Quantum Information Processing (2020) 19:319
https://doi.org/10.1007/s11128-020-02825-z

New quantum codes from constacyclic and additive constacyclic codes

Habibul Islam[1] · **Om Prakash**[1]

Received: 10 April 2020 / Accepted: 17 August 2020 / Published online: 28 August 2020

Abstract

Let p be a prime and $q = p^r$, for an integer $r \geq 1$. This article studies $\lambda = (\lambda_1 + u\lambda_2 + v\lambda_3)$-constacyclic codes of length n over a class of finite commutative non-chain rings $R = \mathbb{F}_q[u, v]/\langle u^2 - \gamma u, v^2 - \delta v, uv = vu = 0\rangle$, where $\gamma, \delta \in \mathbb{F}_q^*$. First, we decompose $(\lambda_1 + u\lambda_2 + v\lambda_3)$-constacyclic code into the direct sum of λ_1-constacyclic, $(\lambda_1 + \gamma\lambda_2)$-constacyclic and $(\lambda_1 + \delta\lambda_3)$-constacyclic codes over $\mathbb{F}_q$, respectively. Then, we determine the necessary and sufficient condition for these codes to contain their Euclidean duals. Further, we extend the study to $\mathbb{F}_q R$-additive λ-constacyclic codes of length (n, m) which are $R[x]$-submodules of $S_{n,m} = \mathbb{F}_q[x]/\langle x^n - 1\rangle \times R[x]/\langle x^m - \lambda\rangle$. Apart from other results, we also discuss the dual-containing separable $\mathbb{F}_q R$-additive λ-constacyclic codes. Finally, by using the CSS construction on the Gray images of these codes, we obtain many new and better quantum codes that improve on the known existing quantum codes available in recent articles.

Keywords Non-chain ring · Constacyclic code · Gray map · Additive code · Quantum code

Mathematics Subject Classification 94B05 · 94B15 · 94B35 · 94B60

1 Introduction

Like classical linear codes, quantum codes help to protect quantum information during transmission through a quantum channel. These codes have been extensively used in quantum computation which solves challenging problems faster than the classical computation. For instance, the running time of the *Shor's Algorithm* [36] to find the

✉ Om Prakash
om@iitp.ac.in

Habibul Islam
habibul.pma17@iitp.ac.in

1 Department of Mathematics, Indian Institute of Technology Patna, Patna 801 106, India

prime factors of a large integer is polynomial time in quantum computation, whereas sub-exponential in classical computation. Quantum code was introduced by Shor [35]. Later, Calderbank et al. [9] constructed the quantum codes from classical codes in a formal way. Recall that a q-ary quantum code denoted by $[[n,k,d]]_q$ satisfies the quantum singleton bound $2d+k \leq n+2$ and called maximum distance separable (MDS) if the bound is attained. Clearly, MDS codes have the best error control (highest distance) and best code rate (larger non-redundant bits) compared to the other codes with the same parameters. But, these codes are rare to find. Hence, people have been constructing quantum codes close to MDS and store them to some online platform, like [16]. Usually, to validate the novelty of the approach, researchers are comparing their obtained codes to the codes which are known by most recent articles.

Kai and Zhu [26] determined the quantum codes over $\mathbb{F}_4$ from the cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Qian [31] obtained binary quantum codes by using cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Later, the study of cyclic codes over finite commutative non-chain rings has been contributed significantly in quantum codes, refer [2,3,12,18,22,24,31,33]. Further, the constacyclic codes, being a generalized class of cyclic codes, also play an important role in quantum codes construction [10,23]. In 2018, the u-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p, u^2 = 1$ by Gao and Wang [17] and constacyclic codes over $\mathbb{F}_q + v\mathbb{F}_p + v^2\mathbb{F}_p, v^3 = v$ by Ma et al. [28] were studied to obtain non-binary quantum codes. Recently, Ma et al. [29] studied the constacyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-1, v^2-v, uv-vu\rangle$ and produced many new quantum codes. Also, Dinh et al. [15] explored some quantum codes from the constacyclic codes over the non-chain ring $\mathbb{F}_p[u]/\langle u^{k+1}-u\rangle$. In continuation, Islam et al. [20] considered the structure of constacyclic codes over a class of finite commutative non-chain rings $R_{k,m} = \mathbb{F}_{p^m}[u_1,u_2,\ldots,u_k]/\langle u_i^2-1, u_iu_j-u_ju_i\rangle_{i\neq j=1,2,\ldots,k}$, where $m \geq 1, k \geq 2$ are integers and constructed many MDS and good quantum codes compared to the best-known codes. In addition, Alkenani et al. [1] studied the constacyclic codes over the finite non-chain ring $\mathbb{F}_q[u_1,u_2]/\langle u_1^2-u_1, u_2^2-u_2, u_1u_2-u_2u_1\rangle$ to obtain quantum codes. Therefore, it is clear that the constacyclic code over finite non-chain rings is one of the rich resources to produce new quantum codes. Hence, it is logical to study these codes over different and new non-chain rings which are capable to explore more new codes. This motivates us to study the constacyclic codes over a class of finite commutative non-chain rings $R = \mathbb{F}_q[u,v]/\langle u^2-\gamma u, v^2-\delta v, uv = vu = 0\rangle$, where $\gamma, \delta \in \mathbb{F}_q^*$.

On the other side, the additive codes were introduced by Delsarte and Levenshtein [11] in 1998. One of the most common tasks in the study of additive codes is to find their generator polynomials, dual codes and bounds on minimum distances [6,7,21,34]. Despite the application in steganography [32], these codes are also useful to construct good quantum codes [4]. In 2019, Aydogdu and Abualrub [5] studied the quantum codes from $\mathbb{Z}_2 \times (\mathbb{Z}_2 + u\mathbb{Z}_2)$ and Diao et al. [14] considered $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes to obtain good quantum codes. To the best of our knowledge, very few articles [4,5,13,14,27] have engaged to construct new quantum codes using additive codes. So, still there is a huge scope to explore quantum codes using cyclic and constacyclic codes over the mixed alphabets. Toward this, we extend our study to the constacyclic codes over the mixed alphabets $\mathbb{F}_qR$ with two main motives as follows:

(i) The article obtains many new and better quantum codes compared to the existing codes (available in recent articles) from the constacyclic codes over the class of non-chain rings R.

(ii) The article determines the structure of $\mathbb{F}_q R$-additive constacyclic codes of length (n, m) and constructs better quantum codes compared to the known codes.

2 Preliminary

For a prime p and $q = p^r$, let $R = \mathbb{F}_q[u, v]/\langle u^2 - \gamma u, v^2 - \delta v, uv = vu = 0\rangle$, where $\gamma, \delta \in \mathbb{F}_q^*$. Thus, R is a finite commutative Frobenius, non-chain and semi-local ring (with unity) of characteristic p. Also, R has q^3 elements and three maximal ideals $\langle u + v\rangle$, $\langle \gamma - u\rangle$ and $\langle \delta - v\rangle$. The explicit representation of R is

$$R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q, \quad \text{where } u^2 = \gamma u, v^2 = \delta v, uv = vu = 0,$$

and each member of R is of the form $z = z_1 + uz_2 + vz_3$, where $z_i \in \mathbb{F}_q$, for $i = 1, 2, 3$. Let $\xi_1 = \frac{\gamma\delta - \gamma v - \delta u}{\gamma\delta}$, $\xi_2 = \frac{u}{\gamma}$ and $\xi_3 = \frac{v}{\delta}$. Then, $\xi_i^2 = \xi_i$, $\xi_i\xi_j = 0$ if $i \neq j$, and $\sum_{i=1}^{3} \xi_i = 1$. Therefore, $R = \bigoplus_{i=1}^{3} \xi_i R \cong \bigoplus_{i=1}^{3} \xi_i \mathbb{F}_q$. Hence, an element $\lambda = \lambda_1 + u\lambda_2 + v\lambda_3 \in R$ has a unique representation $\lambda = \lambda_1\xi_1 + (\lambda_1 + \gamma\lambda_2)\xi_2 + (\lambda_1 + \delta\lambda_3)\xi_3$. Further, the units of R are classified by the below lemma.

