Article

Not peer-reviewed version

Associated Complementary Dual and Quantum Codes of Skew Constacyclic Codes

Shikha Yadav , Ashutosh Singh , Om Prakash , Patrick Solé *

Posted Date: 24 October 2024

doi: 10.20944/preprints202410.1716.v1

Keywords: Constacyclic codes; Skew constacyclic codes; LCD codes; Quantum codes; Gray map.

Article

Associated Complementary Dual and Quantum Codes of Skew Constacyclic Codes

Shikha Yadav [1], Ashutosh Singh [1], Om Prakash [1] and Patrick Solé [2,*]

[1] Department of Mathematics, Indian Institute of Technology Patna, Patna 801106, India
[2] I2M, (CNRS, Aix-Marseille University) Marseilles, France
* Correspondence: sole@enst.fr

Abstract: Consider the ring $\mathcal{B}_e = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$, $u^e = u$ $(e \geq 2)$, where $\mathbb{F}_q$ denotes the finite field having $q = p^m$ elements (for $m \geq 1$ and a prime p), and $q \equiv 1 \pmod{e-1}$. Skew constacyclic codes over $\mathcal{B}_e$ are studied in this paper. We present their generator polynomial and describe the criteria for their complementary duality. Moreover, we derive criteria for these codes to contain their dual and obtain quantum codes. Additionally, we establish a Gray map that preserves duality and investigate its properties. We also take into account additive skew constacyclic codes for this purpose and also derive criteria for the complementary duality of these codes. Finally, we provide several LCD and quantum codes (MDS/ near MDS). The latter are compared with the quantum codes obtained in the recent literature.

Keywords: constacyclic codes; skew constacyclic codes; LCD codes; quantum codes; gray map

MSC: 94B05; 94B15; 94B60

---

1. Introduction

Rich algebraic structures and ease of practical application are two of the most well-known attributes of cyclic codes. On identifying a vector by a polynomial, one can consider any cyclic code over $\mathbb{F}_q$ as a submodule of the $\mathbb{F}_q[x]$-module $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ for the length n. Further, these codes can also be considered as ideals generated by divisors of $x^n - 1$. It is worth noting that $\mathbb{F}_q[x]$ is a unique factorization domain, a fact which restricts the divisors of $x^n - 1$ in $\mathbb{F}_q[x]$. As an extension of these codes, constacyclic codes may be regarded as ideals of $\mathbb{F}_q[x]/\langle x^n - \gamma\rangle$ for some non-zero element $\gamma \in \mathbb{F}_q$. Further, these codes were examined over some finite commutative rings [1,2]. Later, by relaxing the linearity condition, additive codes were considered over mixed alphabets [3,4].
On the other hand, in the desire to obtain more factorizations of $x^n - 1$ than over a factorial ring, skew cyclic codes [5,6] were introduced with the notion of skew polynomial rings [7]. These codes over a finite field $\mathbb{F}_q$ are basically left submodules of the module $\mathbb{F}_q[x,\Theta]/\langle x^n - 1\rangle$ for an automorphism Θ of $\mathbb{F}_q$. Later, these codes were investigated by Abualrub and Seneviratne [8] over $\mathbb{F}_q + v\mathbb{F}_q$, where $v^2 = v$. Additionally, Gao [9], and Gursoy et al. [10] presented skew cyclic codes by considering different automorphisms. Later, as a continuation of these efforts, skew constacyclic codes were examined [11,12].

In 1992, Massey [13] proposed LCD codes ($\mathcal{V} \cap \mathcal{V}^{\perp} = \{\mathbf{0}\}$). It was demonstrated that these codes were the best linear coding solution to 2-BAC. Sufficient and necessary condition for the complementary duality of cyclic codes over finite fields was derived in 1994 by Yang and Massey [14]. Additionally, they deduced a relationship among the reversible and LCD cyclic codes. Later, DNA applications made full use of the former idea [15,16]. On the other hand, the Gilbert-Varshamov bound is satisfied by LCD codes, as demonstrated by Sendrier [17] in 2004. Subsequently, these codes were examined over chain rings in [18]. In 2016, these codes were shown to have applications in cryptosystems [19]. Afterwards, LCD codes were studied over different commutative rings in [20–26] , and applications of these codes were presented in Multi-secret Sharing Schemes [27]. Recently, LCD codes were studied in [28,29] using the skew polynomial rings. Besides, additive codes were investigated for the complementary duality over the structure $\mathbb{Z}_2\mathbb{Z}_2[u^3]$ in [30], and they were called additive complementary dual (ACD)

 doi:10.20944/preprints202410.1716.v1

codes.

In the last decades of the 20th century, it was noticed that quantum mechanics might improve the complexity of certain classical algorithms, like the DFT transform, list searching, or integer factorization. This last algorithm is a key ingredient in the RSA cryptosystem. For this reason, quantum computation got the attention of many researchers. To securitize quantum computation, Shor [31] introduced Quantum Error-Correcting Codes (QECCs) in 1995. In 1998, classical error-correcting codes were employed to obtain QECCs via some constructions such as CSS construction [32]. Afterwards, linear codes over different commutative rings were used to obtain good QECCs in [33–36]. As an extension of these works, additive codes over the commutative structure were also utilized [37]. Recently, cyclic and constacyclic codes using non-commutative rings have been employed for obtaining QECCs due to more possibility of factorization of a polynomial. Many good QECCs were obtained from cyclic and constacyclic codes [38–41] . Motivated by these works, we consider skew constacyclic and additive codes for obtaining new and better LCD and quantum codes.

This paper has been arranged as follows: Firstly, the structure of linear codes over $\mathcal{B}_e$ is presented in Section 2. Section 3 presents skew constacyclic codes over $\mathcal{B}_e$, defines a Gray map and analyzes its properties. In Section 4, we derive some results for LCD codes. Further, we derive quantum codes by utilizing CSS construction in Section 5. Section 6 presents the structure and properties of additive skew constacyclic codes over $\mathbb{F}_q\mathcal{B}_e$. In Section 7, we present various LCD codes as well as new quantum codes. Our work is concluded in Section 8.

2. Preliminaries

Let us suppose that $\mathbb{F}_q$ denotes a finite field having cardinality q. Let us consider a ring $\mathcal{B}_e = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$, $u^e = u$, with $q \equiv 1 \pmod{e-1}$ ($e \geq 2$). We represent the collection of units in $\mathcal{B}_e$ by $\mathcal{B}_e^*$.

Consider a primitive element $\alpha \in \mathbb{F}_q$ and take $\xi = \alpha^{\frac{q-1}{e-1}}$. Following [42], consider

$$\begin{aligned}
\epsilon_1 &= 1 - u^{e-1}, \\
\epsilon_2 &= \frac{1}{e-1}(u + u^2 + \cdots + u^{e-2} + u^{e-1}), \\
\epsilon_3 &= \frac{1}{e-1}(\xi u + \xi^2 u^2 + \cdots + \xi^{e-2} u^{e-2} + u^{e-1}), \\
\epsilon_4 &= \frac{1}{e-1}(\xi^2 u + (\xi^2)^2 u^2 + \cdots + (\xi^2)^{e-2} u^{e-2} + u^{e-1}), \\
&\vdots \\
\epsilon_e &= \frac{1}{e-1}(\xi^{e-2} u + (\xi^{e-2})^2 u^2 + \cdots + (\xi^{e-2})^{e-2} u^{e-2} + u^{e-1}).
\end{aligned}$$

Then, we have $\mathcal{B}_e \cong \bigoplus_{i=1}^{e} \epsilon_i \mathbb{F}_q$ and each $s \in \mathcal{B}_e$ has a unique representation $s = \sum_{i=1}^{e} \epsilon_i s_i$, $s_i \in \mathbb{F}_q$. Moreover, any linear code $\mathcal{V}$ over $\mathcal{B}_e$ with length n has a representation

$$\mathcal{V} = \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e,$$

for some linear codes $\mathcal{V}_i = \{r_i \in \mathbb{F}_q^n : \exists\, r_j \in \mathbb{F}_q^n, 1 \leq j \neq i \leq e \text{ such that } \sum_{k=1}^{e} \epsilon_k r_k \in \mathcal{V}\}$ over $\mathbb{F}_q$ $(1 \leq i \leq e)$ and the dual code of $\mathcal{V}$ is $\mathcal{V}^\perp = \epsilon_1 \mathcal{V}_1^\perp \oplus \cdots \oplus \epsilon_e \mathcal{V}_e^\perp$. Subsequently, the following result holds.

Theorem 1. *Let us assume that $\mathcal{V} = \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e$ is any γ-constacyclic code over $\mathcal{B}_e$ ($\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$). Then $\mathcal{V}$ has $g(x) = \sum_{i=1}^{e} \epsilon_i g_i(x)$ as its generator polynomial, where each $\mathcal{V}_i$ has $g_i(x)$ as their generator polynomial ($1 \leq i \leq e$).*

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

3. Skew Constacyclic Codes over $\mathcal{B}_e$

The current section presents the generator polynomials for skew constacyclic codes over $\mathcal{B}_e$ and the dual codes. In order to proceed with the investigation, we first require an automorphism of $\mathcal{B}_e$ as defined below.

Define an automorphism $\Theta_l : \mathcal{B}_e \to \mathcal{B}_e$ by

$$\Theta_l(\epsilon_1 a_1 + \epsilon_2 a_2 + \cdots + \epsilon_e a_e) = \epsilon_1 \Theta_l(a_1) + \epsilon_2 \Theta_l(a_2) + \cdots + \epsilon_e \Theta_l(a_e) = \epsilon_1 a_1^{p^l} + \epsilon_2 a_2^{p^l} + \cdots + \epsilon_e a_e^{p^l},$$

for $0 \leq l \leq m-1$. Using this, the definition for skew constacyclic codes is as mentioned below.

Definition 2. *Suppose Θ_l is an automorphism of the ring $\mathcal{B}_e$, $\gamma \in \mathcal{B}_e^*$. Then a linear code $\mathcal{V}$ over $\mathcal{B}_e$ is called a skew constacyclic (or skew $\Theta_l - \gamma$- constacyclic) code over $\mathcal{B}_e$, if $\tau_{\Theta_l,\gamma}(\mathcal{V}) = \mathcal{V}$, where $\tau_{\Theta_l,\gamma} : \mathcal{B}_e^n \longrightarrow \mathcal{B}_e^n$ is the skew $\Theta_l - \gamma$-constacyclic shift given by*

$$\tau_{\Theta_l,\gamma}(c_0, c_1, \ldots, c_{n-1}) = (\gamma\Theta_l(c_{n-1}), \Theta_l(c_0), \Theta_l(c_1), \ldots, \Theta_l(c_{n-2})).$$

For $\gamma = -1$ (resp. $\gamma = 1$), these codes are said to be skew negacyclic (resp. skew cyclic) codes, respectively. Further, for identity automorphism Θ_l and $\gamma = -1$ (resp. $\gamma = 1$), these codes are said to be negacyclic (resp. cyclic) codes with the corresponding negacyclic and cyclic shifts represented by τ_{-1} and τ_1, respectively.

