Defence Science Journal, Vol. 71, No. 5, September 2021, pp. 656-661, DOI : 10.14429/dsj.71.16641

New Quantum and LCD Codes over Finite Fields of Even Characteristic

Habibul Islam and Om Prakash[*]

Indian Institute of Technology, Patna - 801 106, India
[*]E-mail: om@iitp.ac.in

ABSTRACT

For an integer $m \geq 1$, we study cyclic codes of length ℓ over a commutative non-chain ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, where $u^2 = u$. With a new Gray map and Euclidean dual-containing cyclic codes, we provide many new and superior codes to the best-known quantum error-correcting codes. Also, we characterise LCD codes of length ℓ with respect to their generator polynomials and prove that $\mathbb{F}_{2^m}$–image of an LCD code of length ℓ is an LCD code of length 2ℓ. Finally, we provide several optimal LCD codes from the Gray images of LCD codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$.

Keywords: Cyclic codes; Gray map; Quantum code; LCD codes

1. INTRODUCTION

Quantum error-correcting codes have used to minimise the errors that occurred during the transmission of quantum information through a quantum channel. It has been playing an important role in quantum computing to solve a severe problem faster than a classical computer. For instance, the running time of the *Shor's Algorithm* (1994, Peter Shor), which aims to find prime factors of a reasonably large integer N, is polynomial for the case of quantum computing and sub-exponential for the case of classical computing. Quantum information is different from classical information in many winsome and unfamiliar ways. For example, the fundamental unit of classical information is bit (discrete-valued) which can take binary digit 0 or 1 while the basic unit of quantum information is qubit (continuous-valued) which can take both 0, 1 and a unit circle by the principle of superposition. Moreover, a qubit cannot be converted into a classical bit (No-Teleportation Theorem), cannot be copied (No-Cloning Theorem), cannot be deleted (No-Deleting Theorem) and cannot be transported from one to multiple places (No-Broadcast Theorem). Therefore, the storing of quantum information is more difficult than classical information. Recently, quantum computing has been received remarkable attention in research due to its possible application in the description of modern computation and cryptography. Shor[36] constructed the first binary quantum code[9,1,13]. Later, Calderbank[5], *et al.* proposed a systematic method for constructing quantum codes from classical codes. Since then, many significant quantum codes were determined from linear codes over finite fields and rings[12,16,28]. In this context, the most used linear codes are cyclic codes which efficiently help to pursue. Kai & Zhu[21] obtained quantum codes over $\mathbb{F}_4$ by using cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$. To obtain quantum codes over fields of odd characteristic, several papers on cyclic (constacyclic) codes over non-chain rings are available[1,2,10,15,17,18,19,24,25] while for even characteristic, papers[7,13,29,32,33,34] contributed some elegant quantum codes by using algebraic properties of cyclic codes over finite rings. Despite these works, a lot of quantum codes remain to determine over fields of even characteristic. To confront the possibilities, here we study cyclic codes of length ℓ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}, u^2 = u$ (a family of non-chain rings) and obtain many new and better quantum codes than existing codes. Interestingly[29], for $m = 2$, constructed many quantum codes over $\mathbb{F}_4$ but with the help of a new Gray map here, we obtained many better quantum codes than the codes appeared in[29]. Interested readers can find more works on cyclic codes in[4,20,26,30,31].

A linear code that meets trivially with its dual is known as a *linear complementary dual* code (abbreviated as LCD). Some specific benefits of LCD codes over linear codes are (i) nearest-codeword decoding problem for an LCD code is simpler than linear code, and (ii) an LCD code with possibly large minimum distance simultaneously prevents two popular attacks, namely, SCA (side-channel attack) and FIA (fault-injection attack) in a cryptosystem[6]. Note that LCD codes were introduced by Massey[27]. Later, Yang and Massey[38] provided LCD codes as cyclic codes under some restrictions on their generator polynomials. In order to extend these codes over finite rings, recently many authors[8,22,23] studied LCD codes over finite chain rings. Another side, it is still open to determine these codes over finite non-chain rings. Towards this, recently Yadav[37], *et al.* studied LCD circulant codes over a non-chain ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. However, here we consider a family of non-chain rings $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, where $u^2 = u, m \geq 1$ is an integer and study LCD codes of length ℓ. There are other non-chain rings still left to study but our paper has a novelty of

Received : 01 January 2021, Revised : 05 April 2021
Accepted : 16 April 2021, Online published : 02 September 2021

producing many optimal LCD codes. Two major contributions of the article are (i) it provides many new and superior to the best-known quantum codes over $\mathbb{F}_{2^m}$, and (ii) it determines the structure of LCD codes over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ which are capable to produce good and optimal LCD codes over $\mathbb{F}_{2^m}$ under the Gray images.

