A Novel and Efficient Stabilizer Codes Over Non-Cyclic Hadamard Difference Sets for Quantum System

Shivender Goswami, Manoj Kumar, R.K. Mishra, Akash Rathor

***ABSTRACT*—Quantum error correction lies at the heart of building reliable quantum information processing systems. Stabilizer codes, a fundamental class of quantum error-correcting codes, play a pivotal role in mitigating the adverse effects of noise and decoherence in quantum systems. This paper introduces a novel construction of quantum stabilizer codes using Hadamard difference sets, an elegant mathematical concept derived from combinatorial design theory. In this paper, the construction of the quantum stabilizer codes over non- cyclic Hadamard difference sets with parameters $(4m^2, 2m^2-m, m^2-m)$, where m is a positive integer is discussed. Firstly, the parity check matrices are constructed from the Circulant permutation matrices with the help of Hadamard difference sets and then, the Symplectic inner product condition for Hadamard difference sets over binary operation for parity check matrices are obtained to affirm the commutative condition for Stabilizer operators which is vital for the error detection. For application, we constructed a Hadamard difference sets with parameters $(16, 6, 2)$ for $m = 2$ of ordered pair of the group $\mathbb{Z}_2 \times \mathbb{Z}_8$ (non-cyclic group) and quantum stabilizer codes are obtained by parity-check matrix.**

***Index Terms*—Difference sets, Parity-check matrices, Quantum information, Quantum stabilizer codes, Symplectic inner product**

I. INTRODUCTION

In the field of computer science, quantum information pertains to the information within a quantum system. Unlike classical information, where bits are the fundamental units of data, quantum information relies on qubits. Quantum computing exhibits significant speedups in polynomial time, particularly when factoring large integers, as compared to classical computing [1],[2],[3]. Correcting errors in quantum communication systems is a challenging task due to the continuous nature of qubits, as opposed to the two-state characteristic of classical bits. In 1995, Peter Shor introduced the concept of quantum error-correcting codes (QECCs) [4], followed by Steane's development of the general theory of QECCs in 1996 [5]. This work laid the foundation for the distinguished CSS (Calderbank–Shor–Steane) formalism, leading to the creation of a 7-qubit CSS code capable of single-error correction [6]. Extensive research has been conducted on QECCs [7],[8]. The ability of QECCs to simultaneously correct the two most common types of error, the bit-flip error and the phase-flip error, ensures the correction of any error on a single qubit. [9]. But the impact of noisy environment of the quantum system would decrease the performance. Therefore, QECCs [10], [11], [12] have been proposed as a result to insulate the quantum information from the effect of noisy environments. QECCs which attain the quantum singleton bound are called MDS codes [13], [14]. After establishment in 1997 [15], Quantum stabilizer codes (QSCs) have played an important role in QECCs and enabled numerous new and powerful codes. A QSC exploits supplementary qubits known as ancilla to protect the original qubit from noise. The main significant and consequential advantage of QSCs are that the occurred errors can be identified and corrected with the help of the stabilizer operators [4]. Therefore, QSCs are very impactful to amplify the utilisation of stabilizer theory in quantum systems. Furthermore, the notion of stabilizer permits the classical codes on binary system and quaternary systems to their equivalent QSCs. As a result, several QSCs have been constructed based on classical codes [16], [17],[18]. The main idea of constructing a QSC is interpreting the stabilizer codes in the form of a parity-check matrix such that binary or quaternary elements of the matrix hold good the SIP constraint. As shown in Fig. 1, the process of quantum error correction entails encoding quantum data using error-correcting codes, identifying errors through syndrome measurements, implementing error correction actions guided by the detected syndromes, and ultimately deciphering the corrected quantum state to recover the initial information. The objective is to uphold the dependability of quantum computations even when errors occur, with the overarching aim of enabling fault-tolerant quantum computing. Quantum BCH codes [19], quantum Reed-Solomon codes [20], quantum convolutional codes [21], [22], [23],[24] and more recently, quantum low density parity-check (LDPC) codes [25], [26], [27],[28] are just a few of the many constructs that have been proposed and examined. These more recent stabilizer codes, unlike the earlier ones that only corrected one error in a block of numerous qubits, correct numerous faults in a block of many qubits. The majority of them have their roots in traditional binary or nonbinary error correction codes. The only exception to construct QSC which is not related to classical codes is [29], [30], where Boolean functions are utilised. Recently, quantum codes from constacyclic codes over a semi-local ring are explored [31], [32]. More recently stabilizer quantum codes based on trace-depending polynomials and Hermitian self-orthogonal codes

Manuscript received July 31, 2023; revised May 17, 2024.