Consider the skew-polynomial ring

$$\mathcal{B}_e[x;\Theta_l] = \{b_0 + b_1 x + \cdots + b_{n'} x^{n'} | b_i \in \mathcal{B}_e, n' \in \mathbb{N}\}$$

in which the multiplication is given by $x * b = \Theta_l(b)x$. Then the center $Z(\mathcal{B}_e[x;\Theta_l])$ of $\mathcal{B}_e[x;\Theta_l]$ (which will be used to study skew constacyclic codes) can be obtained by the below-mentioned result.

Lemma 3. *Let us assume that $\gamma \in \mathcal{B}_e^*$ such that $\Theta_l(\gamma) = \gamma$, where Θ_l is an automorphism of $\mathcal{B}_e$. The order of Θ_l divides n iff $x^n - \gamma$ lies in $Z(\mathcal{B}_e[x;\Theta_l])$.*

Proof. Let $\Theta_l(\gamma) = \gamma$ and order of Θ_l divides n, i.e., $\Theta_l^n(s) = s \; \forall s \in \mathcal{B}_e$. Then, for any $s_0 + s_1 x + \cdots + s_{n'} x^{n'} \in \mathcal{B}_e[x;\Theta_l]$, we have

$$\begin{aligned}(x^n - \gamma)(s_0 + s_1 x + \cdots + s_{n'} x^{n'}) =& \Theta_l^n(s_0)x^n + \Theta_l^n(s_1)x^{n+1} + \cdots + \Theta_l^n(s_{n'})x^{n+n'} \\ &- \gamma(s_0 + s_1 x + \cdots + s_{n'} x^{n'}) \\ =& s_0 x^n + s_1 x^{n+1} + \cdots + s_{n'} x^{n+n'} \\ &- (\gamma s_0 + \gamma s_1 x + \cdots + \gamma s_{n'} x^{n'})\end{aligned}$$

and

$$\begin{aligned}(s_0 + s_1 x + \cdots + s_{n'} x^{n'})(x^n - \gamma) =& s_0 x^n + s_1 x^{n+1} + \cdots + s_{n'} x^{n+n'} \\ &- (s_0\gamma + s_1\Theta_l(\gamma)x + \cdots + s_{n'}\Theta_l^{n'}(\gamma)x^{n'}) \\ =& s_0 x^n + s_1 x^{n+1} + \cdots + s_{n'} x^{n+n'} \\ &- (s_0\gamma + s_1\gamma x + \cdots + s_{n'}\gamma x^{n'}).\end{aligned}$$

That is, $(x^n - \gamma)(s_0 + s_1 x + \cdots + s_{n'} x^{n'}) = (s_0 + s_1 x + \cdots + s_{n'} x^{n'})(x^n - \gamma)$ and hence $x^n - \gamma \in Z(\mathcal{B}_e[x;\Theta_l])$.

Conversely, assume that $x^n - \gamma \in Z(\mathcal{B}_e[x;\Theta_l])$. Then $(x^n - \gamma)(sx^i) = (sx^i)(x^n - \gamma)$, for all $s \in \mathcal{B}_e$ and

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

$i \in \mathbb{N}$. Now,

$$(x^n - \gamma)(sx^i) = (\Theta_l^n(s)x^{n+i} - \gamma sx^i) \text{ and } (sx^i)(x^n - \gamma) = (sx^{i+n} - s\Theta_l^i(\gamma)x^i) = (sx^{i+n} - s\gamma x^i).$$

It implies that $\Theta_l^n(s) = s$ for all $s \in \mathcal{B}_e$. Therefore, we conclude that order of Θ_l divides n. □

As we have already seen that for an automorphism Θ_l of $\mathcal{B}_e$ whose order divides n and $\gamma \in \mathcal{B}_e^*$ such that γ is fixed by Θ_l, we have $(x^n - \gamma) \in Z(\mathcal{B}_e[x;\Theta_l])$. Therefore, $\frac{\mathcal{B}_e[x;\Theta_l]}{\langle x^n-\gamma\rangle}$ is a ring. On the contrary, if n is not divisible by order of Θ_l then $\frac{\mathcal{B}_e[x;\Theta_l]}{\langle x^n-\gamma\rangle}$ doesn't form a ring but a left $\mathcal{B}_e[x;\Theta_l]$-module and any skew constacyclic code is characterized by the result given below.

Lemma 4. *Any linear code $\mathcal{V}$ over $\mathcal{B}_e$ having length n is a skew $\Theta_l - \gamma$-constacyclic code iff $\mathcal{V}$ forms a left $\mathcal{B}_e[x;\Theta_l]$-submodule of $\frac{\mathcal{B}_e[x;\Theta_l]}{\langle x^n-\gamma\rangle}$.*

Theorem 5. *Suppose $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ and $\mathcal{V} = \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2 \oplus \cdots \oplus \epsilon_e\mathcal{V}_e$ is a linear code over $\mathcal{B}_e$. Then $\mathcal{V}$ is a skew $\Theta_l - \gamma$-constacyclic code iff each $\mathcal{V}_i$ is skew $\Theta_l - \alpha_i$-constacyclic code ($1 \le i \le e$).*

Proof. Let us suppose that $\mathcal{V}$ is a skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$ and $a_j = (a_{0,j}, a_{1,j}, \ldots, a_{(n-1),j}) \in \mathcal{V}_j$ for every j lying in the set $\{1, 2, \ldots, e\}$. Then $v = (v_0, v_1, \ldots, v_{n-1}) = \sum_{j=1}^{e} \epsilon_j a_j \in \mathcal{V}$, where $v_i = \sum_{j=1}^{e} \epsilon_j a_{i,j}$ for each i lying in the set $\{0, 1, \ldots, n-1\}$. As $\mathcal{V}$ is a skew $\Theta_l - \gamma$-constacyclic code, we have $\tau_{\Theta_l,\gamma}(v) \in \mathcal{V}$. Note that

$$\begin{aligned}
\tau_{\Theta_l,\gamma}(v) &= (\gamma\Theta_l(v_{n-1}), \Theta_l(v_0), \Theta_l(v_1), \ldots, \Theta_l(v_{n-2})) \\
&= (\gamma\Theta_l(\sum_{j=1}^{e} \epsilon_j a_{(n-1),j}), \Theta_l(\sum_{j=1}^{e} \epsilon_j a_{0,j}), \ldots, \Theta_l(\sum_{j=1}^{e} \epsilon_j a_{(n-2),j}) \\
&= (\sum_{j=1}^{e} \epsilon_j \alpha_j \Theta_l(a_{(n-1),j}), \sum_{j=1}^{e} \epsilon_j \Theta_l(a_{0,j}), \ldots, \sum_{j=1}^{e} \epsilon_j \Theta_l(a_{(n-2),j}) \\
&= \sum_{j=1}^{e} \epsilon_j (\alpha_j \Theta_l(a_{(n-1),j}), \Theta_l(a_{0,j}), \ldots, \Theta_l(a_{(n-2),j}).
\end{aligned}$$

It implies that $(\alpha_j\Theta_l(a_{(n-1),j}), \Theta_l(a_{0,j}), \ldots, \Theta_l(a_{(n-2),j}) \in \mathcal{V}_j$ for each $1 \le j \le e$. Consequently, $\mathcal{V}_j$ is a skew $\Theta_l - \alpha_j$-constacyclic code for each j lying in the set $\{1, 2, \ldots, e\}$.
For the other side, assume that $\mathcal{V}_i$ is skew $\Theta_l - \alpha_i$-constacyclic code over $\mathbb{F}_q$ and $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathcal{V}$, where $v_j = \sum_{i=1}^{e} \epsilon_i a_{j,i}$ for each j lying in the set $\{0, 1, \ldots, n-1\}$. Then $a_i = (a_{0,i}, a_{1,i}, \ldots, a_{(n-1),i}) \in \mathcal{V}_i$ for each i lying in the set $\{1, 2, \ldots, e\}$ as $v = \sum_{i=1}^{e} \epsilon_i a_i$. Since $\mathcal{V}_i$ are skew $\Theta_l - \alpha_i$-constacyclic codes, we have $\tau_{\Theta_l,\alpha_i}(a_i) \in \mathcal{V}_i$ for each $1 \le i \le e$ which further implies that $\sum_{i=1}^{e} \epsilon_i \tau_{\Theta_l,\alpha_i}(a_i) \in \mathcal{V}$. Now,

$$\begin{aligned}
\sum_{i=1}^{e} \epsilon_i \tau_{\Theta_l,\alpha_i}(a_i) &= \sum_{i=1}^{e} \epsilon_i (\alpha_i\Theta_l(a_{(n-1),i}), \Theta_l(a_{0,i}), \ldots, \Theta_l(a_{(n-2),i})) \\
&= (\sum_{i=1}^{e} \epsilon_i \alpha_i \Theta_l(a_{(n-1),i}), \sum_{i=1}^{e} \epsilon_i \Theta_l(a_{0,i}), \ldots, \sum_{i=1}^{e} \epsilon_i \Theta_l(a_{(n-2),i})) \\
&= (\gamma\Theta_l(\sum_{i=1}^{e} \epsilon_i a_{(n-1),i}), \Theta_l(\sum_{i=1}^{e} \epsilon_i a_{0,i}), \ldots, \Theta_l(\sum_{i=1}^{e} \epsilon_i a_{(n-2),i})) \\
&= (\gamma\Theta_l(v_{n-1}), \Theta_l(v_0), \Theta_l(v_1), \ldots, \Theta_l(v_{n-2})) \\
&= \tau_{\Theta_l,\gamma}(v).
\end{aligned}$$

Consequently, $\mathcal{V}$ is a skew $\Theta_l - \gamma$-constacyclic code as $\tau_{\Theta_l,\gamma}(v) \in \mathcal{V}$. □

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

From [12], any skew $\Theta_l - \alpha$-constacyclic code $\mathcal{V}$ having length n over $\mathbb{F}_q$ for $\alpha \in \mathbb{F}_q^*$ is principally generated by a polynomial $g(x)$ as a left $\mathbb{F}_q[x;\Theta_l]$-submodule of the module $\frac{\mathbb{F}_q[x;\Theta_l]}{\langle x^n-\alpha\rangle}$ and $\mathcal{V} = \langle g(x)\rangle$, where $g(x)$ divides $x^n - \alpha$ on the right and regarded as the generator polynomial of the code $\mathcal{V}$. Using these arguments and Theorem 5, the below mentioned conclusion can be derived.