2. PRELIMINARY

Let $\mathbb{F}_{2^m}$ be a Galois field of order 2^m with characteristic 2. Throughout, we use the notation $\mathbb{S}=\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$. where $u^2=u$. Thus $\mathbb{S}$ is a commutative ring with unity and of characteristic 2. Also, $\mathbb{S}$ is a Frobenius, non-chain, semi-local ring with two maximal ideals $\langle 1-u\rangle$ and $\langle u\rangle$. Recall that for any positive integer ℓ, $\mathbb{S}^\ell=\underbrace{\mathbb{S}\times\mathbb{S}\times\cdots\times\mathbb{S}}_{\ell}$ forms an $\mathbb{S}-$module and any $\mathbb{S}-$submodule of $\mathbb{S}^\ell$ is called a *linear code* over $\mathbb{S}$ of length ℓ. Further, each vector of a linear code $\mathfrak{I}$ is known as a *codeword*. The dual of $\mathfrak{I}$ is defined as $\mathfrak{I}^\perp=\{\alpha\in\mathbb{S}^\ell:\alpha\cdot\beta=0,\forall\beta\in\mathfrak{I}\}$, where the Euclidean inner product of any two vectors $\alpha=(\alpha_0,\alpha_1,\cdots,\alpha_{\ell-1}),\beta=(\beta_0,\beta_1,\cdots,\beta_{\ell-1})$ is defined by $\alpha\cdot\beta=\sum_{i=0}^{\ell-1}\alpha_i\beta_i$. Clearly, $\mathfrak{I}^\perp$ is itself a linear code. Now, $\mathfrak{I}$ is called *self-dual* if $\mathfrak{I}=\mathfrak{I}^\perp$, and *self-orthogonal* if $\mathfrak{I}\subseteq\mathfrak{I}^\perp$. From the elementary concept of ring theory, we have $\mathbb{S}\cong\langle 1-u\rangle\mathbb{S}\oplus\langle u\rangle\mathbb{S}\cong\langle 1-u\rangle\mathbb{F}_{2^m}\oplus\langle u\rangle\mathbb{F}_{2^m}$ (see[14]). Therefore, every element $\vartheta\in\mathbb{S}$ can be expressed as $\vartheta=(1-u)\vartheta'+u\vartheta''$, where $\vartheta',\vartheta''\in\mathbb{F}_{2^m}$. In[14,29], they defined the Gray map from $\mathbb{S}\to\mathbb{F}_{2^m}^2$ as $\vartheta\mapsto(\vartheta',\vartheta'')$, where $\vartheta=(1-u)\vartheta'+u\vartheta''$. But, here we define the Gray map $\varphi:\mathbb{S}\to\mathbb{F}_{2^m}^2$ by $\varphi(\vartheta)=(\vartheta',\vartheta'')M=\overline{\vartheta}M$, where $\overline{\vartheta}=(\vartheta',\vartheta'')\in\mathbb{F}_{2^m}^2, M\in GL_2(\mathbb{F}_{2^m}), MM^T=\rho I_2$ with $\rho\in\mathbb{F}_{2^m}^*$ and $GL_2(\mathbb{F}_{2^m})$ is the set of all 2×2 invertible matrices over $\mathbb{F}_{2^m}$. Similar maps were found in[18,19,24,25], but the advantage of φ is that the $\mathbb{F}_{2^m}-$ images of codes have better parameters, for instance, in Example 5.1 (also in Table 2), our obtained quantum codes have larger distance than the code appeared in[29] with the same length and dimension. Clearly, the map φ is bijective and can be extended over $\mathbb{S}^\ell$ component-wise. Now, as in[14], we review few basic facts for a linear code $\mathfrak{I}$ of length ℓ over $\mathbb{S}$. Let $\mathfrak{I}_1=\{\vartheta'\in\mathbb{S}^\ell:(1-u)\vartheta'+u\vartheta''\in\mathfrak{I}\},\mathfrak{I}_2=\{\vartheta''\in\mathbb{S}^\ell:(1-u)\vartheta'+u\vartheta''\in\mathfrak{I}\}$. Then $\mathfrak{I}_1\,\&\,\mathfrak{I}_2$ both are linear codes over $\mathbb{F}_{2^m}$ of length ℓ. Further, $\mathfrak{I}$ has a unique representation $\mathfrak{I}=(1-u)\mathfrak{I}_1\oplus u\mathfrak{I}_2$ and its dual is $\mathfrak{I}^\perp=(1-u)\mathfrak{I}_1^\perp\oplus u\mathfrak{I}_2^\perp$. The generator matrix of $\mathfrak{I}$ is given by $G=\begin{pmatrix}(1-u)G_1\\ uG_2\end{pmatrix}$ where G_1,G_2 are generator matrices of $\mathfrak{I}_1,\mathfrak{I}_2$, respectively and $|\mathfrak{I}|=|\mathfrak{I}_1|\cdot|\mathfrak{I}_2|$. It is well-known that the *Hamming weight* of $\chi\in\mathfrak{I}$, denoted by $w_H(\chi)$, is the number of non-zero components in χ and the distance of $\mathfrak{I}$ is given by $d_H(\mathfrak{I})=\min\{w_H(\chi):0\neq\chi\in\mathfrak{I}\}$. We define the *Gray weight* for $\chi\in\mathbb{S}$ by $w_G(\chi)=w_H(\varphi(\chi))$, and for a vector $\chi=(\chi_0,\chi_1,\cdots,\chi_{\ell-1})\in\mathfrak{I}$ by $w_G(\chi)=\sum_{i=0}^{\ell-1}w_G(\chi_i)$. Again, the Gray distance d_G between $\chi',\chi''\in\mathfrak{I}$ is $d_G(\chi',\chi'')=w_G(\chi'-\chi'')$, and d_G of $\mathfrak{I}$ is $d_G(\mathfrak{I})=\min\{w_G(\chi):0\neq\chi\in\mathfrak{I}\}$. By the above discussion, it is clear that φ is a linear and isometric map from ($\mathbb{S}^\ell$, d_G) to ($\mathbb{F}_{2^m}^{2\ell}$, d_H). Consequently, for an $[\ell,k,d_G]$ linear code $\mathfrak{I}$ over $\mathbb{S}$, its Gray image $\varphi(\mathfrak{I})$ is a $[2\ell,k,d_G]$ linear code over $\mathbb{F}_{2^m}$ with $d_G=d_H$. Now, the next theorem is useful to obtain self-orthogonal codes over $\mathbb{F}_{2^m}$.

