# Hermitian hull of constacyclic codes over a class of non-chain rings and new quantum codes

Shikha Yadav, Ashutosh Singh, Habibul Islam, Om Prakash, Patrick Solé

# Hermitian hull of constacyclic codes over a class of non-chain rings and new quantum codes

Shikha Yadav[1], Ashutosh Singh[1], Habibul Islam[2], Om Prakash[1*], Patrick Solé[3]

[1*]Department of Mathematics, Indian Institute of Technology Patna, Bihta, Patna, 801106, Bihar, India.
[2]School of Computer Science, University of St. Gallen, Torstrasse 25, St. Gallen, 9000, Switzerland.
[3] Aix-Marseille University, I2M, Marseille, 13284, France.

*Corresponding author(s). E-mail(s): om@iitp.ac.in;
Contributing authors: 1821ma10@iitp.ac.in;
ashutosh_1921ma05@iitp.ac.in; habibul.islam@unisg.ch; sole@enst.fr;

**Abstract**

Let $p$ be a prime number and $q = p^m$ for some positive integer $m$. In this paper, we find the possible Hermitian hull dimensions of $\lambda$-constacyclic codes over $R_e = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + u^2\mathbb{F}_{q^2} + \cdots + u^{e-1}\mathbb{F}_{q^2}$, $u^e = 1$ where $\mathbb{F}_{q^2}$ is the finite field of $q^2$ elements, $e|(q+1)$ and $\lambda = \eta_1\alpha_1 + \eta_2\alpha_2 + \cdots + \eta_e\alpha_e$ for $\alpha_l \in \mathbb{F}_{q^2}^*$ of order $r_l$ such that $r_l \mid q+1$ (for each $1 \leq l \leq e$). Further, we obtain some conditions for these codes to be Hermitian LCD. Also, under certain conditions, we establish a strong result that converts every constacyclic code to a Hermitian LCD code (Corollaries 3.2 and 3.3). Moreover, we study the structure of generator polynomials for Hermitian dual-containing constacyclic codes and obtain parameters of quantum codes using the Hermitian construction. The approach that we used to derive Hermitian dual-containing conditions *via* the hull has not been used earlier. As an application, we obtain several optimal and near-to-optimal LCD codes, constacyclic codes having small hull dimensions, and quantum codes.

**Keywords:** Hull of linear codes, Hull dimension, LCD codes, Gray map, Quantum codes

# 1 Introduction

The hull of a linear code is defined as the intersection of the code with its dual. It was introduced and employed by Assmus and Key [2] to Euclidean dual for the classification of finite projective planes. The hulls of linear codes play a significant role in obtaining the complexity of some algorithms for determining the automorphism group and examining the permutation equivalence of linear codes (see [23, 37, 38]). It is worth noting that most of these algorithms work for small hull dimensions. Therefore, the linear codes with small hull dimensions are of great importance for the implementation of these algorithms, which have been studied in [9, 24]. In 1997, Sendrier [36] obtained the number of different linear codes over $\mathbb{F}_q$ having the given hull dimension. In 2003, Skersys [40] studied the average hull dimension of cyclic codes over finite fields and established that the hull of most cyclic codes of given length $n$ is large for almost all $n$. For some other related works on hulls, refer [18–21, 34, 35]. In 2018, Guenda et al. [12] constructed maximal entanglement EAQECCs by establishing a relation between the number of maximally entangled states and the hull (Euclidean and Hermitian) of linear codes. Recently, Mankean and Jitman constructed optimal binary and ternary linear codes with hull dimension one in [28] and quaternary linear codes of dimension 2 having the Hermitian hull dimension one in [29]. They also obtained some bounds on the minimum weight of these codes.

LCD codes are linear codes having a hull dimension zero. These codes were introduced and implemented by Massey [30] in 1992 to obtain an optimum linear coding solution for a two-user binary adder channel (2-BAC). In 1994, a necessary and sufficient condition for cyclic codes over a finite field to be LCD was derived by Yang and Massey [48]. Later, some bounds for these codes were derived, and these codes were studied over finite chain rings in [27, 31, 39]. Recently, LCD codes were shown to have applications in cryptography for protection against SCA and FIA [8]. Subsequently, many articles were written about these codes over finite fields and various rings [10, 15–17, 25, 26, 33, 43–46]. Apart from these, LCD codes were also shown to have applications in a multi-secret sharing scheme (see [1, 32]). On the contrary, there is a class of linear codes that contain their dual. This class of codes plays a crucial role in constructing quantum error-correcting codes (QECC) to be used in quantum computation. In 1995, Shor [42] discovered QECCs. Later, some constructions were provided to obtain QECCs from classical error-correcting codes. Among these, one of the famous construction is CSS construction [6]. By using this construction, many good QECCs were obtained [4, 7, 13, 14, 16, 41].

Motivated by the above-mentioned works, we first obtain the Hermitian hull dimension of $\lambda$-constacyclic codes (with the help of their generator polynomial) over the ring $R_e = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + u^2\mathbb{F}_{q^2} + \cdots + u^{e-1}\mathbb{F}_{q^2}$, $u^e = 1$ such that $e|(q+1)$ and $\lambda = \eta_1\alpha_1 + \eta_2\alpha_2 + \cdots + \eta_e\alpha_e$ for $\alpha_l \in \mathbb{F}_{q^2}^*$ of order $r_l$ such that $r_l \mid q+1$ (for each $1 \leq l \leq e$). We also present a Gray map in terms of a matrix to obtain codes over finite field from the codes over the ring $R_e$. Further, we obtain some conditions for these codes to satisfy complementary duality and dual containing property. We establish a strong result that converts every constacyclic code to a Hermitian LCD code (Corollaries 3.2 and 3.3). Moreover, we study the structure of generator polynomials for Hermitian dual-containing constacyclic codes. As an application of these, we

obtain several LCD and quantum codes over a finite field through a Gray map. We use the notation $[[n,k,d]]_q$ to represent a QECC over $\mathbb{F}_q$ of length $n$, dimension $q^k$ and minimum distance $d$. For ease of understanding, we first present results for $e=2$ with their proofs and later present their analogues for $e>2$.
This paper is organized as follows: Section 2 contains some basic definitions, a Gray map in terms of a matrix with certain properties, and some related results essential for further study. In Section 3, we study the Hermitian hull dimension of constacyclic codes over $R_e$ and obtain conditions for these codes to be LCD. Section 4 presents certain conditions under which a constacyclic code over $R_e$ has dual containing property and is employed to obtain quantum codes by using the Hermitian construction. In Section 5, we present some examples of LCD codes, quantum codes, and constacyclic codes with small hull dimensions. Section 6 concludes the work.

# 2 Preliminary

Let $q=p^m$ for an odd prime $p$ and a positive integer $m$. Following [32], we choose $\gamma \in \mathbb{F}_{q^2}$ such that $2\gamma \equiv 1 \pmod p$ and consider the ring $R_2 = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$ where $u^2=1$. Then, by the Chinese Remainder Theorem, we have $R_2 \cong \epsilon_1\mathbb{F}_{q^2} \oplus \epsilon_2\mathbb{F}_{q^2}$ where $\epsilon_1 = \gamma(1+u), \epsilon_2 = \gamma(1-u)$ and every element $r \in R_2$ can be uniquely written as $r = \epsilon_1 r_1 + \epsilon_2 r_2$ for some $r_1, r_2 \in \mathbb{F}_{q^2}$. It is worth noting that $r$ is a unit in $R_2$, i.e., $r \in R_2^*$ if and only if $r_1$ and $r_2$ are non-zero. Consider another ring $R_e = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + u^2\mathbb{F}_{q^2} + \cdots + u^{e-1}\mathbb{F}_{q^2}$, $u^e = 1$ such that $e|(q+1)$ ($q$ can also be even depending upon $e$). Then, following [41], we have $R_e \cong \bigoplus_{i=1}^{e} \eta_i \mathbb{F}_{q^2}$, where $\eta_i = (u^e-1)/(u-\mu^{i-1})$ for $1 \le i \le e$ and $\mu$ is a primitive $e$-th root of unity. Now, every element $\mathfrak{r} \in R_e$ can be uniquely expressed as $\mathfrak{r} = \sum_{i=1}^{e} \eta_i r_i$, where each $r_i \in \mathbb{F}_{q^2}$. Further, $\mathfrak{r} \in R_e$ is a unit element if and only if each $r_i$ is a unit in $\mathbb{F}_{q^2}$.
For any polynomial $p(x) = a_0 + a_1 x + \cdots + a_s x^s \in \mathbb{F}_{q^2}[x]$ with $a_0, a_s \neq 0$, the monic conjugate-reciprocal polynomial is defined as $p^\dagger(x) = a_0^{-q} \sum_{i=0}^{s} a_i^q x^{s-i}$. Note that $(p^\dagger)^\dagger(x) = p(x)$. If $p^\dagger(x) = p(x)$, then $p(x)$ is said to be a self-conjugate-reciprocal polynomial, otherwise $p(x), p^\dagger(x)$ are said to be a conjugate-reciprocal polynomial pair. For a matrix $M = [m_{ij}]$, we denote its transpose matrix by $M^T$ which is defined as $M^T = [m_{ji}]$. The conjugate transpose of a matrix $M$ is denoted by $M^*$ and defined as $M^* = [m_{ij}^q]^T = [m_{ji}^q]$.