Shivender Goswami is a Ph.D. candidate of Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India, 249404. (e-mail: shivendrgoswami@gmail.com).

Manoj Kumar is an Associate Professor at Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India, 249404. (Corresponding author to provide phone: +91 8755386009; e-mail: sdmkg1@gmail.com).

R.K. Mishra is a Professor of G.L. Bajaj Institute of Technology, Management and Research, Greater Noida, U.P., India, 201306. (e-mail: rkmsit@rediffmail.com).

Akash Rathor is a Ph.D. candidate of Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India, 249404. (e-mail: akashrathor9760@gmail.com).

are demonstrated [33], [34] which give rise to wider range of lengths and good parameters.

In this paper, the particular focus is placed on the construction of QSCs grounded on the concept of difference sets (DS). Firstly, in 2004, difference sets were implemented in the construction of QSC [35]. In combinatorics, difference set [36], [37] is any subset of a group such that difference of any two elements lies in the group. The proposed construction method handles the use of non-cyclic Hadamard difference sets (HDS) [38] in formation of the QSCs. In the research work by Dillon, the idea of HDS for commutative groups is effectively illustrated [39]. This paper contains a general product construction method for HDS. See Lander's monograph [40] for more information on the broader theory of symmetric designs and DS. The $(16,6,2)$ designs are detailed in depth in [41]. In 1978, researcher Kibler found, all DS of parameter $(16,6,2)$ by computer in which 27 are non-identical DS in 12 groups of order 16 enlisted in the survey of Kibler [42]. In Fig. 2, the process of constructing QSCs is depicted, starting with the selection of a difference set to derive the parity check matrix for the designated code. This ensures compliance with the Symplectic Inner Product (SIP) constraint. Subsequently, stabilizer generators and logical operators are obtained to aid in identifying a stabilizer code. This systematic approach forms the basis for establishing robust quantum error correction mechanisms, ultimately enhancing the reliability and integrity of quantum information processing systems. This paper proposes a novel algorithm for quantum stabilizer codes using non-cyclic HDSs. Unlike existing approaches [43,44], the presented algorithm achieves higher code distances such as the obtained code from the proposed method $[[16,6,2]]$ which is crucial for error correction as higher code distances generally allow for better error detection and correction capabilities. Using non-cyclic HDSs open up the possibility of exploring new families of QSC with unique properties and characteristics together with better performance under various noise models. This study brings exciting progress to quantum error correction and computation by introducing a fresh approach: quantum stabilizer codes built from non-cyclic HDS. Through this method, we have managed to enhance error correction performance, significantly improving our ability to detect and fix errors in quantum systems compared to traditional methods. These codes have a higher code distance and lower overhead, making them more resilient to errors and noise while also boosting efficiency and scalability. This approach is not just about fixing errors better, it also offers us greater freedom in designing codes. We can now tailor-make codes to suit specific tasks or hardware setups, opening up new possibilities for practical applications. Moreover, delving into non-cyclic structures gives us fresh ground to explore in quantum information processing, pushing us closer to real-world implementation. Ultimately, this study marks a big leap in quantum error correction techniques, promising more dependable and efficient quantum computing in real-world scenarios. The organization of the paper is as follows.

Section II contains some definitions related to the work. Section III introduces the theory of QSCs. Our new construction method is discussed in section IV. We give some simulation results on the relative performance of codes constructed by our method in section V. Finally, section VI concludes the paper.

II. RELATED WORK

The following definitions will be utilized in the formation of Stabilizer codes.

A. Qubits

The fundamental unit of information in quantum systems is qubit, which can be modelled as a two-state Hilbert space $H^{\otimes 2}$ with dimension 2. Therefore, there are two basis quantum states denoted by $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. A linear superposition of a qubit's two orthogonal basis states can be used to represent the most arbitrary state of a qubit as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, where the probability of obtaining the state $|0\rangle$ is $|a|^2$ and the probability of obtaining the state $|1\rangle$ is $|b|^2$. The criterion must be met in accordance with the qubit norm condition, $|a|^2 + |b|^2 = 1$.