Theorem 2.1 Consider a linear code $\mathfrak{I}$ of length ℓ over $\mathbb{S}$ such that $\mathfrak{I}\subseteq\mathfrak{I}^\perp$ (i.e., self-orthogonal). Then $\varphi(\mathfrak{I})$ satisfies $\varphi(\mathfrak{I})\subseteq\varphi(\mathfrak{I})^\perp$ (i.e., self-orthogonal).

Proof: Let a linear code $\mathfrak{I}$ satisfies $\mathfrak{I}\subseteq\mathfrak{I}^\perp$ and $\alpha,\beta\in\varphi(\mathfrak{I})$. Then there exist $\chi,\mu\in\mathfrak{I}$ and $M\in GL_2(\mathbb{F}_{2^m})$ with $MM^T=\rho I_2$ such that $\alpha=\varphi(\chi)=(\overline{\chi_0}M,\overline{\chi_1}M,\cdots,\overline{\chi_{\ell-1}}M)\,\&\,\beta=\varphi(\mu)=(\overline{\mu_0}M,\overline{\mu_1}M,\cdots,\overline{\mu_{\ell-1}}M)$. In order to prove $\varphi(\mathfrak{I})$ is self-orthogonal, we show $\alpha\cdot\beta=0$. Since $\mathfrak{I}$ is self-orthogonal, $\chi\cdot\mu=\sum_{i=0}^{\ell-1}\chi_i\mu_i=0$. Therefore, $\alpha\cdot\beta=\alpha\beta^T=\sum_{i=0}^{\ell-1}\chi_iMM^T\mu_i^T=\rho\sum_{i=0}^{\ell-1}\chi_i\mu_i^T=0$. Also, $\alpha,\beta\in\mathfrak{I}$ were arbitrary, $\varphi(\mathfrak{I})\subseteq\varphi(\mathfrak{I})^\perp$. Thus, $\varphi(\mathfrak{I})$ is a self-orthogonal linear code of length 2ℓ over $\mathbb{F}_{2^m}$.

3. QUANTUM CODES

Definition 3.1 A linear code $\mathfrak{I}$ of length ℓ over $\mathbb{S}$ is said to be a cyclic code if for each codeword $(\chi_0,\chi_1,\cdots,\chi_{\ell-1})\in\mathfrak{I}$, its circular shift $(\chi_{\ell-1},\chi_0,\cdots,\chi_{\ell-2})\in\mathfrak{I}$.

Recall that a cyclic code $\mathfrak{I}$ of length ℓ over a finite commutative ring $\mathbb{S}$ is equivalent to an ideal of $\frac{\mathbb{S}[x]}{\langle x^\ell-1\rangle}$. This section aims to obtain quantum codes (Theorem 3.5) under the CSS (Calderbank-Shor-Steane) construction (Lemma 3.1), where dual-containing cyclic codes are instrumental. Toward this, we first determine a condition for cyclic codes to contain their dual codes (Theorem 3.4). Before that, we review some important results (Theorem 3.1 to Theorem 3.4) which characterise cyclic codes and their duals, see[29,35] for proofs of similar results.

Theorem 3.1[35] A linear code $\mathfrak{I}=(1-u)\mathfrak{I}_1\oplus u\mathfrak{I}_2$ of length ℓ over $\mathbb{S}$ is cyclic if and only if $\mathfrak{I}_1,\mathfrak{I}_2$ are cyclic codes over $\mathbb{F}_{2^m}$.

Theorem 3.2[35] Let $\mathfrak{I}=(1-u)\mathfrak{I}_1\oplus u\mathfrak{I}_2$ be a cyclic code of length ℓ over $\mathbb{S}$. Then $\mathfrak{I}=\langle\xi(x)\rangle$ where $\xi(x)=(1-u)\xi_1(x)+u\xi_2(x)$ and $x^\ell-1=\xi_i(x)\eta_i(x)$ in $\mathbb{F}_{2^m}[x]$ for $i=1,2$.

Theorem 3.3[35] Consider a cyclic code $\mathfrak{I}=(1-u)\mathfrak{I}_1\oplus u\mathfrak{I}_2$ of length ℓ over $\mathbb{S}$ such that $\mathfrak{I}=\langle(1-u)\xi_1(x)+u\xi_2(x)\rangle$, where $x^\ell-1=\xi_i(x)\eta_i(x)$, for $i=1,2$. Then

1. $\Im^\perp = (1-u)\Im_1{}^\perp \oplus u\Im_2{}^\perp$ is a cyclic code of length ℓ over $\mathbb{S}$.
2. $\Im^\perp = \langle (1-u)\eta_1^*(x) + u\eta_2^*(x)\rangle$, where $\eta_i^*(x)$ is reciprocal of the polynomial $\eta_i(x)$, for $i = 1,2$.
3. $\left|\Im^\perp\right| = 2^{m\{\deg(\xi_1(x))+\deg(\xi_2(x))\}}$.

Theorem 3.4[29] Let $\Im = (1-u)\Im_1 \oplus u\Im_2$ be a cyclic code of length ℓ over $\mathbb{S}$ and $\Im = \langle (1-u)\xi_1(x) + u\xi_2(x)\rangle$. Then $\Im^\perp \subseteq \Im$ if and only if $x^\ell - 1 \equiv 0 (\mathrm{mod}\, \xi_i(x)\xi_i^*(x))$, where $\xi_i^*(x)$ is reciprocal of $\xi_i(x)$ for $i = 1,2$.