## 2.1 Linear codes over $\mathbb{F}_{q^2}$

A linear code $C$ of length $n$ and dimension $k$ over a finite field $\mathbb{F}_{q^2}$ is defined as a $k$-dimensional subspace of $\mathbb{F}_{q^2}^n$, and the elements of $C$ are called codewords. Recall that a code $C$ is said to be an $\alpha-$*constacyclic code* over $\mathbb{F}_{q^2}$ for some $\alpha \in \mathbb{F}_{q^2}^*$, if for every $c=(c_0, c_1, \ldots, c_{n-1}) \in C$, we also have $\tau_\alpha(c) = (\alpha c_{n-1}, c_0, \ldots, c_{n-2})$ in $C$. The Hermitian dual $C^{\perp_H}$ of a linear code $C$ over the finite field $\mathbb{F}_{q^2}$ is defined as

$$C^{\perp_H} = \{x \in \mathbb{F}_{q^2}^n : \langle x, c\rangle_H = \sum_{i=0}^{n-1} x_i c_i^q = 0, \ \forall\ c \in C\}$$

where $x = (x_0, x_1, \ldots, x_{n-1})$ and $c = (c_0, c_1, \ldots, c_{n-1})$. If $C \cap C^{\perp_H} = \{\mathbf{0}\}$, then we say that $C$ is a Hermitian LCD code. The code $C$ is said to be a Hermitian dual-containing code (resp. self-dual code with respect to the Hermitian inner product) if $C^{\perp_H} \subseteq C$ (resp. $C = C^{\perp_H}$). Any $\alpha-$constacyclic code $C$ of length $n$ over $\mathbb{F}_{q^2}$ can also be considered as an ideal of $\frac{\mathbb{F}_{q^2}[x]}{\langle x^n-\alpha\rangle}$ on identifying $(c_0, c_1, \ldots, c_{n-1})$ with the polynomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. In particular, an $\alpha-$constacyclic code $C$ can be considered as a principal ideal generated by a monic polynomial $g(x)$ such that $g(x) \mid x^n - \alpha$ and this monic polynomial $g(x)$ is called the *generator polynomial* of $C$. If we take $\alpha$ in $\mathbb{F}_{q^2}$ of order $r$ such that $r \mid q+1$, then the Hermitian dual of an $\alpha$-constacyclic code is again an $\alpha$-constacyclic code and so is its Hermitian hull $Hull_H(C) = C \cap C^{\perp_H}$ (see [47]). In that case, the generator polynomial of $C^{\perp_H}$ is $\left(\frac{x^n-\alpha}{g(x)}\right)^\dagger$ and the generator polynomial of $Hull_H(C)$ (using [34, Theorem 1]) is lcm $\left(g(x), \left(\frac{x^n-\alpha}{g(x)}\right)^\dagger\right)$. Thus, the code $C$ is a Hermitian LCD code if and only if lcm $\left(g(x), \left(\frac{x^n-\alpha}{g(x)}\right)^\dagger\right) = x^n - \alpha$. The Hamming distance $d(x, y)$ between two vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ in $\mathbb{F}_{q^2}^n$ is defined as

$$d(x, y) = |\{i : x_i \neq y_i\}|.$$

The minimum (Hamming) distance $d(C)$ of a linear code $C$ is defined as

$$d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

We represent a linear code over the finite field $\mathbb{F}_{q^2}$ having length $n$, dimension $k$, and the minimum (Hamming) distance $d$ by $[n, k, d]_{q^2}$.

## 2.2 Linear codes over $R_e$

A *linear code* $C$ of length $n$ over $R_e$ is an $R_e$-submodule of the module $R_e^n$. The code $C$ is said to be a $\lambda-$*constacyclic code* over $R_e$ for some $\lambda \in R_e^*$, if for every $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, we have $\tau_\lambda(c) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2})$ in $C$. If $\lambda = 1$, then a $\lambda-$constacyclic code is said to be a cyclic code, and if $\lambda = -1$, then we call it as a *negacyclic code*. We define the *Hermitian inner product* of $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1})$ in $R_e^n$ as $\langle x, y\rangle_H = \sum_{i=0}^{n-1} x_i y_i^q = xy^*$, where $y^* = (y_0^q, y_1^q, \ldots, y_{n-1}^q)^T$. Using this inner product, the *Hermitian dual* $C^{\perp_H}$ of $C$ is defined as

$$C^{\perp_H} = \{x \in R_e^n : \langle x, c\rangle_H = 0, \text{ for all } c \in C\}.$$

Let $C$ be a linear code of length $n$ over $R_2$. We define

$$C_1 = \{x \in \mathbb{F}_{q^2}^n : \exists\ y \in \mathbb{F}_{q^2}^n \text{ such that } \epsilon_1 x + \epsilon_2 y \in C\};$$

$$C_2 = \{y \in \mathbb{F}_{q^2}^n : \exists\ x \in \mathbb{F}_{q^2}^n \text{ such that } \epsilon_1 x + \epsilon_2 y \in C\}.$$

Then $C_1, C_2$ are linear codes of length $n$ over $\mathbb{F}_{q^2}$. Moreover, $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2 = \{\epsilon_1 a_1 + \epsilon_2 a_2 : a_1 \in C_1, a_2 \in C_2\}$ and $C^{\perp_H} = \epsilon_1 C_1^{\perp_H} \oplus \epsilon_2 C_2^{\perp_H}$. Also, it can easily be

checked that $C \cap C^{\perp_H} = \epsilon_1(C_1 \cap C_1^{\perp_H}) \oplus \epsilon_2(C_2 \cap C_2^{\perp_H})$. The following result gives a criterion for checking a linear code over $R_2$ to be constacyclic.

**Theorem 1.** *Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a linear code of length $n$ over $R_2$. Then it is a $\lambda-$constacyclic code over $R_2$ for $\lambda = \epsilon_1\alpha_1 + \epsilon_2\alpha_2 \in R_2^*$ if and only if $C_1, C_2$ are $\alpha_1-$constacyclic and $\alpha_2-$constacyclic codes over $\mathbb{F}_{q^2}$, respectively.*

*Proof.* Let $C$ be a $\lambda-$constacyclic code over $R_2$ and $(a_0, a_1, \ldots, a_{n-1}) \in C_1$, $(b_0, b_1, \ldots, b_{n-1}) \in C_2$ be arbitrary elements. Then $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ where $c_i = \epsilon_1 a_i + \epsilon_2 b_i$ for $0 \leq i \leq n-1$. Since $C$ is a $\lambda-$constacyclic code, $\tau_\lambda(c) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2})$ in $C$. Now,

$$\begin{aligned}\tau_\lambda(c) =&((\epsilon_1\alpha_1 + \epsilon_2\alpha_2)(\epsilon_1 a_{n-1} + \epsilon_2 b_{n-1}), \epsilon_1 a_0 + \epsilon_2 b_0, \ldots, \epsilon_1 a_{n-2} + \epsilon_2 b_{n-2})\\ =&(\epsilon_1\alpha_1 a_{n-1} + \epsilon_2\alpha_2 b_{n-1}, \epsilon_1 a_0 + \epsilon_2 b_0, \ldots, \epsilon_1 a_{n-2} + \epsilon_2 b_{n-2})\\ =&\epsilon_1(\alpha_1 a_{n-1}, a_0, \ldots, a_{n-2}) + \epsilon_2(\alpha_2 b_{n-1}, b_0, \ldots, b_{n-2}) \in C.\end{aligned}$$

Therefore, we have $(\alpha_1 a_{n-1}, a_0, \ldots, a_{n-2}) \in C_1$ and $(\alpha_2 b_{n-1}, b_0, \ldots, b_{n-2}) \in C_2$. Hence, we conclude that $C_1, C_2$ are $\alpha_1$, $\alpha_2-$ constacyclic codes over $\mathbb{F}_{q^2}$, respectively.

Conversely, let $C_1, C_2$ be $\alpha_1$ and $\alpha_2-$constacyclic codes, respectively. If $c \in C$, then there exist $a = (a_0, a_1, \ldots, a_{n-1}) \in C_1$ and $b = (b_0, b_1, \ldots, b_{n-1}) \in C_2$ such that $c = \epsilon_1 a + \epsilon_2 b$. As $C_1, C_2$ are $\alpha_1$ and $\alpha_2-$constacyclic codes, we have $\tau_{\alpha_1}(a) \in C_1$ and $\tau_{\alpha_2}(b) \in C_2$. Therefore,

$$\begin{aligned}\tau_\lambda(c) =&\epsilon_1(\alpha_1 a_{n-1}, a_0, \ldots, a_{n-2}) + \epsilon_2(\alpha_2 b_{n-1}, b_0, \ldots, b_{n-2})\\ =&\epsilon_1\tau_{\alpha_1}(a) + \epsilon_2\tau_{\alpha_2}(b) \in C.\end{aligned}$$

Hence, $C$ is a $\lambda-$constacyclic code of length $n$ over $R_2$. □

Similar to linear codes over $R_2$, we can also decompose linear codes over $R_e$ (see [41]). Hence, a linear code $C$ of length $n$ over $R_e$ can be written as

$$C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \cdots \oplus \eta_e C_e$$

where $C_i = \{r_i \in \mathbb{F}_{q^2}^n : \exists\ r_j \in \mathbb{F}_{q^2}^n, 1 \leq j \neq i \leq e$ such that $\sum_{k=1}^{e} \eta_k r_k \in C\}$ for $1 \leq i \leq e$. Further, $C^{\perp_H} = \eta_1 C_1^{\perp_H} \oplus \cdots \oplus \eta_e C_e^{\perp_H}$ and $C \cap C^{\perp_H} = \eta_1(C_1 \cap C_1^{\perp_H}) \oplus \cdots \oplus \eta_e(C_e \cap C_e^{\perp_H})$. Also, $C$ is a $\lambda-$constacyclic code over $R_e$ for $\lambda = \sum_{i=1}^{e} \eta_i\alpha_i \in R_e^*$ if and only if $C_i$ are $\alpha_i-$constacyclic codes over $\mathbb{F}_{q^2}$, for $1 \leq i \leq e$. Further, the generator polynomial of a constacyclic code of length $n$ over $R_e$ can be obtained by the next theorem.