B. Hadamard Difference Set

A DS D with parametric equation $(4m^2, 2m^2 - m, m^2 - m)$, where $m \in \mathbb{Z}^+$, is called a Hadamard difference set (HDS).

C. Difference Sets and Shifted Difference sets

A subset D (having k elements) of a group $(G,+)$ with order n is known to be a difference set (DS) of parameters (n,k,λ) if each element $g \in G$ can be represented as a difference of two distinct elements of G in exactly λ ways. The necessary condition for the parameters (n,k,λ) to represent a DS is that $k(k-1) = \lambda(n-1)$ [35]. For a DS $D = \{d_1, d_2, \ldots, d_k\}$, let the set be shifted by s is

$$D + s = \{d_1 + s, d_2 + s, \ldots, d_k + s\}$$

Then $D+s$ also forms a DS for same parameters (n,k,λ).

For example, let $G = \mathbb{Z}_5$ and $D = \{0,1,3,4\}$ be a subset of G, then D forms a DS with parameters $(5,4,3)$ as

$0-1=4$ $\quad$ $1-0=1$

$3-0=3$ $\quad$ $4-0=4$

$0-3=2$ $\quad$ $1-3=3$

$3-1=2$ $\quad$ $4-1=3$

$0-4=1$ $\quad$ $1-4=2$

$3-4=4$ $\quad$ $4-3=1$

The shifted DS $(5,4,3)$ with a shift 2 is given as,

$D+2 = \{0,1,2,3\}$,

$0-1=4$ $\quad$ $1-0=1$

$2-0=2$ $\quad$ $3-0=3$

$0-2=3$ $\quad 1-2=4$

$2-1=1$ $\quad 3-1=2$

$0-3=2$ $\quad 1-3=3$

$2-3=4$ $\quad 3-2=1$

D. Symplectic Inner Product (SIP) condition

The generators of stabilizer group associated to a binary check matrix $A=\left[A_1 \mid A_2\right]$ satisfy the commutativity property if and only if $A_1 \times A_2^T + A_2 + A_1^T = 0$.

E. Pauli Group

The group of Pauli's on n qubits , P_n , is the set of the Pauli operators in which tensor product is done n times.

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

i.e., $P_n=\left\{\alpha \times p_0 \otimes p_1 \otimes \cdots \otimes p_n \middle| \alpha \in \{\pm 1, \pm i\}\right\}$ and $p_i \in \{I, X, Y, Z\}$.

III. MATHEMATICAL BACKGROUND

In quantum computing, QSCs are extensively useful to secure the quantum information due to the noise in the environment and decoherence. In classical system it is possible to copy information, but in quantum system, it is not possible to copy information in light of the No-Cloning Theorem [45]. But information in quantum system can be entangled with ancillary qubits to encode the information using unitary operations [46],[47]. Stabilizer codes are a vital type of quantum codes which are closely related to the counterpart linear codes in information. As syndrome measurement is frequently used by classical codes to identify errors on the encoded state, QECCs too utilize the syndrome identification through the assistance of quantum stabilizer operators. Stabilizer code C_S is a subspace of $H^{\otimes n}$ which contains the quantum states that are fixed by a commutative subgroup S of P_n, where P_n is the Pauli group on n -qubits, where any element of S has the eigenvalue +1. That is,

$$C_s=\left\{|\psi\rangle \in H^{\otimes n} \middle| s|\psi\rangle=|\psi\rangle, \forall s \in S\right\}.$$

The subgroup S is generated by elements $s_1, s_2, \ldots, s_m$ and any of the two operators in S are commutative. With $(n-k)$ linearly independent Pauli operators $s_1, s_2, \ldots, s_m$, the subgroup S forms a subspace C_S to be $[[n, k, \mathrm{d}_{\min}]]$ QSC [15] where k logical qubits are encoded to n physical qubits, correcting $t=[(d_{\min}-1)/2]$ errors [5]. When the error operator E enforces upon the state $|\psi\rangle$, then the affected state $E|\psi\rangle$ can be recovered with the help of the stabilizer generators s_i from the code space C_S. For example, the QSC [[5,1,3]] can correct one error and has four generators in Table 1 which helps to produce the full quantum stabilizer set S.

