such\ that\ (a + \nu b) \ \in \ \mathscr{K}\}$$

$$\mathscr{K}_\in \ = \ \{a + b \ \in \ Z_p^n | \ such\ that\ (a + \nu b) \ \in \ \mathscr{K}\}$$

are 2 p-ary codes such that

$$(1-\nu)\ \mathscr{K}_\infty \ = \ \mathscr{K}\ mod\ \nu$$

and

$$\nu\ \mathscr{K}_\in \ = \ \mathscr{K}\ mod\ (1-\nu).$$

Therefore, $\mathscr{K}_\infty$ and $\mathscr{K}_\in$ are linear codes over the ring Z_p of length n. Moreover, the linear code $\mathscr{K}$ can be uniquely expressed as

$$\mathscr{K} \ = \ (1-\nu)\ \mathscr{K}_\infty \oplus \nu\ \mathscr{K}_\in$$

and also $|\mathscr{K}| = |\mathscr{K}_\infty||\mathscr{K}_\in|$.

The following proposition can be obtained directly by the above defined Gray map φ.

Proposition 3.1. *Let $\mathscr{K}$ be a linear code over the ring $\mathfrak{R}$ of length n. If $\mathscr{K}$ is self orthogonal, then $\varphi(\mathscr{K})$ is also self orthogonal.*

Proof. Let $\mathscr{K}$ be a self orthogonal code and $\eta_1,\eta_2 \in \mathscr{K}$ such that $\eta_1 = \xi_1 + \nu\varpi_1$ and $\eta_2 = \xi_2 + \nu\varpi_2$ where $\xi_1,\xi_2,\varpi_1,\varpi_2 \in Z_p$. From the definition of self orthogonality, $\eta_1.\eta_2 = 0$, that is, $\xi_1\xi_2 + \nu(\xi_1\varpi_2 + \xi_2\varpi_1 + \varpi_1\varpi_2) = 0$, it follow that $\xi_1\xi_2 = \xi_1\varpi_2 + \xi_2\varpi_1 + \varpi_1\varpi_2 = 0$. Now, applying φ on η_1,η_2 we have $\varphi(\eta_1) = (\xi_1,\xi_1+\varpi_1)$ and $\varphi(\eta_2) = (\xi_2,\xi_2+\varpi_2)$ and hence $\varphi(\eta_1).\varphi(\eta_2) = 2\xi_1\xi_2 + \xi_1\varpi_2 + \xi_2\varpi_1 + \varpi_1\varpi_2 = 0$ this implies $\varphi(\mathscr{K})$ is self orthogonal. □

Proposition 3.2. *Let $\mathscr{K} = (1+\nu)\mathscr{K}_\infty \oplus \nu\mathscr{K}_\in$ be a linear code over the ring $\Re$ of length n such that $\mathscr{K}_\infty$ be a linear code having parameters $[n,\ k_1,\ d_1]$ and $\mathscr{K}_\in$ be a linear code having parameters $[n,\ k_2,\ d_2]$. Then $\varphi(\mathscr{K})$ is a q-ary linear code having parameters $[2n,\ k_1+k_2,\ min(d_1,d_2)]$.*

Lemma 3.3. *Let $\mathscr{K} = (1-\nu)\mathscr{K}_\infty \oplus \nu\mathscr{K}_\in$ be linear code over the ring $\Re$ of length n where $\mathscr{K}_\infty$, $\mathscr{K}_\in$, are linear codes over the ring Z_p. Then $\mathscr{K}$ is a $(1+(p-2)\nu)$-constacyclic codes over the ring $\Re$ of length n if and only if $\mathscr{K}_\infty$ is Cyclic code and $\mathscr{K}_\in$ is negaacyclic code over the ring Z_p of length n.*