Lemma 1 *Let $\lambda = \lambda_1 + u\lambda_2 + v\lambda_3 \in R$ be a nonzero element. Then, λ is a unit in R if and only if $\lambda_1, \lambda_1 + \gamma\lambda_2, \lambda_1 + \delta\lambda_3$ are units in $\mathbb{F}_q$.*

Proof Let $\lambda \in R$ be a unit such that $\lambda = \lambda_1\xi_1 + (\lambda_1 + \gamma\lambda_2)\xi_2 + (\lambda_1 + \delta\lambda_3)\xi_3$. There exists $\lambda' = \sum_{i=1}^{3} \xi_i\lambda_i' \in R$ where $\lambda_i' \in \mathbb{F}_q^*$ such that $\lambda\lambda' = 1$. Then, $\lambda_1\lambda_1'\xi_1 + (\lambda_1 + \gamma\lambda_2)\lambda_2'\xi_2 + (\lambda_1 + \delta\lambda_3)\lambda_3'\xi_3 = 1$. Now, multiplying by ξ_1 in both sides, we get $\lambda_1\lambda_1'\xi_1 = \xi_1$, and this implies $\lambda_1\lambda_1' = 1$. Hence, λ_1 is a unit. Similarly, $\lambda_1 + \gamma\lambda_2, \lambda_1 + \delta\lambda_3$ are units in $\mathbb{F}_q$.

Conversely, let $\lambda_1, \lambda_1 + \gamma\lambda_2, \lambda_1 + \delta\lambda_3$ be units in $\mathbb{F}_q$. Let $\lambda' = \lambda_1^{-1}\xi_1 + (\lambda_1 + \gamma\lambda_2)^{-1}\xi_2 + (\lambda_1 + \delta\lambda_3)^{-1}\xi_3$. Then, $\lambda\lambda' = 1$. Hence, λ is a unit in R. □

Now, we recall that a non-empty subset C of R^n is said to be a *linear code* of length n if it is an R-submodule of R^n and each element of C is known as *codeword*. Let $\lambda \in R$ be a unit in R. Then, a linear code C is said to be a λ-*constacyclic* code if for any codeword $(c_0, c_1, \dots, c_{n-1}) \in C$ implies $(\lambda c_{n-1}, c_0, \dots, c_{n-2}) \in C$. It is a cyclic code for $\lambda = 1$ and negacyclic code for $\lambda = -1$. Algebraically, a λ-constacyclic code of length n is identified as an ideal of $R[x]/\langle x^n - \lambda\rangle$ and each codeword is represented by a polynomial of degree $n - 1$. Throughout the article, we fix $\lambda = \lambda_1 + u\lambda_2 + v\lambda_3$, where $\lambda_i \in \mathbb{F}_q$, for $i = 1, 2, 3$. For a linear code C of length n, its dual code $C^\perp = \{a \in R^n \mid a \cdot b = 0 \text{ for all } b \in C\}$ is also a linear code where the Euclidean inner product between two vectors $a = (a_0, a_1, \dots, a_{n-1})$, $b = (b_0, b_1, \dots, b_{n-1})$ is defined by $a \cdot b = \sum_{i=0}^{n-1} a_i b_i$. Here, we see that for a λ-constacyclic code C, dual $C^\perp$ is a λ^{-1}-constacyclic code of length n over R (Theorem 3). The linear code C is said to be *self-dual* if $C = C^\perp$ and *self-orthogonal* if $C \subseteq C^\perp$. Next, we define a Gray map

φ which preserves the orthogonality and it is useful to obtain $\mathbb{F}_q$-parameters of the constacyclic codes over R.

Definition 1 A map $\varphi : R \longrightarrow \mathbb{F}_q^3$ is defined by

$$\varphi(z) = (z_1, z_2, z_3)M, \tag{1}$$

where $z = \sum_{i=1}^{3} \xi_i z_i \in R$ and $M \in GL_3(\mathbb{F}_q)$ is a 3×3 invertible matrix such that $MM^{\mathrm{T}} = \tau I_3$. Here, M^{T} represents the transpose matrix of M, I_3 is the identity matrix of order 3 and $\tau \in \mathbb{F}_q^*$.

The map φ is a bijection and can be extended over R^n componentwise. We define the Gray weight for $z \in R$ by $w_G(z) = w_H(\varphi(z))$ and for $z = (z_1, z_2, \ldots, z_n) \in R^n$ by $w_G(z) = \sum_{i=1}^{n} w_G(z_i)$, where w_H is the Hamming weight in $\mathbb{F}_q$. The Gray distance between $z, z' \in R^n$ is $d_G(z, z') = w_G(z - z')$ and for a linear code C is $d_G(C) = \min\{w_G(z) | 0 \neq z \in C\}$. By the above discussion, the following result is easy to verify.

Lemma 2 *The map φ defined in Eq. (1) is linear and distance preserving from (R^n, d_G) to $(\mathbb{F}_q^{3n}, d_H)$, where d_H is the Hamming distance.*

Lemma 3 *Let C be a linear code of length n over R. Then,*

1. $\varphi(C^{\perp}) = \varphi(C)^{\perp}$.
2. *C is a self-dual code of length n if and only if $\varphi(C)$ is a self-dual linear code of length $3n$ over $\mathbb{F}_q$.*
3. *$\varphi(C)$ is a self-orthogonal linear code of length $3n$ if C is a self-orthogonal linear code of length n over R.*

Proof 1. Let $z = (z_0, z_1, \ldots, z_{n-1}) \in C^{\perp}$, where $z_i = \xi_1 z_i' + \xi_2 z_i'' + \xi_3 z_i'''$, for $0 \leq i \leq n-1$. Then, $\varphi(z) \in \varphi(C^{\perp})$. In order to prove $\varphi(z) \in \varphi(C)^{\perp}$, let $y = (y_0, y_1, \ldots, y_{n-1}) \in C$, where $y_i = \xi_1 y_i' + \xi_2 y_i'' + \xi_3 y_i'''$ for $0 \leq i \leq n-1$. Now, $y \cdot z = 0$ implies $\sum_{i=0}^{n-1} y_i z_i = 0$, i.e., $\sum_{i=0}^{n-1}(\xi_1 y_i' z_i' + \xi_2 y_i'' z_i'' + \xi_3 y_i''' z_i''') = 0$. Hence, $\sum_{i=0}^{n-1} y_i' z_i' = \sum_{i=0}^{n-1} y_i'' z_i'' = \sum_{i=0}^{n-1} y_i''' z_i''' = 0$. Again,

$$\varphi(y) = \left[(y_0', y_0'', y_0''')M, \ldots, (y_{n-1}', y_{n-1}'', y_{n-1}''')M\right] = (s_0 M, \ldots, s_{n-1} M),$$
$$\varphi(z) = \left[(z_0', z_0'', z_0''')M, \ldots, (z_{n-1}', z_{n-1}'', z_{n-1}''')M\right] = (t_0 M, \ldots, t_{n-1} M),$$

where $s_i = (y_i', y_i'', y_i''')$, $t_i = (z_i', z_i'', z_i''')$ for $0 \leq i \leq n-1$.

Then,

$$\varphi(y) \cdot \varphi(z) = \varphi(y)\varphi(z)^{\mathrm{T}} = \sum_{i=0}^{n-1} s_i M M^{\mathrm{T}} t_i^{\mathrm{T}} = \tau \sum_{i=0}^{n-1} s_i t_i^{\mathrm{T}}$$
$$= \tau \sum_{i=0}^{n-1} (y_i' z_i' + y_i'' z_i'' + y_i''' z_i''') = 0.$$

Therefore, $\varphi(z) \in \varphi(C)^{\perp}$ and hence $\varphi(C^{\perp}) \subseteq \varphi(C)^{\perp}$. Since φ is a bijection, $|\varphi(C^{\perp})| = |\varphi(C)^{\perp}|$. Thus, $\varphi(C^{\perp}) = \varphi(C)^{\perp}$.