Theorem 6. *Suppose $\gamma = \sum_{i=1}^{e} \epsilon_i\alpha_i \in \mathcal{B}_e^*$ and $\mathcal{V} = \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2 \oplus \cdots \oplus \epsilon_e\mathcal{V}_e$ is a skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$ with $\mathcal{V}_i = \langle g_i(x)\rangle$, where each $g_i(x)$ divides $x^n - \alpha_i$ on the right (i lying in the set $\{1, 2, \ldots, e\}$). Then $\mathcal{V} = \langle g(x)\rangle$, where $g(x) = \sum_{i=1}^{e} \epsilon_i g_i(x)$ divides $x^n - \gamma$ on the right.*

We now consider a Gray map $\Phi : \mathcal{B}_e^n \to \mathbb{F}_q^{en}$ defined as

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

where $r_i = \sum_{k=1}^{e} \epsilon_k s_{ki}$ for each i lying in the set $\{0, 1, \ldots, n-1\}$ and a square matrix M satisfies $MM^t = \nu I$ for the identity matrix I and $\nu \in \mathbb{F}_q^*$. Then Φ is a bijective linear map, and the following result can be deduced.

Lemma 7. *Let us suppose that $\mathcal{V}$ is a linear code over $\mathcal{B}_e$ having dual code $\mathcal{V}^\perp$. Then $\Phi(\mathcal{V}^\perp) = \Phi(\mathcal{V})^\perp$.*

Proof. Suppose $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathcal{V}$ and $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{V}^\perp$, where $v_i = \sum_{j=1}^{e} \epsilon_j r_{ji}$ and $x_i = \sum_{j=1}^{e} \epsilon_j s_{ji}$ for each i lying in the set $\{0, 1, \ldots, n-1\}$. Then

$$\langle v, x\rangle = \epsilon_1 \sum_{i=0}^{n-1} r_{1i}s_{1i} + \epsilon_2 \sum_{i=0}^{n-1} r_{2i}s_{2i} + \cdots + \epsilon_e \sum_{i=0}^{n-1} r_{ei}s_{ei} = 0,$$

which implies that $\sum_{i=0}^{n-1} r_{ji}s_{ji} = 0$ for all $j \in \{1, \ldots, e\}$. Now,

$$\Phi(v) = ((r_{10}, r_{20}, \ldots, r_{e0})M, (r_{11}, r_{21}, \ldots, r_{e1})M, \ldots, (r_{1(n-1)}, r_{2(n-1)}, \ldots, r_{e(n-1)})M),$$

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

and

$$\begin{aligned}\langle \Phi(v), \Phi(x)\rangle = \Phi(v)[\Phi(x)]^t &= \sum_{i=0}^{n-1} (r_{1i}, r_{2i}, \ldots, r_{ei})MM^t(s_{1i}, s_{2i}, \ldots, s_{ei})^t \\ &= \nu \sum_{i=0}^{n-1} (r_{1i}, r_{2i}, \ldots, r_{ei})(s_{1i}, s_{2i}, \ldots, s_{ei})^t \\ &= \nu \sum_{i=0}^{n-1} r_{1i}s_{1i} + \nu \sum_{i=0}^{n-1} r_{2i}s_{2i} + \cdots + \nu \sum_{i=0}^{n-1} r_{ei}s_{ei} \\ &= 0,\end{aligned}$$

i.e., $\Phi(x) \in \Phi(\mathcal{V})^\perp$. Therefore, $\Phi(\mathcal{V})^\perp \supseteq \Phi(\mathcal{V}^\perp)$. Moreover, $|\Phi(\mathcal{V}^\perp)| = |\Phi(\mathcal{V})^\perp|$ as Φ is a bijective map. Hence $\Phi(\mathcal{V})^\perp = \Phi(\mathcal{V}^\perp)$. □

4. LCD Codes

This section first presents the dual of a skew constacyclic code, and then obtains conditions under which these codes must be LCD. Further, we study their Gray images.

For any $p(x) = \sum_{i=0}^{r} p_i x^i \in \mathcal{B}_e[x;\Theta_l]$ of degree r with $p_0 \in \mathcal{B}_e^*$, its left monic skew reciprocal polynomial is defined as $p^\natural(x) = (\Theta_l^r(p_0))^{-1} \sum_{i=0}^{r} \Theta_l^i(p_{r-i})x^i$. The polynomial $p(x)$ is called as self-reciprocal iff $p(x) = p^\natural(x)$. This monic skew reciprocal polynomial is useful for the investigation of dual code $\mathcal{V}^\perp$. If $\Theta_l(\alpha) = \alpha$ and n is divisible by order of Θ_l, then the dual $\mathcal{V}^\perp$ of a skew $\Theta_l - \alpha$-

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

constacyclic code $\mathcal{V} = \langle g(x) \rangle$ over $\mathbb{F}_q$ is a skew $\Theta_l - \alpha^{-1}$-constacyclic code over $\mathbb{F}_q$, which is given by $\mathcal{V}^\perp = \langle h^\natural(x) \rangle$, where $g(x)h(x) = h(x)g(x) = x^n - \alpha$ for the length n of $\mathcal{V}$. Now, under the same conditions on n and considering α_i ($1 \leq i \leq e$) fixed by Θ_l, we obtain the following result.

Theorem 8. *Suppose $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ and $\mathcal{V} = \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e$ is a skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$ having the generator polynomial $g(x) = \sum_{i=1}^{e} \epsilon_i g_i(x)$, where $g_i(x)$ is the generator polynomial of $\mathcal{V}_i$ and $g_i(x)h_i(x) = h_i(x)g_i(x) = x^n - \alpha_i$ for each $1 \leq i \leq e$. Then the generator polynomial of $\mathcal{V}^\perp$ is $h^\natural(x)$, where $h^\natural(x) = \sum_{i=1}^{e} \epsilon_i h_i^\natural(x)$ for $h(x) = \sum_{i=1}^{e} \epsilon_i h_i(x)$.*

Definition 9 (LCD codes)**.** *If $\mathcal{V} \cap \mathcal{V}^\perp = \{\mathbf{0}\}$ for any linear code $\mathcal{V}$ over $\mathcal{B}_e$, then the code $\mathcal{V}$ is considered as LCD (or complementary dual).*

In order to check the complementary duality of skew constacyclic codes over $\mathcal{B}_e$, we first need a criterion for evaluating the complementary duality of a skew constacyclic code over finite field.

Lemma 10. *[28, Theorem 4.1] Suppose that n is divisible by order of Θ_l, $\alpha \in \mathbb{F}_q^*$ such that $\alpha^2 = 1$ and $\mathcal{V}$ is a skew $\Theta_l - \alpha$-constacyclic code over finite field with skew generator polynomial $g(x)$. Choose $h(x)$ in order to ensure $g(x)h(x) = h(x)g(x) = x^n - \alpha$. Then $\mathcal{V}$ is a Euclidean LCD code iff $gcrd(g(x), h^\natural(x)) = 1$, where $gcrd(g(x), h^\natural(x))$ denotes the greatest common right divisor of $h^\natural(x)$ and $g(x)$.*

Once we get a link among the complementary duality of a linear code over $\mathcal{B}_e$ with its constituent codes, we can get requirements for complementary duality of any skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$. So, first we establish that link which is presented in the below mentioned result.

Proposition 11. *Suppose $\mathcal{V} = \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e$ is a linear code over $\mathcal{B}_e$. Then $\mathcal{V}$ is an LCD code iff each $\mathcal{V}_i$ is an LCD code over $\mathbb{F}_q$.*

Proof. Suppose $\mathcal{V} = \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e$ is a linear code over $\mathcal{B}_e$. The dual code is $\mathcal{V}^\perp = \epsilon_1 \mathcal{V}_1^\perp \oplus \epsilon_2 \mathcal{V}_2^\perp \oplus \cdots \oplus \epsilon_e \mathcal{V}_e^\perp$ and

$$\mathcal{V} \cap \mathcal{V}^\perp = \epsilon_1(\mathcal{V}_1 \cap \mathcal{V}_1^\perp) \oplus \epsilon_2(\mathcal{V}_2 \cap \mathcal{V}_2^\perp) \oplus \cdots \oplus \epsilon_e(\mathcal{V}_e \cap \mathcal{V}_e^\perp).$$

Consequently, it is evident that $\mathcal{V} \cap \mathcal{V}^\perp = \{\mathbf{0}\}$ iff $\mathcal{V}_i \cap \mathcal{V}_i^\perp = \{\mathbf{0}\}$ for every $1 \leq i \leq e$. □

From now onwards, we work under the assumption that α_i's are fixed by Θ_l for $1 \leq i \leq e$, and the order of Θ_l divides n. Using the Proposition 11 and Lemma 10, we now obtain requirements for skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$ to be complementary dual, where $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ for $\alpha_i = \pm 1$.

Theorem 12. *Suppose $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ for $\alpha_i \in \{1, -1\}$ and n is a multiple of order of Θ_l. Then a skew $\Theta_l - \gamma$-constacyclic code $\mathcal{V} = \langle \epsilon_1 g_1(x) + \epsilon_2 g_2(x) + \cdots + \epsilon_e g_e(x) \rangle$ having length n over $\mathcal{B}_e$ is an LCD code iff $gcrd(g_i(x), h_i^\natural(x)) = 1$, where $gcrd(g_i(x), h_i^\natural(x))$ denotes the greatest common right divisor of $h_i^\natural(x)$ and $g_i(x)$ for each $1 \leq i \leq e$.*

Proof. Suppose $\mathcal{V}_i = \langle g_i(x) \rangle$ is a skew $\Theta_l - \alpha_i$ constacyclic code over $\mathbb{F}_q$ and $h_i(x)$ is such that $g_i(x)h_i(x) = h_i(x)g_i(x) = x^n - \alpha_i$ for $1 \leq i \leq e$. Then, by Lemma 10, $\mathcal{V}_i$ is an LCD code iff $gcrd(g_i(x), h_i^\natural(x)) = 1$ for each $1 \leq i \leq e$. Therefore, $\mathcal{V}$ is an LCD code iff $gcrd(g_i(x), h_i^\natural(x)) = 1$ for each $1 \leq i \leq e$. □

Next, we present a relation between the Gray image of the intersection of a code and its dual with the intersection of their Gray images, which can be proved by using Lemma 7.

Lemma 13. *Suppose $\mathcal{V}$ is a linear code having length n over $\mathcal{B}_e$. Then $\Phi(\mathcal{V} \cap \mathcal{V}^\perp) = \Phi(\mathcal{V}) \cap \Phi(\mathcal{V})^\perp$, where Φ is the Gray map defined in Section 3.*

Proof. Suppose $c \in \Phi(\mathcal{V}) \cap \Phi(\mathcal{V})^{\perp}$. Then there exist $a \in \mathcal{V}$ and $b \in \mathcal{V}^{\perp}$ such that $c = \Phi(a) = \Phi(b)$ as $\Phi(\mathcal{V}^{\perp}) = \Phi(\mathcal{V})^{\perp}$ by Lemma 7. But Φ is injective, so we have $a = b$ and hence $c \in \Phi(\mathcal{V} \cap \mathcal{V}^{\perp})$. Therefore, $\Phi(\mathcal{V}) \cap \Phi(\mathcal{V}^{\perp}) \subseteq \Phi(\mathcal{V} \cap \mathcal{V}^{\perp})$.
Conversely, assume that $c \in \Phi(\mathcal{V} \cap \mathcal{V}^{\perp})$. Then $c = \Phi(a)$ for some $a \in \mathcal{V} \cap \mathcal{V}^{\perp}$. Further, $c = \Phi(a) \in \Phi(\mathcal{V}) \cap \Phi(\mathcal{V}^{\perp})$. Using Lemma 7, we get $c = \Phi(a) \in \Phi(\mathcal{V}) \cap \Phi(\mathcal{V})^{\perp}$ as $\Phi(\mathcal{V}^{\perp}) = \Phi(\mathcal{V})^{\perp}$. Therefore, $\Phi(\mathcal{V} \cap \mathcal{V}^{\perp}) \subseteq \Phi(\mathcal{V}) \cap \Phi(\mathcal{V})^{\perp}$ and the result follows. □

By applying this lemma, we are able to derive a relationship between the complementary duality of a linear code over $\mathcal{B}_e$ and its Gray image under the map Φ.

