Indian J. Pure Appl. Math., **51**(1): 265-275, March 2020

DOI: 10.1007/s13226-020-0399-3

APPLICATION OF CONSTACYCLIC CODES OVER THE SEMI LOCAL RING $F_{p^m} + vF_{p^m}$

Tushar Bag*, Abdullah Dertli**, Yasemin Cengellenmis*** and Ashish K. Upadhyay*

**Department of Mathematics, Indian Institute of Technology Patna,*
Patna 801 103, *India*

***Mathematics Department, Ondokuz Mayis University, Faculty of Arts and Sciences,*
Samsun, Turkey

****Mathematics Department, Trakya University, Faculty of Sciences,*
Edirne, Turkey

e-mails: tushar.pma16@iitp.ac.in; abdullah.dertli@gmail.com;
ycengellenmis@gmail.com; upadhyay@iitp.ac.in

(*Received* 31 *July* 2018, *accepted* 24 *January* 2019)

In this paper, we study the quantum codes over F_{p^m}, which are obtained from $(\lambda_1 + v\lambda_2)$-constacyclic codes over the semi local ring $F_{p^m} + vF_{p^m}$, where $v^2 = 1$, p is odd prime. We decompose a $(\lambda_1 + v\lambda_2)$-constacyclic code over $F_{p^m} + vF_{p^m}$ into two constacyclic codes over F_{p^m} such as $(\lambda_1 + \lambda_2)$-constacyclic and $(\lambda_1 - \lambda_2)$-constacyclic. We give the necessary and sufficient condition that the $(\lambda_1 + v\lambda_2)$-constacyclic codes over $F_{p^m} + vF_{p^m}$ contain their duals. We give some examples of non binary quantum codes.

Key words : Gray map; cyclic code; negacyclic code; constacyclic codes; quantum codes.

2010 Mathematics Subject Classification : 94B05, 94B15, 94B60

1. Introduction

The class of constacyclic codes, which have two subclasses such as negacyclic and cyclic is very important subject in coding theory. As the constacyclic codes can be encoded with shift register, they have practical applications.

The area of the other application is the theory of the quantum error-correcting codes. Someone can derive quantum error-correcting codes over the finite fields by using the CSS quantum error-correcting code construction and constacyclic codes. It is known that errors prompted by inevitable interaction with environments - such as decoherence, quantum noise and other inaccuracies are among the prominent impediments leading to erroneousness in quantum information. Quantum error-correcting codes secures the quantum information from being exploited by such inaccuracy. Chronologically speaking, the first quantum error-correcting code was studied by Shor [17] in 1995. A year later, Steane [5] studied some important properties of quantum error-correcting codes. However, it was in the year 1998, when Calderbank *et al*. [6] showed his pioneer steps of constructing quantum error-correcting codes from the classical error-correcting codes over $GF(4)$. This paper gave a massive headway in the researches to the theory of quantum error-correcting codes.

Many good quantum codes had been constructed by using classical linear codes by using this construction. Recently, some authors have constructed quantum codes by using the linear codes over finite rings. For example, Qian [9] studied a construction of quantum error-correcting codes from cyclic codes over the finite non-chain ring $F_2 + vF_2, v^2 = v$. Motivated by this study, Ashraf and Mohammad [12, 14, 15] constructed quantum codes from cyclic codes over the ring $F_3 + vF_3$ with $v^2 = 1$ and then generalized the results over the ring $F_p + vF_p$ with $v^2 = v$. In the last few years, algebraic coding theorists [1-4, 16, 18] have studied quantum error-correcting codes over various finite rings. Recently quantum codes are being constructed from constacyclic codes, which are important generalization of cyclic codes. Also, [7, 10, 11, 19] have studied quantum MDS codes with the help of constacyclic codes and BCH like constacyclic codes. Very recently, Gao and Yang [8] have studied non-binary quantum codes using u-constacyclic codes over $F_p + uF_p$ with $u^2 = 1$.