2. Let C be a self-dual linear code of length n, i.e., $C = C^{\perp}$. Then, $\varphi(C) = \varphi(C^{\perp}) = \varphi(C)^{\perp}$. Hence, $\varphi(C)$ is a self-dual linear code of length $3n$ over $\mathbb{F}_q$. On the other side, let $\varphi(C)$ be a self-dual linear code, i.e., $\varphi(C) = \varphi(C)^{\perp} = \varphi(C^{\perp})$. Since φ is a bijection, $C = C^{\perp}$. Hence, C is a self-dual linear code.
3. Let C be a self-orthogonal linear code of length n over R. Then, $C \subseteq C^{\perp}$, i.e., $\varphi(C) \subseteq \varphi(C^{\perp}) = \varphi(C)^{\perp}$. Thus, $\varphi(C)$ is a self-orthogonal linear code of length $3n$ over $\mathbb{F}_q$. □

Let C be a linear code of length n over R. Let $C_1 = \{z_1 \in \mathbb{F}_q^n |$, there exist $z_2, z_3 \in \mathbb{F}_q^n$ such that $\xi_1 z_1 + \xi_2 z_2 + \xi_3 z_3 \in C\}$, $C_2 = \{z_2 \in \mathbb{F}_q^n |$ there exist $z_1, z_3 \in \mathbb{F}_q^n$ such that $\xi_1 z_1 + \xi_2 z_2 + \xi_3 z_3 \in C\}$, and $C_3 = \{z_3 \in \mathbb{F}_q^n |$ there exist $z_1, z_2 \in \mathbb{F}_q^n$ such that $\xi_1 z_1 + \xi_2 z_2 + \xi_3 z_3 \in C\}$. Then, C_1, C_2, C_3 are linear codes of length n over $\mathbb{F}_q$ and C can be uniquely expressed as $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3$. Also, the dual code of C is $C^{\perp} = \xi_1 C_1^{\perp} \oplus \xi_2 C_2^{\perp} \oplus \xi_3 C_3^{\perp}$ (see [25,28] for proof of similar results) and generator matrix of C is

$$M = \begin{bmatrix} \xi_1 M_1 \\ \xi_2 M_2 \\ \xi_3 M_3 \end{bmatrix}$$

where M_1, M_2, M_3 are generator matrices of C_1, C_2, C_3, respectively.

Now, we look for the structure of λ-constacyclic codes from Theorems 1 to 3 without proofs. These results are helpful to obtain quantum codes in the subsequent section. For similar type of results, interested readers can find in [25,28].

Theorem 1 *Let $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3$ be a linear code of length n over R. Then, C is a λ-constacyclic code if and only if C_1, C_2 and C_3 are λ_1-constacyclic, $(\lambda_1 + \gamma\lambda_2)$-constacyclic and $(\lambda_1 + \delta\lambda_3)$-constacyclic codes of length n over $\mathbb{F}_q$, respectively.*

Theorem 2 *Let $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3$ be a λ-constacyclic code of length n over R. Then, there exists a polynomial $g(x) \in R[x]$ such that $C = \langle g(x)\rangle$ and $g(x) \mid x^n - (\lambda_1 + u\lambda_2 + v\lambda_3)$, where $g(x) = \sum_{i=1}^{3} \xi_i g_i(x)$ and $C_i = \langle g_i(x)\rangle$ for $i = 1, 2, 3$.*

Theorem 3 *Let $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3$ be a λ-constacyclic code of length n over R. Let $C = \langle \sum_{i=1}^{3} \xi_i g_i(x)\rangle$, where $x^n - \lambda_1 = g_1(x)h_1(x)$, $x^n - (\lambda_1 + \gamma\lambda_2) = g_2(x)h_2(x)$, $x^n - (\lambda_1 + \delta\lambda_3) = g_3(x)h_3(x)$. Then, $C^{\perp} = \xi_1 C_1^{\perp} \oplus \xi_2 C_2^{\perp} \oplus \xi_3 C_3^{\perp}$ is a λ^{-1}-constacyclic code and $C^{\perp} = \langle \sum_{i=1}^{3} \xi_i h_i^*(x)\rangle$, where $h_i^*(x)$ is reciprocal polynomial of $h_i(x)$, for $i = 1, 2, 3$.*

3 Quantum codes from constacyclic codes over *R*

In the present section, we construct quantum codes from the dual-containing λ-constacyclic codes by using the CSS construction. First, we determine the necessary and sufficient conditions (Theorem 4) of these codes to contain their duals. Then, we apply CSS construction (Lemma 5) on their Gray images to construct quantum codes. In this connection, first we recall some basic definitions and facts as follows.

Definition 2 Let $\mathbb{C}^q$ be the Hilbert space of dimension q. Then, $(\mathbb{C}^q)^{\otimes n} = \mathbb{C}^q \otimes \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$ (n times) is also a Hilbert space of dimension q^n. Any q^k-dimensional subspace of $(\mathbb{C}^q)^{\otimes n}$ is called a quantum code and denoted by $[[n, k, d]]_q$ where d is the minimum distance. Note that the minimum distance d is defined by using the metric of $(\mathbb{C}^q)^{\otimes n}$. Every quantum code satisfies the quantum singleton bound $2d+k \leq n+2$ and known as maximum distance separable (or shortly, MDS) code if the bound is attained. A quantum code $[[n, k, d]]_q$ is said to be better than the quantum code $[[n', k', d']]_q$ if any of the following or both hold:

1. $d > d'$ when $\frac{k}{n} = \frac{k'}{n'}$ (larger distance with same code rate).
2. $\frac{k}{n} > \frac{k'}{n'}$ when $d = d'$ (larger code rate with same distance).

Now, we recall two important results: Lemma 4 (condition for dual-containing codes over $\mathbb{F}_q$) and Lemma 5 (CSS construction), which will help to determine dual-containing λ-constacyclic codes and quantum codes from these codes, respectively.

Lemma 4 [9] *Let $C = \langle g(x) \rangle$ be an α-constacyclic code of length n over $\mathbb{F}_q$, where $\alpha = \pm 1$. Then, $C^\perp \subseteq C$ if and only if $x^n - \alpha \equiv 0 \pmod{g(x)g^*(x)}$.*

Lemma 5 [19] *Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ such that $C^\perp \subseteq C$. Then, there exists a quantum code $[[n, 2k-n, d]]_q$ over $\mathbb{F}_q$.*

With the help of Lemma 4, we determine the necessary and sufficient conditions of λ-constacyclic codes to contain their duals in the next theorem.

Theorem 4 *Let $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3$ be a λ-constacyclic code of length n over R where $\lambda_1 = \pm 1, \lambda_1 + \gamma\lambda_2 = \pm 1, \lambda_1 + \delta\lambda_3 = \pm 1$. Also, let $C_i = \langle g_i(x) \rangle$ where $x^n - \lambda_1 = g_1(x)h_1(x)$, $x^n - (\lambda_1 + \gamma\lambda_2) = g_2(x)h_2(x)$, $x^n - (\lambda_1 + \delta\lambda_3) = g_3(x)h_3(x)$. Then, $C^\perp \subseteq C$ if and only if*

$$\begin{aligned} x^n - \lambda_1 &\equiv 0 \pmod{g_1(x)g_1^*(x)} \\ x^n - (\lambda_1 + \gamma\lambda_2) &\equiv 0 \pmod{g_2(x)g_2^*(x)} \\ x^n - (\lambda_1 + \delta\lambda_3) &\equiv 0 \pmod{g_3(x)g_3^*(x)}. \end{aligned}$$

Proof Let $C_i = \langle g_i(x) \rangle$ for $i = 1, 2, 3$ where

$$\begin{aligned} x^n - \lambda_1 &\equiv 0 \pmod{g_1(x)g_1^*(x)} \\ x^n - (\lambda_1 + \gamma\lambda_2) &\equiv 0 \pmod{g_2(x)g_2^*(x)} \\ x^n - (\lambda_1 + \delta\lambda_3) &\equiv 0 \pmod{g_3(x)g_3^*(x)}. \end{aligned}$$

By Lemma 4, we have $C_i^\perp \subseteq C_i$ for $i = 1, 2, 3$. Now, $C^\perp = \xi_1 C_1^\perp \oplus \xi_2 C_2^\perp \oplus \xi_3 C_3^\perp \subseteq \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3 = C$.

On the other hand, let $C^{\perp} \subseteq C$. Since C_i is a q-ary linear code such that $C \equiv \xi_i C_i \pmod{\xi_i}$, $C_i^{\perp} \subseteq C_i$ for $i = 1, 2, 3$. Hence, by Lemma 4, we have

$$\begin{aligned} x^n - \lambda_1 &\equiv 0 \pmod{g_1(x)g_1^*(x)} \\ x^n - (\lambda_1 + \gamma\lambda_2) &\equiv 0 \pmod{g_2(x)g_2^*(x)} \\ x^n - (\lambda_1 + \delta\lambda_3) &\equiv 0 \pmod{g_3(x)g_3^*(x)}. \end{aligned}$$

□

Now, we are in a position to construct quantum codes by using Lemma 5 and Theorem 4 in the next result.

