Quantum codes via binary codes over symbol-pair metric

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY 4.0

SUBMISSION DATE / POSTED DATE

01-09-2021 / 03-02-2022

CITATION

Jha, Vatsal Pramod; Parampalli, Udaya; Singh, Abhay Kumar (2021): Quantum codes via binary codes over symbol-pair metric. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.16552878.v2>

DOI

[10.36227/techrxiv.16552878.v2](https://doi.org/10.36227/techrxiv.16552878.v2)

Quantum codes via binary codes over symbol-pair metric

Vatsal Pramod Jha, Udaya Parampalli, Abhay Kumar Singh

Abstract

Stabilizer codes, introduced in [3], [4], have been a prominent example of quantum codes constructed via classical codes. The paper [4], introduces the stabilizer formalism for obtaining additive quantum codes of length n from Hermitian self-orthogonal codes of length n over $\text{GF}(4)$. In the present work, we present a few stabilizer code constructions considering binary codes over the symbol-pair metric (see [10]). Specifically, the present work constructs additive quantum codes of length n from certain binary codes of length n considered over the symbol-pair metric. We also present the Modified CSS Construction which is used to obtain quantum codes with parameters $[[15, 4, 3 \leq d \leq 7]]$, $[[31, 10, 5 \leq d \leq 9]]$, $[[62, 20, 5 \leq d]]$, $[[63, 18, 7 \leq d]]$.

Index Terms

Stabilizer Codes, Hermitian Self-orthogonal codes, Symplectic inner product, Cyclic LCD codes.

I. INTRODUCTION

Additive codes, also known as Stabilizer codes, serve as a prominent example of using classical codes for constructing quantum codes (see [3], [4]). The stabilizer formalism introduced in [4] characterizes additive quantum codes of length n via binary self-orthogonal codes of length $2n$ considered with respect to the symplectic inner product and symplectic weight. The paper [4] also presents the method of obtaining a subclass of additive codes of length n from Hermitian self-orthogonal codes of length n over $\text{GF}(4)$, which is a widely used approach (see [5], [8]). Now it would be interesting to consider the problem of obtaining additive quantum codes of length n via binary codes of length n itself due to the simplicity of $\mathbb{F}_2$ over $\text{GF}(4)$. We address the aforementioned problem in our present work by considering codes over the symbol-pair metric, which provides a natural way of embedding a code of length n into the space $(\mathbb{F}_2^n)^2$. A similar discussion has been done in [2] though without any reference to codes over symbol-pair metric and its various properties thereof.

As already mentioned above, in this paper binary codes of length n considered with respect to the symbol-pair metric (see [10]) have been used to construct certain additive quantum codes of length n . Interestingly, the definition of symbol-pair metric provides a natural way to convert a length n binary vector $x := (x_0, x_1, \dots, x_{n-1})$ into a length $2n$ binary vector $\pi(x) := ((x_0, x_1), (x_1, x_2), \dots, (x_{n-1}, x_0))$. An important aspect of considering symbol-pair metric, where symbol-pair weight of x is defined as $\text{wt}_{\text{sp}}(x) := |\{0 \leq i \leq n-1 : (x_i, x_{i+1}) \neq (0, 0)\}|$, comes from the key observation that it satisfies the inequality $\text{wt}_{\text{H}}(x) + 1 \leq \text{wt}_{\text{sp}}(x) \leq 2\text{wt}_{\text{H}}(x)$ and hence creates a possibility of obtaining quantum codes with larger distances.

The main motivation for considering the symbol-pair metric is the observation $\text{wt}_{\text{symp}}(c|L(c)) = \text{wt}_{\text{sp}}(c)$, where wt_{symp} refers to the symplectic weight of a binary vector of length $2n$ formed with concatenation operator $|$ (see [4]) and L refers to the left-shift operator acting on $\mathbb{F}_2^n$ i.e. $L(c_0, c_1, \dots, c_{n-1}) := (c_1, c_2, \dots, c_0)$.

In the current paper, we present a method for constructing additive quantum codes by identifying certain subspaces of a given binary code and by relating them to Euclidean dual of the considered code (see Theorem 10 for details). As a direct consequence of our method, we have obtained a modified version of CSS Construction which allows us to construct CSS codes (a particular class of additive quantum codes) from certain binary cyclic linear complementary dual (LCD) codes given in [15] (see Table I). It turns out that the quantum codes obtained by the Modified CSS Construction have better error-correcting capabilities than the CSS Construction introduced in [1]. In particular we have obtained additive quantum codes with parameters $[[15, 4, 3 \leq d \leq 7]]$, $[[31, 10, 5 \leq d \leq 9]]$, $[[62, 20, 5 \leq d]]$, $[[63, 18, 7 \leq d]]$.

The paper starts by introducing the preliminaries on symbol-pair metric, quantum error-correcting codes and Stabilizer Formalism in Section II. Section III introduces the Symbol-Pair Additive Code Construction and applies it to obtain additive codes by considering certain binary cyclic LCD codes. At the end of section III, we consider the quantum codes obtained from cyclic LCD codes as codes obtained from a modified Calderbank-Shor-Steane Construction. We conclude the paper in Section IV by providing some open problems.

II. PRELIMINARIES

This section reviews the standard coding theory terms like Hamming distance, linear codes, cyclic codes, etc., that have been used in the current paper.

By a q -ary code C of length n over a q -ary alphabet Σ we mean a subset C of Σ^n . For our purposes we consider the binary alphabet $\mathbb{F}_2 := \{0, 1\}$, equipped with the operations of addition and multiplication modulo 2.

By a binary linear code of length n we refer to a linear subspace C of $\mathbb{F}_2^n$.