Theorem 14. *Suppose $\mathcal{V}$ is a linear code over $\mathcal{B}_e$. Then $\mathcal{V}$ is an LCD code iff $\Phi(\mathcal{V})$ is an LCD code over $\mathbb{F}_q$.*

Proof. As Φ is injective, the proof follows using Lemma 13. □

5. Quantum Codes

In this section, we consider γ to be a unit in $\mathcal{B}_e$ which is fixed by Θ_l and n be divisible by order of Θ_l. We obtain the dual containing conditions for a skew γ-constacyclic code over $\mathcal{B}_e$ and then establish the existence of a quantum code by applying the CSS construction on their Gray images. In this direction, we first recall some preliminary definitions and results.

Following [34], for a Hilbert space $\mathbb{H}^q$ of dimension q over the field of complex numbers $\mathbb{C}$, $(\mathbb{H}^q)^{\otimes n} = \mathbb{H}^q \otimes \cdots \otimes \mathbb{H}^q$ is also a Hilbert space of dimension q^n. Further, any q^k-dimensional subspace of the Hilbert space $(\mathbb{H}^q)^{\otimes n}$ is called a quantum code denoted by $[[n,k,d]]_q$, where d is the minimum distance of the code. Further, for the comparison of two quantum codes with parameters $[[n,k,d]]_q$ and $[[n',k',d']]_q$, we have the following conditions:

- $d = d'$ and $\frac{k}{n} > \frac{k'}{n'}$
- $d > d'$ and $\frac{k}{n} = \frac{k'}{n'}$
- $d > d'$ and $\frac{k}{n} > \frac{k'}{n'}$.

If any one of the above conditions is satisfied, then we say that the quantum code with the parameters $[[n,k,d]]_q$ is better than the one with the parameters $[[n',k',d']]_q$. Now, we recall the condition for a skew constacyclic code over $\mathbb{F}_q$ to contain its dual.

Lemma 15. *[41, Lemma 5.3] Suppose $\mathcal{V} = \langle g(x) \rangle$ is a skew $\Theta_l - \alpha$-constacyclic code having length n over $\mathbb{F}_q$, where $x^n - \alpha = h(x)g(x)$ for $\alpha = \pm 1$ and n be a multiple of the order of Θ_l. Then $\mathcal{V}^{\perp} \subseteq \mathcal{V}$ iff $x^n - \alpha$ is right divisible by $h^{\natural}(x)h(x)$.*

The following result presents a relation between the dual containing property of a skew constacyclic code over $\mathcal{B}_e$ in terms of its constituent codes in the decomposition.

Lemma 16. *Suppose $\mathcal{V} = \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2 \oplus \cdots \oplus \epsilon_e\mathcal{V}_e$ is a skew $\Theta_l - \gamma$-constacyclic code having length n over $\mathcal{B}_e$. Then $\mathcal{V}^{\perp} \subseteq \mathcal{V}$ iff $\mathcal{V}_i^{\perp} \subseteq \mathcal{V}_i$ for $1 \leq i \leq e$.*

Proof. Suppose $\mathcal{V} = \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2 \oplus \cdots \oplus \epsilon_e\mathcal{V}_e$ is a skew $\Theta_l - \gamma$-constacyclic code having length n over $\mathcal{B}_e$, $\mathcal{V}^{\perp} = \epsilon_1\mathcal{V}_1^{\perp} \oplus \epsilon_2\mathcal{V}_2^{\perp} \oplus \cdots \oplus \epsilon_e\mathcal{V}_e^{\perp}$ be its dual code such that $\mathcal{V}^{\perp} \subseteq \mathcal{V}$. Then multiplying by ϵ_i in the equation

$$\epsilon_1\mathcal{V}_1^{\perp} \oplus \epsilon_2\mathcal{V}_2^{\perp} \oplus \cdots \oplus \epsilon_e\mathcal{V}_e^{\perp} \subseteq \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2 \oplus \cdots \oplus \epsilon_e\mathcal{V}_e,$$

we get $\epsilon_i\mathcal{V}_i^{\perp} \subseteq \epsilon_i\mathcal{V}_i$ for each $1 \leq i \leq e$. As $\mathcal{V}_i$'s are codes over $\mathbb{F}_q$, it further implies that $\mathcal{V}_i^{\perp} \subseteq \mathcal{V}_i$ for each $1 \leq i \leq e$.
Conversely, assume that $\mathcal{V}_i^{\perp} \subseteq \mathcal{V}_i$ for each $1 \leq i \leq e$. Then $\epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2 \oplus \cdots \oplus \epsilon_e\mathcal{V}_e \subseteq \epsilon_1\mathcal{V}_1^{\perp} \oplus \epsilon_2\mathcal{V}_2^{\perp} \oplus \cdots \oplus \epsilon_e\mathcal{V}_e^{\perp}$, i.e., $\mathcal{V}^{\perp} \subseteq \mathcal{V}$ which completes the proof. □

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

Using this relation and Lemma 15, we now obtain conditions for skew constacyclic code over $\mathcal{B}_e$ to contain its dual code.

Theorem 17. *Suppose $\mathcal{V} = \langle g(x) \rangle$ is a skew $\Theta_l - \gamma$-constacyclic code having length n over $\mathcal{B}_e$, where n is a multiple of the order of Θ_l, $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i$ for $\alpha_i = \pm 1$, $g(x) = \sum_{i=1}^{e} \epsilon_i g_i(x)$ such that $x^n - \alpha_i = h_i(x) g_i(x)$ for $1 \le i \le e$. Then $\mathcal{V}^\perp \subseteq \mathcal{V}$ iff $x^n - \alpha_i$ is right divisible by $h_i^\natural(x) h_i(x)$ for each $1 \le i \le e$.*

Proof. Suppose $x^n - \alpha_i$ is right divisible by $h_i^\natural(x) h_i(x)$ for each $1 \le i \le e$. Then $\mathcal{V}_i^\perp \subseteq \mathcal{V}_i$ by Lemma 15, where $\mathcal{V}_i = \langle g_i(x) \rangle$ for $1 \le i \le e$. It implies that

$$\mathcal{V}^\perp = \epsilon_1 \mathcal{V}_1^\perp \oplus \epsilon_2 \mathcal{V}_2^\perp \oplus \cdots \oplus \epsilon_e \mathcal{V}_e^\perp \subseteq \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e = \mathcal{V}.$$

Conversely, assume that $\mathcal{V}^\perp \subseteq \mathcal{V}$, i.e.,

$$\epsilon_1 \mathcal{V}_1^\perp \oplus \epsilon_2 \mathcal{V}_2^\perp \oplus \cdots \oplus \epsilon_e \mathcal{V}_e^\perp \subseteq \epsilon_1 \mathcal{V}_1 \oplus \epsilon_2 \mathcal{V}_2 \oplus \cdots \oplus \epsilon_e \mathcal{V}_e.$$

Then multiplying by ϵ_i on both the sides, we get

$$\epsilon_i \mathcal{V}_i^\perp \subseteq \epsilon_i \mathcal{V}_i \text{ for each } 1 \le i \le e.$$

It further implies that $\mathcal{V}_i^\perp \subseteq \mathcal{V}_i$ as $\mathcal{V}_i$'s are linear codes over $\mathbb{F}_q$ and hence $x^n - \alpha_i$ is right divisible by $h_i^\natural(x) h_i(x)$ for each $1 \le i \le e$. □

To obtain quantum codes from dual containing codes, we use the CSS construction [35, Theorem 3], which is given below.

Lemma 18 (CSS construction)**.** *Suppose $\mathcal{V}_1 = [n, k_1, d_1]_q$ and $\mathcal{V}_2 = [n, k_2, d_2]_q$ are linear codes over $\mathbb{F}_q$ with $\mathcal{V}_2^\perp \subseteq \mathcal{V}_1$. Assume that $d = \min\{w_H(v) : v \in (\mathcal{V}_1 \setminus \mathcal{V}_2^\perp) \cup (\mathcal{V}_2 \setminus \mathcal{V}_1^\perp)\} \ge \min\{d_1, d_2\}$. Then there exists a QECC with parameters $[[n, k_1 + k_2 - n, d]]_q$. In particular, if $\mathcal{V}_1 = \mathcal{V}_2$ and let $d = \min\{w_H(v) : v \in (\mathcal{V}_1 \setminus \mathcal{V}_1^\perp)\}$, then there exists a QECC with parameters $[[n, 2k_1 - n, d]]_q$.*

Now, we employ the above CSS construction to obtain quantum codes from the dual containing skew $\Theta_l - \gamma$-constacyclic codes over $\mathcal{B}_e$, where $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i$ for $\alpha_i = \pm 1$.

Theorem 19. *Suppose $\mathcal{V}$ is a skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$ such that $\mathcal{V}^\perp \subseteq \mathcal{V}$ and $\Phi(\mathcal{V})$ have the parameters $[en, k, d]$. Then, the existence of a quantum code over $\mathbb{F}_q$ having the parameters $[[en, 2k - en, d]]_q$ is guaranteed.*

Proof. Suppose $\mathcal{V}$ is a skew $\Theta_l - \gamma$-constacyclic code over $\mathcal{B}_e$ with $\mathcal{V} \supseteq \mathcal{V}^\perp$. Then $\Phi(\mathcal{V})$ is a linear code over $\mathbb{F}_q$ with $\Phi(\mathcal{V}) \supseteq \Phi(\mathcal{V}^\perp) = \Phi(\mathcal{V})^\perp$. By using Lemma 18, the existence of a quantum code over $\mathbb{F}_q$ having the parameters $[[en, 2k - en, d]]_q$ is guaranteed. □

6. Complementary Dual and Quantum Codes from $\mathbb{F}_q\mathcal{B}_e$-Additive Skew Constacyclic Codes

In this section, we examine $\mathbb{F}_q\mathcal{B}_e$-additive codes. We first obtain dual containing conditions for an additive skew constacyclic code over $\mathbb{F}_q\mathcal{B}_e$ and establish the existence of a quantum code with certain parameters. Further, we obtain conditions for an additive skew constacyclic code to be ACD (additive complementary dual) in some instances. Throughout this section, we consider γ to be a unit in $\mathcal{B}_e$ which is fixed by Θ_l and n is divisible by the order of Θ_l.