Motivated by the above work, in this paper, we attempt to compute quantum codes using $(\lambda_1 + v\lambda_2)$-constacyclic code over the ring $F_{p^m} + vF_{p^m}$, where $v^2 = 1$ for odd prime p. This paper is organized as follows, in Section 3, we have discussed about the results based on the construction of Gray map and linear codes over this ring $F_{p^m} + vF_{p^m}$. In Section 4, we have studied the results of $(\lambda_1 + v\lambda_2)$-constacyclic codes over F_{p^m} and their duals. In Section 5, results for finding quantum codes over this ring have been presented and worked out examples have been shown.

2. Preliminaries

Let R be the ring $F_{p^m} + vF_{p^m}$, with $v^2 = 1$ and odd prime p. This is a commutative, semi-local ring with two maximal ideals $\langle 1+v\rangle$ and $\langle 1-v\rangle$. Both $R/\langle 1+v\rangle$ and $R/\langle 1-v\rangle$ are isomorphic to F_{p^m}.

A linear code C of length n over R is a R-submodule of R^n. An element $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is called a codeword. A linear code C of length n over R is said to be a λ-constacyclic code if and only if C is invariant under the constacyclic shift operator $\rho_\lambda : R^n \mapsto R^n$ defined by

$\rho_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2})$. Note that a constacyclic code is a cyclic code for $\lambda = 1$ and negacyclic code for $\lambda = -1$. By identifying each codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ to a polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ in $R[x]/\langle x^n - \lambda\rangle$, a linear code C is a λ-constacyclic code of length n over R if and only if it is an ideal of the ring $R[x]/\langle x^n - \lambda\rangle$.

Let $a \in F_{p^m}^{kn}$ with $a = (a^1|a^2|\ldots|a^{k-1}|a^k)$, where $a^i \in F_{p^m}^n$ for $i = 1, \ldots, k$. Let η_k be a map from $F_{p^m}^{kn}$ to $F_{p^m}^{kn}$ defined by $\eta_k(a) = (\rho(a^1)|\ldots|\rho(a^k))$, where ρ be the cyclic shift from $F_{p^m}^n$ to $F_{p^m}^n$ and $'\ |'$ is the usual vector concatenation. A code of length kn over F_{p^m} is called a quasi cyclic code of index k if $\eta_k(C) = C$.

Let $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ be two elements of R^n. Then the Euclidean inner product of x and y is defined as $x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in R^n |\ x \cdot y = 0,\ \text{for all } y \in C\}$. A code C is called self-orthogonal if $C \subseteq C^\perp$ and self dual if $C = C^\perp$.

The reciprocal of a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is defined as $f^*(x) = x^{deg(f(x))}f(x^{-1})$. A polynomial $f(x)$ is called self-reciprocal if $f(x) = f^*(x)$.

A matrix is called generator matrix of C if the rows of that matrix generates C.

By [13], any code C over R is permutation equivalent to a code with a generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & (1-v)B_1 & (1+v)A_1 & (1+v)A_2 + (1-v)B_2 & (1+v)A_3 + (1-v)B_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)B_4 \end{pmatrix},$$

where A_i and B_j are matrices with $1 \le i,\ j \le 4$ and all entries from F_{p^m}.

For a code C over R, denote

$$C_1 = \{a \in F_{p^m}^n \mid (1+v)a + (1-v)b \in C;\ b \in F_{p^m}^n\}$$

and

$$C_2 = \{b \in F_{p^m}^n \mid (1+v)a + (1-v)b \in C;\ a \in F_{p^m}^n\}$$

such that $(1+v)C_1$ is equal to $C\ mod\ (1-v)$ and $(1-v)C_2$ is equal to $C\ mod\ (1+v)$ respectively. If C is a linear code, then $C = (1+v)C_1 \oplus (1-v)C_2$. Such a code C contains $(p^m)^{2k_1+k_2+k_3}$

codewords. According to the generator matrix G, the code C_1 is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix}$$

and the code C_2 is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix},$$

where $A_i,\ B_j$ are matrices with $1 \leq i,\ j \leq 4$ and all entries from F_{p^m}.

Let G_1 and G_2 be the generator matrices of C_1 and C_2 respectively. Then

$$\begin{pmatrix} (1+v)G_1 \\ \\ (1-v)G_2 \end{pmatrix}$$

is the generator matrix of C.