Proof. Let $\dot{a} = (\dot{a_0},\dot{a_1},...,\dot{a_{n-1}}) \in \mathscr{K}_\infty$ and $\dot{b} = (\dot{b_0},\dot{b_1},...,\dot{b_{n-1}}) \in \mathscr{K}_\in$. For an arbitrary element $\zeta_i = (1-\nu)\dot{a}_i + \nu\dot{b}_i$ where $\dot{a}_i,\dot{b}_i \in Z_p$ for $i = 0,1,...,n-1$.
Let $\zeta = (\zeta_0,\zeta_1,...,\zeta_{n-1}) \in \mathscr{K}$.
First we assume that $\mathscr{K}$ is a $(1+(p-2)\nu)$-constacyclic code over the ring $\Re$ of length n then,

$$\begin{aligned}
\mho(\zeta) &= ((1+(p-2)\nu)\zeta_{n-1},\zeta_0,...,\zeta_{n-2}) \\
&= ((1-\nu)\dot{a_{n-1}} - (\nu)\dot{b_{n-1}},(1-\nu)\dot{a_0} + (\nu)\dot{b_0},...,(1-\nu)\dot{a_{n-2}} + (\nu)\dot{b_{n-2}}) \\
&= (1-\nu)\Upsilon(\dot{a}) + (\nu)\Lambda(\dot{b})
\end{aligned}$$

which is an element of the linear code $\mathscr{K}$. Therefore, $\mathscr{K}_\infty$ is a cyclic and $\mathscr{K}_\in$ is a negacyclic codes over the ring Z_p of length n.
Conversely, for any $\zeta = (\zeta_0,\zeta_1,...,\zeta_{n-1}) \in \mathscr{K}$, where $\zeta_i = (1-\nu)\dot{a}_i+(\nu)\dot{b}_i$ and $\dot{a}_i,\dot{b}_i \in Z_p$ for $i = 0,1,...,n-1$. If $\mathscr{K}_\infty$ is a cyclic codes and $\mathscr{K}_\in$ is a negacyclic codes over the ring Z_p of length n, then $\Upsilon(\dot{a}) \in \mathscr{K}_\infty$ and $\Lambda(\dot{b}) \in \mathscr{K}_\in$. Hence, we have $(1-\nu)\Upsilon(\dot{a}) + (\nu)\Lambda(\dot{b}) \in \mathscr{K}$ where $\mho(\zeta) = (1-\nu)\Upsilon(\dot{a}) + (\nu)\Lambda(\dot{b})$, which implies that $\mho(\zeta) \in \mathscr{K}$.
Therefore, $\mathscr{K}$ is a $(1+(p-2)\nu)$-constacyclic codes over the ring $\Re$ of length n. □

The following lemma is similar to Theorem **4.2** [11].

Lemma 3.4. *Let $\mathscr{K}$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R}$ of length n. Then*

$$\mathscr{K} = <(1-\nu)g_1(x), \nu g_2(x)> = <(1-\nu)g_1(x)+\nu g_2(x)>$$

with $|\mathscr{K}| = p^{2n-deg(g_1(x))-deg(g_2(x))}$

where $g_i(x)$ for $i=1,2$ are the generator polynomials of $\mathscr{K}_\infty$ and $\mathscr{K}_\in$ respectively.
Moreover $\mathscr{K}^\perp = (1-\nu)\mathscr{K}_\infty^\perp \oplus \nu\mathscr{K}_\in^\perp$ is also $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R}$ of length n and

$$\mathscr{K}^\perp = <(1-\nu)g_1^\star(x), \nu g_2^\star(x)> = <(1-\nu)g_1^\star(x)+\nu g_2^\star(x)>$$

with $|\mathscr{K}\perp| = p^{deg(g_1(x))+deg(g_2(x))}$
where $g_i^\star(x)$ for $i=1,2$ are reciprocal polynomials of $\frac{x^n+1}{g_1(x)}$ and $\frac{x^n-1}{g_2(x)}$ respectively.