Consider the set $\mathbb{F}_q\mathcal{B}_e = \{(a, b) : a \in \mathbb{F}_q, b \in \mathcal{B}_e\}$ which forms a group under component-wise addition. Define a projection map $\pi : \mathcal{B}_e \to \mathbb{F}_q$ as $\pi(s_0 + us_1 + \cdots + u^{e-1}s_{e-1}) = s_0$, where $s_i \in \mathbb{F}_q$ for $0 \le i \le e - 1$. Further, we define a multiplication $* : \mathcal{B}_e \times \mathbb{F}_q^m\mathcal{B}_e^n \to \mathbb{F}_q^m\mathcal{B}_e^n$ as

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

$s * (a_0, a_1, \dots, a_{m-1}, b_0, b_1, \dots, b_{n-1}) = (\pi(s)a_0, \pi(s)a_1, \dots, \pi(s)a_{m-1}, sb_0, sb_1, \dots, sb_{n-1})$, where $s, b_i \in \mathcal{B}_e$ and $a_j \in \mathbb{F}_q$ for $0 \leq i \leq n-1, 0 \leq j \leq m-1$. Then, it can be checked that the set $\mathbb{F}_q^m \mathcal{B}_e^n$ defined as

$$\mathbb{F}_q^m \mathcal{B}_e^n = \{(a, b) : a \in \mathbb{F}_q^m, b \in \mathcal{B}_e^n\}$$

forms a $\mathcal{B}_e$-module under the componentwise addition and the multiplication defined by '$*$'. Further, we recall that any $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$ having length (m, n) is a non-empty subset of $\mathbb{F}_q^m \mathcal{B}_e^n$ such that $\mathcal{V}$ forms a $\mathcal{B}_e$-submodule of the module $\mathbb{F}_q^m \mathcal{B}_e^n$. The dual code $\mathcal{V}^\perp$ of an $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$, which is defined as

$$\mathcal{V}^\perp = \{z \in \mathbb{F}_q^m \mathcal{B}_e^n : [z, c] = 0 \; \forall \, c \in \mathcal{V}\}$$

where

$$[z, c] = u^{e-1} \left(\sum_{i=0}^{m-1} a_i a_i' \right) + \sum_{j=0}^{n-1} b_j b_j'$$

for $z = (a_0', a_1', \dots, a_{m-1}', b_0', b_1', \dots, b_{n-1}')$ and $c = (a_0, a_1, \dots, a_{m-1}, b_0, b_1, \dots, b_{n-1})$, is also a $\mathbb{F}_q\mathcal{B}_e$-additive code having length (m, n). We say that an $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$ is an additive complementary dual (ACD) code if $\mathcal{V} \cap \mathcal{V}^\perp = \{\mathbf{0}\}$. Now, we define an $\mathbb{F}_q\mathcal{B}_e$-additive skew constacyclic code.

Definition 20. *For a unit element $\gamma \in \mathcal{B}_e$ and an automorphism Θ_l, an $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$ having length (m, n) is said to be an $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code if $(\tau_1(a), \tau_{\Theta_l, \gamma}(b)) \in \mathcal{V}$ for every $(a, b) \in \mathcal{V}$ where τ_1, $\tau_{\Theta_l, \gamma}$ are the cyclic and the skew $\Theta_l - \gamma$-constacyclic shifts, respectively.*

For a unit element $\gamma \in \mathcal{B}_e$, consider the set $S_{(m,n)} = \frac{\mathbb{F}_q[x]}{\langle x^m - 1 \rangle} \times \frac{\mathcal{B}_e[x; \Theta_l]}{\langle x^n - \gamma \rangle}$. We identify an element $(a, b) \in \mathbb{F}_q^m \mathcal{B}_e^n$ by the polynomials $(a(x), b(x)) \in S_{(m,n)}$ where $a = (a_0, a_1, \dots, a_{m-1}), b = (b_0, b_1, \dots, b_{n-1}), a(x) = a_0 + a_1 x + \dots, a_{m-1} x^{m-1}$ and $b(x) = b_0 + b_1 x + \dots + b_{n-1} x^{n-1}$. Now, we define the corresponding multiplication $* : \mathcal{B}_e[x] \times S_{(m,n)} \to S_{(m,n)}$ as

$$z(x) * (a(x), b(x)) = (\pi(z(x)) a(x), z(x) b(x))$$

where $\pi(z(x)) = \sum_i \pi(z_i) x^i$ for any $z(x) = \sum_i z_i x^i \in \mathcal{B}_e[x]$ and $(a(x), b(x)) \in S_{(m,n)}$. The set $S_{(m,n)}$ forms a $\mathcal{B}_e[x]$-module with respect to the usual componentwise addition of polynomials and the multiplication defined by $*$. Now, under the above identification of vectors by polynomials and considering the above module structure of $S_{(m,n)}$, an $\mathbb{F}_q\mathcal{B}_e$-additive skew constacyclic code can be seen as a $\mathcal{B}_e[x]$-submodule of $S_{(m,n)}$ as given below.

Theorem 21. *Suppose $\mathcal{V}$ is an $\mathbb{F}_q\mathcal{B}_e$-additive code having length (m, n). Then, it is an $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n) iff $\mathcal{V}$ is a $\mathcal{B}_e[x]$-submodule of the module $S_{(m,n)}$.*

Proof. Suppose $\mathcal{V}$ is an $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n) and $(a(x), b(x)) \in \mathcal{V}$ with the vector representation (a, b). Then $(\tau_1(a), \tau_{\Theta_l, \gamma}(b)) \in \mathcal{V}$. Note that

$$x * (a(x), b(x)) = (a_{m-1} + a_0 x + \dots + a_{m-2} x^{m-1}, \gamma \Theta_l(b_{n-1}) + \Theta_l(b_0) x + \dots, \Theta_l(b_{n-2}) x^{n-1})$$

which corresponds to $(\tau_1(a), \tau_{\Theta_l, \gamma}(b)) \in \mathcal{V}$. It implies that $x * (a(x), b(x)) \in \mathcal{V}$ and hence $x^i * (a(x), b(x)) \in \mathcal{V}$ for any non-negative integer i. Also, using the polynomial identification, we get $z(x) * (a(x), b(x)) \in \mathcal{V}$ for any $z(x) \in \mathcal{B}_e[x]$ as $\mathcal{V}$ is a $\mathcal{B}_e$-submodule of the module $\mathbb{F}_q^m \mathcal{B}_e^n$. Therefore, $\mathcal{V}$ is a $\mathcal{B}_e[x]$-submodule of the module $S_{(m,n)}$.
Conversely, assume that $\mathcal{V}$ is a $\mathcal{B}_e[x]$-submodule of the module $S_{(m,n)}$ and $(a, b) \in \mathcal{V}$ with the polynomial representation $(a(x), b(x))$. Then $x * (a(x), b(x)) \in \mathcal{V}$. Note that the polynomial representation of $(\tau_1(a), \tau_{\Theta_l, \gamma}(b))$ is $x * (a(x), b(x))$. Therefore, $(\tau_1(a), \tau_{\Theta_l, \gamma}(b)) \in \mathcal{V}$ and hence $\mathcal{V}$ is an $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code. $\square$

Now, we define a Gray map $\Psi : \mathbb{F}_q^m \mathcal{B}_e^n \to \mathbb{F}_q^{m+en}$ as

$$\Psi(a, r) = (a, \Phi(r))$$

where $a \in \mathbb{F}_q^m, r \in \mathcal{B}_e^n$ and Φ is the map defined in Section 3. It can be checked that Ψ is a linear map, which is also bijective. Further, Ψ preserves duality as stated in the next result which can be proved on similar lines to [37, Lemma 6].

Lemma 22. *Suppose $\mathcal{V}$ is an $\mathbb{F}_q\mathcal{B}_e$-additive code having length (m, n) with its dual code $\mathcal{V}^\perp$. Then $\Psi(\mathcal{V}^\perp) = \Psi(\mathcal{V})^\perp$.*

Now, we define two projection maps $\pi_n : \mathbb{F}_q^m\mathcal{B}_e^n \to \mathcal{B}_e^n$, $\pi_m : \mathbb{F}_q^m\mathcal{B}_e^n \to \mathbb{F}_q^m$ as $\pi_n(a, b) = b, \pi_m(a, b) = a$ where $a \in \mathbb{F}_q^m$ and $b \in \mathcal{B}_e^n$. Then, for any $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$ having length (m, n), $\pi_m(\mathcal{V})$ and $\pi_n(\mathcal{V})$ are linear codes having lengths m, n over $\mathbb{F}_q$ and $\mathcal{B}_e$, respectively. Further, we call an $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$ to be a separable code if it can be written in terms of the codes $\pi_m(\mathcal{V})$ and $\pi_n(\mathcal{V})$ as given below.

Definition 23. *An $\mathbb{F}_q\mathcal{B}_e$-additive code $\mathcal{V}$ having length (m, n) is said to be a separable code, if $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$.*

If $\mathcal{V}$ is a separable code then its dual code is $\mathcal{V}^\perp = \pi_m(\mathcal{V})^\perp \times \pi_n(\mathcal{V})^\perp$. Further, the below result can classify a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew constacyclic code.

Theorem 24. *Suppose $\mathcal{V}$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive code having length (m, n). Then, it is an $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n) iff $\pi_m(\mathcal{V}), \pi_n(\mathcal{V})$ are cyclic and skew $\Theta_l - \gamma$-constacyclic codes over $\mathbb{F}_q$ and $\mathcal{B}_e$, respectively.*

Proof. Suppose $\mathcal{V}$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n), $a \in \pi_m(\mathcal{V})$ and $b \in \pi_n(\mathcal{V})$. Then $(a, b) \in \mathcal{V}$ and $(\tau_1(a), \tau_{\Theta_l,\gamma}(b)) \in \mathcal{V}$. That is, $\tau_1(a) \in \pi_m(\mathcal{V})$ and $\tau_{\Theta_l,\gamma}(b) \in \pi_n(\mathcal{V})$. Therefore, $\pi_m(\mathcal{V}), \pi_n(\mathcal{V})$ are cyclic and skew $\Theta_l - \gamma$-constacyclic codes, respectively. Conversely, assume that $\pi_m(\mathcal{V}), \pi_n(\mathcal{V})$ be cyclic and skew $\Theta_l - \gamma$-constacyclic codes and $(a, b) \in \mathcal{V}$. Then $a \in \pi_m(\mathcal{V})$ and $b \in \pi_n(\mathcal{V})$. Therefore, $\tau_1(a) \in \pi_m(\mathcal{V})$ and $\tau_{\Theta_l,\gamma}(b) \in \pi_n(\mathcal{V})$ as $\pi_m(\mathcal{V}), \pi_n(\mathcal{V})$ are cyclic and skew $\Theta_l - \gamma$-constacyclic codes, respectively. Hence, $(\tau_1(a), \tau_{\Theta_l,\gamma}(b)) \in \mathcal{V}$, i.e., $\mathcal{V}$ is an $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code. □

The above classification is later used to obtain quantum codes from separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic codes. For achieving this, we first derive the necessary and sufficient conditions for a separable $\mathbb{F}_q\mathcal{B}_e$-additive code to contain its dual code.