Theorem 5 *Let $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3$ be a λ-constacyclic code of length n over R such that $C^{\perp} \subseteq C$. Then, there exists a quantum code with parameters $[[3n, 2k - 3n, d_H]]_q$ over $\mathbb{F}_q$, where d_H is the minimum Hamming distance.*

Proof Since $C^{\perp} \subseteq C$, we have $\varphi(C^{\perp}) \subseteq \varphi(C)$. Now, by Lemma 3, $\varphi(C^{\perp}) = \varphi(C)^{\perp}$, and this implies that $\varphi(C)^{\perp} \subseteq \varphi(C)$. Therefore, $\varphi(C)$ is a dual-containing $[3n, k, d_H]$ linear code over $\mathbb{F}_q$. Hence, by Lemma 5, there exists a quantum code $[[3n, 2k - 3n, d_H]]_q$ over $\mathbb{F}_q$. □

Remark 1 The dimension $2k-3n$ of the quantum code obtained in Theorem 5 is always nonnegative due to the fact that $C^{\perp} \subseteq C$.

4 Quantum codes from $\mathbb{F}_q R$-additive constacyclic codes

The set $\mathbb{F}_q R = \{(a, b) | \, a \in \mathbb{F}_q, b \in R\}$ is a group under componentwise addition. Now, we define a projection map $\pi : R \longrightarrow \mathbb{F}_q$ by $\pi(z_1 + uz_2 + vz_3) = z_1$, where $z_i \in \mathbb{F}_q$ for $i = 1, 2, 3$. With the help of π, we define a multiplication $* : R \times \mathbb{F}_q^n R^n \longrightarrow \mathbb{F}_q^n R^n$ by $z * (a_0, a_1, \dots, a_{n-1}, b_0, b_1 \dots, b_{m-1}) = (\pi(z)a_0, \pi(z)a_1, \dots, \pi(z)a_{n-1}, zb_0, zb_1 \dots, zb_{m-1})$ where $z, b_i \in R, a_i \in \mathbb{F}_q$ for all i. Then, it is easy to show that under the multiplication $*$, the set $\mathbb{F}_q^n R^m = \{(a, b) | \, a \in \mathbb{F}_q^n, b \in R^m\}$ is an R-module. Recall that a non-empty $C \subseteq \mathbb{F}_q^n R^m$ is called an $\mathbb{F}_q R$-additive linear code of length (n, m) if C is an R-submodule of $\mathbb{F}_q^n R^m$. For $\mathbb{F}_q R$-additive linear code C of length (n, m), its dual is defined as $C^{\perp} = \{c \in \mathbb{F}_q^n R^m | \, c \cdot c' = 0 \text{ for all } c' \in C\}$, where the inner product of any two vectors $c = (a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{m-1})$, $c' = (a'_0, a'_1, \dots, a'_{n-1}, b'_0, b'_1, \dots, b'_{m-1})$ is defined by $c \cdot c' = (u + v) \sum_{i=0}^{n-1} a_i a' + \sum_{i=0}^{n-1} b_i b'_i$. It is a routine work to check that $C^{\perp}$ is also an $\mathbb{F}_q R$-additive linear code of length (n, m).

Let λ be a unit in R and denote $S_{n,m} = \mathbb{F}_q[x]/\langle x^n - 1\rangle \times R[x]/\langle x^m - \lambda\rangle$. Now, we identify each vector $(a, b) \in \mathbb{F}_q^n R^m$ to the polynomial $(a(x), b(x)) \in S_{n,m}$, where $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$, $b = (b_0, b_1, \dots, b_{m-1}) \in R^m$ and $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$, $b(x) = b_0 + b_1 x + \cdots + b_{m-1}x^{m-1} \in R[x]/\langle x^m - \lambda\rangle$. The projection map π acts on the polynomial ring $R[x] \longrightarrow \mathbb{F}_q[x]$ as $\pi(\sum_i r_i x^i) = \sum_i \pi(r_i)x^i$, where $r_i \in R$ for all i. Hence, the extended corresponding multiplication $* : R[x] \times S_{n,m} \longrightarrow S_{n,m}$ is defined as $g(x) * (a(x), b(x)) =$

$(\pi(g(x))a(x), g(x)b(x))$, where $b(x), g(x) \in R[x], a(x) \in \mathbb{F}_q[x]$. Thus, $S_{n,m}$ is an $R[x]$-module under the multiplication $*$.

Definition 3 Let λ be a unit in R. Then, an $\mathbb{F}_q R$-additive linear code C of length (n, m) is said to be $\mathbb{F}_q R$-additive λ-constacyclic if for any $(a, b) \in C$, we have $(\sigma(a), \sigma_\lambda(b)) \in C$, where σ_λ is the λ-constacyclic shift and σ is the cyclic shift operator.

It is worth mentioning that an $\mathbb{F}_q R$-additive linear code generalizes both the linear code over $\mathbb{F}_q$ and over R. In fact, if $n = 0$, then an $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m) is indeed a λ-constacyclic code over R. On the other side, for $m = 0$, an $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m) is a cyclic code of length n over $\mathbb{F}_q$. In this way, we can conclude that the construction ($\mathbb{F}_q R$-additive codes) in the present section is a more general version of earlier construction of λ-constacyclic codes. The next result characterizes the $\mathbb{F}_q R$-additive λ-constacyclic codes of length (n, m) as submodules of $S_{n,m}$.

Proposition 1 *Let C be an $\mathbb{F}_q R$-additive linear code of length (n, m). Then, C is an $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m) if and only if C is an $R[x]$-submodule of $S_{n,m}$.*

Proof Let C be an $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m). Let $z(x) \in R[x]$ and $(a, b) \in C$ whose polynomial representation is $(a(x), b(x))$ where $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, $b(x) = b_0 + b_1 x + \cdots + b_{m-1}x^{m-1}$. Now, $x * (a(x), b(x)) = (a_{n-1} + x a_0 + \cdots + a_{n-2}x^{n-1}, \lambda b_{m-1} + x b_0 + \cdots + b_{m-2}x^{m-1}) = (\sigma(a), \sigma_\lambda(b)) \in C$. Similarly, for any $i \geq 2$, we have $x^i * (a(x), b(x)) \in C$. Since C is an R-submodule of $\mathbb{F}_q^n R^m$, $z(x) * (a(x), b(x)) \in C$. Hence, C is an $R[x]$-submodule of $S_{n,m}$.

Conversely, let C be an $R[x]$-submodule of $S_{n,m}$. Suppose $(a, b) \in C$ whose polynomial representation is $(a(x), b(x))$. Now, $x * (a(x), b(x)) \in C$ where $x * (a(x), b(x)) = (\sigma(a), \sigma_\lambda(b))$. Therefore, C is an $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m). $\square$

Now, with the help of map φ defined in Eq. (1), we define another Gray map $\Phi : \mathbb{F}_q R \longrightarrow \mathbb{F}_q^4$ by

$$\Phi(a, z) = (a, \varphi(z)) = (a, (z_1, z_2, z_3)M), \quad \text{where } z = \sum_{i=1}^{3} \xi_i z_i \in R, a, z_i \in \mathbb{F}_q \text{ for } i = 1, 2, 3. \tag{2}$$

Since φ is a linear and bijective map, so is Φ. Then, the map Φ can be extended over $\mathbb{F}_q^n R^m \longrightarrow \mathbb{F}_q^{(n+3m)}$ componentwise and preserves the orthogonality as shown in the next result.

Lemma 6 *Let C be an $\mathbb{F}_q R$-additive linear code of length (n, m). Then, $\Phi(C^\perp) = \Phi(C)^\perp$. Further, C is self-dual if and only if $\Phi(C)$ is self-dual.*