Lemma 3.5. [1] *If $\mathscr{K}$ is a cyclic or negacyclic code over the ring Z_q with generator polynomial g(x). Then, $\mathscr{K}$ contains its dual code if and only if $x^n - \iota \equiv 0 \ mod(g(x)g^\star(x))$, where $\iota = \pm 1$*

Theorem 3.6. *If $\mathscr{K} = <(1-\nu)g_1(x), \nu g_2(x)>$ is a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R}$ of length n. Then $\mathscr{K}^\perp \subseteq \mathscr{K}$ if and only if $x^n-1 \equiv 0 \ mod(g_1(x)g_1^\star(x))$ for $\mathscr{K}_\infty$ and $x^n+1 \equiv 0 \ mod(g_2(x)g_2^\star(x))$ for $\mathscr{K}_\in$.*

Proof. Let $\mathscr{K} = <g(x)> = <(1-\nu)g_1(x)+\nu g_2(x)>$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R}$ of length n. Then $\mathscr{K} = (1-\nu)\mathscr{K}_\infty \oplus \nu\mathscr{K}_\in$ where $g_i(x)$ are generator polynomial of $\mathscr{K}_\infty$ and $\mathscr{K}_\in$ for $i=1,2$ respectively.
First we consider $x^n-1 \equiv 0 \ mod(g_1(x)g_1^\star(x))$ for $\mathscr{K}_\infty$ and $x^n+1 \equiv 0 \ mod(g_2(x)g_2^\star(x))$ for $\mathscr{K}_\in$ respectively, then by above lemma, we have

$$\mathscr{K}_\infty^\perp \subseteq \mathscr{K}_\infty \text{ and } \mathscr{K}_\in^\perp \subseteq \mathscr{K}_\in$$

and therefore $(1-\nu)\mathscr{K}_\infty^\perp \subseteq (1-\nu)\mathscr{K}_\infty$ and $\nu\mathscr{K}_\in^\perp \subseteq \nu\mathscr{K}_\in$ which implies that

$$(1-\nu)\mathscr{K}_\infty^\perp \oplus \nu\mathscr{K}_\in^\perp \subseteq (1-\nu)\mathscr{K}_\infty \oplus \nu\mathscr{K}_\in$$

Thus, we have $<(1-\nu)g_1^\star(x)+\nu g_2^\star(x)> \subseteq <(1-\nu)g_1(x)+\nu g_2(x)>$
and hence, $\mathscr{K}^\perp \subseteq \mathscr{K}$.

Conversely, let us consider $\mathscr{K}^{\perp} \subseteq \mathscr{K}$, then

$$(1-\nu)\mathscr{K}_{\infty}^{\perp} \oplus \nu\mathscr{K}_{\in}^{\perp} \subseteq (1-\nu)\mathscr{K}_{\infty} \oplus \nu\mathscr{K}_{\in},$$

which implies that

$$(1-\nu)\mathscr{K}_{\infty}^{\perp} \subseteq (1-\nu)\mathscr{K}_{\infty} \text{ and } \nu\mathscr{K}_{\in}^{\perp} \subseteq \nu\mathscr{K}_{\in},$$

hence

$$\mathscr{K}_{\infty}^{\perp} \subseteq \mathscr{K}_{\infty} \text{ and } \mathscr{K}_{\in}^{\perp} \subseteq \mathscr{K}_{\in},$$

therefore we have

$x^n - 1 \equiv 0 \; mod(g_1(x)g_1^{\star}(x))$ for $\mathscr{K}_{\infty}$ and $x^n + 1 \equiv 0 \; mod(g_2(x)g_2^{\star}(x))$ for $\mathscr{K}_{\in}$. □

By the above Theorem, we have the following corollary.