The linear space $\mathbb{F}_2^n$ is generally associated with a bilinear map, known as the Euclidean inner product, which is defined as follows:

$$a.b := \sum_{i=0}^{n-1} a_i b_i,$$

where $a = (a_0, a_1, \dots, a_{n-1})$, $b = (b_0, b_1, \dots, b_{n-1}) \in \mathbb{F}_2^n$. Every code C can be associated to a unique code, known as the Euclidean dual of C . The Euclidean dual of a code C , denoted by $C^{\perp_{\text{Euc}}}$, is defined as follows:

$$C^{\perp_{\text{Euc}}} : \{c' \in \mathbb{F}_2^n : c.c' = 0, \forall c \in C\}.$$

To quantify the error-correcting capability of a code C we have the Hamming metric $d_H : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \{0, 1, \dots, n\}$, which is defined as follows:

$$d_H(a, b) := |\{0 \leq i \leq n-1 : a_i \neq b_i\}|.$$

⁰ IIT(ISM) Dhanbad, e-mail: vatsalvats@gmail.com,
 . (Corresponding author: Udaya Parampalli) The University of Melbourne, email: udaya@unimelb.edu.au,
 . IIT(ISM) Dhanbad, e-mail: abhay@iitism.ac.in,

For the binary space the quantity $d_H(a, 0)$ is referred to as the Hamming weight of a i.e. :

$$\text{wt}_H(a) := d_H(a, 0) = |\{0 \leq i \leq n-1 : a_i \neq 0\}|.$$

A code C can be associated with a quantity known as the Hamming distance of C , defined as:

$$d_H(C) := \min\{d_H(x, y) : x, y \in C, x, y \neq 0\}.$$

If C happens to be a linear code then the its Hamming distance has a simpler characterization given by:

$$d_H(C) := \min\{\text{wt}_H(c) : c \in C, c \neq 0\}.$$

The Hamming distance is indeed a measure of the error-correcting capability of a code and is evident from the following theorem:

Theorem 1. (cf. [6]) *A binary code C with Hamming distance equal to d can correct $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$ errors on any of the codewords of C , where $\lfloor \cdot \rfloor$ refers to the greatest integer function.*

We now review the theory of symbol-pair metric, introduced in [10].

A. Symbol-Pair Metric

The concept of symbol-pair metric was introduced in [10] to address the high-density data storage systems having differences in resolution in writing and reading of symbols on the channel. This difference in resolution causes the low resolution reader to read the pair adjacent (potentially corrupted) symbols in every read, referred to as symbol-pair, rather than a single symbol. Considering the binary alphabet, $\mathbb{F}_2$, the decoder for the symbol-pair setup is a map $D : (\mathbb{F}_2^2)^n \rightarrow \mathbb{F}_2^n$.

We now recall a few definitions relating to the symbol-pair formalism.

Definition 2. (Symbol-Pair Read Vector (cf. [10])) *For a binary vector $a := (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_2^n$, its symbol-pair read vector is defined as:*

$$\pi(a) := ((a_0, a_1), (a_1, a_2), \dots, (a_{n-1}, a_0)).$$

A particular symbol-pair is read in error if at least one of its symbols is read in error and to correct these symbol-pair errors we need the symbol-pair metric.

Definition 3. (Symbol-Pair Metric (cf. [10])) *For binary vectors $a, b \in (\mathbb{F}_2^2)^n$ where $a = ((\langle a_0, a_0 \rangle), \dots, (\langle a_{n-1}, a_{n-1} \rangle))$ and $b = ((\langle b_0, b_0 \rangle), \dots, (\langle b_{n-1}, b_{n-1} \rangle))$ the symbol-pair distance between them is defined as :*

$$d_{\text{sp}}(a, b) := |\{0 \leq i \leq n-1 : (\langle a_i, a_i \rangle) \neq (\langle b_i, b_i \rangle)\}|,$$

while the symbol-pair weight of a vector $a \in (\mathbb{F}_2^2)^n$ is defined as:

$$\text{wt}_{\text{sp}}(a) := |\{0 \leq i \leq n-1 : (\langle a_i, a_i \rangle) \neq (0, 0)\}|.$$

For simplicity $d_{\text{sp}}(x, y)$ denotes the quantity $d_{\text{sp}}(\pi(x), \pi(y))$ while $\text{wt}_{\text{sp}}(x)$ refers to $\text{wt}_{\text{sp}}(\pi(x))$ for $x, y \in \mathbb{F}_2^n$.

Following along the lines of the Hamming metric the symbol-pair distance of a code C is defined (see [10] for details) as follows.

Definition 4. Consider a binary code $C \subset \mathbb{F}_2^n$ with respect to the symbol-pair metric. The symbol-pair distance of a code C is defined as:

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

If C is a linear code then the above expression simplifies to:

$$d_{\text{sp}}(C) = \min\{\text{wt}_{\text{sp}}(c) : c \in C, c \neq 0\}.$$

Due to the similarities with the Hamming metric, a code C with $d_{\text{sp}}(C) := d_{\text{sp}}$ is a $\left\lceil \frac{d_{\text{sp}}-1}{2} \right\rceil$ pair error-correcting code, with $\lceil \cdot \rceil$ being the greatest integer function.

The relation between the Hamming weight and the symbol-pair weight of a vector $x \in \mathbb{F}_2^n$ is stated in the succeeding lemma.

Lemma 5. (cf. [10]) For binary vectors $x \in \mathbb{F}_2^n$ with $0 < \text{wt}_{\text{H}}(x) < n$ the following relation holds

$$\text{wt}_{\text{H}}(x) + 1 \leq \text{wt}_{\text{sp}}(x) \leq 2\text{wt}_{\text{H}}(x).$$

We now review the theory of quantum error-correcting codes.