Definition 3.2 Let p be a prime and $q = p^m$, for a positive integer m. Let $\mathbb{C}^q$ be a $q-$dimensional Hilbert space over the complex field $\mathbb{C}$ Then the set of $\ell-$folded tensor product $(\mathbb{C}^q)^{\otimes \ell} = \underbrace{\mathbb{C}^q \otimes \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{\ell}$ is also a $q^\ell-$dimensional Hilbert space. Moreover, a quantum code represented by $[[\ell,k,d]]_q$ is defined as a subspace of $(\mathbb{C}^q)^{\otimes \ell}$ with dimension q^k and minimum distance d. Again, we call $[[\ell,k,d]]_q$ is superior to $[[\ell',k',d']]_q$ if any one or both of the following holds:

1. $d > d'$ whenever the code rate $\frac{k}{\ell} = \frac{k'}{\ell'}$ (Larger distance).
2. $\frac{k}{\ell} > \frac{k'}{\ell'}$ whenever the distance $d = d'$ (Larger code rate).

Lemma 3.1 (CSS construction)[12] If $\Im$ is an $[\ell,k,d]_q$ linear code with $\Im^\perp \subseteq \Im$ over $\mathbb{F}_q$, then a $q-$ary quantum code with parameters $[[\ell, 2k-\ell, d]]_q$ exists.

Now, by using Lemma 3.1 we construct quantum codes as below.

Theorem 3.5 Let $\Im = (1-u)\Im_1 \oplus u\Im_2$ be a cyclic code over $\mathbb{S}$ of length ℓ and $\varphi(\Im)$ has the parameters $[2\ell, k, d_H]$. If $\Im^\perp \subseteq \Im$, then a 2^m-ary quantum code with parameters $[[2\ell, 2k-2\ell, d_H]]_{2^m}$ exists.

Proof: We have $\Im^\perp \subseteq \Im$, which implies that $\varphi(\Im)^\perp \subseteq \varphi(\Im)$. Again we have $\varphi(\Im^\perp) = \varphi(\Im)^\perp$. Hence, $\varphi(\Im)$ is a 2^m-ary $[2\ell, k, d_H]$ linear code containing its dual code. Finally, by using Lemma 3.1, we construct a 2^m-ary quantum code $[[2\ell, 2k-2\ell, d_H]]_{2^m}$.

4. LCD CODES

Definition 4.1[27] A linear code $\Im$ of length ℓ over $\mathbb{S}$ is called a linear complementary dual (LCD) code if $\Im \cap \Im^\perp = \{0\}$.

The goal of this section is to characterise LCD cyclic code of even length (Theorem 4.2) and odd length (Theorem 4.4) with respect to their generator polynomials, respectively. In this regard, first we recall the structure of LCD codes over finite fields $\mathbb{F}_q$ given by Lemma 4.1 and Lemma 4.2.

Lemma 4.1[38] Let $\Im = \langle \xi(x)\rangle$ be a cyclic code of length ℓ over $\mathbb{F}_{p^m}$, where $\ell = p^t s$ and $\gcd(p,s) = 1$. Then $\Im$ is LCD if and only if $\xi(x) = \xi^*(x)$ and each monic irreducible factor of $\xi(x)$ has the same multiplicity in $x^\ell - 1$ and in $\xi(x)$.

Lemma 4.2[38] Consider a cyclic code $\Im$ of length ℓ over $\mathbb{F}_{p^m}$ where $\gcd(\ell, p) = 1$. Then $\Im$ is LCD if and only if $\Im$ is a reversible cyclic code.

Theorem 4.1 Let $\Im = (1-u)\Im_1 \oplus u\Im_2$ be a cyclic code of length ℓ over $\mathbb{S}$. Then $\Im$ is an LCD code if and only if $\Im_1, \Im_2$ are LCD codes over $\mathbb{F}_{2^m}$.

Proof: The result follows from the fact that $\Im \cap \Im^\perp = \{0\} \Leftrightarrow \Im_i \cap \Im_i{}^\perp = \{0\}$, for $i = 1,2..$

Theorem 4.2 Let $\Im = (1-u)\Im_1 \oplus u\Im_2$ be a cyclic code of even length ℓ over $\mathbb{S}$ such that $\Im_i = \langle \xi_i(x)\rangle$, for $i = 1,2$. Then $\Im$ is LCD if and only if $\xi_i(x) = \xi^*{}_i(x)$ and each monic irreducible factor of $\xi_i(x)$ has the same multiplicity in $x^\ell - 1$ and in $\xi_i(x)$ for $i = 1,2$.

Proof: Follows from Lemma 4.1 and Theorem 4.1.

Theorem 4.3 Let $\Im = (1-u)\Im_1 \oplus u\Im_2$ be a cyclic code of odd length ℓ over $\mathbb{S}$. Then $\Im$ is LCD if and only if $\Im_1, \Im_2$ are reversible cyclic codes.

Proof: Let $\Im$ be an LCD cyclic code of odd length ℓ over $\mathbb{S}$. Then by Theorem 4.1, $\Im_1, \Im_2$ are LCD codes of length ℓ over $\mathbb{F}_{2^m}$. Hence, by Lemma 4.2, $\Im_1$ and $\Im_2$ are reversible cyclic codes.

Conversely, let $\Im_1, \Im_2$ be reversible cyclic codes of odd length ℓ over $\mathbb{F}_{2^m}$. Then by Lemma 4.2, we have $\Im_1, \Im_2$ are LCD cyclic codes, and hence by Theorem 4.1, $\Im$ is LCD over $\mathbb{S}$.

Theorem 4.4 Let $\Im = (1-u)\Im_1 \oplus u\Im_2$ be a cyclic code of odd length ℓ over $\mathbb{S}$, where $\Im_i = \langle \xi_i(x)\rangle$, for $i = 1,2$. Then $\Im$ is LCD if and only if $\xi_i(x) = \xi_i^*(x)$ (i.e., $\xi_i(x)$ is self-reciprocal) for $i = 1,2$.