Any arbitrary element of $R = F_{p^m} + vF_{p^m}$ is of the form $a + vb$, where $a, b \in F_{p^m}$. As in [13], using the same Gray map, Φ from R to $F_{p^m}^2$ as follows

$$\Phi(a + vb) = (a, b)$$

This is a linear map and can be extended component-wise in following way,

$$\Phi : R^n \longrightarrow F_{p^m}^{2n}$$

such that

$$\Phi(c_0, c_2, \cdots, c_{n-1}) = (a_0, a_1, \cdots, a_{n-1}, b_0, b_1, \cdots, b_{n-1}),$$

where $c_i = a_i + vb_i$ for $i = 0, 1, \cdots, n-1$.

Define the Lee weight of c as $w_L(c) = w_H(\Phi(c)) = w_H(a, b)$, where $w_H(\Phi(c))$ denotes the Hamming weight of $\Phi(c)$, is defined as the number of nonzero components. Let $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, then the Hamming distance between x and y is defined as $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$ such that $d_H(x, y) = w_H(x - y)$. The minimum Hamming distance of a code C is defined as $d_H(C) = min\{d_H(x, y);\ x \neq y\}$ or shortly d_H. The Lee distance between x and $y \in R^n$ is defined by $d_L(x, y) = w_L(x - y) = w_H(\Phi(x - y))$. The Lee distance of C is defined as $d_L(C) = min\{d_L(x, y);\ x \neq y\}$, or shortly d_L.

3. RESULTS ON GRAY MAP AND LINEAR CODES OVER R

Proposition 3.1 — The Gray map Φ is a F_{p^m}-linear distance preserving map from R^n (Lee distance) to $F_{p^m}^{2n}$ (Hamming distance).

PROOF : Let $x = a_1 + vb_1$ and $y = a_2 + vb_2 \in R^n$. Then

$$\Phi(x + y) = (a_1 + a_2, b_1 + b_2) = (a_1, b_1) + (a_2, b_2) = \Phi(x) + \Phi(y).$$

And,

$$\Phi(\alpha x) = \Phi(\alpha a_1 + \alpha v b_1) = \alpha\Phi(x) \text{ for } \alpha \in F_{p^m}.$$

Therefore, Φ is F_{p^m}-linear.

For the distance preserving property, as we have defined $d_L(x, y) = w_L(x - y)$, so, $d_L(x, y) = w_L(x - y) = w_H(\Phi(x - y)) = w_H(\Phi(x) - \Phi(y)) = d_H(\Phi(x), \Phi(y))$. Therefore Φ is a F_{p^m}-linear distance preserving map. □

Proposition 3.2 — If C is a $[n, k, d_L]$ linear code over R then $\Phi(C)$ is a $[2n, k, d_H]$ linear code over F_{p^m}, where $d_L = d_H$.

PROOF : By the previous result, Φ is a F_{p^m}-linear distance preserving map. Therefore $d_L = d_H$. Also as, Φ is bijection therefore $|C| = |\Phi(C)| = (p^m)^k$. Hence the result follows. □

***Theorem* 3.1** — *Let C be a linear code of length n over R. Then $\Phi(C^\perp) = \Phi(C)^\perp$. Moreover, if C is self dual, then $\Phi(C)$ is also self dual.*

PROOF : Let $x = a_1 + vb_1 \in C$ and $y = a_2 + vb_2 \in C^\perp$. Then by the inner product of x and y we get, $x \cdot y = (a_1a_2 + b_1b_2) + v(a_1b_2 + a_2b_1) = 0$, which implies, $a_1a_2 + b_1b_2 = a_1b_2 + a_2b_1 = 0$.

Also $\Phi(x) \cdot \Phi(y) = (a_1, b_1) \cdot (a_2, b_2) = a_1a_2 + b_1b_2 = 0$. Therefore, $\Phi(C^\perp) \subseteq \Phi(C)^\perp$. For the other part note that, $|\Phi(C^\perp)| = |\Phi(C)^\perp|$, therefore $\Phi(C^\perp) = \Phi(C)^\perp$.

Considering the fact that, C is self dual, so $C = C^\perp$. Then $\Phi(C) = \Phi(C)^\perp$. Hence, $\Phi(C)$ is also self dual. □

PROPOSITION 3.3 — Let C be a linear code of length n over R. Then $\Phi(C) = C_1 \otimes C_2$ and $\mid C \mid = \mid C_1 \mid\mid C_2 \mid$.