TABLE I. Generators of [[5,1,3]] QSC

Generators	Operators
s_1	*XZZXI*
s_2	*IXZZX*
s_3	*XIXZZ*
s_4	*ZXIXZ*

Let I_n be the identity matrix of size $n \times n$. Then, $I_n + x$ is the shift of I_n where the rows of I_n are circularly shifted to the right by x positions $(0 \le x \le n-1)$,

$$C_{n\times n}=\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}.$$

An $n \times n$ Circulant Permutation (CP) matrix C_n, is a binary matrix written in the form where $c_k \in \{0,1\}$. $C_{n\times n}$ can be written as the linear combination of identity matrix and its shifted matrices.

$$C_{n\times n}=c_0 \times I_n(0)+c_1 \times I_n(1)+\ldots+c_{n-1} \times I_n(\mathrm{n}-1).$$

It is assumed that $c_0+c_1+\ldots+c_{n-1}=k$. The matrix C_n can also be expressed by using the Hall-polynomial form $h_p(x)$ [30] as

$$h_p(x)=x^{p_1}+x^{p_2}+\ldots+x^{p_i} \qquad (1)$$

here, $\{p_1, p_2, \ldots, p_i\}$ are places of 1 in the initial row of $C_{n\times n}$ such that $p_1 \neq p_2 \neq \ldots \neq p_i$.

Let ${C_{n\times n}}^T$ be the transpose of the matrix $C_{n\times n}$ and let $h_p(x)^T$ be the Hall-polynomial form of ${C_{n\times n}}^T$, then the polynomial $h_p(x)^T$ is expressed as $h_p(x)^T=x^{-p_1}+x^{-p_2}+\ldots+x^{-p_i}$.. For a $(\mathrm{n}, \mathrm{k}, \lambda)$ DS $D=\{d_1, d_2, \ldots d_k\}$, the CP matrix C_n in equation (1) is made where the element c_j is 1 if $j \in D$ and is 0 otherwise. Then, the Hall-polynomial form for the difference set D is

$$h_p(x)^D=x^{d_1}+x^{d_2}+\ldots+x^{d_k} \qquad (1^*)$$

Let $\{E_1, E_2, \ldots, \mathrm{E}_r\}$ denote the set of errors on the corrupted state $E|\psi\rangle$. As all elements of the group P_n either commutes or anti-commutes, so the element from the error set either commutes or anti-commutes with the elements of the group of stabilizer S.

Hence, the affected state $E|\psi\rangle$ is determined by the elements of S.

$$s_i \times E|\psi\rangle=\begin{cases} E \times s_i|\psi\rangle=E|\psi\rangle, & \text{Error not detected} \\ -E \times s_i|\psi\rangle=-E|\psi\rangle, & \text{Error detected} \end{cases}$$

The error operator E_i is corrected by the stabilizer group if

$$E_i^{\dagger} E_j \notin N(S)/S, \forall E_i, E_j \in E$$

where $E_i^{\dagger}$ denotes the conjugated transpose of E_i and $N(S)$ denotes the normalizer of the group S in P_n.

The normalizer of the group S is defined as $N(S)=\{N \in P_n \mid N^{\dagger}EN \in S, \forall E \in S\}$. $N(S)$ is defined to be the set of all those Pauli operators which are commutative with each element of S. The minimum distance $d_{\min}$ of the code is calculated as

$$d_{\min} = \min(W(E)) \text{ s.t.} E \in N(S)/S,$$

where $W(E)$ denotes the number of operators which are not equal to Pauli operator I in N.

As every Pauli operator can be described in the terms of X and Z operators such as $IYYZI = IXXII \times IZZZI$. Hence, there is a straightforward and practical correspondence between Pauli operators and binary vectors, where I corresponds to $(0,0)$, X corresponds to $(1,0)$, Z corresponds to $(0,1)$ and Y corresponds to $(1,1)$. Distinct Pauli operators are either scalar multiple of each other or linearly independent with respect to multiplication. Therefore, the $n-k$ generators of $[[n,k]]$ code are formulated by a concatenation of H_X and H_Z resulting in a parity-check matrix H as

$$H = [H_X \mid H_Z] \tag{2}$$

where the matrices H_X and H_Z denotes the binary matrices of size $(n-k)\times n$. The rows represent distinct stabilizer generators, and the columns represent different qubits. One of the matrices contains a '1' in a specific position if the corresponding stabilizer generator has either a X or a Y operator, while the other matrix contains a '1' when the generator has either a Y or a Z operator. For example, the QSC $[[5,1,3]]$ in Table 1 has the corresponding parity check matrices as