**Theorem 2.** *Let $C$ be a $\lambda-$constacyclic code of length $n$ over $R_e$, where $\lambda = \sum_{i=1}^{e} \eta_i\alpha_i \in R_e^*$. Then there exists a unique monic polynomial $g(x) \in R_e[x]$ such that $C = \langle g(x) \rangle$ for $g(x) = \sum_{i=1}^{e} \eta_i g_i(x)$ where $g_i(x) | x^n - \alpha_i$ for $1 \leq i \leq e$.*

Now, we define a Gray map $\psi : R_e^n \to \mathbb{F}_{q^2}^{en}$ by

$$\begin{aligned}\psi(r_0, r_1, \ldots, r_{n-1}) = [(s_{10}, s_{20}, \ldots, s_{e0})M, (s_{11}, s_{21}, \ldots, s_{e1})M, \ldots, (s_{1(n-1)}, s_{2(n-1)},\\ \ldots, s_{e(n-1)})M]\end{aligned}$$

where $r_i = \sum_{k=1}^{e} \eta_k s_{ki}$ for $0 \le i \le n-1$ and $M$ is a square matrix of order $e$ satisfying $MM^* = \nu I_e$ where $I_e$ is the identity matrix of order $e$ and $\nu \in \mathbb{F}_{q^2}^*$. Then $\psi$ is a bijective linear map, and the following results hold.

**Lemma 3.** *Let $C$ be a linear code of length $n$ over $R_e$ and $C^{\perp_H}$ be the dual code of $C$. Then $\psi(C^{\perp_H}) = \psi(C)^{\perp_H}$.*

*Proof.* Let $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ and $x = (x_0, x_1, \ldots, x_{n-1}) \in C^{\perp_H}$ where $c_i = \sum_{k=1}^{e} \eta_k r_{ki}$ and $x_i = \sum_{k=1}^{e} \eta_k s_{ki}$ for $0 \le i \le n-1$. Then

$$\langle c, x \rangle_H = \eta_1 \left( \sum_{i=0}^{n-1} r_{1i} s_{1i}^q \right) + \eta_2 \left( \sum_{i=0}^{n-1} r_{2i} s_{2i}^q \right) + \cdots + \eta_e \left( \sum_{i=0}^{n-1} r_{ei} s_{ei}^q \right) = 0,$$

which implies that $\sum_{i=0}^{n-1} r_{ki} s_{ki}^q = 0$ for $1 \le k \le e$. Now,

$$\psi(c) = ((r_{10}, r_{20}, \ldots, r_{e0})M, (r_{11}, r_{21}, \ldots, r_{e1})M, \ldots, (r_{1(n-1)}, r_{2(n-1)}, \ldots, r_{e(n-1)})M),$$
$$\psi(x) = ((s_{10}, s_{20}, \ldots, s_{e0})M, (s_{11}, s_{21}, \ldots, s_{e1})M, \ldots, (s_{1(n-1)}, s_{2(n-1)}, \ldots, s_{e(n-1)})M)$$

and

$$\begin{aligned}
\langle \psi(c), \psi(x) \rangle_H = \psi(c)[\psi(x)]^* &= \sum_{i=0}^{n-1} (r_{1i}, r_{2i}, \ldots, r_{ei}) MM^* (s_{1i}^q, s_{2i}^q, \ldots, s_{ei}^q)^T \\
&= \nu \sum_{i=0}^{n-1} (r_{1i}, r_{2i}, \ldots, r_{ei}) (s_{1i}^q, s_{2i}^q, \ldots, s_{ei}^q)^T \\
&= \nu \sum_{i=0}^{n-1} \sum_{k=1}^{e} r_{ki} s_{ki}^q \\
&= \nu \sum_{k=1}^{e} \sum_{i=0}^{n-1} r_{ki} s_{ki}^q \\
&= 0,
\end{aligned}$$

which implies that $\psi(C^{\perp_H}) \subseteq \psi(C)^{\perp_H}$. Moreover, $|\psi(C^{\perp_H})| = |\psi(C)^{\perp_H}|$ as $\psi$ is a bijective map. Thus, $\psi(C^{\perp_H}) = \psi(C)^{\perp_H}$. □

**Lemma 4.** *Let $C$ be a self-orthogonal code with respect to the Hermitian inner product over $R_e$ of length $n$. Then $\psi(C)$ is a self-orthogonal code with respect to the Hermitian inner product over $\mathbb{F}_{q^2}$ of length $en$.*

*Proof.* Since $C$ is a self-orthogonal code with respect to the Hermitian inner product, i.e., $C \subseteq C^{\perp_H}$, we have $\psi(C) \subseteq \psi(C^{\perp_H})$. Using Lemma 3, we have

$$\psi(C) \subseteq \psi(C)^{\perp_H}.$$

Thus, $\psi(C)$ is a self-orthogonal code with respect to the Hermitian inner product over $\mathbb{F}_{q^2}$. □

**Lemma 5.** *Let $C$ be a linear code over $R_e$ of length $n$. Then $C$ is a self-dual code with respect to the Hermitian inner product if and only if $\psi(C)$ is a self-dual code with respect to the Hermitian inner product.*

*Proof.* Let $C$ be a self-dual code with respect to the Hermitian inner product, i.e., $C = C^{\perp_H}$. Then, by Lemma 3, we have

$$\psi(C) = \psi(C^{\perp_H}) = \psi(C)^{\perp_H}.$$

Therefore, $\psi(C)$ is a self-dual code with respect to the Hermitian inner product over $\mathbb{F}_{q^2}$.
Conversely, let $\psi(C)$ be a self-dual code with respect to the Hermitian inner product over $\mathbb{F}_{q^2}$. Then $\psi(C) = \psi(C)^{\perp_H} = \psi(C^{\perp_H})$ by Lemma 3. As $\psi$ is bijective, we have $C = C^{\perp_H}$ and hence $C$ is a self-dual code with respect to the Hermitian inner product. □

**Theorem 6.** *Let $C$ be a linear code over $R_e$ of length $n$. Then $C$ is a Hermitian LCD code if and only if $\psi(C)$ is a Hermitian LCD code over $\mathbb{F}_{q^2}$.*

*Proof.* It can be proved by following the steps of Theorem 6.2 in [32]. □

The Hamming weight $w_H(c)$ of an element $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^2}^n$ is the number of non-zero components in it. The Gray weight $w_G$ of an element $\mathfrak{r} \in R_e$ is defined as $w_G(\mathfrak{r}) = w_H(\psi(\mathfrak{r}))$, the Gray distance between two codewords $c_1, c_2$ is defined as $d_G(c_1, c_2) = w_G(c_1 - c_2)$ while the Gray distance of a code $C$ is defined as

$$d_G(C) = \min\{d_G(c_1, c_2) \mid c_1, c_2 \in C, c_1 \neq c_2\}.$$

# 3 Hermitian Hull of Constacyclic codes over $R_e$

In this section, we find possible hull dimensions of constacyclic codes over $R_e$. In this regard, we first present the factorization of $x^n - \alpha$ over a finite field $\mathbb{F}_{q^2}$, for some non-zero element $\alpha$ in $\mathbb{F}_{q^2}$ of order $r$ such that $r \mid q+1$ which makes the Hermitian dual of an $\alpha$-constacyclic code also an $\alpha$-constacyclic code (see [47]). Further, we obtain the necessary and sufficient conditions for these codes to be Hermitian LCD. In the rest of the paper, we consider $\alpha$ and $\alpha_l$ in $\mathbb{F}_{q^2}$ of order $r$ and $r_l$, respectively, such that $r \mid q+1$ and $r_l | q+1$ for each $1 \leq l \leq e$.

Let $\alpha \in \mathbb{F}_{q^2}^*$ be an element of order $r$ such that $r \mid q+1$ and $n = p^v n'$ be a positive integer such that $v \geq 0, p \nmid n'$ where $p = \mathrm{char}(\mathbb{F}_{q^2})$. For a positive integer $j$, we define a map $\pi$ by

$$\pi(j, q^2) = \begin{cases} 0 & \text{if } j \mid (q^{2k} + q) \text{ for some non-negative integer } k, \\ 1 & \text{otherwise.} \end{cases}$$

Also, we define two sets

$$\Omega = \{j \in \mathbb{N} : j \mid n'r, \pi(j, q^2) = 0 \text{ and } \gcd\left(\frac{n'r}{j}, r\right) = 1\}$$

and

$$\Omega^{'} = \{j \in \mathbb{N} : j \mid n'r, \pi(j, q^2) = 1 \text{ and } \gcd\left(\frac{n'r}{j}, r\right) = 1\}$$

where $\mathbb{N}$ is the set of positive integers. Then, following [35], the factorization of $x^n - \alpha$ into monic irreducible polynomials over $\mathbb{F}_{q^2}$ is

$$x^n - \alpha = \prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} g_{ij}(x)^{p^v} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} f_{ij}(x)^{p^v} f_{ij}^{\dagger}(x)^{p^v}$$

where

$$\gamma(j) := \frac{\phi(j)}{\phi(r)\text{ord}_j(q^2)},$$
$$\beta(j) := \frac{\phi(j)}{2\phi(r)\text{ord}_j(q^2)},$$

for Euler's totient function $\phi$, $\text{ord}_j(q^2)$ denotes the order of $q^2$ in the multiplicative group $\mathbb{Z}_j^{\times}$, for some positive integer $j \neq 1$, coprime to $q^2$ and consider $\text{ord}_1(q^2) = 1$. In the above factorization, each polynomial $g_{ij}$ is a self conjugate-reciprocal of degree $\text{ord}_j(q^2)$ for $j \in \Omega$ and $f_{ij}, f_{ij}^{\dagger}$ are conjugate-reciprocal polynomial pairs with each polynomial of degree $\text{ord}_j(q^2)$ for $j \in \Omega'$, i.e., the number of self-conjugate-reciprocal polynomials are $s = p^v \sum_{j\in\Omega} \gamma(j)$ and the number of conjugate-reciprocal polynomial pairs are $t = p^v \sum_{j\in\Omega'} \beta(j)$. That is,

$$n = \sum_{j\in\Omega} \text{ord}_j(q^2)\gamma(j)p^v + \sum_{j\in\Omega'} 2\text{ord}_j(q^2)\beta(j)p^v.$$

Now, we obtain some bounds which will be used for finding the hull dimension of constacyclic codes over $R_2$.