4. RESULTS ON $(\lambda_1 + v\lambda_2)$-CONSTACYCLIC CODES AND IT'S DUAL OVER R

***Theorem* 4.1** — *Let $(\lambda_1 + v\lambda_2)$ be a unit in R and $C = (1 + v)C_1 \oplus (1 - v)C_2$ be a linear code of length n over R. Then C is a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R if and only if C_1 is $(\lambda_1 + \lambda_2)$-constacyclic and C_2 is $(\lambda_1 - \lambda_2)$-constacyclic codes of length n over F_{p^m}.*

PROOF : Let C be a $(\lambda_1 + v\lambda_2)$-constacyclic code and $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, where $c_i = (1+v)a_i + (1-v)b_i$, and $a_i, b_i \in F_{p^m}$ for $i = 0, 1, \ldots, n-1$. Then $(a_0, a_1, \ldots, a_{n-1}) \in C_1$ and $(b_0, b_1, \ldots, b_{n-1}) \in C_2$. Note that,

$$(1+v).(\lambda_1 + v\lambda_2) = (\lambda_1 + \lambda_2)(1+v) \text{ and } (1-v).(\lambda_1 + v\lambda_2) = (\lambda_1 - \lambda_2)(1-v).$$

Then by direct calculation we get,

$$((\lambda_1 + v\lambda_2)c_{n-1}, c_0, c_1, \ldots, c_{n-2}) = (1+v)((\lambda_1 + \lambda_2)a_{n-1}, a_0, a_1, \ldots, a_{n-2})$$
$$+(1-v)((\lambda_1 - \lambda_2)b_{n-1}, b_0, b_1, \ldots, b_{n-2}),$$

which implies $((\lambda_1 + \lambda_2)a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C_1$ and $((\lambda_1 - \lambda_2)b_{n-1}, b_0, b_1, \ldots, b_{n-2}) \in C_2$. Therefore C_1 is $(\lambda_1 + \lambda_2)$-constacyclic and C_2 is $(\lambda_1 - \lambda_2)$-constacyclic codes of length n over F_{p^m}.

Conversely, suppose C_1 is $(\lambda_1 + \lambda_2)$-constacyclic and C_2 is $(\lambda_1 - \lambda_2)$-constacyclic codes of length n over F_{p^m} and also suppose $(a_0, a_1, \ldots, a_{n-1}) \in C_1$ and $(b_0, b_1, \ldots, b_{n-1}) \in C_2$. Let $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, where $c_i = (1+v)a_i + (1-v)b_i$, and $a_i, b_i \in F_{p^m}$ for $i = 0, 1, \ldots, n-1$. As C_1 is $(\lambda_1 + \lambda_2)$-constacyclic and C_2 is $(\lambda_1 - \lambda_2)$-constacyclic codes therefore $((\lambda_1 + \lambda_2)a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C_1$ and $((\lambda_1 - \lambda_2)b_{n-1}, b_0, b_1, \ldots, b_{n-2}) \in C_2$. Note that,

$$(1+v)((\lambda_1 + \lambda_2)a_{n-1}, a_0, a_1, \ldots, a_{n-2}) + (1-v)((\lambda_1 - \lambda_2)b_{n-1}, b_0, b_1, \ldots, b_{n-2})$$
$$= ((\lambda_1 + v\lambda_2)c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

Therefore, C is a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R. □

Corollary 4.1 — Let C be a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R. Then it's dual $C^\perp = (1+v)C_1^\perp \oplus (1-v)C_2^\perp$ is a $(\lambda_1 + v\lambda_2)^{-1}$-constacyclic code of length n over R.