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since, there exists the requirement for quantum stabilizer operators to be commutative, the SIP constraint is acted on H, such that $H_X \times H_Z{}^T + H_Z \times H_X{}^T = 0_{n-k} \bmod 2$ (3)

The parity-check matrix H obtained in (2) is of rank $(n-k)$ where the dual space of H has the dimension $2n-m(=m+2k)$. Hence, the normalizer group denoted by $N(S)$ can be generated by $(2n-m)\times 2n$ binary matrix. The initial m rows represent the parity-check matrix and the last $2k$ rows represent the logical operators denoted by $\bar{X}$ and $\bar{Z}$. Here, the logical operators must hold the conditions

$$\begin{cases} \bar{X}_i \circ \bar{X}_j = +1 \\ \bar{Z}_i \circ \bar{Z}_j = +1 \\ \bar{X}_i \circ \bar{Z}_j = +1 \text{ for i} \neq \text{j} \\ \bar{X}_i \circ \bar{Z}_j = -1 \text{ for i} = \text{j} \end{cases}$$

By implying the method of Gaussian elimination, we can convert the parity-check matrix into its standard form as follows:

$$\begin{bmatrix} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & I & E \end{bmatrix} \tag{4}$$

The general standard form of logical operators is

$$\begin{cases} \bar{X} = \begin{bmatrix} 0 & E^T & I & (E^T C_1 + C_2{}^T) & 0 & 0 \end{bmatrix} \\ \bar{Z} = \begin{bmatrix} 0 & 0 & 0 & A_2{}^T & 0 & I \end{bmatrix} \end{cases}. \tag{5}$$

Consequently, the codeword of the QSC are written as [14],

$$|c_1 c_2 \ldots c_k\rangle = \frac{1}{\sqrt{2^m}} \times \left(\prod_{i=1}^{m} (I + s_i) \right) \times \bar{X}_1^{c_1} \times \bar{X}_2^{c_2} \times \ldots \times \bar{X}_k^{c_k} |00_{\ldots}0\rangle_n, \tag{6}$$

where $c_i \in \{0,1\}$.

The following theorem helps us in verifying the commutative property for stabilizer generators constructed in the proposed scheme.

IV. PROPOSED SCHEME

For a Hadamard Difference set D, the multiplication of two CP matrices can be represented in terms of parameter of HDS and the shifted HDS in the following theorem.

Theorem 1:

Let $h_{p_1}(x)$ and $h_{p_2}(x)$ are the two hall polynomials (h-polynomials) with respect of shifted HDS $D+t_1$ and $D+t_2$ which can be defined as $h_{p_1}(x) = p_n{}^{D+t_1}$ and $h_{p_2}(x) = p_n{}^{D+t_2}$ respectively. And, let CP matrices H_X and H_Z be in correspondence to $h_{p_1}(x)$ and $h_{p_2}(x)$ respectively, then we can write the product of two polynomials $h_{p_1}(x)$, $h_{p_2}(x)^T$ and the product of the two matrices H_X and $H_Z{}^T$ as

$$h_{p_1}(x) \times h_{p_2}(x)^T = (k-\lambda) \times x^{t_1 - t_2} + \lambda \times \sum_{i=0}^{n-1} x^i$$

And,

$$H_X \times H_Z{}^T = (k-\lambda) \times I_n(t_1 - t_2) + \lambda \times J_n$$

where the size of the matrix J_n is $n \times n$ and entries are all 1.

Proof.