Proof: Note that a cyclic code $\Im = \langle \xi(x)\rangle$ of length ℓ over $\mathbb{F}_{2^m}$ is reversible if and only if $\xi(x) = \xi^*(x)$ (i.e., $\xi(x)$ is self-reciprocal). The rest part of the proof is easily verified by using Theorem 4.3.

Lemma 4.3 For a linear code $\Im$ of length ℓ over $\mathbb{S}$, $\varphi(\Im \cap \Im^\perp) = \varphi(\Im) \cap \varphi(\Im^\perp)$.

Proof: Let $\alpha \in \varphi(\Im \cap \Im^\perp)$. Then there exists $\beta \in \Im \cap \Im^\perp$ such that $\varphi(\beta) = \alpha$. Also, $\beta \in \Im \cap \Im^\perp$ implies that $\alpha = \varphi(\beta) \in \varphi(\Im) \cap \varphi(\Im^\perp)$. Therefore, $\varphi(\Im \cap \Im^\perp) \subseteq \varphi(\Im) \cap \varphi(\Im^\perp)$. On the other hand, let $\alpha \in \varphi(\Im) \cap \varphi(\Im^\perp)$. Then there exist $\beta \in \Im, \gamma \in \Im^\perp$ such that $\varphi(\beta) = \alpha, \varphi(\gamma) = \alpha$. Since φ is injective, $\beta = \gamma$. Therefore, $\beta \in \Im \cap \Im^\perp$, and $\alpha = \varphi(\beta) \in \varphi(\Im \cap \Im^\perp)$. Hence, $\varphi(\Im) \cap \varphi(\Im^\perp) \subseteq \varphi(\Im \cap \Im^\perp)$. Thus, $\varphi(\Im \cap \Im^\perp) = \varphi(\Im) \cap \varphi(\Im^\perp)$. Again, we know that $\varphi(\Im^\perp) = \varphi(\Im)^\perp$. Hence, the desired result.

Theorem 4.5 A linear code $\Im$ of length ℓ over $\mathbb{S}$ is LCD if and only if $\varphi(\Im)$ is an LCD code of length 2ℓ over $\mathbb{F}_{2^m}$.

Proof: Let $\mathfrak{I}$ be an LCD code of length ℓ over $\mathbb{S}$. Then $\mathfrak{I} \cap \mathfrak{I}^{\perp} = \{0\}$, i.e., $\varphi(\mathfrak{I} \cap \mathfrak{I}^{\perp}) = \{0\}$. Now, by Lemma 4.3, $\varphi(\mathfrak{I} \cap \mathfrak{I}^{\perp}) = \varphi(\mathfrak{I}) \cap \varphi(\mathfrak{I})^{\perp} = \{0\}$. Hence, $\varphi(\mathfrak{I})$ is an LCD code of length 2ℓ over $\mathbb{F}_{2^m}$.

Conversely, let $\varphi(\mathfrak{I})$ be an LCD code of length 2ℓ over $\mathbb{F}_{2^m}$. Then $\varphi(\mathfrak{I}) \cap \varphi(\mathfrak{I})^{\perp} = \{0\}$. By Lemma 4.3, we have $\varphi(\mathfrak{I} \cap \mathfrak{I}^{\perp}) = \varphi(\mathfrak{I}) \cap \varphi(\mathfrak{I})^{\perp} = \{0\}$. Since, the map φ is injective, $\mathfrak{I} \cap \mathfrak{I}^{\perp} = \{0\}$. Hence, $\mathfrak{I}$ is an LCD code of length ℓ over $\mathbb{S}$.

5. EXAMPLES

There are a few online databases[9,11] for quantum codes over fields of size upto 9. Even these have been updated regularly, still a lot of gaps are there to fill. Therefore, to compare our obtained quantum codes, we use these databases as well as few published papers[13,29,34] (for small and larger fields). Here, we obtain many optimal as per[11], and superior to the best-known quantum codes. On the other side, as the Gray images of LCD codes over $\mathbb{S}$, we also find many optimal and near-optimal (good) LCD codes according to the database[11]. We used the Magma computation system[3] to find out these examples.

Example 5.1 Let $\mathbb{S} = \mathbb{F}_4 + u\mathbb{F}_4, u^2 = u$ and $\ell = 11$. Then $x^{11} - 1 = (x+1)(x^5 + wx^4 + x^3 + x^2 + w^2x + 1)(x^5 + w^2x^4 + x^3 + x^2 + wx + 1) \in \mathbb{F}_4[x]$, where $w^2 + w + 1 = 0.$ Let $\xi_1(x) = x^5 + wx^4 + x^3 + x^2 + w^2x + 1, \xi_2(x) = x^5 + w^2x^4 + x^3 + x^2 + wx + 1$ and $M = \begin{bmatrix} w & 1 \\ 1 & w \end{bmatrix} \in GL_2(\mathbb{F}_4), satisfying\, MM^T = w^2 I_2$. Hence, $\mathfrak{I} = \langle (1-u)\xi_1(x) + u\xi_2(x) \rangle$ is a cyclic code of length 11 over $\mathbb{S}$ and $\varphi(\mathfrak{I})$ has the parameters $[22, 12, 6]$. Since $x^{11} - 1 \equiv 0 \ (\mathrm{mod}\, \xi_i(x)\xi_i^*(x))$, for $i = 1, 2$, we have $\mathfrak{I}^{\perp} \subseteq \mathfrak{I}$ (by Theorem 3.4). Finally, by Theorem 3.5, we have the associated quantum code $[[22, 2, 6]]_4$, which has the same code rate but larger minimum distance than the existing code $[[22, 2, 5]]_4$ given by[29].