Lemma 25. *Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive code having length (m, n). Then $\mathcal{V}^\perp \subseteq \mathcal{V}$ iff $\pi_m(\mathcal{V})^\perp \subseteq \pi_m(\mathcal{V})$ and $\pi_n(\mathcal{V})^\perp \subseteq \pi_n(\mathcal{V})$.*

Proof. As $\mathcal{V}$ is a separable code, we have $\mathcal{V}^\perp = \pi_m(\mathcal{V})^\perp \times \pi_n(\mathcal{V})^\perp$. Therefore, $\mathcal{V}^\perp \subseteq \mathcal{V}$ iff $\pi_m(\mathcal{V})^\perp \subseteq \pi_m(\mathcal{V})$ and $\pi_n(\mathcal{V})^\perp \subseteq \pi_n(\mathcal{V})$. □

The following result obtains the condition for constacyclic code over $\mathbb{F}_q$ to contain its dual code.

Lemma 26. *[32] Suppose $\mathcal{V} = \langle f(x) \rangle$ is an α-constacyclic code having length m over $\mathbb{F}_q$ for $\alpha = \pm 1$. Then $\mathcal{V}^\perp \subseteq \mathcal{V}$ iff $x^m - \alpha \equiv 0 \pmod{f(x)f^*(x)}$.*

Proposition 27. *Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n), where $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ for $\alpha_i = \pm 1$. Assume that $\pi_m(\mathcal{V}) = \langle f(x) \rangle$ and $\pi_n(\mathcal{V}) = \langle \sum_{i=1}^{e} \epsilon_i g_i(x) \rangle$. Choose $h(x), h_i(x)$ for $1 \le i \le e$ such that $x^m - 1 = f(x)h(x)$ and $x^n - \alpha_i = h_i(x)g_i(x)$*

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

for $1 \leq i \leq e$. Then $\mathcal{V}^{\perp} \subseteq \mathcal{V}$ iff $x^n - \alpha_i$ is right divisible by $h_i^{\natural}(x)h_i(x)$ for each $1 \leq i \leq e$ and $x^m - 1 \equiv 0 \pmod{f(x)f^*(x)}$.

Proof. From Lemma 25, $\mathcal{V}^{\perp} \subseteq \mathcal{V}$ iff $\pi_m(\mathcal{V})^{\perp} \subseteq \pi_m(\mathcal{V})$, $\pi_n(\mathcal{V})^{\perp} \subseteq \pi_n(\mathcal{V})$ where $\pi_m(\mathcal{V}), \pi_n(\mathcal{V})$ are cyclic and skew $\Theta_l - \gamma$-constacyclic codes having lengths m, n over $\mathbb{F}_q$ and $\mathcal{B}_e$, respectively. Rest of the result follows using Lemma 26 and Theorem 17. □

Proposition 27 gives the necessary and sufficient condition for a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code to contain its dual. Using the CSS construction and Proposition 27, we now present the construction of quantum codes from separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic codes in the next theorem.

Theorem 28. *Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n) such that $\mathcal{V}^{\perp} \subseteq \mathcal{V}$, where $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ for $\alpha_i = \pm 1$. Assume that the parameters of the code $\Psi(\mathcal{V})$ be $[m + en, k, d_H]$. Then, there exists a quantum code with the parameters $[[m + en, 2k - (m + en), d_H]]_q$ over $\mathbb{F}_q$.*

Proof. Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code such that $\mathcal{V}^{\perp} \subseteq \mathcal{V}$. Then $\Psi(\mathcal{V}^{\perp}) \subseteq \Psi(\mathcal{V})$ which implies that $\Psi(\mathcal{V})^{\perp} \subseteq \Psi(\mathcal{V})$ as $\Psi(\mathcal{V}^{\perp}) = \Psi(\mathcal{V})^{\perp}$ by Lemma 22. That is, $\Psi(\mathcal{V})$ is a $[m + en, k, d_H]$ linear code over $\mathbb{F}_q$ which contains its dual. Therefore, by Lemma 18, there exists a quantum code with the parameters $[[m + en, 2k - (m + en), d_H]]_q$ over $\mathbb{F}_q$. □

Besides getting quantum codes from additive codes over $\mathbb{F}_q\mathcal{B}_e$, these codes can be investigated to obtain conditions for complementary duality. In particular, we obtain conditions for an $\mathbb{F}_q\mathcal{B}_e$-additive skew constacyclic code to be ACD for which we need two basic results which are given below.

Lemma 29. *[14] Suppose $\mathcal{V}$ is a cyclic code over $\mathbb{F}_q$ with generator polynomial $f(x)$. Then $\mathcal{V}$ is an LCD code iff $\gcd(f(x), h^*(x)) = 1$, where $\gcd(f(x), h^*(x))$ denotes the greatest common divisor of $f(x)$ and $h^*(x)$.*

Proposition 30. *Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive code having length (m, n). Then $\mathcal{V}$ is an ACD code iff $\pi_m(\mathcal{V})$ and $\pi_n(\mathcal{V})$ are LCD codes over $\mathbb{F}_q$ and $\mathcal{B}_e$, respectively.*

Proof. Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is an ACD code and its dual code be $\mathcal{V}^{\perp} = \pi_m(\mathcal{V})^{\perp} \times \pi_n(\mathcal{V})^{\perp}$. If $x \in \pi_m(\mathcal{V}) \cap \pi_m(\mathcal{V})^{\perp}$ and $y \in \pi_n(\mathcal{V}) \cap \pi_n(\mathcal{V})^{\perp}$ then $(x, y) \in \mathcal{V} \cap \mathcal{V}^{\perp} = \{0\}$. Therefore, $x = y = 0$ which implies that $\pi_m(\mathcal{V})$ and $\pi_n(\mathcal{V})$ are LCD codes over $\mathbb{F}_q$ and $\mathcal{B}_e$, respectively.
Conversely, assume that $\pi_m(\mathcal{V}), \pi_n(\mathcal{V})$ be LCD codes over $\mathbb{F}_q$ and $\mathcal{B}_e$, respectively. For any $(x, y) \in \mathcal{V} \cap \mathcal{V}^{\perp}$, we have $x \in \pi_m(\mathcal{V}) \cap \pi_m(\mathcal{V})^{\perp} = \{0\}$ and $y \in \pi_n(\mathcal{V}) \cap \pi_n(\mathcal{V})^{\perp} = \{0\}$. That is, $(x, y) = (0, 0)$ which implies that $\mathcal{V}$ is an ACD code. □

Using the above classification for complementary duality, we now present necessary and sufficient conditions for a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew constacyclic code to be ACD.

Theorem 31. *Suppose $\mathcal{V} = \pi_m(\mathcal{V}) \times \pi_n(\mathcal{V})$ is a separable $\mathbb{F}_q\mathcal{B}_e$-additive skew $\Theta_l - \gamma$-constacyclic code having length (m, n), where $\gamma = \sum_{i=1}^{e} \epsilon_i \alpha_i \in \mathcal{B}_e^*$ for $\alpha_i = \pm 1$. Assume that $\pi_m(\mathcal{V}) = \langle f(x) \rangle$ and $\pi_n(\mathcal{V}) = \langle \sum_{i=1}^{e} \epsilon_i g_i(x) \rangle$. Choose $h(x), h_i(x)$ such that $x^m - 1 = f(x)h(x)$ and $x^n - \alpha_i = h_i(x)g_i(x)$ for $1 \leq i \leq e$. Then $\mathcal{V}$ is an ACD code iff the following conditions hold:*

1. *$\gcd(f(x), h^*(x)) = 1$, where $\gcd(f(x), h^*(x))$ denotes the greatest common divisor of $f(x)$ and $h^*(x)$.*
2. *$\mathrm{gcrd}(g_i(x), h_i^{\natural}(x)) = 1$, where $\mathrm{gcrd}(g_i(x), h_i^{\natural}(x))$ denotes the greatest common right divisor of $g_i(x)$ and $h_i^{\natural}(x)$, for $1 \leq i \leq e$.*

Proof. It can be verified by using Lemma 29, Theorems 12 and 24. □

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

7. Examples

In the present section, we derive several LCD and quantum codes in support of our study. Most of the codes are either MDS or near MDS. Moreover, a comparison is made between the resulting quantum codes and the codes found in recent literature.

To obtain the Gray image of any skew constacyclic code over $\mathcal{B}_2$ under Φ, we consider the matrix $M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Notably, all linear codes over a finite field having parameters $[n,k,d]$ satisfy the *Singleton bound*, which is determined by $d \leq n-k+1$. If $d = n-k+1$, it is considered as an MDS code; if $d = n-k$, it is considered as near MDS. In case of an $[[n,k,d]]_q$ quantum code, we have the *Singleton bound* $k+2d \leq n+2$. The quantum code satisfying the equality $k+2d = n+2$ is called as an MDS code, and the code satisfying $k+2d = n$ is called a near MDS code. Now, we go through a few examples of codes in detail.

Example 32. *Take $n = 12$, $e = 2$. Consider the factorization of $x^{12}-1$ over $\mathbb{F}_{5^2}$ given by*

$$x^{12}-1 =(x^9+2x^8+t^{20}x^7+3x^6+t^{22}x^5+2x^4+tx^3+t^{11}x+4)(x^3+3x^2+t^{11}x+1)$$

and take $\mathcal{V}_1 = \langle x^3+3x^2+t^{11}x+1\rangle$. Further, consider the factorization

$$x^{12}-1 =(x^{11}+t^{22}x^{10}+4x^9+t^{10}x^8+x^7+t^{22}x^6+4x^5+t^{10}x^4+x^3+t^{22}x^2+4x+t^{10})(x+t^2)$$

and take $\mathcal{V}_2 = \langle x+t^2\rangle$. Then $\mathcal{V} = \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2$ is a cyclic code over $\mathbb{F}_{5^2}+u\mathbb{F}_{5^2}$ and $\Phi(\mathcal{V})$ is an LCD code with the parameters $[24,20,4]_{5^2}$ which is a near MDS code.