**Lemma 7.** *For any positive integer $v$ and $0 \leq a, b, c \leq p^v$, we have the following:*

1. $0 \leq p^v - \max\{a, p^v - a\} \leq \left\lfloor \frac{p^v}{2} \right\rfloor$,
2. $0 \leq 2p^v - \max\{b, p^v - c\} - \max\{c, p^v - b\} \leq p^v$.

*Proof.* For Statement 1, we know that

$$\left\lceil \frac{p^v}{2} \right\rceil \leq \max\{a, p^v - a\} \leq p^v.$$

Therefore, we have

$$0 \leq p^v - \max\{a, p^v - a\} \leq \left\lfloor \frac{p^v}{2} \right\rfloor.$$

For Statement 2, we have the following two cases:
**Case (i):** If $\max\{b, p^v - c\} = b$, then $\max\{c, p^v - b\} = c$ and $p^v \leq b + c \leq 2p^v$. Therefore, $p^v \leq \max\{b, p^v - c\} + \max\{c, p^v - b\} = b + c \leq 2p^v$ and hence $0 \leq$

$2p^v - \max\{b, p^v - c\} - \max\{c, p^v - b\} \leq p^v$.
**Case (ii):** If $\max\{b, p^v - c\} = p^v - c$, then $\max\{c, p^v - b\} = p^v - b$ and $0 \leq b + c \leq p^v$. Therefore, $p^v \leq \max\{b, p^v - c\} + \max\{c, p^v - b\} = 2p^v - b - c \leq 2p^v$ and hence $0 \leq 2p^v - \max\{b, p^v - c\} - \max\{c, p^v - b\} \leq p^v$. □

Using this lemma, we now find the hull dimension of constacyclic codes over $R_2$.

**Theorem 8.** *Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a $\lambda-$constacyclic code over $R_2$, for some $\alpha$-constacyclic codes $C_1 = \langle g_1(x) \rangle$, $C_2 = \langle g_2(x) \rangle$ over $\mathbb{F}_{q^2}$, where $\lambda = \epsilon_1\alpha + \epsilon_2\alpha$ for $\alpha \in \mathbb{F}_{q^2}^*$ and $g_1(x), g_2(x)$ are given below:*

$$g_1(x) = \prod_{j\in\Omega} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{a_{ij}} \prod_{j\in\Omega'} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{b_{ij}} f_{ij}^{\dagger}(x)^{c_{ij}},$$

$$g_2(x) = \prod_{j\in\Omega} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{u_{ij}} \prod_{j\in\Omega'} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{v_{ij}} f_{ij}^{\dagger}(x)^{w_{ij}}.$$

*Then, the dimension of $Hull_H(C)$ is of the form*

$$\sum_{j\in\Omega} ord_j(q^2)a_j + \sum_{j\in\Omega'} ord_j(q^2)b_j,$$

*where $0 \leq a_j \leq 2\gamma(j)\left\lfloor \frac{p^v}{2} \right\rfloor$ and $0 \leq b_j \leq 2\beta(j)p^v$.*

*Proof.* Let $C$ be a $\lambda-$constacyclic code over $R_2$ where $\lambda = \epsilon_1\alpha + \epsilon_2\alpha$. Then,

$$\begin{aligned} Hull_H(C) &= \epsilon_1 Hull_H(C_1) \oplus \epsilon_2 Hull_H(C_2) \\ &= \langle \epsilon_1 \text{ lcm}\left(g_1(x), \left(\frac{x^n - \alpha}{g_1(x)}\right)^{\dagger}\right), \epsilon_2 \text{ lcm}\left(g_2(x), \left(\frac{x^n - \alpha}{g_2(x)}\right)^{\dagger}\right)\rangle. \end{aligned}$$

Now,

$$\begin{aligned} \dim(Hull_H(C)) = &\ \dim(Hull_H(C_1)) + \dim(Hull_H(C_2)) \\ = &\ n - \sum_{j\in\Omega} \text{ord}_j(q^2) \sum_{i=1}^{\gamma(j)} \max\{a_{ij}, p^v - a_{ij}\} - \\ &\sum_{j\in\Omega'} \text{ord}_j(q^2) \sum_{i=1}^{\beta(j)} \big(\max\{b_{ij}, p^v - c_{ij}\} + \max\{c_{ij}, p^v - b_{ij}\}\big) + \\ &n - \sum_{j\in\Omega} \text{ord}_j(q^2) \sum_{i=1}^{\gamma(j)} \max\{u_{ij}, p^v - u_{ij}\} - \end{aligned}$$

$$\sum_{j\in\Omega'} \mathrm{ord}_j(q^2) \sum_{i=1}^{\beta(j)} (\max\{v_{ij}, p^v - w_{ij}\} + \max\{w_{ij}, p^v - v_{ij}\})$$

$$= \sum_{j\in\Omega} \mathrm{ord}_j(q^2) \sum_{i=1}^{\gamma(j)} (p^v - \max\{a_{ij}, p^v - a_{ij}\}) +$$

$$\sum_{j\in\Omega'} \mathrm{ord}_j(q^2) \sum_{i=1}^{\beta(j)} (2p^v - \max\{b_{ij}, p^v - c_{ij}\} - \max\{c_{ij}, p^v - b_{ij}\}) +$$

$$\sum_{j\in\Omega} \mathrm{ord}_j(q^2) \sum_{i=1}^{\gamma(j)} (p^v - \max\{u_{ij}, p^v - u_{ij}\}) +$$

$$\sum_{j\in\Omega'} \mathrm{ord}_j(q^2) \sum_{i=1}^{\beta(j)} (2p^v - \max\{v_{ij}, p^v - w_{ij}\} - \max\{w_{ij}, p^v - v_{ij}\})$$

$$= \sum_{j\in\Omega} \mathrm{ord}_j(q^2) \sum_{i=1}^{\gamma(j)} (2p^v - \max\{a_{ij}, p^v - a_{ij}\} - \max\{u_{ij}, p^v - u_{ij}\}) +$$

$$\sum_{j\in\Omega'} \mathrm{ord}_j(q^2) \sum_{i=1}^{\beta(j)} (4p^v - \max\{b_{ij}, p^v - c_{ij}\} - \max\{c_{ij}, p^v - b_{ij}\} -$$

$$\max\{v_{ij}, p^v - w_{ij}\} - \max\{w_{ij}, p^v - v_{ij}\}).$$

Using Lemma 7, we have

$$0 \le 2p^v - \max\{a_{ij}, p^v - a_{ij}\} - \max\{u_{ij}, p^v - u_{ij}\}) \le 2 \left\lfloor \frac{p^v}{2} \right\rfloor$$

and

$$0 \le 4p^v - \max\{b_{ij}, p^v - c_{ij}\} - \max\{c_{ij}, p^v - b_{ij}\} - \max\{v_{ij}, p^v - w_{ij}\} - \max\{w_{ij}, p^v - v_{ij}\} \le 2p^v.$$

Taking $a_j = \sum_{i=1}^{\gamma(j)} (2p^v - \max\{a_{ij}, p^v - a_{ij}\} - \max\{u_{ij}, p^v - u_{ij}\})$ and $b_j = \sum_{i=1}^{\beta(j)} (4p^v - \max\{b_{ij}, p^v - c_{ij}\} - \max\{c_{ij}, p^v - b_{ij}\} - \max\{v_{ij}, p^v - w_{ij}\} - \max\{w_{ij}, p^v - v_{ij}\})$, we get

$$\dim(Hull_H(C)) = \sum_{j\in\Omega} \mathrm{ord}_j(q^2) a_j + \sum_{j\in\Omega'} \mathrm{ord}_j(q^2) b_j,$$

where $0 \le a_j \le 2\gamma(j) \left\lfloor \frac{p^v}{2} \right\rfloor$ and $0 \le b_j \le 2\beta(j)p^v$. □

**Corollary 9.** *If* $\gcd(n,p) = 1$, *then the dimension of the Hermitian hull of constacyclic code given in the above theorem is*

$$\sum_{j\in\Omega'} ord_j(q^2)b_j$$

*where* $0 \leq b_j \leq 2\beta(j)$.