***Theorem* 4.2** — *Let $C = (1+v)C_1 \oplus (1-v)C_2$ be a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R. Suppose f_1, f_2 are the generator polynomials of C_1 and C_2 respectively. Then $C =< (1+v)f_1, (1-v)f_2 >$ and $\mid C \mid = (p^m)^{2n-(deg(f_1)+deg(f_2))}$.*

PROOF : Suppose C is a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R, then by Theorem 4.1, C_1 is $(\lambda_1 + \lambda_2)$-constacyclic and C_2 is $(\lambda_1 - \lambda_2)$-constacyclic codes of length n over F_{p^m}. This implies, $C_1 = (f_1(x)) \subseteq F_{p^m}[x]/(x^n - (\lambda_1 + \lambda_2))$ and $C_2 = (f_2(x)) \subseteq F_{p^m}[x]/(x^n - (\lambda_1 - \lambda_2))$. Also as $C = (1+v)C_1 \oplus (1-v)C_2$, we can write C as,

$$C = \{f(x) \mid f(x) = (1+v)f_1(x) + (1-v)f_2(x), \text{where } f_1(x) \in C_1,\ f_2(x) \in C_2\}.$$

This implies $C \subseteq <(1+v)f_1,(1-v)f_2> \subseteq\ R[x]/(x^n-(\lambda_1+v\lambda_2))$.
As, $|\Phi(C)| = |C|$, then

$$|C| = |C_1||C_2| = (p^m)^{n-deg(f_1)}(p^m)^{n-deg(f_2)} =| C |= (p^m)^{2n-(deg(f_1)+deg(f_2))}.$$

On the other hand, let $(1+v)f_1(x)r_1(x)+(1-v)f_2(x)r_2(x) \in<(1+v)f_1,(1-v)f_2>$, where $r_1(x)$ and $r_2(x)$ be elements of $R[x]/(x^n-(\lambda_1+v\lambda_2))$. There exists $k_1(x) \in\ F_{p^m}[x]/(x^n-(\lambda_1+\lambda_2))$ and $k_2(x) \in F_{p^m}[x]/(x^n-(\lambda_1-\lambda_2))$ such that $(1+v)r_1(x) = (1+v)k_1(x)$ and $(1-v)r_2(x) = (1-v)k_2(x)$. Then $<(1+v)f_1,(1-v)f_2> \subseteq\ C$. Hence $C =<(1+v)f_1,(1-v)f_2>$. □

Corollary 4.2 — Let $C = (1+v)C_1 \oplus (1-v)C_2$ be a $(\lambda_1+v\lambda_2)$-constacyclic code of length n over R. Suppose f_i is the generator polynomial of C_i and g_i^* is the reciprocal polynomial of g_i for $i = 1, 2$. Then $C^{\perp} =<(1+v)g_1^*,(1-v)g_2^*>\ \text{and}\ \mid C^{\perp}\mid= (p^{2m})^{(deg(f_1)+deg(f_2))}$.

***Theorem* 4.3** — *Let C be a $(\lambda_1+v\lambda_2)$-constacyclic code of length n over R. Then there is a unique polynomial $f(x)$ such that $C =< f(x) >\ where\ f(x) = (1+v)f_1(x)+(1-v)f_2(x)$.*

PROOF: Let f_i be the generator polynomial of C_i for $i = 1, 2$. By Theorem 4.2, $C =<(1+v)f_1,(1-v)f_2>$. Let $f(x) = (1+v)f_1(x)+(1-v)f_2(x)$ and suppose $C' =<(1+v)f_1(x)+(1-v)f_2(x)>$, which implies $C' \subseteq C$. Note that, $(1+v)f_1(x) = \gamma(1+v)f(x)$ and $(1-v)f_2 = \gamma(1-v)f(x)$, where $2\gamma \equiv 1(mod\ p)$, therefore $C \subseteq C'$. Hence $C = C'$, where $C =< f(x) >$, where $f(x) = (1+v)f_1(x)+(1-v)f_2(x)$. □

Corollary 4.3 — Let C be a $(\lambda_1+v\lambda_2)$-constacyclic code of length n over R. Suppose f_i is the generator polynomial of C_i and g_i^* is the reciprocal polynomial of g_i for $i = 1, 2$. Then $C^{\perp} =< g^*(x) >,\ \text{where}\ g^*(x) = (1+v)g_1^*(x)+(1-v)g_2^*(x)$ satisfying $g_1f_1 = x^n-(\lambda_1+\lambda_2)$ and $g_2f_2 = x^n-(\lambda_1-\lambda_2)$.