B. Quantum Error-Correcting Codes

A qubit extends the idea of representing information via classical bits to the quantum domain. A qubit encapsulates a two dimensional complex vector space implying that a qubit can lie in infinitely many states unlike the discrete state space of classical bits. The state space of a single qubit is denoted by H_2 . The computational basis states of a qubit is the orthonormal set $\{|0\rangle, |1\rangle\}$. Hence for any single qubit state, say $|\psi\rangle$, we have:

$$|\psi\rangle = \lambda_1 |0\rangle + \lambda_2 |1\rangle,$$

where $\lambda_1, \lambda_2 \in \mathbb{C}, |\lambda_1|^2 + |\lambda_2|^2 = 1$. The state space of n qubits is the space $H_2^{\otimes n}$ i.e. the n -fold tensor product of a single qubit state space.

A $[[n, k, d]]$ quantum error-correcting code is defined by a unitary map that encodes a k -qubit state into n -qubit state and is capable of correcting errors on $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$ qubits, where $\lfloor \cdot \rfloor$ is the greatest integer function. Errors on a quantum system are quantum operators on the system. The Pauli operators i.e.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

characterize the errors on a single qubit. The codes presented in the present paper are for the quantum channel considered in [1] and [4]. In the aforementioned channel, the probability that a qubit remains unaffected is $1 - p$ while with probability $p/3$ each, the Pauli operators X, Y, Z act on a qubit, where p is a characteristic of the quantum channel satisfying $0 \leq p \leq \frac{1}{2}$.

A quantum code corrects errors on a single qubit if it corrects the X and the Z error on a single qubit. Similarly a quantum code is t -error correcting if and only if it can correct the errors characterized by the

t-fold tensor products of the Pauli operators (see [12], [13], [14]).

Now to state the construction in [4] we recall the definitions of symplectic weight of a vector and symplectic inner product of vectors in $(\mathbb{F}_2^n)^2$.

The symplectic weight of a vector $(a|b) \in (\mathbb{F}_2^n)^2$ is defined as $\text{wt}_{\text{symp}}(a|b) := \{0 \leq i \leq n-1 : (a_i|b_i) \neq (0,0)\}$ and hence symplectic distance between $(a|b), (c|d)$ is the quantity $d_{\text{symp}}((a|b), (c|d)) := \text{wt}_{\text{symp}}((a|b) - (c|d))$. The symplectic inner product of vectors $(a|b), (c|d)$ on the other hand is defined as $\langle (a|b), (c|d) \rangle_{\text{symp}} := a \cdot d + b \cdot c$, where $\cdot$ refers to the Euclidean inner product.

It is important to note that for vectors $(a|b), (c|d) \in (\mathbb{F}_2^n)^2$ the operation of addition and multiplication by a scalar $\lambda \in \mathbb{F}_2$ has been defined naturally as:

$$(a|b) + (c|d) := (a + b|c + d),$$

and

$$\lambda(a|b) := (\lambda a|\lambda b).$$

We now move towards reviewing the stabilizer formalism introduced in [4].

Theorem 6. (cf. [4]) *Consider the binary linear space $(\mathbb{F}_2^n)^2$ equipped with the symplectic inner product. If S is a self-orthogonal code in $(\mathbb{F}_2^n)^2$ with dimension $n - k$ and if there are no vectors in $S^{\perp_{\text{symp}}} \setminus S$ having symplectic weight $< d$ then there exists a $[[n, k, d]]$ additive quantum code.*

As a consequence to the above Theorem we have the following construction using codes over GF(4) i.e. the Galois Field of order 4. which was also introduced in [4].

Theorem 7. (cf. [4]) *Consider a linear code C of length n and size 2^{n-k} in GF(4) which is self-orthogonal with respect to the Hermitian inner product. If there are no vectors of Hamming weight $< d$ in $C^{\perp_{\text{Herm}}} \setminus C$ then there exists a $[[n, k, d]]$ additive quantum code, where $C^{\perp_{\text{Herm}}}$ denotes the Hermitian dual of C .*

A key point to notice is that to construct additive quantum codes of a given length n we need self-orthogonal binary codes of double the length while if we use codes over GF(4) then the length remains the same. The present work becomes relevant for it constructs additive quantum codes of length n using binary codes of length n itself.

At this point we would like to emphasize that though CSS construction also deals with constructing stabilizer codes from binary codes it does not talk about the symbol-pair picture or the possibility of replacing the GF(4) picture with $\mathbb{F}_2$ completely.

Having developed the setup and the motivation for the present work we introduce the Symbol-Pair Additive Code Construction.

Remark. We would like to point out that a seemingly similar problem was put forth in [22] where the authors have asked about the possibility of defining a quantum symbol-pair channel like the classical symbol-pair channel. We would like to highlight that the present work focuses on using the classical symbol-pair metric to construct quantum codes over the existing quantum channel described in [4]. To emphasize, in this paper we have simply used codes over the symbol-pair metric and have not defined a quantum symbol-pair channel as opposed to what was asked in [22].

III. SYMBOL-PAIR ADDITIVE CODE CONSTRUCTION

Consider the embedding maps $Emb_R : \mathbb{F}_2^n \rightarrow (\mathbb{F}_2^n)^2$ and $Emb_L : \mathbb{F}_2^n \rightarrow (\mathbb{F}_2^n)^2$ defined as:

$$Emb_R(a) := (a|R(a))$$

and

$$Emb_L(a) := (a|L(a))$$

respectively. The image of a code $C \subset \mathbb{F}_2^n$ under the map Emb_R, Emb_L is defined naturally as:

$$Emb_R(C) := \{(c|R(c)) : c \in C\}$$

and

$$Emb_L(C) := \{(c|L(c)) : c \in C\}.$$

We now state an important property of the embedding map Emb_R (which also holds for Emb_L) in the following lemma.