Example 33. *Take $n = 30$, $e = 2$. Consider the factorization of $x^{30}+1$ over $\mathbb{F}_{11^2}$ given by*

$$\begin{aligned}x^{30}+1 =&(x^{28}+t^{78}x^{27}+2x^{26}+t^{78}x^{25}+x^{24}+10x^{22}+t^{18}x^{21}+9x^{20}+t^{18}x^{19}+10x^{18}+x^{16}\\&+t^{78}x^{15}+2x^{14}+t^{78}x^{13}+x^{12}+10x^{10}+t^{18}x^9+9x^8+t^{18}x^7+10x^6+x^4+t^{78}x^3\\&+2x^2+t^{78}x+1)(x^2+t^{18}x+1)\end{aligned}$$

and take $\mathcal{V}_1 = \langle x^2+t^{18}x+1\rangle$. Further, consider the factorization

$$\begin{aligned}x^{30}+1 =&(x^{29}+t^{71}x^{28}+2x^{27}+t^{83}x^{26}+4x^{25}+t^{95}x^{24}+8x^{23}+t^{107}x^{22}+5x^{21}+t^{119}x^{20}+\\&10x^{19}+t^{11}x^{18}+9x^{17}+t^{23}x^{16}+7x^{15}+t^{35}x^{14}+3x^{13}+t^{47}x^{12}+6x^{11}+t^{59}x^{10}+\\&x^9+t^{71}x^8+2x^7+t^{83}x^6+4x^5+t^{95}x^4+8x^3+t^{107}x^2+5x+t^{119})(x+t)\end{aligned}$$

and take $\mathcal{V}_2 = \langle x+t\rangle$. Then $\mathcal{V} = \epsilon_1\mathcal{V}_1 \oplus \epsilon_2\mathcal{V}_2$ is a skew negacyclic code over $\mathbb{F}_{11^2}+u\mathbb{F}_{11^2}$ and the parameters of $\Phi(\mathcal{V})$ are $[60,57,3]_{11^2}$. By using Theorem 19, we obtain a quantum code having the parameters $[[60,54,3]]_{11^2}$ which is better than the code $[[60,50,3]]_{11^2}$ given in [40].

Example 34. *Take $m = 48$, $n = 8$, $e = 2$. Consider the factorization of $x^{48}-1$ over $\mathbb{F}_{7^2}$ given by*

$$\begin{aligned}x^{48}-1 =&(x^{46}+t^6x^{45}+t^{31}x^{44}+t^{25}x^{43}+t^{10}x^{42}+t^{19}x^{41}+6x^{40}+t^{28}x^{39}+t^{17}x^{38}+t^{35}x^{37}+\\&t^{35}x^{36}+t^{30}x^{35}+t^{31}x^{34}+t^{18}x^{33}+t^{47}x^{32}+t^{20}x^{31}+t^{19}x^{30}+t^{33}x^{29}+t^{44}x^{28}+\\&t^{19}x^{27}+tx^{26}+t^{29}x^{25}+t^{13}x^{24}+t^{20}x^{23}+t^{10}x^{22}+t^{23}x^{21}+5x^{20}+t^7x^{19}+t^{29}x^{18}+\\&t^{15}x^{17}+t^{46}x^{16}+t^{44}x^{15}+t^{20}x^{14}+t^{36}x^{13}+t^{46}x^{12}+t^{42}x^{11}+t^{44}x^{10}+t^{41}x^9+t^{20}x^8\\&+t^{28}x^7+t^{21}x^6+t^{13}x^5+tx^4+t^{13}x^3+2x^2+t^{36}x+t^{27})(x^2+t^{30}x+t^{45})\end{aligned}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

and take $f(x) = x^2 + t^{30}x + t^{45}$. *Further, consider the factorizations*

$$x^8 + 1 = (x^6 + t^{30}x^4 + t^{12}x^2 + t^{42})(x^2 + t^6)$$

and

$$x^8 - 1 = (x^7 + t^{12}x^6 + x^5 + t^{12}x^4 + x^3 + t^{12}x^2 + x + t^{12})(x + t^{12})$$

and take $g_1(x) = x^2 + t^6$ *and* $g_2(x) = x + t^{12}$. *Then, the code* $\mathcal{V}$ *given by Proposition 27 is a* $\mathbb{F}_{7^2}(\mathbb{F}_{7^2} + u\mathbb{F}_{7^2})-$*additive skew constacyclic code containing its dual. The Gray image* $\Phi(\mathcal{V})$ *of the code* $\mathcal{V}$ *is a* $[64, 59, 3]_{7^2}$ *code which contains its dual. Therefore, a quantum code having the parameters* $[[64, 54, 3]]_{7^2}$ *is obtained by using Theorem 28.*

In Tables 1 and 2, we present LCD and quantum codes obtained from skew $\Theta_1 - \gamma$-constacyclic code $\mathcal{V} = \langle \epsilon_1 g_1(x) + \epsilon_2 g_2(x) \rangle$ over $\mathcal{B}_2$, respectively. In both the tables, the first column represents the length of the code $\mathcal{V}$, and the second column represents (α_1, α_2) such that $\gamma = \epsilon_1\alpha_1 + \epsilon_2\alpha_2$. The third column represents the polynomials $g_1(x), g_2(x)$ such that $\mathcal{V}$ is generated by $\epsilon_1 g_1(x) + \epsilon_2 g_2(x)$ while the parameters of $\Phi(\mathcal{V})$ are presented in the fourth column. In Table 2, the parameters of the quantum codes obtained from the code $\Phi(\mathcal{V})$ (using Theorem 19) are presented in the fifth column. In the sixth column, the comparison of these obtained codes is made with the known quantum codes that have been reported recently in the literature.

Table 1. LCD codes obtained from skew $\Theta_1 - \gamma$-constacyclic code $\mathcal{V}$ over $\mathcal{B}_2$.

n	(α_1, α_2)	$g_1(x), g_2(x)$	$\Phi(\mathcal{V})$	Remark
8	$(1, 1)$	$t^2 1,\ t^2 1$	$[16, 14, 2]_{25}$	near MDS
12	$(1, 1)$	$1t^{11}31,\ t^2 1$	$[24, 20, 4]_{25}$	near MDS
12	$(1, 1)$	$t^2 1,\ t^2 1$	$[24, 22, 2]_{25}$	near MDS
8	$(1, 1)$	$6t^{36}1,\ t^3 1$	$[16, 13, 4]_{49}$	MDS
12	$(1, 1)$	$t^3 t^{22} t^{22} 1,\ t^3 1$	$[24, 20, 4]_{49}$	near MDS
12	$(1, 1)$	$t^5 1,\ t^5 1$	$[24, 22, 2]_{121}$	near MDS
12	$(1, 1)$	$t^{65} t^{81} 1,\ t^5 1$	$[24, 20, 4]_{121}$	near MDS
20	$(1, 1)$	$t^{75} t^{54} t1,\ t^{75} 1$	$[40, 36, 4]_{121}$	near MDS

Table 2. Quantum codes obtained from dual containing skew $\Theta_1 - \gamma$-constacyclic code over $\mathcal{B}_2$.

n	(α_1, α_2)	$g_1(x), g_2(x)$	$\Phi(\mathcal{V})$	$[[en, k, \geq d]]_q$	Existing/Remark
8	$(-1, 1)$	$t01,\ t^2 1$	$[16, 13, 3]$	$[[16, 10, 3]]_{3^2}$	−
8	$(-1, 1)$	$t^3 01,\ t1$	$[16, 13, 3]$	$[[16, 10, 3]]_{5^2}$	−
30	$(-1, -1)$	$1t^3 1,\ t^4 t^2 1$	$[60, 56, 3]$	$[[60, 52, 3]]_{5^2}$	−
48	$(1, 1)$	$t^5 t^7 1,\ 10t1$	$[96, 91, 4]$	$[[96, 86, 4]]_{5^2}$	$[[96, 84, 4]]_{5^2}$ [41]
8	$(-1, 1)$	$t^6 01,\ t^{12} 1$	$[16, 13, 3]$	$[[16, 10, 3]]_{7^2}$	−
48	$(-1, 1)$	$t^3 t1,\ t0t^{17} 1$	$[96, 91, 4]$	$[[96, 86, 4]]_{7^2}$	$[[96, 84, 4]]_{7^2}$ [41]
8	$(-1, 1)$	$t^{65} 11,\ t^{30} 1$	$[16, 13, 4]$	$[[16, 10, 4]]_{11^2}$	MDS
30	$(-1, -1)$	$1t^{18} 1,\ t1$	$[60, 57, 3]$	$[[60, 54, 3]]_{11^2}$	$[[60, 50, 3]]_{11^2}$ [40]
30	$(-1, -1)$	$1t^{18} 1,\ t^{90} t^{33} 1$	$[60, 56, 4]$	$[[60, 52, 4]]_{11^2}$	$[[60, 50, 3]]_{11^2}$ [40]

Further, we obtain quantum codes from $\mathbb{F}_q\mathcal{B}_2$-additive skew $\Theta_1 - \gamma$-constacyclic codes having length (m, n) where $\gamma = \epsilon_1\alpha_1 + \epsilon_2\alpha_2$. In Table 3, we tabulate α_1, α_2, the polynomials $f(x), g_1(x), g_2(x)$ such that $\pi_m(\mathcal{V}) = \langle f(x) \rangle$ and $\pi_n(\mathcal{V}) = \langle \sum_{i=1}^{2} \epsilon_i g_i(x) \rangle$ where $f(x) | x^m - 1$ and $g_i(x)$ is a right divisor of $x^n - \alpha_i$ for $i = 1, 2$. The parameters of the code $\Psi(\mathcal{V})$ are presented in the fifth column, whereas the parameters of the derived quantum codes are presented in the sixth column by using Theorem 28.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 October 2024 doi:10.20944/preprints202410.1716.v1

Table 3. Quantum codes obtained from $\mathbb{F}_q\mathcal{B}_2$-additive skew $\Theta_1 - \gamma$-constacyclic codes.

(m,n)	$(1,\alpha_1,\alpha_2)$	$f(x)$	$g_1(x), g_2(x)$	$\Psi(\mathcal{V})$	$[[en,k,\geq d]]_q$
$(24,30)$	$(1,-1,-1)$	$t^{23}t^{11}1$	$1t^{3}1,\ t^{4}t^{2}1$	$[84,78,3]$	$[[84,72,3]]_{5^2}$
$(48,30)$	$(1,-1,-1)$	$t^{5}t^{21}t^{8}1$	$1t^{3}1,\ t^{4}t^{2}1$	$[108,101,3]$	$[[108,94,3]]_{5^2}$
$(24,48)$	$(1,1,1)$	$t^{3}t^{17}t^{8}1$	$t^{5}t^{7}1,\ 10t1$	$[120,112,4]$	$[[120,104,4]]_{5^2}$
$(48,8)$	$(1,-1,1)$	$t^{45}t^{30}1$	$t^{6}01,\ t^{12}1$	$[64,59,3]$	$[[64,54,3]]_{7^2}$
$(24,28)$	$(1,-1,1)$	$t^{14}11$	$t^{30}t^{34}1,\ t^{12}t^{5}1$	$[80,74,3]$	$[[80,68,3]]_{7^2}$
$(24,48)$	$(1,-1,1)$	$t^{36}t^{13}t1$	$t^{3}t1,\ t0t^{17}1$	$[120,112,4]$	$[[120,104,4]]_{7^2}$
$(40,30)$	$(1,-1,-1)$	$t^{75}t^{47}1$	$1t^{18}1,\ t1$	$[100,95,3]$	$[[100,90,3]]_{11^2}$
$(40,30)$	$(1,-1,-1)$	$t^{63}t^{21}11$	$1t^{18}1,\ t^{90}t^{33}1$	$[100,93,4]$	$[[100,86,4]]_{11^2}$

Remark: In the tables, the polynomials are represented by their coefficients in increasing powers of x. For instance, $t^{23}t^{11}1$ represents the polynomial $t^{23} + t^{11}x + x^2$, where t is the primitive element of the corresponding field $\mathbb{F}_q$.