Proof Let C be an $\mathbb{F}_q R$-additive linear code of length (n, m). Let $w = (a_0, a_1, \ldots, a_{n-1}, z_0, z_1, \ldots, z_{m-1}) \in C^{\perp}$ where $z_i = \xi_1 z_i' + \xi_2 z_i'' + \xi_3 z_i'''$ for $0 \leq i \leq m-1$. In order to show $\Phi(w) \in \Phi(C)^{\perp}$, let $s = (b_0, b_1, \ldots, b_{n-1}, y_0, y_1, \ldots, y_{m-1}) \in C$, where $y_i = \xi_1 y_i' + \xi_2 y_2'' + \xi_3 y_i'''$ for $0 \leq i \leq m-1$. Now, $w \cdot s = 0$ implies that $(u+v)\sum_{i=0}^{n-1} a_i b_i + \sum_{i=0}^{m-1} y_i z_i = 0$, i.e., $(u+v)\sum_{i=0}^{n-1} a_i b_i + \sum_{i=0}^{m-1}(\xi_1 y_i' z_i' + \xi_2 y_i'' z_i'' + \xi_3 y_i''' z_i''') = 0$, which implies $\sum_{i=0}^{n-1} a_i b_i = 0$ and $\sum_{i=0}^{m-1}(y_i' z_i' + y_i'' z_i'' + y_i''' z_i''') = 0$. Again,

$$\begin{aligned}
\Phi(w) &= \left[a_0, a_1, \ldots, a_{n-1}, (z_0', z_0'', z_0''')M, \ldots, (z_{m-1}', z_{m-1}'', z_{m-1}''')M\right] \\
&= [a_0, a_1, \ldots, a_{n-1}, \alpha_0 M, \ldots, \alpha_{m-1} M] \\
\Phi(s) &= \left[b_0, b_1, \ldots, b_{n-1}, (y_0', y_0'', y_0''')M, \ldots, (y_{m-1}', y_{m-1}'', y_{m-1}''')M\right] \\
&= [b_0, b_1, \ldots, b_{n-1}, \beta_0 M, \ldots, \beta_{m-1} M],
\end{aligned}$$

where $\alpha_i = (z_i', z_i'', z_i''')$, $\beta_i = (y_i', y_i'', y_i''')$ for $0 \leq i \leq m-1$. Also,

$$\begin{aligned}
\Phi(w) \cdot \Phi(s) = \Phi(w)\Phi(s)^{\mathrm{T}} &= (u+v)\sum_{i=0}^{n-1} a_i b_i + \sum_{i=0}^{m-1} \alpha_i M M^{\mathrm{T}} \beta_i^{\mathrm{T}} \\
&= (u+v)\sum_{i=0}^{n-1} a_i b_i + \tau \sum_{i=0}^{m-1} \alpha_i \beta_i^{\mathrm{T}} \\
&= (u+v)\sum_{i=0}^{n-1} a_i b_i + \tau \sum_{i=0}^{m-1} (y_i' z_i' + y_i'' z_i'' + y_i''' z_i''') = 0.
\end{aligned}$$

Then, $\Phi(w) \in \Phi(C)^{\perp}$, and hence, $\Phi(C^{\perp}) \subseteq \Phi(C)^{\perp}$. Now, Φ being bijection, $\mid \Phi(C^{\perp}) \mid = \mid \Phi(C)^{\perp} \mid$. Therefore, $\Phi(C^{\perp}) = \Phi(C)^{\perp}$.

Further, let C be self-dual, i.e., $C = C^{\perp}$. Then, $\Phi(C) = \Phi(C^{\perp}) = \Phi(C)^{\perp}$. Hence, $\Phi(C)$ is self-dual. On the other hand, let $\Phi(C)$ be self-dual, i.e., $\Phi(C) = \Phi(C)^{\perp} = \Phi(C^{\perp})$. Since Φ is a bijection, $C = C^{\perp}$. Thus, C is self-dual. □

Now, $\pi_n : \mathbb{F}_q^n R^m \longrightarrow \mathbb{F}_q^n$ defined by $\pi_n(a, b) = a$ and $\pi_m : \mathbb{F}_q^n R^m \longrightarrow R^m$ defined by $\pi_n(a, b) = b$, where $a \in \mathbb{F}_q^n, b \in R^m$ are two projective R-module homomorphisms. Let C be an $\mathbb{F}_q R$-additive linear code of length (n, m). Then, $C_n = \pi_n(C)$ is a linear code of length n over $\mathbb{F}_q$ and $C_m = \pi_m(C)$ is a linear code of length m over R. If $C = C_n \times C_m$, then C is said to be separable. Also, for a separable code C, its dual is $C^{\perp} = C_n^{\perp} \times C_m^{\perp}$. We classify the separable $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m) in the next result.

Theorem 6 *Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive linear code of length (n, m). Then, C is an $\mathbb{F}_q R$-additive λ-constacyclic code if and only if C_n is a cyclic code and C_m is a λ-constacyclic code, respectively.*

Proof Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m). Now, let $a = (a_0, a_1, \ldots, a_{n-1}) \in C_n$ and $z = (z_0, z_1, \ldots, z_{m-1}) \in C_m$.

Then, $(a, z) \in C$ and $(\sigma(a), \sigma_\lambda(z)) \in C$. Therefore, $\sigma(a) \in C_n, \sigma_\lambda(z) \in C_m$. Hence, C_n is a cyclic code and C_m is a λ-constacyclic code, respectively.

Conversely, let C_n be a cyclic code and C_m be a λ-constacyclic code. Let $(a, z) \in C$. Then, $a \in C_n$ and $z \in C_m$, and this implies $\sigma(a) \in C_n, \sigma_\lambda(z) \in C_m$. Hence, $(\sigma(a), \sigma_\lambda(z)) \in C$. Thus, C is an $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m). □

Corollary 1 *Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive linear code of length (n, m), where C_n is a linear code of length n over $\mathbb{F}_q$ and $C_m = \bigoplus_{i=1}^{3} \xi_i C_i$ is a linear code of length m over R. Then, C is an $\mathbb{F}_q R$-additive λ-constacyclic code if and only if C_n is cyclic, C_1 is λ_1-constacyclic, C_2 is $(\lambda_1 + \gamma\lambda_2)$-constacyclic and C_3 is $(\lambda_1 + \delta\lambda_3)$-constacyclic codes over $\mathbb{F}_q$, respectively.*

Here, we use the separable $\mathbb{F}_q R$-additive linear codes to obtain quantum codes. Before that, we discuss the necessary and sufficient conditions of these codes to contain their duals.

Lemma 7 *Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive linear code of length (n, m). Then, $C^\perp \subseteq C$ if and only if $C_n^\perp \subseteq C_n$ and $C_m^\perp \subseteq C_m$.*

Proof Let $C^\perp = C_n^\perp \times C_m^\perp \subseteq C = C_n \times C_m$. Then, $C_n^\perp \subseteq C_n$ and $C_m^\perp \subseteq C_m$. On the other hand, if $C_n^\perp \subseteq C_n$ and $C_m^\perp \subseteq C_m$, then $C^\perp = C_n^\perp \times C_m^\perp \subseteq C_n \times C_m = C$. □

Theorem 7 *Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m), where $C_n = \langle f(x) \rangle$ and $C_m = \langle \sum_{i=1}^{3} \xi_i g_i(x) \rangle$. Then, $C^\perp \subseteq C$ if and only if*

$$\begin{aligned} x^n - 1 &\equiv 0 \,(\mathrm{mod}\, f(x) f^*(x)) \\ x^m - \lambda_1 &\equiv 0 \,(\mathrm{mod}\, g_1(x) g_1^*(x)) \\ x^m - (\lambda_1 + \gamma\lambda_2) &\equiv 0 \,(\mathrm{mod}\, g_2(x) g_2^*(x)) \\ x^m - (\lambda_1 + \delta\lambda_3) &\equiv 0 \,(\mathrm{mod}\, g_3(x) g_3^*(x)), \end{aligned}$$

where $\lambda_1 = \pm 1, \lambda_1 + \gamma\lambda_2 = \pm 1, \lambda_1 + \delta\lambda_3 = \pm 1$.

Proof Combining Lemmas 4 and 7, it is verified. □

Theorem 7 gives the necessary and sufficient condition for separable $\mathbb{F}_q R$-additive λ-constacyclic codes to contain their duals. Now, in light of Lemma 5 and fact $\Phi(C^\perp) = \Phi(C)^\perp$, we present the construction of quantum codes from separable $\mathbb{F}_q R$-additive λ-constacyclic code in the next theorem.

Theorem 8 *Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m) such that $C^\perp \subseteq C$. Then, there exists a quantum code $[[n + 3m, 2k - (n + 3m), d_H]]_q$ over $\mathbb{F}_q$.*

Proof Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m) such that $C^\perp \subseteq C$. Then, $\Phi(C^\perp) \subseteq \Phi(C)$. By Lemma 6, we have $\Phi(C^\perp) =$

$\Phi(C)^{\perp}$, and hence, $\Phi(C)^{\perp} \subseteq \Phi(C)$. In this way, $\Phi(C)$ is a dual-containing $[n+3m, k, d_H]$ linear code over $\mathbb{F}_q$ where d_H is the minimum Hamming distance. Now, applying Lemma 5 on $\Phi(C)$, we have a quantum code over $\mathbb{F}_q$ with parameters $[[n+3m, 2k-(n+3m), d_H]]_q$. □

Remark 2 Note that the length of the quantum code obtained by using Theorem 5 must be an integral multiple of 3, whereas the code length in Theorem 8 has no such limitation, i.e., we can find code of any length $(n+3m)$ with some suitable choices of n and m. For example, in order to obtain a code of length 40, there are finitely many options for n and m such that $n+3m=40$, and $n=m=10$ is one of them. This is one of the advantages to study the $\mathbb{F}_q R$-additive λ-constacyclic codes in quantum codes construction.