In Table 2, we provide cyclic code $\mathfrak{I} = \langle (1-u)\xi_1(x) + u\xi_2(x) \rangle$ of length ℓ, where $\xi_1(x), \xi_2(x)$ are factors of $x^{\ell} - 1$ in $\mathbb{F}_{2^m}[x]$ such that $x^{\ell} - 1 \equiv 0 \ (\mathrm{mod}\, \xi_i(x)\xi_i^*(x))$, for $i = 1, 2$. Also, we compute their Gray images $\varphi(\mathfrak{I})$ by using the matrix $M = \begin{bmatrix} w & 1 \\ 1 & w \end{bmatrix} \in GL_2(\mathbb{F}_{2^m})$ satisfying $MM^T = (w+1)I_2$. By comparing them, we conclude that our obtained quantum codes $[[\ell, k, d]]_{2^m}$ (in 6th column) are better than the existing quantum codes $[[\ell', k', d']]_{2^m}$ (in 7th column) in respect of larger code rates or larger minimum distances.

Following Theorem 4.4, we present LCD code $\mathfrak{I}$ of length ℓ, whose generator polynomials $\xi_1(x), \xi_2(x)$ are enlisted in Table 1. The Gray images $\varphi(\mathfrak{I})$ are given in 5th column, which presents several optimal and near-optimal linear codes as per the database[11]. Note that we call a linear code $[\ell, k, d]_{2^m}$ is *near-optimal* (or, *near to optimal*) $[\ell, k, d']_{2^m}$ (given by[11]) if $d' - d \leq 2$. The codes in 5th column of Table 1 marked by symbol $*$ are optimal and marked by symbol # are near-optimal.

Table 1. Optimal LCD codes as Gray images of LCD codes

m	ℓ	$\xi_1(x)$	$\xi_2(x)$	$\varphi(\mathfrak{I})$	d in[11]
2	3	111	11	$[6,3,3]_4^{\#}$	$d = 4$
2	5	11	$1w1$	$[10,7,3]_4^{*}$	$d = 3$
2	5	11	$1w^2w^21$	$[10,6,4]_4^{*}$	$d = 4$
2	7	11	1111111	$[14,7,4]_4^{\#}$	$d = 6$
2	13	11	$1w0w^20w1$	$[26,19,4]_4^{\#}$	$d = 6$
2	17	$11w11$	$1w^211w11w^21$	$[34,22,7]_4^{\#}$	$d = 9$
2	17	11	$11w11$	$[34,29,4]_4^{*}$	$d = 4$
3	5	11	11111	$[10,5,4]_8^{\#}$	$d = 5$
3	7	11	$1w^51$	$[14,11,3]_8^{*}$	$d = 3$
3	7	$1w^2w^21$	11	$[14,10,4]_8^{*}$	$d = 4$
3	9	11	$1w^41$	$[18,15,3]_8^{*}$	$d = 3$
3	9	$1w^5w^51$	11	$[18,14,4]_8^{*}$	$d = 4$
3	13	11	$1w^3w^5w^31$	$[26,21,4]_8^{\#}$	$d = 5$
3	19	$1w^3w^6w^6w^6w^31$	$1w^5w^3w^3w^3w^51$	$[38,28,7]_8^{\#}$	$d = 8$

In order to concise Tables 1 and 2, we represent the polynomial $\xi_i(x)$ by a string consisting of their coefficients in decreasing order of the degree of x. For instance, we use $1w0w^2w$ to represents the polynomial $x^4 + wx^3 + w^2x + w.$

6. CONCLUSION

We obtained 7 optimal as well as 7 near-optimal (good) LCD codes in Table 1 as per the database[11] while in Table 2, we obtained many non-binary quantum codes better than the existing (in references[9,13,29,34]) non-binary quantum codes. Therefore, our presented non-binary quantum codes have outperforming parameters than the available parameters of the best-known non-binary quantum codes. Further, to obtain codes over finite fields of odd characteristic, in the future this work can be extended over the ring $\mathbb{F}_q + u\mathbb{F}_q$, where $u^2 = u, q = p^m$ and p is a prime.

REFERENCES

1. Alahmadi, A.; Islam, H.; Prakash, O.; Sole, P.; Alkenani, A.; Muthana, N. & Hijazi, R. New quantum codes from constacyclic codes over a non-chain ring. *Quantum Inf. Process.*, 2021, **20** (2), 1-17. doi: 10.1007/s11128-020-02977-y.
2. Ashraf, M. & Mohammad, G. Quantum codes from cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$. *Int. J. Quantum Inf.,* 2014, **12**(6), 1450042 doi:10.1142/S0219749914500427. doi: 10.1142/S0219749914500427.
3. Bosma, W. & Cannon, J. Handbook of Magma Functions*,* Univ. of Sydney, 1995.
4. Bonnecaze, A. & Udaya, P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory,* 1999, **45**, 1250–1255. doi: 10.1109/18.761278.
5. Calderbank, A. R.; Rains, E. M.; Shor, P. M. & Sloane,