Proposition 4.1 — Let C be a $(\lambda_1+v\lambda_2)$-constacyclic code of length n over R. Then C is non trivial dual containing code if $(\lambda_1+v\lambda_2) = \{1,-1,v,-v\}$.

PROOF : It can be easily shown upon considering the fact that $(\lambda_1+\lambda_2) = \pm 1$ and $(\lambda_1-\lambda_2) = \pm 1$. □

Remark 4.1 : We can classify $(\lambda_1+v\lambda_2)$-constacyclic codes over this ring. By Theorem 4.1 we get the followings.

If $(\lambda_1+v\lambda_2) = 1$, then C_1 and C_2 both are cyclic codes over F_{p^m}.

If $(\lambda_1+v\lambda_2) = -1$, then C_1 and C_2 both are negacyclic codes over F_{p^m}.

If $(\lambda_1+v\lambda_2) = v$, then C_1 is cyclic and C_2 is negacyclic codes over F_{p^m}.

If $(\lambda_1 + v\lambda_2) = -v$, then C_1 is negacyclic and C_2 is cyclic codes over F_{p^m}.

5. Quantum Codes From $(\lambda_1 + v\lambda_2)$-Constacyclic Codes Using Cyclic and Negacyclic Codes Over R

By [15], let H be a p dimensional Hilbert space over the complex numbers $\mathbb{C}$. Define $H^{\otimes n}$ to be n-fold tensor product of the Hilbert space H, that is, $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$($n$-times). Then $H^{\otimes n}$ is a Hilbert space of p^n dimension. A quantum code of length n and dimension k over F_p is defined to be the Hilbert subspace of $H^{\otimes n}$. A quantum code with length n, dimension k and minimum distance d over F_p is denoted by $[[n, k, d]]_p$.

***Theorem* 5.1** — *[6] (CSS Construction). Let C_1 and C_2 be $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ linear codes over $GF(q)$ respectively with $C_2^{\perp} \subseteq C_1$. Furthermore, let $d = min\{d_1, d_2\}$. Then there exists a quantum error-correcting code C with parameters $[[n, k_1 + k_2 - n, d]]_q$. In particular, if $C_1^{\perp} \subseteq C_1$, then there exists a quantum error-correcting code with parameters $[[n, 2k_1 - n, d_1]]$.*

Lemma 5.1 — [6]. Let C be a linear cyclic or negacyclic code with generator polynomial $f(x)$ over F_{p^m}. Then C contains its dual code if and only if

$$x^n - \lambda \equiv 0(mod\, f f^*)$$

where f^* is the reciprocal polynomial of f and $\lambda = \pm 1$

***Theorem* 5.2** — *Let $C = (1 + v)C_1 \oplus (1 - v)C_2$ be a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R. Then $C^{\perp} \subseteq C$ if and only if $x^n - (\lambda_1 + \lambda_2) \equiv 0\,(mod\, f_1 f_1^*)$, $x^n - (\lambda_1 - \lambda_2) \equiv 0\,(mod\, f_2 f_2^*)$ where f_i^* is the reciprocal polynomial of f_i for $i = 1, 2$ and $(\lambda_1 - \lambda_2) = (\lambda_1 + \lambda_2) = \pm 1$.*

Proof : Let $x^n - (\lambda_1 + \lambda_2) \equiv 0\,(mod\, f_1 f_1^*)$ and $x^n - (\lambda_1 - \lambda_2) \equiv 0\,(mod\, f_2 f_2^*)$. Then by Lemma 5.1, we have $C_i^{\perp} \subseteq C_i,\ i = 1, 2$. This implies $(1 + v)C_1^{\perp} \subseteq (1 + v)C_1$ and $(1 - v)C_2^{\perp} \subseteq (1 - v)C_2$. Therefore, $(1 + v)C_1^{\perp} \oplus (1 - v)C_2^{\perp} \subseteq (1 + v)C_1 \oplus (1 - v)C_2$. Hence, $C^{\perp} \subseteq C$.