5 New codes and comparison

It is well known that some good quantum codes are available in the online database [16]. Along with the database, we also use few recent articles [1,3,14,15,18,20,22,24,28–30] (published within last two year) to compare our obtained quantum codes. It is worth mentioning that with the help of Theorems 5 and 8, we determine several new and better quantum codes than existing codes which are appeared in the above-mentioned articles. All computations involved in the examples are carried out by the Magma computation system [8].

Example 1 Let $q=17, n=8$ and $R=\mathbb{F}_{17}[u,v]/\langle u^2-\gamma u, v^2-\delta v, uv=vu=0\rangle$ where $\gamma, \delta \in \mathbb{F}_{17}^{*}$. If $\lambda = 1-2u\gamma^{-1}-2v\delta^{-1}$, then $\lambda_1=1, \lambda_1+\gamma\lambda_2=\lambda_1+\delta\lambda_3=-1$. Now,

$$x^8-1=(x+1)(x+2)(x+4)(x+8)(x+9)(x+13)(x+15)(x+16) \in \mathbb{F}_{17}[x]$$
$$x^8+1=(x+3)(x+5)(x+6)(x+7)(x+10)(x+11)(x+12)(x+14) \in \mathbb{F}_{17}[x].$$

Let $C=\langle \sum_{i=1}^{3} \xi_i g_i(x)\rangle$ be an $(1-2u\gamma^{-1}-2v\delta^{-1})$-constacyclic code of length 8 over R, where $g_1(x)=(x+2)(x+4)=x^2+6x+8$, $g_2(x)=(x+5)(x+6)=x^2+11x+13$ and $g_3(x)=(x+3)(x+5)(x+10)=x^3+x^2+10x+14$. Let

$$M=\begin{bmatrix} 2 & 1 & 2 \\ 15 & 2 & 1 \\ 1 & 2 & 15 \end{bmatrix}$$

be a 3×3 invertible matrix such that $MM^{\mathrm{T}}=9I_3$. Since $x^8-1 \equiv 0 \pmod{g_1(x)g_1^{*}(x)}$ and $x^8+1 \equiv 0 \pmod{g_i(x)g_i^{*}(x)}$ for $i=2,3$, by Theorem 4, we have $C^{\perp} \subseteq C$. Therefore, $\varphi(C)$ is a dual-containing $[24, 17, 5]$ linear code over $\mathbb{F}_{17}$. Hence, by Theorem 5, we have a quantum code $[[24, 10, 5]]_{17}$, which has same length and minimum distance but larger code rate than the known code $[[24, 8, 5]]_{17}$ given by [28].

Example 2 Let $q=9, n=6, R=\mathbb{F}_9[u,v]/\langle u^2-\gamma u, v^2-\delta v, uv=vu=0\rangle$ where $\gamma,\delta\in\mathbb{F}_9^*$. If $\lambda=1-2u\gamma^{-1}-2v\delta^{-1}$, then $\lambda_1=1, \lambda_1+\gamma\lambda_2=\lambda_1+\delta\lambda_3=-1$. Now,

$$x^6-1=(x+1)^3(x+2)^3\in\mathbb{F}_9[x]$$
$$x^6+1=(x+w^2)^3(x+w^6)^3\in\mathbb{F}_9[x].$$

Let $C=\langle\sum_{i=1}^{3}\xi_i g_i(x)\rangle$ be an $(1-2u\gamma^{-1}-2v\delta^{-1})$-constacyclic code of length 6 over R, where $g_1(x)=x+2, g_2(x)=x+w^2, g_3(x)=(x+w^2)(x+w^6)^2=x^3+w^6x^2+x+w^6$ and $w^2+2w+2=0$. Also, let

$$M=\begin{bmatrix} w & -w^7 & 1\\ -w^7 & 1 & w\\ 1 & w & -w^7\end{bmatrix}$$

be a 3×3 invertible matrix over $\mathbb{F}_9$ such that $MM^{\mathrm{T}}=I_3$. Since $x^6-1\equiv 0\,(\mathrm{mod}\, g_1(x)g_1^*(x))$ and $x^6+1\equiv 0\,(\mathrm{mod}\, g_i(x)g_i^*(x))$, for $i=2,3$, by Theorem 4 we have $C^{\perp}\subseteq C$. Therefore, $\varphi(C)$ is a dual-containing $[18,13,4]$ linear code over $\mathbb{F}_9$. Thus, by Theorem 5, there exists a quantum code $[[18,8,4]]_9$ which has same minimum distance but larger code rate compared to the known code $[[24,8,4]]_9$ given by [29].

Example 3 Let $\lambda=\lambda_1+u\lambda_2+v\lambda_3$ be a unit in $R=\mathbb{F}_q[u,v]/\langle u^2-\gamma u, v^2-\delta v, uv=vu=0\rangle$ such that $\lambda_1=\pm1, \lambda_1+\gamma\lambda_2=\pm1, \lambda_1+\delta\lambda_3=\pm1$, where $\lambda_i\in\mathbb{F}_q, \gamma,\delta\in\mathbb{F}_q^*$, for $i=1,2,3$. Let $C=\langle\sum_{i=1}^{3}\xi_i g_i(x)\rangle$ be a λ-constacyclic code over R such that $x^n-\lambda_1\equiv 0\,(g_1(x)g_1^*(x)), x^n-(\lambda_1+\gamma\lambda_2)\equiv 0\,(g_2(x)g_2^*(x)), x^n-(\lambda_1+\delta\lambda_3)\equiv 0\,(g_3(x)g_3^*(x))$. Also, let

$$M=\begin{bmatrix} 2 & 1 & 2\\ -2 & 2 & 1\\ 1 & 2 & -2\end{bmatrix}, \quad \text{satisfying } MM^{\mathrm{T}}=9I_3 \text{ for } q\neq 9,$$
$$M=\begin{bmatrix} w & -w^7 & 1\\ -w^7 & 1 & w\\ 1 & w & -w^7\end{bmatrix}, \quad \text{satisfying } MM^{\mathrm{T}}=I_3 \text{ for } q=9.$$

Then, $\varphi(C)$ is a dual-containing $[n,k,d]$ linear code enlisted in the seventh column of Table 1. In the eighth column, we construct $[[n,k,d]]_q$ quantum codes which are better (by means of distance or code rate) compared to the existing codes $[[n',k',d']]_q$ given in the ninth column. In Table 1, the first column represents the length n, the second column represents the value of q, the third column represents the value of λ and the fourth to sixth columns represent the generator polynomials $g_i(x)$, for $i=1,2,3$, respectively. In order to precise Table 1, we write the string containing the coefficients of the polynomials $g_i(x)$ in descending order. For instance, we write the string $1w^3w^5w^6$ to represent the polynomial $x^3+w^3x^2+w^5x+w^6$.