*Proof.* If $\gcd(n,p) = 1$, then $p^v = 1$. Therefore, $0 \leq a_j \leq 2\gamma(j)\left\lfloor \frac{p^v}{2} \right\rfloor = 2\gamma(j)\left\lfloor \frac{1}{2} \right\rfloor = 0$ and hence the result follows. □

Now, we recall basic theory to provide the hull dimension of $\lambda-$constacyclic code over $R_e$ where $\lambda$ is a unit in $R_e$. Let $\alpha_l \in \mathbb{F}_{q^2}^*$ be elements of order $r_l$ such that $r_l \mid q+1$ for $1 \leq l \leq e$, respectively. For $1 \leq l \leq e$, we define the following sets:

$$\Omega_l = \{j \mid n'r_l : \pi(j,q^2) = 0 \text{ and } \gcd\left(\frac{n'r_l}{j}, r_l\right) = 1\}$$

and

$$\Omega_l' = \{j \mid n'r_l : \pi(j,q^2) = 1 \text{ and } \gcd\left(\frac{n'r_l}{j}, r_l\right) = 1\}.$$

Then the factorization of $x^n - \alpha_l$ into monic irreducible polynomials over $\mathbb{F}_{q^2}$ is of the form

$$x^n - \alpha_l = \prod_{j\in\Omega_l}\prod_{i=1}^{\gamma_l(j)}(g_{ij}^{(l)}(x))^{p^v} \prod_{j\in\Omega_l'}\prod_{i=1}^{\beta_l(j)}(f_{ij}^{(l)}(x))^{p^v}((f_{ij}^{(l)})^\dagger(x))^{p^v},$$

where

$$\gamma_l(j) := \frac{\phi(j)}{\phi(r_l)\mathrm{ord}_j(q^2)},$$
$$\beta_l(j) := \frac{\phi(j)}{2\phi(r_l)\mathrm{ord}_j(q^2)},$$

for $1 \leq l \leq e$ where each $g_{ij}^{(l)}$ is a self conjugate-reciprocal polynomial of degree $\mathrm{ord}_j(q^2)$ and $f_{ij}^{(l)}, (f_{ij}^{(l)})^\dagger$ are conjugate-reciprocal polynomial pairs with each polynomial of degree $\mathrm{ord}_j(q^2)$. The following theorem is the general case of Theorem 8 and can be proved using similar arguments.

**Theorem 10.** *Let* $C = \eta_1C_1 \oplus \eta_2C_2 \oplus \cdots \oplus \eta_eC_e$ *be a* $\lambda-$*constacyclic code over* $R_e$ *for some* $\alpha_l$*-constacyclic codes* $C_l = \langle g_l(x)\rangle$ *over* $\mathbb{F}_{q^2}$ *where* $\lambda = \eta_1\alpha_1 + \eta_2\alpha_2 + \cdots + \eta_e\alpha_e$ *for* $\alpha_l \in \mathbb{F}_{q^2}^*$ *and* $g_l(x)$ *are given below:*

$$g_l(x) = \prod_{j\in\Omega_l}\prod_{i=1}^{\gamma_l(j)}(g_{ij}^{(l)}(x))^{a_{ij}^{(l)}} \prod_{j\in\Omega_l'}\prod_{i=1}^{\beta_l(j)}(f_{ij}^{(l)}(x))^{b_{ij}^{(l)}}((f_{ij}^{(l)})^\dagger(x))^{c_{ij}^{(l)}}, 1 \leq l \leq e.$$

*Then the dimension of* $Hull_H(C)$ *is of the form*

$$\sum_{l=1}^{e}\left(\sum_{j\in\Omega_l} ord_j(q^2)a_j^{(l)} + \sum_{j\in\Omega_l'} ord_j(q^2)b_j^{(l)}\right)$$

*where* $0 \le a_j^{(l)} \le \gamma_l(j)\left\lfloor \frac{p^v}{2} \right\rfloor$, $0 \le b_j^{(l)} \le \beta_l(j)p^v$, *for* $1 \le l \le e$.

To obtain a necessary and sufficient condition for a constacyclic code over $R_2$ to be Hermitian LCD, we define a set $\mathcal{S}_{q^2} = \{j \ge 1 : j \mid (q^{2k}+q)$ for some non-negative integer $k\}$. The following theorem gives a condition under which there is only one possibility for the hull dimension of a constacyclic code over $R_2$, which leave us with the trivial choice of Hermitian hull, i.e., the code is Hermitian LCD.

**Theorem 11.** *Let* $\gcd(n,p) = 1$ *and* $D_{q^2}(n)$ *denotes the set of hull dimensions of* $\alpha-$*constacyclic codes of length* $n$ *over* $R_2$ *where* $\alpha \in \mathbb{F}_{q^2}^*$ *is an element of multiplicative order* $r$. *Then* $D_{q^2}(n) = \{0\}$ *if and only if* $nr \in \mathcal{S}_{q^2}$.

*Proof.* Note that $n = n'$, as $\gcd(n,p) = 1$. If $nr \in \mathcal{S}_{q^2}$, then there exists $k \ge 0$ such that $nr \mid (q^{2k}+q)$. In this case, $j \mid (q^{2k}+q)$ for each divisor of $nr$ and we get $\Omega' = \varphi$. Now, using Corollary 9, we get $a_j = 0$ for all $j \in \Omega$. It concludes that the only possibility for hull dimension is 0, and hence the result follows.

Conversely, assume that $nr \notin \mathcal{S}_{q^2}$. Then $\pi(nr, q^2) = 1$, i.e., $nr \in \Omega'$ and $0 < \beta(nr)$. Therefore, there exists $0 < b_{nr} \le \beta(nr)$, which makes the hull dimension non-zero. □

From the above theorem, we can conclude the following result:

**Corollary 12.** *Let* $\gcd(n,p) = 1$ *and* $\alpha \in \mathbb{F}_{q^2}^*$ *be an element of multiplicative order* $r$. *Then every* $\alpha-$*constacyclic code of length* $n$ *over* $R_2$ *is a Hermitian LCD code if and only if* $nr \in \mathcal{S}_{q^2}$.

Similarly, we can obtain the following results corresponding to Theorem 11 and Corollary 12, respectively.

**Theorem 13.** *Let* $\gcd(n,p) = 1$ *and* $D_{q^2}(n)$ *denotes the set of hull dimensions of* $\alpha-$*constacyclic codes of length* $n$ *over* $R_e$ *where* $\alpha \in \mathbb{F}_{q^2}^*$ *is an element of multiplicative order* $r$. *Then* $D_{q^2}(n) = \{0\}$ *if and only if* $nr \in \mathcal{S}_{q^2}$.

**Corollary 14.** *Let* $\gcd(n,p) = 1$ *and* $\alpha \in \mathbb{F}_{q^2}^*$ *be an element of multiplicative order* $r$. *Then every* $\alpha-$*constacyclic code of length* $n$ *over* $R_e$ *is a Hermitian LCD code if and only if* $nr \in \mathcal{S}_{q^2}$.

# 4 Quantum Codes

In this section, we obtain quantum error-correcting codes (QECC) by using the Hermitian construction for which we require Hermitian dual-containing codes. We use the notation $[[n,k,d]]_q$ to represent a QECC over $\mathbb{F}_q$ which has already been mentioned in the Introduction. The following theorem gives a criterion for obtaining codes containing their Hermitian dual.

**Theorem 15.** *Let* $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ *be a* $\lambda-$*constacyclic code over* $R_2$ *for some constacyclic codes* $C_1 = \langle g_1(x)\rangle$, $C_2 = \langle g_2(x)\rangle$ *over* $\mathbb{F}_{q^2}$ *where* $\lambda = \epsilon_1\alpha_1 + \epsilon_2\alpha_2$ *for*

$\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$ *and* $g_1(x), g_2(x)$ *are given below:*

$$g_1(x) = \prod_{j\in\Omega_1} \prod_{i=1}^{\gamma_1(j)} (g_{ij}^{(1)}(x))^{a_{ij}} \prod_{j\in\Omega_1'} \prod_{i=1}^{\beta_1(j)} (f_{ij}^{(1)}(x))^{b_{ij}} ((f_{ij}^{(1)})^\dagger(x))^{c_{ij}},$$

$$g_2(x) = \prod_{j\in\Omega_2} \prod_{i=1}^{\gamma_2(j)} (g_{ij}^{(2)}(x))^{u_{ij}} \prod_{j\in\Omega_2'} \prod_{i=1}^{\beta_2(j)} (f_{ij}^{(2)}(x))^{v_{ij}} ((f_{ij}^{(2)})^\dagger(x))^{w_{ij}}.$$

*Then* $C^{\perp_H} \subseteq C$ *if and only if* $0 \leq a_{ij}, u_{ij} \leq \left\lfloor \frac{p^v}{2} \right\rfloor$ *and* $0 \leq b_{ij} + c_{ij}, v_{ij} + w_{ij} \leq p^v$.

*Proof.* Note that $C^{\perp_H} \subseteq C$ if and only if $C_1^{\perp_H} \subseteq C_1$ and $C_2^{\perp_H} \subseteq C_2$, or equivalently, $Hull_H(C_1) = C_1^{\perp_H}$ and $Hull_H(C_2) = C_2^{\perp_H}$. That is,

$$\text{lcm}\left(g_1(x), \left(\frac{x^n - \alpha_1}{g_1(x)}\right)^\dagger\right) = \left(\frac{x^n - \alpha_1}{g_1(x)}\right)^\dagger$$

and

$$\text{lcm}\left(g_2(x), \left(\frac{x^n - \alpha_2}{g_2(x)}\right)^\dagger\right) = \left(\frac{x^n - \alpha_2}{g_2(x)}\right)^\dagger.$$

This implies that $a_{ij} \leq p^v - a_{ij}, u_{ij} \leq p^v - u_{ij}$, $b_{ij} \leq p^v - c_{ij}$ and $v_{ij} \leq p^v - w_{ij}$, i.e., $0 \leq 2a_{ij}, 2u_{ij} \leq p^v$ and $0 \leq b_{ij} + c_{ij}, v_{ij} + w_{ij} \leq p^v$. Hence, we get the required result. □

Analogues to this result, we can find the dual containing property for the general case, which is given by the following result.