Proposition 8. *For a $2k$ -dimensional binary linear code C of length n , the space $Emb_R(C)$ is a $2k$ -dimensional subspace of $(\mathbb{F}_2^n)^2$. Further, if $\{c_1, c_2, \dots, c_{2k}\}$ is a basis of C then $\{Emb_R(c_1), Emb_R(c_2), \dots, Emb_R(c_{2k})\}$ is a basis of $Emb_R(C)$.*

Proof. For a binary linear code C with length n and dimension $2k$ it can be verified that for any two vectors $(c_1|R(c_1)), (c_2|R(c_2)) \in Emb_R(C)$ we have:

$$(c_1|R(c_1)) + (c_2|R(c_2)) = (c_1 + c_2|R(c_1) + R(c_2)).$$

From the linearity of the right-shift operator and in light of the given condition that C is a linear code it follows that :

$$(c_1 + c_2|R(c_1 + c_2)) \in Emb_R(C).$$

This implies that $Emb_R(C)$ is a linear subspace of $(\mathbb{F}_2^n)^2$. It can be further verified that as there exists a one-one correspondence between a codeword $c \in C$ and its image $Emb_R(c)$ we have that $|Emb_R(C)| = |C| = 2^{2k}$.

Going ahead with the proof, a basis $\{c_1, c_2, \dots, c_{2k}\}$ of C is considered with the following linear combination:

$$\alpha_1(c_1|L(c_1)) + \alpha_2(c_2|L(c_2)) + \dots + \alpha_{2k}(c_{2k}|L(c_{2k})) = 0$$

or,

$$(\alpha_1 c_1 + \alpha_2 c_2 + \dots + \alpha_{2k} c_{2k} | \alpha_1 L(c_1) + \dots + \alpha_{2k} L(c_{2k})) = 0.$$

By using the given condition that $\{c_0, c_1, \dots, c_{2k}\}$ is a basis of C , we get the result that Emb_R preserves the basis of C .

□

Moving ahead, the construction given in this paper uses binary linear codes $\hat{C}$ satisfying the condition $Emb_R(\hat{C}) \subset Emb_R(\hat{C})^{\perp_{\text{symp}}}$ i.e. $Emb_R(\hat{C})$ is self orthogonal with respect to the symplectic inner product. A simplified characterization for the above condition has been stated in the following lemma.

Proposition 9. *For a binary linear code C of length n , the condition $R(c) + L(c) \in C^{\perp_{\text{Euc}}}$ for all codewords $c \in C$, with R, L being the right-shift and left-shift operators respectively is necessary and sufficient for $Emb_R(C) \subset Emb_R(C)^{\perp_{\text{symp}}}$ to hold.*

Proof. Consider a binary linear code C of length n and assume that there exists a non-zero vector $c \in C$ for which $(c|R(c)) \in \text{Emb}_R(C)^{\perp_{\text{symp}}}$ (as for c being the zero vector the result follows trivially). Using the aforementioned condition we get :

$$\langle (c|R(c)), (c'|R(c')) \rangle_{\text{symp}} = 0,$$

for all $(c'|R(c')) \in \text{Emb}_R(C)$ which can be further simplified to:

$$c.R(c') + c'.R(c) = 0$$

or,

$$c'_0(c_{n-1} + c_1) + c'_1(c_0 + c_2) + \dots + c'_{n-1}(c_{n-2} + c_0) = 0$$

or,

$$R(c) + L(c) \in C^{\perp_{\text{Euc}}}.$$

□

To quantify the error-correcting capability of the additive quantum codes obtained in this paper we introduce the quantity $\text{minwt}_H(C_1 \setminus C_2) := \min\{\text{wt}_H(c) : c \in C_1 \setminus C_2\}$. We also introduce the linear map $RL : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ defined as:

$$RL(a) := R(a) + L(a).$$

We now state the Symbol-Pair Additive Code Construction-I:

Theorem 10. *Let C be a $[n, 2k, d_H]$ binary linear code with $d_{\text{sp}}(C) := d_{\text{sp}}$. If there exists a k -dimensional subcode $\hat{C} \subset C$, satisfying $R(\hat{c}) + L(\hat{c}) \in \hat{C}^{\perp_{\text{Euc}}} \setminus C^{\perp_{\text{Euc}}}$ for all non-zero codewords $\hat{c} \in \hat{C}$ then there exists an additive quantum code with parameters $[[n, k, d]]$, where $\min\{d_H, \text{minwt}_H((RL(\hat{C}) + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}})\} \leq d \leq d_{\text{sp}}$.*

Proof. Let C be a $[n, 2k, d_H]$ binary linear code over the symbol-pair metric with the symbol-pair distance equal to $d_{\text{sp}}(C) = d_{\text{sp}}$ and suppose that there exists a subcode $\hat{C}$ of C having dimension k such that $R(\hat{c}) + L(\hat{c}) \in \hat{C}^{\perp_{\text{Euc}}} \setminus C^{\perp_{\text{Euc}}}$ for all non-zero codewords $\hat{c} \in \hat{C}$. Let $\{c_1, c_2, \dots, c_k\}$ be a basis of $\hat{C}$ which extends to a basis $\{c_1, c_2, \dots, c_{2k}\}$ of C .