Table 1 New quantum codes from λ-constacyclic codes of length n over R

q	n	λ	$g_1(x)$	$g_2(x)$	$g_3(x)$	$\varphi(C)$	$[[n,k,d]]_q$	$[[n',k',d']]_q$
5	5	$1-2u\gamma^{-1}-2v\delta^{-1}$	131	11	11	[15, 11, 3]	$[[15,7,3]]_5$	$[[15,3,3]]_5$ [14]
5	6	$1-2u\gamma^{-1}-2v\delta^{-1}$	1433	1433	134	[18, 10, 5]	$[[18,2,5]]_5$	$[[19,1,5]]_5$ [16]
5	10	$1-2u\gamma^{-1}-2v\delta^{-1}$	1441	1212	13421	[30, 20, 6]	$[[30,10,6]]_5$	$[[30,6,6]]_5$ [20]
5	60	$1-2u\gamma^{-1}$	14401	103	14	[180, 173, 3]	$[[180,166,3]]_5$	$[[180,166,2]]_5$ [1]
9	7	$1-2u\gamma^{-1}-2v\delta^{-1}$	$1ww^7 2$	$1w^5w^7 1$	$1w^7w^5 1$	[21, 12, 5]	$[[21,3,5]]_9$	$[[17,1,4]]_9$ [16]
9	6	$1-2u\gamma^{-1}-2v\delta^{-1}$	12	$1w^2$	$1w^6 1w^6$	[18, 13, 4]	$[[18,8,4]]_9$	$[[24,8,4]]_9$ [29]
9	8	$1-2u\gamma^{-1}-2v\delta^{-1}$	$1w^3w^3$	$10w^2$	$10w^3$	[24, 18, 4]	$[[24,12,4]]_9$	$[[24,10,4]]_9$ [20]
9	4	$1-2u\gamma^{-1}-2v\delta^{-1}$	$1w^2$	112	$1w$	[12, 8, 4]	$[[12,4,4]]_9$	$[[26,4,4]]_9$ [16]
9	10	-1	$1w^2$	$1w^6$	$1w^3w^5w^6$	[30, 25, 4]	$[[30,20,4]]_9$	$[[36,6,4]]_9$ [30]
9	12	$1-2u\gamma^{-1}-2v\delta^{-1}$	$102w^6 0w^2$	$1w^5w^2ww^6w^3$	$1w^3w^6w^7w^2w^5$	[36, 21, 6]	$[[36,6,6]]_9$	$[[36,6,4]]_9$ [30]
9	12	$1-2u\gamma^{-1}-2v\delta^{-1}$	$102w^6 0w^2$	$1w^5w^2ww^6w^3$	$11w^3w^3w^7w^2w^6$	[36, 20, 7]	$[[36,4,7]]_9$	$[[36,4,6]]_9$ [30]
13	6	$1-2u\gamma^{-1}-2v\delta^{-1}$	17(12)	17(10)	18	[18, 13, 4]	$[[18,8,4]]_{13}$	$[[16,6,4]]_{13}$ [29]
13	104	$1-2u\gamma^{-1}-2v\delta^{-1}$	1(11)62081	1005	1008	[312, 300, 4]	$[[312,288,4]]_{13}$	$[[312,276,4]]_{13}$ [15]
17	16	1	12	17(10)	1(14)311	[48, 41, 4]	$[[48,34,4]]_{17}$	$[[48,30,4]]_{17}$ [18]
17	16	1	1(10)(14)(13)	177(14)(11)(10)	1(10)(14)(13)	[48, 37, 5]	$[[48,26,5]]_{17}$	$[[48,24,5]]_{17}$ [18]
17	8	$1-2u\gamma^{-1}-2v\delta^{-1}$	168	1(11)(13)	11(10)(14)	[24, 17, 5]	$[[24,10,5]]_{17}$	$[[24,8,5]]_{17}$ [28]
23	22	1	13	1(15)	1(17)	[66, 63, 4]	$[[66,60,4]]_{23}$	MDS
25	24	1	$1w^3$	$1w^{13}$	$1ww^7$	[72, 68, 5]	$[[72,64,5]]_{25}$	MDS

Table 2 New quantum codes from $\mathbb{F}_q R$-additive λ-constacyclic codes of length (n, m)

q	(n, m)	λ	$f(x)$	$g_1(x)$	$g_2(x)$	$g_3(x)$	$\Phi(C)$	$[[n, k, d]]_q$	$[[n', k', d']]_q$
5	(30, 20)	$1 - 2u\gamma^{-1} - 2v\delta^{-1}$	104401	13332	12	14	[90, 79, 3]	$[[90, 68, 3]]_5$	$[[90, 66, 3]]_5$ [14]
5	(30, 30)	$1 - 2u\gamma^{-1} - 2v\delta^{-1}$	121434	14	13	144233	[120, 108, 3]	$[[120, 96, 3]]_5$	$[[120, 32, 3]]_5$ [22]
5	(30, 20)	1	13431	13	1034	12	[90, 81, 3]	$[[90, 72, 3]]_5$	$[[90, 72, 2]]_5$ [3]
5	(24, 40)	1	1344	12	14	11123	[144, 135, 3]	$[[144, 126, 3]]_5$	$[[144, 120, 3]]_5$ [3]
5	(15, 65)	1	14041	14	1434341	14	[210, 198, 3]	$[[210, 186, 3]]_5$	$[[210, 150, 2]]_5$ [3]
5	(20, 40)	1	1402	14	12342	13	[140, 131, 3]	$[[140, 122, 3]]_5$	$[[140, 116, 3]]_5$ [29]
5	(40, 40)	1	12342	12	14	13	[160, 153, 3]	$[[160, 146, 3]]_5$	$[[160, 146, 2]]_5$ [1]
7	(42, 14)	1	1104	1166	16	16	[84, 76, 3]	$[[84, 68, 3]]_7$	$[[84, 60, 3]]_7$ [24]
7	(14, 7)	$1 - 2u\gamma^{-1} - 2v\delta^{-1}$	1166	151	11	11	[35, 28, 3]	$[[35, 21, 3]]_7$	$[[35, 19, 3]]_7$ [14]
7	(21, 7)	$1 - 2u\gamma^{-1} - 2v\delta^{-1}$	162615	1436	11	11	[42, 32, 4]	$[[42, 22, 4]]_7$	$[[42, 12, 4]]_7$ [14]
7	(24, 24)	$1 - 2u\gamma^{-1} - 2v\delta^{-1}$	12	1215	113	116	[96, 88, 3]	$[[96, 80, 3]]_7$	$[[96, 72, 3]]_7$ [24]
7	(24, 30)	1	16153	163561	12	13	[114, 103, 3]	$[[114, 92, 3]]_7$	$[[114, 90, 3]]_7$ [15]
23	(23, 23)	$1 - 2u\gamma^{-1} - 2v\delta^{-1}$	1(21)1	1(22)	121	11	[92, 86, 3]	$[[92, 80, 3]]_{23}$	$[[92, 78, 3]]_{23}$ [14]

Example 4 Let $q = 5$, $(n, m) = (30, 20)$, $R = \mathbb{F}_5[u, v]/\langle u^2 - \gamma u, v^2 - \delta v, uv = vu = 0\rangle$ and $\lambda = 1$, where $\gamma, \delta \in \mathbb{F}_5^*$. Then, $\lambda_1 = \lambda_1 + \gamma\lambda_2 = \lambda_1 + \delta\lambda_3 = 1$. Now, in $\mathbb{F}_5[x]$ we have

$$x^{30} - 1 = (x+1)^5(x+4)^5(x^2+x+1)^5(x^2+4x+1)^5$$
$$x^{20} - 1 = (x+1)^5(x+2)^5(x+3)^5(x+4)^5.$$

Let $C = C_{30} \times C_{20}$ be a separable $\mathbb{F}_5 R$-additive cyclic code of length (30, 20) where $C_{30} = \langle f(x)\rangle$ and $C_{20} = \langle \sum_{i=1}^{3} \xi_i g_i(x)\rangle$. Let $f_1(x) = (x+1)^2(x^2+x+1) = x^4 + 3x^3 + 4x^2 + 3x + 1$, $g_1(x) = x + 3$, $g_2(x) = (x+1)(x+2)^2 = x^3 + 3x + 4$ and $g_3(x) = x + 2$. Let

$$M = \begin{bmatrix} 2 & 1 & 2 \\ 3 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

be a 3×3 invertible matrix over $\mathbb{F}_5$ such that $MM^{\mathrm{T}} = 9I_3$. Since $x^{30} - 1 \equiv 0 \pmod{f(x)f^*(x)}$ and $x^{20} - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for $i = 1, 2, 3$, by Theorem 7, we have $C^{\perp} \subseteq C$. Moreover, $\Phi(C)$ is a dual-containing [90, 81, 3] linear code over $\mathbb{F}_5$. Hence, by Theorem 8, there exists a quantum code $[[90, 72, 3]]_5$, which has same length and code rate but larger minimum distance than existing code $[[90, 72, 2]]_5$ given by [3].

Example 5 Let $\lambda = \lambda_1 + u\lambda_2 + v\lambda_3$ be a unit in $R = \mathbb{F}_q[u, v]/\langle u^2 - \gamma u, v^2 - \delta v, uv = vu = 0\rangle$ such that $\lambda_1 = \pm 1, \lambda_1 + \gamma\lambda_2 = \pm 1, \lambda_1 + \delta\lambda_3 = \pm 1$, where $\lambda_i \in \mathbb{F}_q, \gamma, \delta \in \mathbb{F}_q^*$, for $i = 1, 2, 3$. Let $C = C_n \times C_m$ be a separable $\mathbb{F}_q R$-additive λ-constacyclic code of length (n, m), where $C_n = \langle f(x)\rangle$ and $C_m = \langle \sum_{i=1}^{3} \xi_i g_i(x)\rangle$ be such that $x^n - 1 \equiv 0\,(f(x)f^*(x))$, $x^m - \lambda_1 \equiv 0\,(g_1(x)g_1^*(x))$, $x^m - (\lambda_1 + \gamma\lambda_2) \equiv 0\,(g_2(x)g_2^*(x))$, $x^m - (\lambda_1 + \delta\lambda_3) \equiv 0\,(g_3(x)g_3^*(x))$. Let

$$M = \begin{bmatrix} 2 & 1 & 2 \\ -2 & 2 & 1 \\ 1 & 2 & -2 \end{bmatrix}, \quad \text{satisfying } MM^{\mathrm{T}} = 9I_3.$$

Then, $\Phi(C)$ is a dual-containing $[n, k, d]$ linear code over $\mathbb{F}_q$ given in the eighth column of Table 2. By Theorem 8, we construct quantum codes $[[n, k, d]]_q$ (in the ninth column) better (by means of larger code rate or larger distance) than the existing codes $[[n', k', d']]_q$ (in the tenth column).