**Theorem 16.** *Let* $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \cdots \oplus \eta_e C_e$ *be a* $\lambda-$*constacyclic code over* $R_e$*, for some* $\alpha_l$*-constacyclic codes* $C_l = \langle g_l(x) \rangle$ *over* $\mathbb{F}_{q^2}$*, where* $\lambda = \eta_1\alpha_1 + \eta_2\alpha_2 + \cdots + \eta_e\alpha_e$ *for* $\alpha_l \in \mathbb{F}_{q^2}^*$ *and* $g_l(x)$ *are given below:*

$$g_l(x) = \prod_{j\in\Omega_l} \prod_{i=1}^{\gamma_l(j)} (g_{ij}^{(l)}(x))^{a_{ij}^{(l)}} \prod_{j\in\Omega_l'} \prod_{i=1}^{\beta_l(j)} (f_{ij}^{(l)}(x))^{b_{ij}^{(l)}} ((f_{ij}^{(l)})^\dagger(x))^{c_{ij}^{(l)}}, 1 \leq l \leq e.$$

*Then* $C^{\perp_H} \subseteq C$ *if and only if* $0 \leq a_{ij}^{(l)} \leq \left\lfloor \frac{p^v}{2} \right\rfloor$ *and* $0 \leq b_{ij}^{(l)} + c_{ij}^{(l)} \leq p^v$*, for all* $1 \leq l \leq e$.

**Lemma 17.** *[22, Hermitian construction] Let* $C$ *be a linear code over* $\mathbb{F}_{q^2}$ *with the parameters* $[n, k, d]_q$ *such that* $C^{\perp_H} \subseteq C$*. Then there exists a quantum code of parameters* $[[n, 2k - n, \geq d]]_q$.

**Theorem 18.** *Let* $C$ *be a linear code over* $R_2$ *such that* $C^{\perp_H} \subseteq C$ *and the parameters of* $\psi(C)$ *be* $[2n, k, d]_q$*. Then there exists a quantum code of parameters* $[[2n, 2k - 2n, \geq d]]_q$.

*Proof.* Let $C$ be a linear code over $R$ such that $C^{\perp_H} \subseteq C$. Then

$$\psi(C)^{\perp_H} = \psi(C^{\perp_H}) \subseteq \psi(C).$$

That is, $\psi(C)$ is a linear code over $\mathbb{F}_{q^2}$ containing its Hermitian dual with the parameters $[2n, k, d]_q$. By Lemma 17, there exists a quantum code of parameters $[[2n, 2k - 2n, \geq d]]_q$. □

Similarly, the following result can be derived.

**Theorem 19.** *Let $C$ be a linear code over $R_e$ such that $C^{\perp_H} \subseteq C$ and the parameters of $\psi(C)$ be $[en, k, d]_q$. Then there exists a quantum code of parameters $[[en, 2k - en, \geq d]]_q$.*

# 5 Examples

In this section, we obtain examples of LCD codes, quantum codes, and constacyclic codes with small hull dimensions over a finite field using constacyclic codes over $R_e$.

To obtain the Gray images of constacyclic codes over $R_e$, we consider the Gray map $\psi$ defined in Section 2 and the matrix $M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ for $e = 2$. For $e = 3$, we consider the matrices $M^{(q)}$ for obtaining the Gray images of constacyclic codes over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + u^2\mathbb{F}_{q^2}$ under $\psi$ where

$$M^{(5)} = \begin{bmatrix} 3 & 2 & 1 \\ 3 & 4 & 3 \\ 4 & 3 & 2 \end{bmatrix}, M^{(11)} = \begin{bmatrix} 7 & 4 & 2 \\ 9 & 7 & 4 \\ 4 & 2 & 4 \end{bmatrix}.$$

Further, we consider $t$ to be a primitive element of a finite field in the examples. For an $[n, k, d]_q$ linear code, we have the *Singleton bound* $d \leq n - k + 1$. A linear code is an MDS code if $d = n - k + 1$ and near to MDS if $d = n - k$. In the case of quantum codes with the parameters $[[n, k, d]]_q$, we have the *quantum Singleton bound* $k + 2d \leq n + 2$ [6]. The quantum codes that satisfy the equality, i.e., $k + 2d = n + 2$, are said to be MDS codes and the codes for which $k + 2d = n$ are said to be near to MDS codes. Now, we obtain some examples of codes where the parameters are calculated using the Magma Computational software [5].

**Example 1.** *Consider $\alpha = 1$, $n = 12$ and $q = p = 5$, then the order of $\alpha$ is $r = 1$, $n' = 12$, and $p^v = 1$. Further, $ord_j(q^2) = 1\ \forall j \in \Omega \cup \Omega'$, where $\Omega = \{1, 2, 3, 6\}, \Omega' = \{4, 12\}$. Also, $\gamma(1) = 1, \gamma(2) = 1, \gamma(3) = 2, \gamma(6) = 2, \beta(4) = 1$ and $\beta(12) = 2$. Therefore, $x^{12} - 1$ can be factored over $\mathbb{F}_{5^2} = \mathbb{F}_5[t]$ into $\gamma(1) + \gamma(2) + \gamma(3) + \gamma(6) = 6$ irreducible self-conjugate reciprocal polynomials and $\beta(4) + \beta(12) = 3$ irreducible conjugate reciprocal polynomial pairs. The factorization of $x^{12} - 1$ into irreducible polynomials over $\mathbb{F}_{5^2} = \mathbb{F}_5[t]$ is*

$$\begin{aligned} x^{12} - 1 =& (x + 1)(x + t^4)(x + t^8)(x + 4)(x + t^{16})(x + t^{20})[(x + t^2)(x + t^{14})][(x + 2) \\ & (x + 3)][(x + t^{10})(x + t^{22})] \end{aligned}$$

*where* $x+1,\ x+t^4,\ x+t^8,\ x+4,\ x+t^{16},\ x+t^{20}$ *are self-conjugate reciprocal polynomials and* $\{x+t^2,\ x+t^{14}\}, \{x+2,\ x+3\}, \{x+t^{10},\ x+t^{22}\}$ *are conjugate reciprocal polynomial pairs. Consider* $g_1(x) = x^3+x^2+t^8x+t^8 = (x+1)(x+t^{10})(x+t^{22})$ *and* $g_2(x) = x+t^2$. *Then cyclic codes* $C_1 = \langle g_1(x)\rangle$ *and* $C_2 = \langle g_2(x)\rangle$ *have hull dimensions* 0 *and* 1, *respectively. Further,* $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ *is a cyclic code over* $\mathbb{F}_{5^2}+u\mathbb{F}_{5^2}$ *and the code* $\psi(C)$ *over* $\mathbb{F}_{5^2}$ *is a near to MDS code having parameters* $[24, 20, 4]_{5^2}$ *and hull dimension* 1.

*Take* $g_1'(x) = g_1(x)$ *and* $g_2'(x) = x+t^8$. *Then cyclic codes* $C_1' = \langle g_1'(x)\rangle$ *and* $C_2' = \langle g_2'(x)\rangle$ *are Hermitian LCD codes and* $C' = \epsilon_1 C_1' \oplus \epsilon_2 C_2'$ *is a Hermitian LCD code over* $\mathbb{F}_{5^2}+u\mathbb{F}_{5^2}$. *Therefore, the code* $\psi(C')$ *over* $\mathbb{F}_{5^2}$ *is Hermitian LCD of parameters* $[24, 20, 4]_{5^2}$.

**Example 2.** *Consider* $\alpha = 12$, $n = 14$ *and* $q = p = 13$, *then the order of* $\alpha$ *is* $r = 2$, $n' = 14$, *and* $p^v = 1$. *Further,* $ord_j(q^2) = 1\ \forall j \in \Omega \cup \Omega'$, *where* $\Omega = \varphi, \Omega' = \{4, 28\}$. *Also,* $\beta(4) = 1$ *and* $\beta(28) = 6$. *Therefore,* $x^{14}-12$ *can be factored over* $\mathbb{F}_{13^2} = \mathbb{F}_{13}[t]$ *into* $\beta(4)+\beta(28) = 7$ *irreducible conjugate reciprocal polynomial pairs. The factorization of* $x^{14}-12$ *into irreducible polynomials over* $\mathbb{F}_{13^2} = \mathbb{F}_{13}[t]$ *is*

$$\begin{aligned} x^{14}-12 =&[(x+t^6)(x+t^{90})][(x+t^{18})(x+t^{102})][(x+t^{30})(x+t^{114})][(x+8)(x+5)] \\ &[(x+t^{54})(x+t^{138})][(x+t^{66})(x+t^{150})][(x+t^{78})(x+t^{162})], \end{aligned}$$

*where* $\{x+t^6,\ x+t^{90}\}, \{x+t^{18},\ x+t^{102}\}, \{x+t^{30},\ x+t^{114}\}, \{x+8,\ x+5\}, \{x+t^{54},\ x+t^{138}\}, \{x+t^{66},\ x+t^{150}\}, \{x+t^{78},\ x+t^{162}\}$ *are conjugate reciprocal polynomial pairs. Take* $g_1(x) = x^2+t^{21}x+1 = (x+t^{18})(x+t^{150})$ *and* $g_2(x) = x+t^6$. *In* $g_1(x)$ *and* $g_2(x)$, *we have at most one factor from each conjugate reciprocal polynomial pair, i.e., the dual containing property* ($b_{ij}+c_{ij} \le p^v = 1$ *for all* $j \in \Omega'$ *and* $1 \le i \le \beta(j)$) *given in Theorem 15 is satisfied. Therefore, the* $12-$*constacyclic codes* $C_1 = \langle g_1(x)\rangle$ *and* $C_2 = \langle g_2(x)\rangle$ *contain their Hermitian dual and* $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ *is a* $(12\epsilon_1+12\epsilon_2)-$*constacyclic code over* $\mathbb{F}_{13^2}+u\mathbb{F}_{13^2}$ *containing its Hermitian dual code. Therefore, the code* $\psi(C)$ *over* $\mathbb{F}_{13^2}$ *contains its dual and has parameters* $[28, 25, 4]_{13^2}$. *Hence, by using the Hermitian construction, we get a quantum code with parameters* $[[28, 22, \ge 4]]_{13}$ *over* $\mathbb{F}_{13}$, *which is an MDS code.*