Proceeding further, we consider the spaces $\text{Emb}_L(C)$ and $\text{Emb}_R(\hat{C})$. By Proposition 8, we have that $\text{Emb}_L(C)$ is a $2k$ -dimensional subspace with $\{\text{Emb}_L(c_1), \text{Emb}_L(c_2), \dots, \text{Emb}_L(c_{2k})\}$ as a basis and $\text{Emb}_R(\hat{C})$ is a k -dimensional subspace with $\text{Emb}_R(c_1), \dots, \text{Emb}_R(c_k)$ as a basis.

Now consider the Euclidean dual of C i.e. $C^{\perp_{\text{Euc}}}$ with $\{c'_1, \dots, c'_{n-2k}\}$ as one of its basis which is lifted to the space $(\mathbb{F}_2^n)^2$ by the map $P : \mathbb{F}_2^n \rightarrow (\mathbb{F}_2^n)^2$ defined by:

$$P(c') := (0|c').$$

It is simple to see that the space

$$P(C^{\perp_{\text{Euc}}}) = \{P(c') : c' \in C^{\perp_{\text{Euc}}}\}$$

is a $(n - 2k)$ -dimensional subspace of $(\mathbb{F}_2^n)^2$.

To complete the proof of the present theorem we use Theorem 6 by considering the space $S := P(C^{\perp_{\text{Euc}}}) + \text{Emb}_R(\hat{C})$. We now claim that $S := P(C^{\perp_{\text{Euc}}}) + \text{Emb}_R(\hat{C})$ is a self-orthogonal subspace

of $(\mathbb{F}_2^n)^2$ with dimension equal to $n - k$, such that $S^{\perp_{\text{symp}}} = \text{Emb}_L(C) + S$. To prove the above claim consider the following equation:

$$\begin{aligned} & \alpha_1(c_1|L(c_1)) + \dots + \alpha_{2k}(c_{2k}|L(c_{2k})) + \beta_1(0|c'_1) + \\ & \dots + \beta_{n-2k}(0|c'_{n-2k}) + \gamma_1(c_1|R(c_1)) + \dots + \gamma_k(c_k|R(c_k)) \\ & = (0|0) \end{aligned}$$

which simplifies to:

$$\alpha_1 c_1 + \dots + \alpha_{2k} c_{2k} + \gamma_1 c_1 + \dots + \gamma_k c_k = 0 \quad (1)$$

and,

$$\begin{aligned} & \alpha_1 L(c_1) + \alpha_2 L(c_2) + \dots + \alpha_{2k} L(c_{2k}) + \beta_1 c'_1 + \dots \\ & + \beta_{n-2k} c'_{n-2k} + \gamma_1 R(c_1) + \dots + \gamma_k R(c_k) = 0 \end{aligned} \quad (2)$$

As $\{c_1, c_2, \dots, c_{2k}\}$ are linearly independent we obtain:

$$\alpha_i = \gamma_i,$$

for $1 \leq i \leq k$ whereas

$$\alpha_i = 0,$$

for $k+1 \leq i \leq 2k$. Substituting the above values in equation 2 leads to the following sequence of equations:

$$\sum_{i=1}^k \alpha_i (L(c_i) + R(c_i)) + \sum_{j=1}^{n-2k} \beta_j c'_j = 0$$

or,

$$\sum_{i=1}^k \alpha_i L(c_i) + \sum_{i=1}^k \alpha_i R(c_i) + \sum_{j=1}^{n-2k} \beta_j c'_j = 0.$$

or,

$$\sum_{i=1}^k L(\alpha_i c_i) + \sum_{i=1}^k R(\alpha_i c_i) + \sum_{j=1}^{n-2k} \beta_j c'_j = 0.$$

or,

$$L\left(\sum_{i=1}^k \alpha_i c_i\right) + R\left(\sum_{i=1}^k \alpha_i c_i\right) + \sum_{j=1}^{n-2k} \beta_j c'_j = 0.$$

Now using following condition $R(\hat{c}) + L(\hat{c}) \in \hat{C}^{\perp_{\text{Euc}}} \setminus C^{\perp_{\text{Euc}}}$ for all non-zero $\hat{c} \in \hat{C}$ it implies that:

$$\alpha_i = 0, \beta_j = 0,$$

for $1 \leq i \leq k$ and $1 \leq j \leq n - 2k$. respectively.

We now proceed to show that $S := \text{Emb}_R(\hat{C}) + P(C^{\perp_{\text{Euc}}})$ is self-orthogonal and that $S^{\perp_{\text{symp}}} = S + \text{Emb}_L(C)$.

It is not difficult to observe that any two vectors $P(c'), P(c'') \in P(C^{\perp_{\text{Euc}}})$, are orthogonal to each other when considered over the symplectic inner product as,

$$\langle (0|c'), (0|c'') \rangle_{\text{symp}} = c'' \cdot 0 + 0 \cdot c' = 0.$$

Similarly, for every vector $(0|c') \in P(C^{\perp_{\text{Euc}}})$ and $(\hat{c}|R(\hat{c})) \in \text{Emb}_R(\hat{C})$ we have

$$\langle (0|c'), (\hat{c}|R(\hat{c})) \rangle_{\text{symp}} = c' \cdot \hat{c} = 0.$$