8. Conclusions

In this article, we have investigated skew $\Theta_l - \gamma$-constacyclic codes over the ring $\mathcal{B}_e$, and obtained requirements for these codes to be LCD for some specific values of γ. Further, we have obtained requirements for a skew constacyclic code over $\mathcal{B}_e$ to satisfy the dual containing property, motivated by the CSS construction for quantum codes. We also defined a duality-preserving Gray map. This yielded several (MDS/near MDS) LCD codes and new quantum codes over finite fields. Moreover, we have also considered additive skew constacyclic codes, and obtained conditions for complementary duality and dual containing property.

Author Contributions: Supervision, O.P.; Resources, O.P.; project administration, O.P.; funding acquisition, P.S.; conceptualization, S.Y.; methodology, S.Y.; software, A.S.; validation, O.P., P.S., S.Y. and A.S.; formal analysis, S.Y. and A.S.; investigation, S.Y.; data curation, A.S.; writing—original draft preparation, S.Y.; writing—review and editing, O.P., P.S.; visualization, S.Y., A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Acknowledgments: The authors are thankful to the Indian Institute of Technology Patna for providing research facilities.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this manuscript.

References

1. H. Islam, T. Bag, O. Prakash, A class of constacyclic codes over $\mathbb{Z}_4[u]/\langle u^k \rangle$, *J. Appl. Math. Comput.*, **60** (2019), 237–251.
https://doi.org/10.1007/s12190-018-1211-y
2. M. Shi, L. Qian, L. Sok, N. Aydin, P. Solé, On constacyclic codes over $\mathbb{Z}_4[u]/(u^2-1)$ and their Gray images, *Finite Fields Appl.*, **45** (2017), 86–95.
https://doi.org/10.1016/j.ffa.2016.11.016
3. I. Aydogdu, T. Abualrub, I. Siap, On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes, *Int. J. Comput. Math.*, **92** (2015), 1806–1814.
https://doi.org/10.1080/00207160.2013.859854
4. O. Prakash, S. Yadav, H. Islam, P. Solé, On $\mathbb{Z}_4\mathbb{Z}_4[u^3]$-additive constacyclic codes, *Adv. Math. Commun.*, **17** (2023), 246–261.
https://doi.org/10.3934/amc.2022017
5. D. Boucher, W. Geiselmann, F. Ulmer, Skew cyclic codes, *Appl. Algebra Engrg. Comm. Comput.*, **18** (2007), 379–389.
https://doi.org/10.1007/s00200-007-0043-z
6. D. Boucher, F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.*, **44** (2009), 1644–1656.

 doi:10.20944/preprints202410.1716.v1

https://doi.org/10.1016/j.jsc.2007.11.008
7. O. Ore, Theory of non-commutative polynomials, *Ann. Math.*, **34** (1933), 480–508.
https://doi.org/10.2307/1968173
8. T. Abualrub, P. Seneviratne, Skew codes over rings, *Hong Kong, IMECS*, **2** (2012), 846–847
https://www.iaeng.org/publication/IMECS2010/IMECS2010_pp846-847.pdf
9. J. Gao, Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *J. Appl. Math. Inform.*, **31** (2013), 337–342.
https://doi.org/10.14317/jami.2013.337
10. F. Gursoy, I. Siap, B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Adv. Math. Commun.*, **8** (2014), 313–322.
https://doi.org/10.3934/amc.2014.8.313
11. D. Boucher, P. Solé, F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292.
https://doi.org/10.3934/amc.2008.2.273
12. J. Gao, F. Ma, F. Fu, Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$, *Appl. Comput. Math.*, **16** (2017), 286–295
https://www.researchgate.net/publication/292205358
13. J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, **106/107** (1992), 337–342.
https://doi.org/10.1016/0012-365X(92)90563-U
14. X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, *Discrete Math.*, **126** (1994), 391–393.
https://doi.org/10.1016/0012-365X(94)90283-6
15. O. Prakash, S. Patel, S. Yadav, Reversible cyclic codes over some finite rings and their application to DNA codes, *Comput. Appl. Math.*, **40** (2021), Article no. 242
https://doi.org/10.1007/s40314-021-01635-y
16. O. Prakash, S. Yadav, P. Sharma, Reversible cyclic codes over a class of chain rings and their application to DNA codes, *Int. J. Inf. Coding Theory*, **6** (2022), 52–70.
http://dx.doi.org/10.1504/IJICOT.2021.10049568
17. N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.*, **285** (2004), 345–347.
http://dx.doi.org/10.1016/j.disc.2004.05.005
18. X. Liu, H. Liu, LCD codes over finite chain rings, *Finite Fields Appl.*, **34** (2015), 1–19.
https://doi.org/10.1016/j.ffa.2015.01.004
19. C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, *Adv. Math. Commun.*, **10** (2016), 131–150.
https://doi.org/10.3934/amc.2016.10.131
20. Z. Liu, J. Wang, Linear complementary dual codes over rings, *Des. Codes Cryptogr.*, **87** (2019), 3077–3086.
https://doi.org/10.1007/s10623-019-00664-3
21. O. Prakash, S. Yadav, R. K. Verma, Constacyclic and Linear Complementary Dual codes over $\mathbb{F}_q + u\mathbb{F}_q$, *Defence Sci. J.*, **70** (2020), 626–632.
https://doi.org/10.14429/dsj.70.15691
22. O. Prakash, S. Yadav, H. Islam, P. Solé, Self-dual and LCD double circulant codes over a class of non-local rings, *Comput. Appl. Math.*, **41** (2022), Article no. 245.
https://doi.org/10.1007/s40314-022-01947-7
23. M. Shi, D. Huang, L. Sok, P. Solé, Double circulant LCD codes over $\mathbb{Z}_4$, *Finite Fields Appl.*, **58** (2019), 133–144.
https://doi.org/10.1016/j.ffa.2019.04.001
24. M. Shi, H. Zhu, L. Qian, L. Sok, P. Solé, On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$, *Cryptogr. Commun.*, **12** (2020), 53–70.
https://doi.org/10.1007/s12095-019-00363-9
25. S. Yadav, H. Islam, O. Prakash, P. Solé, 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** (2021), 689–705.
https://doi.org/10.1007/s12190-021-01499-9
26. S. Yadav, A. Singh, O. Prakash, Complementary dual skew polycyclic codes and their applications to EAQECCs, *Eur. Phys. J. Plus*, **138** (2023), Article no. 637.
https://doi.org/10.1140/epjp/s13360-023-04253-1

27. A. Alahmadi, A. Altassan, A. AlKenani, S. Çalkavur, H. Shoaib, P. Solé, A Multisecret-Sharing Scheme Based on LCD Codes, *Mathematics*, **8** (2020), Article no. 272.
https://doi.org/10.3390/math8020272
28. R. Boulanouar, A. Batoul, D. Boucher, An overview on skew constacyclic codes and their subclass of LCD codes, *Adv. Math. Commun.*, **15** (2021), 611–632.
https://doi.org/10.3934/amc.2020085
29. L. Hui, H. Peng, L. Xiu-sheng, Skew cyclic and LCD codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, *J. of Math.*, **38** (2018), 459–466
http://sxzz.whu.edu.cn/html/2018/3/20180308.htm
30. X. Hou, X. Meng, J. Gao, On $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-Additive Cyclic and Complementary Dual Codes, *IEEE Access*, **9** (2021), 65914–65924.
https://doi.org/10.1109/ACCESS.2021.3076303
31. P. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A*, **52** (1995), Article no. 2493.
https://doi.org/10.1103/PhysRevA.52.R2493
32. A. R. Calderbank, E. M. Rains, P. M. Shor, N.J.A. Sloane, Quantum error-correction via codes over $GF(4)$, *IEEE Trans. Inf. Theory*, **44** (1998), 1369–1387.
https://doi.org/10.1109/18.681315
33. A. N. Alkenani, M. Ashraf, G. Mohammad, Quantum codes from the constacyclic codes over the ring $F_q[u_1, u_2]/\langle u_1^2 - u_1, u_2^2 - u_2, u_1u_2 - u_2u_1\rangle$, *Mathematics*, **8** (2020), 781(1–11).
https://doi.org/10.3390/math8050781
34. M. Ashraf, G. Mohammad, 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** (2019), 325–335.
https://doi.org/10.1007/s12095-018-0299-0
35. M. Grassl, T. Beth, M. Roetteler, On optimal quantum codes, *Int. J. Quantum Inf.*, **2** (2004), 55–64.
https://doi.org/10.1142/S0219749904000079
36. M. Shi, X. Huang, Q. Yue, 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** (2021), 603–620.
https://doi.org/10.1007/s00200-020-00415-1
37. H. Islam, O. Prakash, New quantum codes from constacyclic and additive constacyclic codes, *Quantum Inf. Process.*, **19** (2020), Article no. 319.
https://doi.org/10.1007/s11128-020-02825-z
38. T. Bag, H. Q. Dinh, A. K. Upadhyay, R. Bandi, W. Yamaka, Quantum codes from skew constacyclic codes over the ring $F_q[u, v]/\langle u^2 - 1, v^2 - 1, uv - vu\rangle$, *Discrete Math.*, **343** (2020), Article no. 111737.
https://doi.org/10.1016/j.disc.2019.111737
39. O. Prakash, H. Islam, S. Patel, P. Solé, New quantum codes from skew constacyclic codes over a class of non-chain rings $R_{e,q}$, *Int. J. Theor. Phys.*, **60** (2021), 3334-3352.
https://doi.org/10.1007/s10773-021-04910-0
40. R. K. Verma, O. Prakash, A. Singh, Quantum codes from skew constacyclic codes over $\mathbb{F}_{p^m} + v\mathbb{F}_{p^m} + v^2\mathbb{F}_{p^m}$, *Algebraic and Combinatorial Coding Theory (ACCT)*, (2020), 156–161.
https://doi.org/10.1109/ACCT51235.2020.9383402
41. R. K. Verma, O. Prakash, A. Singh, H. Islam, New quantum codes from skew constacyclic codes, *Adv. Math. Commun.*, **17** (2023), 900–919.
https://doi.org/10.3934/amc.2021028
42. M. Goyal, M. Raka, Duadic codes over the ring $\mathbb{F}_q[u]/\langle u^m - u\rangle$ and their Gray images, *J. Comp. Comm.*, **4** (2016), 50–62.
http://dx.doi.org/10.4236/jcc.2016.412003