Conversely, let $C^{\perp} \subseteq C$, then $(1 + v)C_1^{\perp} \oplus (1 - v)C_2^{\perp} \subseteq (1 + v)C_1 \oplus (1 - v)C_2$. Since C_i are linear codes over F_{p^m} such that $(1 + v)C_1 = C(mod\ (1 + v))$ and $(1 - v)C_2 = C(mod\ (1 - v))$, for $i = 1, 2$. So $C_i^{\perp} \subseteq C_i,\ i = 1, 2$. Therefore, Let $x^n - (\lambda_1 + \lambda_2) \equiv 0\,(mod\, f_1 f_1^*)$, $x^n - (\lambda_1 - \lambda_2) \equiv 0\,(mod\, f_2 f_2^*)$. □

Corollary 5.1 — Let $C = (1 + v)C_1 \oplus (1 - v)C_2$ be a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R. Then $C^{\perp} \subseteq C$ if and only if $C_i^{\perp} \subseteq C_i,\ i = 1, 2$.

***Theorem* 5.3** — *Let $C = (1 + v)C_1 \oplus (1 - v)C_2$ be a $(\lambda_1 + v\lambda_2)$-constacyclic code of length n over R. If $C_i^{\perp} \subseteq C_i,\ i = 1, 2$, then $C^{\perp} \subseteq C$ and there exists a quantum error-correcting code with* *parameters* $[[2n,\ 2k-2n,\ d_H]]$*, where* d_H *denotes the minimum Hamming distance and* k *denotes the dimension of the code* $\Phi(C)$*.*

PROOF : The result follows from the fact that $\Phi(C^{\perp}) = \Phi(C)^{\perp}$. $\square$

Example 5.1 : Let $R = F_9 + vF_9$, where $F_9 = F_3[w], w^2 - 2w + 2 = 0, n = 4$. Then

$$\begin{aligned} x^4 - 1 &= (x+1)(x+2)(x+w^2)(x+2w^2), \\ x^4 + 1 &= (x+w)(x+2w)(x+(w+1))(x+2(w+1)). \end{aligned}$$

Let

$$\begin{aligned} f_1(x) &= x + w^2, \\ f_2(x) &= x + w. \end{aligned}$$

Thus, C is a v-constacyclic code of length 4 over R. Also, $C^{\perp} \subseteq C$ and $\Phi(C)$ is a $[8, 6, 2]$ code. Then we obtain a quantum code with parameters $[[8, 4, 2]]$ over F_9.

Example 5.2 : Let $R = F_9 + vF_9$, where $F_9 = F_3[w], w^2 - 2w + 2 = 0, n = 6$. Then

$$\begin{aligned} x^6 + 1 &= (x+(w+2))^3(x+w^2)^3, \\ x^6 - 1 &= (x+1)^3(x+2)^3. \end{aligned}$$

Let

$$\begin{aligned} f_1(x) &= x + w^2, \\ f_2(x) &= x + 1. \end{aligned}$$

Thus, C is a $-v$-constacyclic code of length 6 over R. Also, $C^{\perp} \subseteq C$ and $\Phi(C)$ is a $[12, 10, 2]$ code. Then we obtain a quantum code with parameters $[[12, 8, 2]]$ over F_9.

Example 5.3 : Let $R = F_{25} + vF_{25}$, where $F_{25} = F_5[w], w^2 + w + 1 = 0, n = 4$. Then

$$\begin{aligned} x^{20} - 1 &= (x+1)^5(x+2)^5(x+3)^5(x+4)^5, \\ x^{20} + 1 &= (x^2+2)^5(x^2+3)^5. \end{aligned}$$

Let

$$\begin{aligned} f_1(x) &= (x^2 + x - 1)(x + 1), \\ f_2(x) &= (x^2 + 3)(x^2 + 2)^2. \end{aligned}$$

Thus, C is a v-constacyclic code of length 20 over R. Also, $C^{\perp} \subseteq C$ and $\Phi(C)$ is a $[40, 31, 3]$ code. Then we obtain a quantum code with parameters $[[40, 22, 3]]$ over F_{25}.