Finally, by using the Proposition 9 and the given condition that $R(\hat{c}) + L(\hat{c}) \in \hat{C}^{\perp_{\text{Euc}}} \setminus C^{\perp_{\text{Euc}}}$ for all $\hat{c} \in \hat{C}$ or to put it more simply $R(\hat{c}) + L(\hat{c}) \in \hat{C}^{\perp_{\text{Euc}}}$ for all $\hat{c} \in \hat{C}$, gives us the result that $S := \text{Emb}_R(\hat{C}) + P(C^{\perp_{\text{Euc}}})$ is self-orthogonal. Now to observe that $S^{\perp_{\text{symp}}} := S + \text{Emb}_L(C)$ we argue as follows:

$$\begin{aligned} \langle (a|R(a)) | (b|L(b)) \rangle &= a \cdot L(b) + R(a) \cdot b \\ &= a_0 b_1 + a_1 b_2 + \dots + a_{n-1} b_0 \\ &\quad + a_{n-1} b_0 + a_0 b_1 + a_1 b_2 + \dots \\ &\quad + a_{n-2} b_{n-1} \\ &= 0 \end{aligned}$$

for all $a \in \hat{C}$, $b \in C$

As it has been already proved above that

$$\begin{aligned} &\dim(\text{Emb}_R(\hat{C}) + C^{\perp_{\text{Euc}}} + \text{Emb}_L(C)) \\ &= \dim(\text{Emb}_R(\hat{C})) + \dim(C^{\perp_{\text{Euc}}}) + \dim(\text{Emb}_L(C)) \\ &= k + n - 2k + 2k = n + k \end{aligned}$$

we get that $S^{\perp_{\text{symp}}} := S + \text{Emb}_L(C)$.

Now to obtain the distance of the quantum code being considered we see that the vectors in $S^{\perp_{\text{symp}}} \setminus S$ are of the form:

- 1) $(c|L(c)), c \in C$.
- 2) $(c|L(c) + c'), c \in C, c' \in C^{\perp_{\text{Euc}}}$
- 3) $(0|R(c) + L(c)), c \in \hat{C}$
- 4) $(c_1 + c_2|R(c_1) + L(c_2)), c_1 \neq c_2 \in \hat{C}$
- 5) $(0|R(c) + L(c) + c'), c \in \hat{C}, c' \in C^{\perp_{\text{Euc}}}$

The observations mentioned above along with the Theorem 6 shows that there the exists an additive quantum code with parameters $[[n, k, d]]$ where $\min\{d_H, \min_{\text{wt}_H}((RL(\hat{C}) + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}})\} \leq d \leq d_{\text{sp}}$. $\square$

For completeness, using the results from [4], the Stabilizer group for quantum codes obtained by Theorem 10 is given by:

$$\{Z(c') : c' \in C^{\perp_{\text{Euc}}}\} \bigcup \{X(\hat{c})Z(R(\hat{c})) : \hat{c} \in \hat{C}\},$$

where,

$$X(a)Z(b) := (X^{a_0} \otimes X^{a_1} \otimes \dots \otimes X^{a_{n-1}})(Z^{b_0} \otimes Z^{b_1} \otimes \dots \otimes Z^{b_{n-1}})$$

for binary vectors $a, b \in \{0, 1\}^n$.

Corollary 11. *Let C be a binary cyclic LCD code (i.e. $C \cap C^{\perp_{\text{Euc}}} = \{0\}$) over the symbol-pair metric having parameters $[n, 2k, d_{\text{H}}]$ and with symbol-pair distance equal to d_{sp} . If there exists a k -dimensional cyclic self-orthogonal subcode $\hat{C}$ of C with $k > 1$, satisfying:*

$$\left\{ \begin{array}{ll} (0, 1, 0, \dots, 0, 1), (1, 0, \dots, 1, 0), (1, 1, \dots, 1) \notin \hat{C}, & n \text{ is even} \\ (1, 1, \dots, 1) \notin \hat{C}, & n \text{ is odd} \end{array} \right\}.$$

then there exists a $[[n, k, d]]$ additive quantum code with $\min\{d_{\text{H}}, \min_{\text{wt}_{\text{H}}}((\hat{C} + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}})\} \leq d \leq d_{\text{sp}}$. If $k = 1$ then the above mentioned condition can be dropped.

Proof. It can be seen that if $\hat{C}$ is cyclic as well as self-orthogonal then $RL(c) := R(c) + L(c) \in \hat{C} \subset \hat{C}^{\perp_{\text{Euc}}}$, hence simplifying the lower bound on the distance of the quantum code obtained by Theorem 10. $\square$

To illustrate the construction using LCD codes i.e. Construction 11 consider the cyclic LCD code C with parameters $[31, 20, 6]$ generated by $g(x) := (x + 1)(x^5 + x^2 + 1)(x^5 + x^3 + 1)$. Following the proof of the Construction 10, the self-orthogonal subcode $\hat{C}$ of C with generator $h(x) := g(x)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^3 + x^2 + x + 1)$, hence dimension equal to 10, is considered. As the generator polynomial for C has $x + 1$ as its factor it follows that the all one vector i.e. $(1, 1, \dots, 1)$ does not lie in C . Evidently, $\hat{C}$ is a cyclic self-orthogonal subcode of C satisfying the conditions in Corollary 11. Further it can also be verified that $d_{\text{sp}}(C) = 9$ and $\min_{\text{wt}_{\text{H}}}((\hat{C} + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}}) = 5$, hence giving a $[[31, 10, 5 \leq d \leq 9]]$ quantum error correcting code by Corollary 11.

A. Explaining the Computation

We give some details about how quantum codes are computed from Corollary 11. Consider a cyclic LCD code, C , with parameters $[n, 2k, d_{\text{H}}]$ and $d_{\text{sp}}(C) := d_{\text{sp}}$. We search for a Euclidean self-orthogonal subcode, $\hat{C}$, of C with parameters $[n, k]$. Proceeding further, the value $\min_{\text{wt}_{\text{H}}}((\hat{C} + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}})$, is computed by obtaining the weight distributions for the codes $\hat{C} + C^{\perp_{\text{Euc}}}$ and $C^{\perp_{\text{Euc}}}$. Finally, the $\min\{d_{\text{H}}, \min_{\text{wt}_{\text{H}}}((\hat{C} + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}})\}$ is computed giving the lower bound on d .