Table 2. New quantum codes from dual-containing cyclic codes

m	ℓ	$\xi_1(x)$	$\xi_2(x)$	$\varphi(\Im)$	$[[\ell,k,d]]_{2^m}$	$[[\ell',k',d']]_{2^m}$
2	7	1011	1101	$[14,8,5]$	$[[14,2,5]]_4$	$[[14,0,3]]_4$[9]
2	6	$1w^2w$	$10w$	$[12,8,4]$	$[[12,4,4]]_4$	$[[12,4,3]]_4$[34]
2	9	$1w$	$1w0ww^2$	$[18,13,3]$	$[[18,8,3]]_4$	$[[24,8,3]]_4$[29]
2	11	$1w11w^21$	$1w^211w1$	$[22,12,6]$	$[[22,2,6]]_4$	$[[22,2,5]]_4$[29]
2	12	$11ww^21ww$	$1ww^2$	$[24,16,4]$	$[[24,8,5]]_4$	$[[24,8,3]]_4$[29]
2	18	$11w^2w^2$	$1w^201w^201w^2$	$[36,26,4]$	$[[36,16,4]]_4$	$[[36,16,3]]_4$[29]
2	21	$1w^2w01w^2w1w^2w^2w$	$1ww^21w^2$	$[42,28,6]$	$[[42,14,6]]_4$	$[[42,14,5]]_4$[29]
2	23	101011100011	110001110101	$[46,24,12]$	$[[46,2,12]]_4$	$[[46,2,7]]_4$[29]
2	18	$10ww0w^2$	$1w^2ww^2w1$	$[36,26,4]$	$[[36,16,4]]_4$	$[[56,16,4]]_4$[29]
3	12	11	11	$[24,22,2]$	$[[24,20,2]]_8$	$[[21,15,2]]_8$[13]
3	7	$1w^6ww^6$	$1w^3w^4w^3$	$[14,8,5]$	$[[14,2,5]]_8$	$[[37,1,5]]_8$[9]
3	14	$1w^3w^4w^5w^2ww^6$	$1111w^4w^4$	$[28,17,6]$	$[[28,6,6]]_8$	$[[38,0,6]]_8$[9]
4	14	1000101	10111	$[28,18,4]$	$[[28,8,4]]_{16}$	$[[28,4,3]]_{16}$[13]
4	14	1000101	1010001	$[28,16,5]$	$[[28,4,5]]_{16}$	$[[28,4,3]]_{16}$[13]
4	18	$1w^{10}w^5000w^51w^{10}$	$10w^5000w^{10}01$	$[36,20,5]$	$[[36,4,5]]_{16}$	$[[36,4,3]]_{16}$[13]
4	22	$10w^{10}01010w^501$	$10w^501010w^{10}01$	$[44,24,7]$	$[[44,4,7]]_{16}$	$[[44,4,5]]_{16}$[13]
5	15	10011	11001	$[30,22,3]$	$[[30,14,3]]_{32}$	$[[35,5,3]]_{32}$[13]

N. J. A. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory,* 1998, **44**(4), 1369-1387. doi 10.1109/18.681315.

6. Carlet, C. & Guilley, S. Complementary dual codes for counter-measures to side-channel attacks. *Adv. Math. Commun.*, 2016, **10**(1), 131-150. doi: 10.3934/amc.2016.10.131.
7. Dertli, A.; Cengellenmis, Y. & Eren, S. On quantum codes obtained from cyclic codes over A_2, *Int. J. Quantum Inf.*, 2015, **13**(3), 1550031. doi: 10.1142/S0219749915500318.
8. Durgun, Y. On LCD codes over finite chain rings. *Bull. Korean Math. Soc.,* 2020, **57**(1), 37-50. doi: 10.4134/BKMS.b181173.
9. Edel, Y. *Some good quantum twisted codes.* available at https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/\\QTBCHIndex.html (accessed on 09/04/2021).
10. Gao, Y.; Gao, Y. & Fu, F. W. On Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q \cdots + v_r\mathbb{F}_q$. *Appl. Algebra Engrg. Comm. Comput*., 2019, **30**(2), 161-174. doi: 10.1007/s00200-018-0366-y.
11. Grassl, M. Code Tables: Bounds on the parameters of various types of codes. http://www.codetables.de/ (Accessed on 09/04/2021).
12. Grassl, M. & Beth, T. On optimal quantum codes. *Int. J. Quantum Inf.,* 2004, **2**(1), 55-64. doi: 10.1142/S0219749904000079.
13. Grassl, M. & Beth, T. Quantum BCH codes. Proc. X. Int. Symp. Theoretic. Elec. Eng. Magdeburg, Germany, 1999, 207-212. arXiv:quant-ph/9910060.
14. Gursoy, F.; Siap, I. & Yildiz, B. Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. *Adv. Math. Commun.,* 2014, **8**, 313–322. doi: 10.3934/amc.2014.8.313.
15. Islam, H. & Prakash, O. Quantum codes from the cyclic codes over $\mathbb{F}_p[u,v,w] \Big/ \left\langle u^2-1, v^2-1, w^2-1, uv-vu, vw-wv, wu-uw \right\rangle$. *J. Appl. Math. Comput,.* 2019, **60**(1-2), 625-635. doi: 10.1007/s12190-018-01230-1.
16. Islam, H.; Prakash, O. & Bhunia, D. K. Quantum codes obtained from constacyclic codes. *Internat. J. Theoret. Phys.,* 2019, **58**(11), 3945-3951. doi: 10.1007/s10773-019-04260-y.
17. Islam, H.; Prakash, O. Verma & R. K. Quantum codes from the cyclic codes over $\mathbb{F}_p[v,w] \Big/ \left\langle v^2-1, w^2-1, vw-wv \right\rangle$. Springer Proceedings in Mathematics & Statistics, 2019, **307**, doi: 10.1007/978-981-15-1157-8-6.
18. Islam, H.; Prakash, O. Verma & R. K. New quantum codes from constacyclic codes over the ring $R_{k,m}$. *Adv. Math. Commun.,* 2020. doi: 10.3934/amc.2020097.
19. Islam, H. & Prakash, O. New quantum codes from

constacyclic and additive constacyclic codes. *Quantum Inf. Process.*, 2020, **19**(9), 1-17.
doi: 10.1007/s11128-020-02825-z.