The following table contains quantum codes over F_5.

n	$\lambda_1 + v\lambda_2$	C_1	C_2	$\Phi(C)$	$[[n, k, d]]$
10	1	$(x+1)^2(x+4)$	$(x+1)(x+4)^2$	$[20, 14, 3]$	$[[20, 8, 3]]$
15	v	$x+4$	$x+1$	$[30, 28, 2]$	$[[30, 26, 2]]$
25	$-v$	$x+1$	$x+4$	$[50, 48, 2]$	$[[50, 46, 2]]$
35	$-v$	$x+1$	$x+4$	$[70, 68, 2]$	$[[70, 66, 2]]$
36	1	$x+2$	$x+3$	$[72, 70, 2]$	$[[72, 68, 2]]$
45	-1	$x+2$	$x+3$	$[92, 90, 2]$	$[[92, 88, 2]]$

6. Conclusion

In this paper, we studied $(\lambda_1 + v\lambda_2)$-constacyclic codes of length n over R. By using the CSS construction and $(\lambda_1 + v\lambda_2)$-constacyclic codes, we obtain parameters of non-binary quantum codes.

Acknowledgement

The first author is thankful to University Grant Commission (UGC), Govt. of India for financial support under Sr. No. 2061441025 with Ref No. 22/06/2014(i)EU-V.

References

1. A. Dertli, Y. Cengellenmis, and S. Eren, On quantum codes obtained from cyclic codes over A_2, *Int. J. Quantum Inf.*, **13**(3) (2015), 1550031.
2. A. Dertli, Y. Cengellenmis, and S. Eren, Some results on the linear codes over the finite ring $F_2 + v_1F_2 + \cdots + v_rF_2$, *Int. J. Quantum Inf.*, **14**(1) (2016), 1650012.
3. A. Dertli, Y. Cengellenmis, and S. Eren, On the linear codes over the ring R_p, *Discrete Math. Algorithms Appl.*, **8**(2) (2016), 1650036.
4. A. K. Singh, S. Pattanayek, and P. Kumar, On Quantum codes from cyclic codes over $F_2 + uF_2 + u^2F_2$, *Asian-Eur. J. Math.*, **11**(1) (2018), 1850009.
5. A. M. Steane, Simple quantum error-correcting codes, *Phys. Rev. A*, **54** (1996), 4741-4751.
6. A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, Quantum error-correction via codes over GF(4), *IEEE Trans. Inf. Theory*, **44** (1998), 1369-1387.

7. B. Chen, S. Ling, and Zhang, Application of constacyclic codes to quantum MDS codes, *IEEE Trans. Inf. Theory*, **61** (2015), 1474-1484.

8. J. Gao and Y. Wang, u-Constacyclic codes over $F_p + uF_p$ and their applications of constructing new non-binary quantum codes, *Quantum Inf. Process*, **17**(4) (2018).

9. J. Qian, Quantum codes from cyclic codes over $F_2 + vF_2$, *J. Inf. Compt. Science*, **10** (2013), 1715-1722.

10. X. Kai, S. Zhu, and P. Li, Constacyclic codes and some new quantum MDS codes, *IEEE Trans. Inf. Theory*, **60** (2014), 2080-2086.

11. Y. Liu, R. Li, L. Lv, and Y. Ma, A class of constacyclic BCH codes and new quantum codes, *Quantum Inf. Process*, **16** (2017).

12. M. Ashraf and G. Mohammad, Quantum codes from cyclic codes over $F_3 + vF_3$, *Int. J. Quantum Inf.*, **12**(6) (2014), 1450042.

13. M. Ashraf and G. Mohammad, On skew cyclic codes over a semi-local ring, *Discrete Math. Algorithms Appl.*, **7**(4) (2015), 1550042.

14. 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.

15. M. Ashraf and G. Mohammad, Quantum codes from cyclic codes over $F_q + uF_q + vF_q + uvF_q$, *Quantum Inf. Process*, **15** (10) (2016), 4089-4098.

16. M. Shi, S. L. Yang, and S. Zhu, Good p-ary quasi cyclic codes from cyclic codes over $F_p + vF_p$, *J. Syst. Sci. Complex*, **25** (2012), 375-384.

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

18. T. Bag, A. K. Upadhyay, M. Ashraf, and G. Mohammad, Quantum codes from cyclic codes over the ring $F_p[u]/ < u^3 - u >$, *Asian-Eur. J. Math.*, **13**(1) (2020), 2050008.

19. L. Wang and S. Zhu, New quantum MDS codes derived from constacyclic codes, *Quantum Inf. Process*, **14** (2015), 881-889.