Corollary 3.7. *Let $\mathscr{K} = (1-\nu)\mathscr{K}_{\infty} \oplus \nu\mathscr{K}_{\in}$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\Re$ of length n where $\mathscr{K}_{\infty}$, $\mathscr{K}_{\in}$ are linear code over the ring Z_p of length n. Then $\mathscr{K}^{\perp} \subseteq \mathscr{K}$ if and only if $\mathscr{K}_{\infty}^{\perp} \subseteq \mathscr{K}_{\infty}$ and $\mathscr{K}_{\in}^{\perp} \subseteq \mathscr{K}_{\in}$.*

Lemma 3.8. [1]*(CSS Construction). Let $\mathscr{K}$ be a linear code over the ring Z_p having parameters [n,k,d]. Then a quantum code having parameter $[n,\ 2k-n,\ \geq d]_p$ can be obtained if $\mathscr{K}^{\perp} \subseteq \mathscr{K}$.*

The following theorem defines the construction of quantum codes by the use of Corollary 3.7 and Lemma 3.8.

Theorem 3.9. *If $\mathscr{K} = (1-\nu)\mathscr{K}_{\infty} \oplus \nu\mathscr{K}_{\in} = \,<(1-\nu)g_1(x)+\nu g_2(x)>$ is a $(1+(p-2)\nu)$-constacyclic codes over the ring $\Re$ of length n where $g_i(x)$ are generator polynomials of $\mathscr{K}_{\infty}$ and $\mathscr{K}_{\in}$ for $i=1,2$ respectively. If $\mathscr{K}_{\infty}^{\perp} \subseteq \mathscr{K}_{\infty}$ and $\mathscr{K}_{\in}^{\perp} \subseteq \mathscr{K}_{\in}$ then $\mathscr{K}^{\perp} \subseteq \mathscr{K}$ and there exists a quantum code having parameters $[2n, 2k-2n, \geq d_L]_p$ where k is the dimension of linear code $\varphi(\mathscr{K})$ and d_L is minimum Lee distance of $\mathscr{K}$.*

4. EXAMPLES

In this section, some examples are provided to illustrate the main result. Here, the quantum codes through $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R} = Z_p + \nu Z_p$ where $\nu^2 = \nu$ are also obtained.

Example 4.1. *In $Z_5(t)$, $t^{10}-1 = (t+4)^5(t+1)^5$ and $t^{10}+1 = (t+2)^5(t+3)^5$. Now, let $\mathscr{K}$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R} = Z_5+\nu Z_5$ where $\nu^2 = \nu$ of length 10. Let $g_1(t) = t+1$, $g_2(t) = t+2$, then $g(t) = (1-\nu)(t+1)+\nu(t+2)$ be the generator polynomial of $\mathscr{K}$. Since $g_1(t)g_1^*(t)|t^{10}-1$, $g_2(t)g_2^*(t)|t^{10}+1$ then by the use of Theorem 3.6, we get $\mathscr{K}^\perp \subseteq \mathscr{K}$ Further $\varphi(\mathscr{K})$ is a linear code over the ring Z_5 having parameters* $[20,\ 18,\ 2]$. *Then, by the application of Theorem 3.9, we obtain the quantum codes having parameters* $[20,\ 16,\ \geq 2]_5$.

Example 4.2. *In $Z_5(t)$, $t^{20}-1 = (t-4)^5(t-2)^5(t-3)^5(t-1)^5$ and $t^{20}+1 = (t^2-3)^5(t^2-2)^5$. Now, let $\mathscr{K}$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R} = Z_5+\nu Z_5$ where $\nu^2 = \nu$ of length 20. Let $g_1(t) = (t-3)^2$ and $g_2(t) = (t^2-3)$ then $g(t) = (1-\nu)(t-3)^2+\nu(t^2-3)$ be the generator polynomial of $\mathscr{K}$. Since $g_1(t)g_1^*(t)|t^{20}-1$, $g_2(t)g_2^*(t)|t^{20}+1$ then by the use of Theorem 3.6, we get $\mathscr{K}^\perp \subseteq \mathscr{K}$ Further $\varphi(\mathscr{K})$ is a linear code over the ring Z_5 having parameters* $[40,\ 36,\ 3]$. *Then, by the application of Theorem 3.9, we obtain the quantum codes having parameters* $[40,\ 32,\ \geq 3]_5$.