6 Conclusion

For the last few years, constacyclic codes over finite non-chain rings have become a great resource to produce good quantum codes. Here, we explore many new quantum codes from these codes over a class of finite commutative non-chain rings R. Further, we extend our study to additive constacyclic codes and construct many quantum codes from them. To validate the novelty of the approach, we also compare our obtained codes to the existing codes that appeared in some recent articles.

Acknowledgements The authors are thankful to the University Grants Commission (UGC), Govt. of India, for financial supports under Sr. No. 2121540952, Ref. No. 20/12/2015(ii)EU-V dated 31/08/2016 and Indian Institute of Technology Patna for providing research facilities. The authors would like to thank the editor and anonymous referee(s) for careful reading and constructive suggestions to improve the presentation of the manuscript.

References

1. Alkenani, A. N., Ashraf, M., Mohammad, G.: Quantum codes from the constacyclic codes over the ring $\mathbb{F}_q[u_1, u_2]/\langle u_1^2 - u_1, u_2^2 - u_2, u_1u_2 - u_2u_1\rangle$. Mathematics **8**(5), 781: https://doi.org/10.3390/math8050781 (2020)
2. Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Quantum Inf. Process. **15**(10), 4089–4098 (2016)
3. Ashraf, M., Mohammad, G.: Quantum codes over $\mathbb{F}_p$ from cyclic codes over $\mathbb{F}_p[u, v]/\langle u^2 - 1, v^3 - v, uv - vu\rangle$. Cryptogr. Commun. **11**(2), 325–335 (2019)
4. Aydin, N., Abualrub, T.: Optimal quantum codes from additive skew cyclic codes. Discrete Math. Algorithms Appl. **8**(3), 1650037 9 pp (2016)
5. Aydogdu, I., Abualrub, T.: Self-Dual Cyclic and Quantum Codes Over $\mathbb{Z}_2 \times (\mathbb{Z}_2 + u\mathbb{Z}_2)$. Discrete Math. Algorithms Appl. **11**(4), 1950041 15 pp (2019)
6. Aydogdu, I., Abualrub, T., Siap, I.: $\mathbb{Z}_2\mathbb{Z}_2[u]$-Cyclic and Constacyclic Codes. IEEE Trans. Inform. Theory. **63**(8), 4883–4893 (2016)
7. Borges, J., Fernandez-Cordoba, C., Pujol, J., Rifa, J., Villanueva, M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator matrices and duality. Designs Codes Cryptogr. **54**(2), 167–179 (2010)
8. Bosma, W., Cannon, J.: Handbook of Magma Functions. Univ. of Sydney (1995)
9. Calderbank, A.R., Rains, E.M., Shor, P.M., Sloane, N.J.A.: Quantum error correction via codes over $GF(4)$. IEEE Trans. Inform. Theory **44**, 1369–1387 (1998)
10. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**(3), 1474–1484 (2015)
11. Delsarte, P., Levenshtein, V.I.: Association schemes and coding theory. IEEE Trans. Inform. Theory **44**, 2477–2504 (1998)
12. Dertli, A., Cengellenmis, Y., Eren, S.: On quantum codes obtained from cyclic codes over A_2. Int. J. Quantum Inf. **13**(3), 1550031 (2015)
13. Diao, L., Gao, J.: $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes. Int. J. Inf. Coding Theory **5**(1), 1–17 (2018)
14. Diao, L., Gao, J., Lu, J.: Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes. Adv. Math. Commun. (2019). https://doi.org/10.3934/amc.2020029
15. Dinh, H.Q., Bag, T., Upadhyay, A.K., Ashraf, M., Mohammad, G.: Quantum codes from a class of constacyclic codes over finite commutative rings. J. Algebra Appl. (2019). https://doi.org/10.1142/S0219498821500031
16. Edel, Y.: Some good quantum twisted codes. https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html
17. Gao, J., Wang, Y.: 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**(1), 9 pp (2018)
18. Gao, Y., Gao, J., Fu, F.W.: On Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$. Appl. Algebra Engrg. Comm. Comput. **30**(2), 161–174 (2019)
19. Grassl, M., Beth, T.: On optimal quantum codes. Int. J. Quantum Inf. **2**, 55–64 (2004)
20. Islam, H., Prakash, O., Verma, R.K.: New quantum codes from constacyclic codes over the ring $R_{k,m}$. Adv. Math. Commun. (2020). https://doi.org/10.3934/amc.2020097
21. Islam, H., Prakash, O., Solé, P.: $\mathbb{Z}_4\mathbb{Z}_4[u]$-additive cyclic and constacyclic codes. Adv. Math. Commun. (2020). https://doi.org/10.3934/amc.2020094
22. Islam, H., Prakash, O.: Quantum codes from the cyclic codes over $\mathbb{F}_p[u, v, w]/\langle u^2 - 1, v^2 - 1, w^2 - 1, uv - vu, vw - wv, wu - uw\rangle$. J. Appl. Math. Comput. **60**(1–2), 625–635 (2019)

23. Islam, H., Prakash, O., Bhunia, D.K.: Quantum codes obtained from constacyclic codes. Internat. J. Theoret. Phys. **58**(11), 3945–3951 (2019)
24. Islam, H., Prakash, O., Verma, R.K.: Quantum codes from the cyclic codes over $\mathbb{F}_p[v, w]/\langle v^2 - 1, w^2 - 1, vw - wv\rangle$. Springer Proceedings in Mathematics & Statistics **307**, 67–74 (2019). https://doi.org/10.1007/978-981-15-1157-8-6
25. Islam, H., Prakash, O., Verma, R.K.: A family of constacyclic codes over $\mathbb{F}_{p^m}[v, w]/\langle v^2 - 1, w^2 - 1, vw - wv\rangle$. Int. J. Inf. Coding Theory (2020). https://doi.org/10.1504/IJICOT.2019.10026515
26. Kai, X., Zhu, S.: Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Int. J. Quantum Inf. **9**, 689–700 (2011)
27. Li, J., Gao, J., Fu, F.W., Ma, F.: $\mathbb{F}_q R$-linear skew constacyclic codes and their application of constructing quantum codes. Quantum Inf. Process (2020). https://doi.org/10.1007/s11128-020-02700-x
28. Ma, F., Gao, J., Fu, F. W.: Constacyclic codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ and their applications of constructing new non-binary quantum codes. Quantum Inf. Process, **17** (6), 19 pp. Art. 122 (2018)
29. Ma, F., Gao, J., Fu, F.W.: New non-binary quantum codes from constacyclic codes over $\mathbb{F}_q[u, v]/\langle u^2 - 1, v^2 - v, uv - vu\rangle$. Adv. Math. Commun. **13**(2), 421–434 (2019)
30. Ozen, M., Ozzaim, N.T., Ince, H.: Skew quasi cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. J. Algebra Appl. **18**(4), 1950077 (2019)
31. Qian, J.: Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. J. Inf. Compt. Sci. **10**, 1715–1722 (2013)
32. Rifa-Pous, H., Rifa, J., Ronquillo, L.: $\mathbb{Z}_2\mathbb{Z}_4$-Additive Perfect Codes in Steganography. Adv. Math. Commun. **5**(3), 425–433 (2011)
33. Sari, M., Siap, I.: On quantum codes from cyclic codes over a class of nonchain rings. Bull. Korean Math. Soc. **53**(6), 1617–1628 (2016)
34. Shi, M., Wu, R., Krotov, D.S.: On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality. IEEE Trans. Inform. Theory **65**(6), 3841–3847 (2019)
35. Shor, P.W.: Scheme for reducing decoherence in quantum memory Phys. Rev. A. **52**, 2493–2496 (1995)
36. 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