20. Islam, H. & Prakash, O. Construction of reversible cyclic codes over $\mathbb{Z}_{p^k}$. *J. Discrete Math. Sci. Cryptogr.*, 2021, doi: 10.1080/09720529.2020.1815341.
21. Kai, X. & Zhu, S. Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. *Int. J. Quantum Inf.,* 2011, **9**(2), 689-700.
doi: 10.1142/S0219749911007757.
22. Liu, X. & Liu, H. LCD codes over finite chain rings. *Finite Fields Appl.*, 2015, **34**, 1–19.
doi: 10.1016/j.ffa.2015.01.004.
23. Liu, X. & Liu, H. $\sigma -$LCD codes over finite chain rings. *Des. Codes Cryptogr.*, 2019,
doi: 10.1007/s10623-019-00706-w.
24. Ma, F.; Gao, J. & Fu, F. W. New non-binary quantum codes from constacyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-1, v^2-v, uv-vu\rangle$. *Adv. Math. Commun.,* 2019, **13**(2), 421-434.
doi: 10.3934/amc.2019027.
25. Ma, F.; Gao, J. & Fu, F. W. Constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and their applications of constructing new non-binary quantum codes. *Quantum Inf. Process.*, 2018, **17**(6), Art. 122, 19 pp.
doi: 10.1007/s11128-018-1898-6.
26. Pruthi, M. & Kumar, S. Cyclic codes with generalized cyclotomic cubic classes. *J. Discrete Math. Sci. Cryptogr.*, 2019, **22**(6), 923-933, DOI: 10.1080/09720529.2019.1627706.
27. Massey, J. L. Linear codes with complementary duals. *Discrete Math.,* 1992, **106/107**, 337-342.
doi: 10.1016/0012-365X(92)90563-U.
28. Ozen, M.; Ozzaim, T. & Ince, H. Skew quasi cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. *J. Algebra Appl.,* 2019, **18**(4), 1950077, 16.
doi: 10.1142/S0219498819500774.
29. Ozen, M.; Cem, E. F. & Ince, H. Quantum codes from cyclic codes over $\mathbb{F}_4 + v\mathbb{F}_4$. *J. Appl. Math. Inform.,* 2016, **34**(5-6), 397-404.
doi: 10.14317/jami.2016.397.
30. Pankaj & Pruthi, M. Cyclic codes from Whiteman's generalized cyclotomic sequences of order 2r, r ≥ 2. *J. Inf. Optim. Sci.*, 2017, **38**(3-4), 621-646,
doi: 10.1080/02522667.2017.1303948.
31. Pankaj & Pruthi, M. Cyclic codes of prime power length from generalized cyclotomic classes of order 2r. *J. Inf. Optim. Sci.*, 2018, **39**(4), 965-971,
doi: 10.1080/02522667.2018.1460136.
32. Qian, J.; Ma, W. & Gou, Quantum codes from cyclic codes over finite ring. *Int. J. Quantum Inf.,* 2009, **7**(6),1277-1283.
doi: 10.1142/S0219749909005560.
33. Qian, J. Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *J. Inform. Comput. Sci.,* 2013, **10**, 1715–1722.
doi: 10.12733/jics20101705.
34. Sharma, A.; Bandi, R. & Bhaintwal, M. On quantum codes via cyclic codes of arbitrary length over $\mathbb{F}_4 + u\mathbb{F}_4$. *Discrete Math. Algorithms Appl.,* 2018, **10**(3), 1850033.
doi: 10.1142/S1793830918500337.
35. Zhu, S.; Wang, Y. & Shi, M. Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *IEEE Trans. Inf. Theory,* 2010, **56**(4), 2120-2128.
doi: 10.1109/TIT.2010.2040896.
36. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A,* 1995, **52**(4), 2493-2496.
doi: 10.1103/physreva.52.r2493.
37. Yadav, S.; Islam, H.; Prakash, O. & Sole, 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.*, 2021,
doi: 10.1007/s12190-021-01499-9.
38. Yang & X. Massey, J. L. The condition for a cyclic code to have a complementary dual. *Discrete Math.*, 1994, **126**, 391-393.
doi: 10.1016/0012-365X(94)90283-6.

ACKNOWLEDGEMENT

The authors are thankful to the University Grants Commission (UGC), Govt. of India for financial support and the Indian Institute of Technology Patna for research facilities. Also, authors would like to thank the anonymous referee(s) and the Editor for their valuable comments to improve the presentation of the manuscript.

CONTRIBUTORS

Mr Habibul Islam received his M. Sc. in pure mathematics degree from University of Calcutta in 2016. He is currently pursuing Ph.D. from Department of Mathematics, Indian Institute of Technology Patna. His research interest includes Algebraic Coding Theory, particularly, codes over finite rings, quantum error-correcting codes. Till now, he has published 19 research articles related to his area of interest in reputed international journals.

In the current investigation, he has developed the results of the manuscript and calculated parameters of LCD and quantum codes, and finally prepared the manuscript.

Dr Om Prakash is an Associate Professor at Department of Mathematics, Indian Institute of Technology Patna. He completed his PhD from Banasthali University, Rajasthan in 2010. He has twenty one years of teaching and research experience in reputed institutions. His main research interest includes Rings and Modules, Algebraic Coding Theory, Algebraic Graph Theory, and Algebraic Number Theory. He has the credit of publishing more than 51 research articles in the refereed international journals of repute.

In the current investigation, he has provided the guidance to develop the results on quantum and LCD codes and reviewed the final manuscript.