We now list a few quantum codes with length $7 \leq n \leq 63$, that have been obtained via Corollary 11. We mention the lower and upper bounds on the distance for some of the quantum codes obtained via the Construction 11 while for the remaining codes where the search exceeded the time limit we have simply mentioned the lower bound.

We would like to highlight that by using the methods of shortening, lengthening, etc., of quantum codes introduced in [4], we might obtain more quantum codes.

Remark. It has been brought to our notice that the parameters for stabilizer codes obtained via Corollary 11 can possibly be obtained by Theorem 1 of [23]. In [23], dual-containing binary codes which can be extended to a bigger code have been considered while in Corollary 11 we make no such assumption. Furthermore, in [24] it was shown that the construction provided in [23] is related to the second generalized-Hamming weights, which basically depends on the subspace property of the code, while the symbol-pair distance of the code does not use the subspace structure and depends only on the locality properties of codewords. Hence, we feel that the two constructions are inherently different.

Table I
QUANTUM CODES FROM CYCLIC LCD CODES

Quantum Codes	Cyclic LCD Code
$[[7, 3, 2 \leq d \leq 3]]$	$[7, 6, 2]$
$[[15, 4, 3 \leq d \leq 7]]$	$[15, 8, 4]$
$[[21, 3, 3 \leq d \leq 9]]$	$[21, 6, 4]$
$[[21, 6, 3 \leq d \leq 7]]$	$[21, 12, 4]$
$[[30, 8, 3 \leq d \leq 8]]$	$[30, 16, 4]$
$[[31, 10, 5 \leq d \leq 9]]$	$[31, 20, 6]$
$[[31, 5, 3 \leq d]]$	$[31, 10, 10]$
$[[35, 12, 3 \leq d]]$	$[35, 24, 4]$
$[[39, 12, 4 \leq d]]$	$[39, 24, 4]$
$[[42, 6, 3 \leq d]]$	$[42, 12, 6]$
$[[42, 12, 3 \leq d]]$	$[42, 24, 4]$
$[[45, 16, 4 \leq d]]$	$[45, 32, 4]$
$[[45, 12, 3 \leq d]]$	$[45, 24, 4]$
$[[51, 16, 4 \leq d]]$	$[51, 32, 4]$
$[[62, 20, 5 \leq d]]$	$[62, 40, 6]$
$[[63, 18, 7 \leq d]], [[63, 18, 5 \leq d]]$	$[63, 36, 8]$
$[[63, 15, 6 \leq d]], [[63, 15, 5 \leq d]]$	$[63, 30, 6]$
$[[63, 12, 4 \leq d]], [[63, 12, 3 \leq d]]$	$[63, 24, 12]$
$[[63, 9, 4 \leq d]], [[63, 9, 3 \leq d]]$	$[63, 18, 18]$

B. Modified CSS Construction

We now relate the stabilizer codes obtained by the Corollary 11 to the family of CSS codes introduced in [1].

We begin by reviewing the CSS-Construction mentioned in [1].

Theorem 12. *Let C_1, C_2 be binary linear codes with C_2 being a subcode of C_1 . If the parameters of the codes $C_1, C_2^{\perp_{\text{Euc}}}$, considered over the Hamming metric, is $[n, k_1, d_1]$ and $[n, n - k_2, d_2]$ respectively then there exists a quantum error-correcting code with parameters $[[n, k_1 - k_2, \min\{d_1, d_2\}]]$.*

On reviewing the Corollary 11 it can be observed that the codes C (of dimension $2k$) and $\hat{C}$ (of dimension k) satisfy the condition $\hat{C} \subset C$ while the obtained additive quantum codes have parameters $[[n, (2k - k) = k, d]]$, where $\min\{d_H, \min_{\text{wt}_H}((\hat{C} + C^{\perp_{\text{Euc}}}) \setminus C^{\perp_{\text{Euc}}})\} \leq d \leq d_{\text{sp}}$.

By the above observation the additive quantum codes obtained by theorem 12 seem to have a natural connection to the CSS codes. Proceeding ahead we formalize the above mentioned observation by viewing the Corollary 11 as a modified CSS Construction. We also claim that for codes $C, \hat{C}$ satisfying the conditions in Corollary 11 the quantum codes obtained from Corollary 11 have better error-correcting capabilities than the quantum codes obtained from the known CSS construction.

Lemma 13. *Let $C, \hat{C}$ be binary cyclic LCD codes with $\hat{C}$ being a subcode of C . If the codes $C, \hat{C}^{\perp_{\text{Euc}}}$ have parameters $[n, 2k, d_1]$ and $[n, k, d_2]$ respectively with $d_{\text{sp}} := d_{\text{sp}}(C)$, then the distance d of the quantum codes obtained via Corollary 11 satisfies the relation:*

$$\min\{d_1, d_2\} \leq d.$$

Proof. Using the condition that C is an LCD code i.e. $C \cap C^{\perp_{\text{Euc}}} = \{0\}$ we have that $\hat{C} \cap C^{\perp_{\text{Euc}}} = \{0\}$, as $\hat{C} \subset C$. It is interesting to observe that by coupling the conditions $\dim(\hat{C}) = k, \dim(C^{\perp_{\text{Euc}}}) = n - 2k$

with the given condition that $\hat{C}$ is a self-orthogonal subcode and C is an LCD code, leads us to the relation:

$$\hat{C}^{\perp_{\text{Euc}}} = \hat{C} + C^{\perp_{\text{Euc}}}.$$

Now by observing that:

$$\min\{d_1, d_2\} \leq \min\{d_1, \min\text{wt}_H(\hat{C}^{\perp_{\text{Euc}}} \setminus C^{\perp_{\text{Euc}}})\},$$

we get the result,

$$\min\{d_1, d_2\} \leq d.$$

□

The above relation verifies the claim that the quantum codes obtained from Corollary 11, which we refer to as the Modified CSS construction, have better error-correcting capabilities than the CSS construction mentioned in [1]. The Table I gives the examples of quantum codes obtained via the Modified CSS Construction.