Example 4.3. *In $Z_3(t)$, $t^3-1 = (t+2)^3$ and $t^3+1 = (t+1)(t^2-t+1)$. Now, let $\mathscr{K}$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R} = Z_3+\nu Z_3$ where $\nu^2 = \nu$ of length 3. Let $g_1(t) = t+2$ and $g_2(t) = t^2-t+1$ then $g(t) = (1-\nu)(t+2)+\nu(t^2-t+1)$ be the generator polynomial of $\mathscr{K}$. Since $g_1(t)g_1^*(t)|t^3-1$, $g_2(t)g_2^*(t)|t^3+1$ then by the use of Theorem 3.6, we get $\mathscr{K}^\perp \subseteq \mathscr{K}$ Further $\varphi(\mathscr{K})$ is a linear code over the ring Z_3 having parameters* $[6,\ 3,\ 3]$. *Then, by the application of Theorem 3.9, we obtain the quantum codes having parameters* $[6,\ 0,\ \geq 3]_3$.

Example 4.4. *In $Z_3(t)$, $t^{12}-1 = (t+1)^3(t+2)^3(t^2+1)^3$ and $t^{12}+1 = (t^2+2t+2)^3(t^2+t+2)^3$. Now, let $\mathscr{K}$ be a $(1+(p-2)\nu)$-constacyclic codes over the ring $\mathfrak{R} = Z_3+\nu Z_3$ where $\nu^2 = \nu$ of length 12. Let $g_1(t) = t+1$ and $g_2(t) = t^2+2t+2$, $g(t) = (1-\nu)(t+1)+\nu(t^2+2t+2)$*

be the generator polynomial of $\mathscr{K}$. *Since* $g_1(t)g_1^*(t)|t^{12}-1$, $g_2(t)g_2^*(t)|t^{12}+1$ *then by the use of Theorem 3.6, we get* $\mathscr{K}^\perp \subseteq \mathscr{K}$ *Further* $\varphi(\mathscr{K})$ *is a linear code over the ring* Z_3 *having parameters* $[24,\ 21,\ 3]$. *Then, by the application of Theorem 3.9, we obtain the quantum codes having parameters* $[24,\ 18,\ \geq 3]_3$.

5. CONCLUSION

In this work, we have given a construction for quantum codes through $(1+(p-2)\nu)$-constacyclic codes over the finite non-chain ring $\mathfrak{R} = Z_p + \nu Z_p$ where $\nu^2 = \nu$. We have derived self-orthogonal codes over the ring Z_p as Gray images of linear codes over the ring $Z_p + \nu Z_p$. In particular, the parameters of quantum codes over the ring Z_p are obtained by decomposing $(1+(p-2)\nu)$-constacyclic codes into cyclic and negacyclic codes over the ring Z_p.

CONFLICT OF INTERESTS

The author(s) declare that there is no conflict of interests.

REFERENCES

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

[2] J. Qian, W. Ma, W. Guo, Quantum codes from cyclic codes over finite ring, Int. J. Quant. Inform. 7 (2009), 1277-1283.

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

[4] K. Feng, S. Ling, C. Xing, Asymptotic bounds on quantum codes from algebraic geometry codes, IEEE Trans. Inform. Theory. 52 (2006), 986–991.

[5] M. Ashraf, G. Mohammad, Quantum codes from cyclic codes $F_3 + vF_3$, Int. J. Quant. Inform. 12 (2014), 1450042 .

[6] M. Ashraf, G. Mohammad, Construction of quantum codes from cyclic codes over $F_p + vF_p$, Int. J. Inform. Coding Theory, 3(2) (2015), 137-146.

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

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

[9] S.A. Aly, A. Klappenecker, P.K. Sarvepalli, On Quantum and Classical BCH Codes, IEEE Trans. Inform. Theory. 53 (2007), 1183–1188.

[10] X. Kai, S. Zhu, Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$, Int. J. Quant. Inform. 9 (2011), 689- 700.

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