**Example 3.** *Consider* $\alpha = 4$, $n = 6$ *and* $q = p = 5$, *then the order of* $\alpha$ *is* $r = 2$, $n' = 6$, *and* $p^v = 1$. *Further,* $ord_j(q^2) = 1\ \forall j \in \Omega \cup \Omega'$, *where* $\Omega = \varphi, \Omega' = \{4, 12\}$. *Also,* $\beta(4) = 1$ *and* $\beta(12) = 2$. *Therefore,* $x^6-4$ *can be factored over* $\mathbb{F}_{5^2} = \mathbb{F}_5[t]$ *into* $\beta(4)+\beta(12) = 3$ *irreducible conjugate reciprocal polynomial pairs. The factorization of* $x^6-4$ *into irreducible polynomials over* $\mathbb{F}_{5^2} = \mathbb{F}_5[t]$ *is*

$$x^6-4 = [(x+t^2)(x+t^{14})][(x+2)(x+3)][(x+t^{10})(x+t^{22})],$$

*where* $\{x+t^2,\ x+t^{14}\}, \{x+2,\ x+3\}, \{x+t^{10},\ x+t^{22}\}$ *are conjugate reciprocal polynomial pairs. Take* $g_1(x) = x^2+tx+t^8 = (x+t^2)(x+2), g_2(x) = x+t^2$ *and* $g_3(x) = x+t^{10}$. *It can be seen that the polynomials* $g_1(x)$, $g_2(x)$, *and* $g_3(x)$ *satisfy the dual containing conditions given in Theorem 16 is satisfied. Therefore, the* $4-$*constacyclic codes* $C_1 = \langle g_1(x)\rangle$, $C_2 = \langle g_2(x)\rangle$ *and* $C_3 = \langle g_2(x)\rangle$ *contain their Hermitian dual and* $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ *is a* $(-\eta_1-\eta_2-\eta_3)-$*constacyclic code over* $\mathbb{F}_{5^2}+u\mathbb{F}_{5^2}+u^2\mathbb{F}_{5^2}$

*containing its Hermitian dual code where*

$$\eta_1 = (u+4)(u+t^{20}), \eta_2 = (u+t^4)(u+t^{20}), \eta_3 = (u+t^4)(u+4).$$

*Hence, the code* $\psi(C)$ *over* $\mathbb{F}_{5^2}$ *contains its Hermitian dual and has parameters* $[18, 14, 4]_{5^2}$. *Now, by using the Hermitian construction, we get a quantum code* $[[18, 10, \geq 4]]_5$ *over* $\mathbb{F}_5$, *which is near to MDS code.*

It is seen that a $\lambda-$constacyclic code $C$ of length $n$ over $R_e$ can be decomposed into a direct sum of constacyclic codes over a finite field where each of these constituent codes is of length $n$. In the tables, we obtain several LCD codes, quantum codes, and $\lambda-$constacyclic codes with hull dimension 1 or 2 over finite fields where $t$ denotes a primitive element of the field. The first column of all the tables represents the length of the constituent codes, the second column represents the value of $\lambda$, the third column represents the generator polynomials of the constituent codes, and the fourth column represents the parameters of $\psi(C)$. The fifth column in Table 2 represents the hull dimension of the code $\psi(C)$ while in Table 3, it represents the parameters of quantum codes obtained from $\psi(C)$ using the Hermitian construction. We compare our obtained quantum codes with existing codes available in different published papers and find that our codes (listed in the fifth column) are either best-known (for a few cases) or superior by means of parameters. Almost all the codes that we present in the tables are near to MDS, whereas the MDS codes have been marked with $*$.

**Table 1** Hermitian LCD codes obtained from $\lambda-$constacyclic codes over $R_e$.

| $n$ | $\lambda$ | $g_1(x), g_2(x)$ | $\psi(C)$ |
|---|---|---|---|
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + x^2 + t^8x + t^8, x + t^8$ | $[24, 20, 4]_{5^2}$ |
| 12 | $\epsilon_1 + 6\epsilon_2$ | $x^3 + t^2x^2 + t^2x + t^{36}, x + t^6$ | $[24, 20, 4]_{7^2}$ |
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + x^2 + t^{40}x + t^{40}, x + t^{10}$ | $[24, 20, 4]_{11^2}$ |
| 30 | $\epsilon_1 + 10\epsilon_2$ | $x^2 + 4x + 1, x + t^{10}$ | $[60, 57, 3]_{11^2}$ |
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + 8x^2 + 5x + 12, x + 1$ | $[24, 20, 4]_{13^2}$ |
| 14 | $\epsilon_1 + \epsilon_2$ | $x^2 + t^{27}x + t^{12}, x + 1$ | $[28, 25, 4]^*_{13^2}$ |
| 30 | $t^{36}\epsilon_1 + \epsilon_2$ | $x^2 + t^4x + t^{120}, x + 1$ | $[60, 57, 3]_{13^2}$ |

**Table 2** $\lambda-$constacyclic codes with hull dimension 1 or 2.

| $n$ | $\lambda$ | $g_1(x), g_2(x)$ | $\psi(C)$ | Hull dimension of $\psi(C)$ |
|---|---|---|---|---|
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + x^2 + t^8x + t^8, x + t^2$ | $[24, 20, 4]_{5^2}$ | 1 |
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + x^2 + t^{13}x + t^{14}, x + 2$ | $[24, 20, 4]_{5^2}$ | 2 |
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + tx^2 + t^{22}x + t^{44}, x + t^4$ | $[24, 20, 4]_{7^2}$ | 2 |
| 12 | $\epsilon_1 + t^{12}\epsilon_2$ | $x^3 + t^2x^2 + t^2x + t^{36}, x + t^5$ | $[24, 20, 4]_{7^2}$ | 1 |
| 12 | $\epsilon_1 + 10\epsilon_2$ | $x^3 + t^3x^2 + t^{103}x + t^{70}, x + t^{25}$ | $[24, 20, 4]_{11^2}$ | 1 |
| 12 | $10\epsilon_1 + 10\epsilon_2$ | $x^3 + t^{45}x^2 + t^{50}x + t^{95}, x + t^5$ | $[24, 20, 4]_{11^2}$ | 2 |
| 30 | $\epsilon_1 + \epsilon_2$ | $x^2 + t^5x + t^4, x + 1$ | $[60, 57, 3]_{11^2}$ | 1 |
| 30 | $\epsilon_1 + \epsilon_2$ | $x^2 + t^5x + t^4, x + t^4$ | $[60, 57, 3]_{11^2}$ | 2 |
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + 11x + 4, x + 1$ | $[24, 20, 4]_{13^2}$ | 1 |
| 12 | $\epsilon_1 + \epsilon_2$ | $x^3 + 4x^2 + x + 4, x + 2$ | $[24, 20, 4]_{13^2}$ | 2 |
| 30 | $\epsilon_1 + t^{120}\epsilon_2$ | $x^2 + 8x + 4, x + t^4$ | $[60, 57, 3]_{13^2}$ | 2 |
| 30 | $\epsilon_1 + t^{120}\epsilon_2$ | $x^2 + 8x + 4, x + t^{60}$ | $[60, 57, 3]_{13^2}$ | 1 |

**Table 3** Quantum codes obtained from Hermitian dual containing $\lambda-$constacyclic codes over $R_e$.

| $n$ | $\lambda$ | $g_1(x), g_2(x)$ | $\psi(C)$ | $[[en, k, \geq d]]_q$ | $en+2-(k+2d)$ | Remark / Comparison |
|---|---|---|---|---|---|---|
| 16 | $\epsilon_1+\epsilon_2$ | $x^3+t^7x^2+tx+1, x+t$ | $[32,28,3]_{3^2}$ | $[[32,24,\geq 3]]_3$ | 4 | New |
| 16 | $\epsilon_1+\epsilon_2$ | $x^3+t^7x^2+tx+1, x^3+tx^2+t^7x+1$ | $[32,26,4]_{3^2}$ | $[[32,20,\geq 4]]_3$ | 6 | New |
| 20 | $2\epsilon_1+2\epsilon_2$ | $x^3+x^2+x+t, x+t$ | $[40,36,3]_{3^2}$ | $[[40,32,\geq 3]]_3$ | 4 | Optimal [11] |
| 26 | $\epsilon_1+t^2\epsilon_2$ | $x^3+2x^2+1, x+t$ | $[52,48,3]_{3^2}$ | $[[52,44,\geq 3]]_3$ | 4 | $[[52,43,\geq 3]]_3$ [11] |
| 28 | $2\epsilon_1+t^2\epsilon_2$ | $x^3+t^6x^2+tx+t^3, x^2+t^3$ | $[56,51,3]_{3^2}$ | $[[56,46,\geq 3]]_3$ | 6 | Optimal [3] [11] |
| 30 | $\epsilon_1+t^2\epsilon_2$ | $x^3+t^2x^2+t^2x+1, x^2+t^3x+t^6$ | $[60,55,4]_{3^2}$ | $[[60,50,\geq 4]]_3$ | 4 | New |
| 20 | $t^4\epsilon_1+\epsilon_2$ | $x^3+t^{11}x^2+t^3, x+1$ | $[40,36,4]_{5^2}$ | $[[40,32,\geq 4]]_5$ | 2 | $[[40,30,4]]_5$ [11] |
| 26 | $4\epsilon_1+4\epsilon_2$ | $x^3+t^7x^2+tx+2, x+2$ | $[52,48,4]_{5^2}$ | $[[52,44,\geq 4]]_5$ | 2 | $[[52,44,\geq 3]]_5$ [3] [11] |
| 28 | $\epsilon_1+4\epsilon_2$ | $x^3+t^{23}x^2+tx+3, x^2+t^{15}x+1$ | $[56,51,4]_{5^2}$ | $[[56,46,\geq 4]]_5$ | 4 | New |
| 30 | $\epsilon_1+4\epsilon_2$ | $x^2+2x+1, x+t^2$ | $[60,57,3]_{5^2}$ | $[[60,54,\geq 3]]_5$ | 2 | $[[60,50,3]]_5$ [14] |
| 30 | $\epsilon_1+t^{12}\epsilon_2$ | $x^2+t^3x+1, x+t^2$ | $[60,57,3]_{7^2}$ | $[[60,54,\geq 3]]_7$ | 2 | Optimal [11] |
| 30 | $\epsilon_1+t^{12}\epsilon_2$ | $x^3+t^7x^2+t^{41}x+4, x+t^2$ | $[60,56,4]_{7^2}$ | $[[60,52,\geq 4]]_7$ | 2 | New |
| 36 | $\epsilon_1+t^{12}\epsilon_2$ | $x^3+t^4, x+t^3$ | $[72,68,3]_{7^2}$ | $[[72,64,\geq 3]]_7$ | 4 | New |
| 14 | $12\epsilon_1+12\epsilon_2$ | $x^2+t^{21}x+1, x+t^6$ | $[28,25,4]_{13^2}$ | $[[28,22,\geq 4]]^*_{13}$ | 0 | MDS |