IV. CONCLUSION

In the current work we presented an approach of using binary codes over the symbol-pair metric of a given length for constructing additive quantum codes of the same length as opposed to considering self-orthogonal codes over GF(4). Specifically, we obtained additive quantum codes from cyclic LCD codes satisfying certain properties.

Future work can be oriented towards finding different families of classical codes satisfying Theorem 10. Another problem that can be considered is obtaining a tighter bound on distance d for quantum codes obtained via Construction 10. Furthermore, we may extend the Symbol-Pair Additive Code Construction presented in this paper by considering different assumptions on the involved binary codes. It would also be interesting to extend the relation of codes obtained by the Modified CSS Construction to the works in [11], [16].

Another possible direction can be extending the Symbol-Pair Additive Construction to the Modified Symplectic inner products presented in [21] as well as to the domain of Non-binary stabilizer codes presented in [17]. Finally, from an implementation perspective we can even consider relating the obtained stabilizer codes via the Modified CSS Construction to the results for CSS codes in [18] and [20].

REFERENCES

- [1] A.R. Calderbank and P.W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, pp. 1098-1106, 1996.
- [2] M. Grassl, "Algebraic quantum codes: linking quantum mechanics and discrete mathematics," *International Journal of Computer Mathematics: Computer Systems Theory*, pp.1-17, 2020.
- [3] D. Gottesman, "Stabilizer codes and quantum error-correction," Ph.D. dissertation, Caltech, 1997.
- [4] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J. Sloane, "Quantum error correction via codes over GF (4)," *IEEE Transactions on Information Theory*, vol. 44, no.4, pp. 1369-1387, 1998.
- [5] A. Thangaraj and S.W. McLaughlin, "Quantum codes from cyclic codes over GF (4)," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1176-1178, 2001.
- [6] S. Ling and C. Xing, *Coding theory: a first course*. Cambridge University Press, 2004.
- [7] M.A. Nielsen and I. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 2002.
- [8] C. Galindo, F. Hernando, and R. Matsumoto, "Quasi-cyclic constructions of quantum codes," *Finite Fields and Their Applications*, vol. 52, pp. 261-280, 2018.
- [9] L. Jin, H. Kan and J. Wen, "Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes," *Designs, Codes and Cryptography*, vol. 84, no. 3, pp. 463-471, 2017.

- [10] Y.Cassuto and M.Blaum, "Codes for symbol-pair read channels," *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 8011-8020, 2011.
- [11] H. Chen, S. Ling and C. Xing, "Quantum codes from concatenated algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2915-2920, 2005.
- [12] E.Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A*, vol. 55, no. 2, pp. 900-911, 1997.
- [13] C. H. Bennett, D. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Physical Review A*, vol. 54, pp. 3824-3851, 1996.
- [14] A. Ekert and C. Macchiavello, "Error correction in quantum communication," *Physical Review Letters*, vol. 77, pp. 2585-2588, 1996.
- [15] Y. Rao, R. Li, L. Lv, G. Chen and F. Zuo, "On binary LCD cyclic codes," *Procedia Computer Science*, vol. 107, pp. 778-783, 2017.
- [16] M.F. Ezerman, S. Jitman, S. Ling, and D.V. Pasechnik, "CSS-like constructions of asymmetric quantum codes," *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6732-6754, 2013.
- [17] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, "Nonbinary Stabilizer Codes Over Finite Fields," in *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4892-4914, Nov. 2006, doi: 10.1109/TIT.2006.883612.
- [18] N. Rengaswamy, R. Calderbank, M. Newman and H. D. Pfister, "On Optimality of CSS Codes for Transversal T," *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 2, pp. 499-514, Aug. 2020, doi: 10.1109/JSAIT.2020.3012914.
- [19] J. Qian and L. Zhang, "On MDS linear complementary dual codes and entanglement-assisted quantum codes," *Designs, Codes and Cryptography*, vol. 86, no. 7, pp. 1565-1572, 2018.
- [20] T. Tansuwanont, C. Chamberland, and D. Leung, "Flag fault-tolerant error correction, measurement, and quantum computation for cyclic Calderbank-Shor-Steane codes," *Physical Review A*, vol. 101, no. 1, 2020.
- [21] T. Gandhi, P. Kurur and R. Mittal, "Stabilizer codes from modified symplectic forms," *IEEE International Symposium on Information Theory (ISIT)*, pp. 2903-2907, 2019, doi: 10.1109/ISIT.2019.8849639.
- [22] H.Q. Dinh, B.T. Nguyen and S. Sriboonchitta, "MDS Symbol-Pair Cyclic Codes of Length $2p^s$ over $\mathbb{F}_{p^m}$," *IEEE Transactions on Information Theory*, vol. 66, no. 1, pp. 240-262, 2019.
- [23] A.M. Steane, "Enlargement of calderbank-shor-steane quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp.2492-2495, 1999.
- [24] G. Cohen, S. Encheva and S. Litsyn, "On binary constructions of quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp.2495-2498, 1999.