# 6 Conclusion

In this article, we have studied the Hermitian hull of constacyclic codes over $R_e$ and obtained their dimension. We derived some results for Hermitian LCD codes and obtained conditions for constacyclic codes to satisfy dual containing property. The approach that we used to obtain conditions for constacyclic codes to satisfy dual containing property is new. Further, we obtained some good LCD and quantum codes by using a Gray map. We have also obtained some constacyclic codes with small hull dimension.

**Acknowledgement.** The authors are thankful to the Department of Science and Technology (DST) (under SERB File Number: MTR/2022/001052, vide Diary No / Finance No SERB/F/8787/2022-2023 dated 29 December 2022) for financial support and the Indian Institute of Technology Patna for providing research facilities.

# Declarations

**Data Availability Statement**: The authors declare that [the/all other] data supporting the findings of this study are available within the article. Any clarification may be requested from the corresponding author, provided it is essential.

**Competing interests**: The authors declare that there is no conflict of interest regarding the publication of this manuscript.

**Use of AI tools declaration** The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

# References

[1] Alahmadi, A., Altassan, A., AlKenani, A., Çalkavur, S., Shoaib, H., Solé, P.: A Multisecret-Sharing Scheme Based on LCD Codes. Mathematics **8**(2), 272-282 (2020).

[2] Assmus Jr, E. F., Key, J. D.: Affine and projective planes. Discrete Math. **83**(2-3), 161-187 (1990).

[3] Aydin, N., Liu, P., Yoshino, B.: http://quantumcodes.info/Z4/, accessed on 15/5/23

[4] Ball, S.: Some constructions of quantum MDS codes. Des. Codes Cryptogr. **89**, 811-821 (2021).

[5] Bosma, W., Cannon, J.: Handbook of Magma Functions. Univ. of Sydney (1995).

[6] 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).

[7] Cao, M., Cui, J.: Construction of new quantum codes via Hermitian dual-containing matrix-product codes. Quantum Inf. Process. **19**(12), 1-26 (2020).

[8] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1), 131-150 (2016).

[9] Carlet C., Li C.J., Mesnager S.: Linear codes with small hulls in semi-primitive case. Des. Codes Cryptogr. **87**, 3063-3075 (2019).

[10] Carlet, C., Mesnager, S., Tang, C., Qi, Y., Pellikaan, R.: Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. IEEE Trans. Inform. Theory **64**(4), 3010-3017 (2018).

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

[12] Guenda, K., Jitman, S., Gulliver, T. A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**(1), 121-136 (2018).

[13] Grassl, M., Rötteler, M.: Quantum MDS codes over small fields, 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, China, 2015, pp. 1104-1108, doi: 10.1109/ISIT.2015.7282626.

[14] Islam, H., Prakash, O., Verma, R.K.: New quantum codes from constacyclic codes over the ring $R_{k,m}$. Adv. Math. Commun. **16**(1), 17-35 (2022).

[15] Islam, H., Martínez-Moro, E., Prakash, O.: Cyclic codes over a non-chain ring $R_{e,q}$ and their application to LCD codes. Discrete Math. **344**(10), 112545 (2021).

[16] Islam, H., Prakash, O.: Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring. Cryptogr. Commun. **14**(1), 59-73 (2022).

[17] Islam, H., Prakash, O.: New Quantum and LCD Codes over Finite Fields of Even Characteristic. Defence Sci. J. **75**(05), 656-661 (2021).

[18] Jitman, S., Sangwisut, E.: The average dimension of the Hermitian hull of cyclic codes over finite fields of square order, AIP Proceedings of ICoMEIA 2016, 1775 (2016) Article ID 030026.

[19] Jitman, S., Sangwisut, E.: The average dimension of the Hermitian Hull of Constacyclic Codes over finite fields of square order. Adv. Math. Commun. **12**(3), 451-463 (2018).

[20] Jitman, S., Sangwisut, E.: Hulls of Cyclic Codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$. Thai J. Math. **33**, 135-144 (2020).

[21] Jitman, S., Sangwisut, E., Udomkavanich, P.: Hulls of cyclic codes over $\mathbb{Z}_4$. Discrete Math. **343**(1), 111621 (2020).

[22] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P. K.: Nonbinary Stabilizer Codes Over Finite Fields. IEEE Trans. Inform. Theory **52**(11), 4892-4914 (2006).

[23] Leon, J.S.: Computing automorphism groups of error-correcting codes. IEEE Trans. Inform. Theory **28**, 496-511 (1982).

[24] Li, C.J., Zeng, P.: Constrctions of linear codes with one-dimensional hull. IEEE Trans. Inform. Theory 65(3), 1668-1676 (2019).

[25] Li, C.: Hermitian LCD codes from cyclic codes. Des. Codes Cryptogr. **86** (2018), 2261-2278.

[26] Liu, Z., Wang, J.: Linear complementary dual codes over rings. Des. Codes Cryptogr. **87**, 3077-3086 (2019).

[27] Liu, X., Liu, H.: LCD codes over finite chain rings. Finite Fields Appl. **34**, 1-19 (2015).

[28] Mankean, T., Jitman, S.: Optimal binary and ternary linear codes with hull dimension one. J. Appl. Math. Comput. **64**(1), 137-155 (2020).

[29] Mankean, T., Jitman, S.: Constructions and bounds on quaternary linear codes with Hermitian hull dimension one. Arab. J. Math. **10**(1), 175-184 (2021).

[30] Massey, J. L.: Linear codes with complementary duals. Discrete Math. **106/107**, 337-342 (1992).

[31] Pang, B.; Zhu, S.; Kai, X.: Some new bounds on LCD codes over finite fields. Cryptogr. Commun. **12**(4), 743-755 (2020).

[32] Prakash, O., Yadav, S., Verma, R. K.: Constacyclic and Linear Complementary Dual codes over $\mathbb{F}_q + u\mathbb{F}_q$. Defence Sci. J. **70**(6), 626-632 (2020).

[33] Prakash, O., Yadav, S., Islam, H., Solé, P.: Self-dual and LCD double circulant codes over a class of non-local rings. Comput. Appl. Math. **41**(6), 1-16 (2022).

[34] Sangwisut, E., Jitman, S., Ling, S., Udomkavanich, P.: Hulls of cyclic and negacyclic codes over finite fields. Finite Fields Appl. **33**, 232-257 (2015).

[35] Sangwisut, E., Jitman, S., Udomkavanich, P.: Constacyclic and quasi-twisted Hermitian self-dual codes over finite fields. Adv. Math. Commun. **11**, 595-613 (2017).

[36] Sendrier, N.: On the dimension of the hull. SIAM J. Appl. Math. **10**, 282-293 (1997).

[37] Sendrier, N.: Finding the permutation between equivalent codes: the support splitting algorithm. IEEE Trans. Inform. Theory **46**, 1193-1203 (2000).

[38] Sendrier, N., Skersys, G.: On the computation of the automorphism group of a linear code, in: Proceedings of IEEE ISIT 2001, Washington, DC, pp. 13 (2001).

[39] Sendrier, N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discrete Math. **285**, 345-347 (2004).

[40] Skersys, G.: The average dimension of the hull of cyclic codes, Discrete Appl. Math., **128**(1), 275-292 (2003).

[41] Shi, X., Huang, X., Yue, Q.: Construction of new quantum codes derived from constacyclic codes over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + \cdots + u^{r-1}\mathbb{F}_{q^2}$. Appl. Algebra Engrg. Comm. Comput. **32**(5), 603-620 (2021).

[42] Shor, P.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), 2493-2496 (1995).

[43] Sok L., Shi M., Solé P.: Constructions of optimal LCD codes over large finite fields. Finite Fields Their Appl. **50**, 138-153 (2018).

[44] Yadav, S., Prakash, O., Islam, H., Solé, P.: Self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. J. Appl. Math. Comput. **67**(1-2), 689-705 (2021).

[45] Yadav S., Prakash, O.: A new construction of Quadratic Double Circulant LCD codes. J. Algebra Comb. Discrete Struct. Appl. (2023) (accepted).

[46] Yadav S., Prakash, O.: Enumeration of LCD and Self-dual Double Circulant Codes Over $\mathbb{F}_q[v]/ < v^2 - 1 >$. Proceedings of Seventh International Congress on Information and Communication Technology, Lecture Notes in Networks and Systems **447**, 241-249 (2023)
https://doi.org/10.1007/978-981-19-1607-6_21

[47] Yang, Y., Cai, W.: On self-dual constacyclic codes over finite fields. Des. Codes Cryptogr. **74**, 355-364 (2015).

[48] Yang, X., Massey, J. L.: The condition for a cyclic code to have a complementary dual. Discrete Math. **126**, 391-393 (1994).