Using the h-polynomials, $h_{p_1}(x)$ and $h_{p_2}(x)$ can be represented as

$$h_{p_1}(x) = x^{d_1+t_1} + x^{d_2+t_1} + \ldots + x^{d_k+t_1} \text{ and,}$$

$$h_{p_2}(x) = x^{d_1+t_2} + x^{d_2+t_2} + \ldots + x^{d_k+t_2}.$$

Now,

$$h_{p_1}(x) \times h_{p_2}(x)^T = \left(x^{d_1+t_1} + x^{d_2+t_1} + \ldots + x^{d_k+t_1} \right) \times \left(x^{-d_1-t_2} + x^{-d_2-t_2} + \ldots + x^{-d_k-t_2} \right)$$

$$= \sum_{i=1}^{k} x^{(d_i+t_1)-(d_1+t_2)} + x^{(d_i+t_1)-(d_i+t_2)} + \ldots + x^{(d_i+t_1)-(d_k+t_2)}$$

$$= \sum_{i=1}^{k} x^{t_1-t_2} \left[x^{(d_i-d_1)} + x^{(d_i-d_2)} + \ldots + x^{(d_i-d_k)} \right]$$

$$= \sum_{i=1}^{k} x^{t_1 - t_2} \times \sum_{u=1}^{k} \sum_{v=1}^{k} x^{d_u - d_v}$$

$$= x^{t_1 - t_2} \times \left[k \times x^0 + \sum_{u=1}^{k} \sum_{v=1, v \neq u}^{k} x^{d_u - d_v} \right]$$

We know that

$$\sum_{u=1}^{k} \sum_{v=1, v \neq u}^{k} x^{d_u - d_v} = \lambda \times \sum_{l=1}^{n-1} x^l = \lambda \times \sum_{l=0}^{n-1} x^l - \lambda \times x^0.$$

Hence,

$$h_{p_1}(x) \times h_{p_2}(x)^T$$

$$= x^{t_1 - t_2} \times \left[k \times x^0 + \sum_{u=1}^{k} \sum_{v=1, v \neq u}^{k} x^{d_u - d_v} \right]$$

$$= \lambda \times \sum_{l=0}^{n-1} x^l - \lambda \times x^0.$$

$$= (k - \lambda) \times x^{t_1 - t_2} + \lambda \times x^{t_1 - t_2} \times \sum_{l=0}^{n-1} x^l$$

$$= (k - \lambda) \times x^{t_1 - t_2} + \lambda \times \sum_{l=0}^{n-1} x^l \quad (7)$$

Also we know that the corresponding CP matrices to the polynomials $x^{t_1 - t_2}$ and $\sum_{l=0}^{n-1} x^l$ are $\mathrm{I}_n(t_1 - t_2)$ and J_n respectively, Therefore,

$$H_X \times H_Z^T = (k - \lambda) \times \mathrm{I}_n(t_1 - t_2) + \lambda \times \mathrm{J}_n. \quad (8)$$

Now, we can see that the product of H_X and H_Z^T in Theorem 1 is a function of k, λ, t_1 and t_2. Therefore, theorem below explains the constraint on HDS parameters needed to satisfy the SIP condition of the parity-check matrix.

Theorem 2:

For a given HDS D whose parameters are $(\mathrm{n}, \mathrm{k}, \lambda) = (4m^2, 2m^2 - m, m^2 - m)$ and any elements t_1, t_2 where $t_1 \neq t_2$, the parity check matrix derived from $H = [H_X \mid H_Z]$ where H_X and H_Z are the matrix corresponding to $h_{p_1}(x) = p_n^{D+t_1}$ and $h_{p_2}(x) = p_n^{D+t_2}$ respectively satisfies the SIP constraint.

Proof.

By using the above theorem, we get

$$H_X \times H_Z^T = (k - \lambda) \times I_n(t_1 - t_2) + \lambda \times J_n \quad (9)$$

$$H_Z \times H_X^T = (k - \lambda) \times I_n(t_2 - t_1) + \lambda \times J_n \quad (10)$$

Using (9) and (10), we can express,

$$H_X \times H_Z^T + H_Z \times H_X^T = (k - \lambda) \times I_n(t_1 - t_2) + \lambda \times J_n$$

$$+ (k - \lambda) \times I_n(t_2 - t_1) + \lambda \times J_n$$

$$= (k - \lambda) \times \left[I_n(t_1 - t_2) + I_n(t_2 - t_1) \right] + 2\lambda \times J_n \quad (11)$$

According to the HDS parameters $n = 4m^2$, $k = 2m^2 - m$ and $\lambda = m^2 - m$ so,

$$k - \lambda = (2m^2 - m) - (m^2 - m) = m^2$$

If m is even then $k - \lambda$ is also even and every element of $(k - \lambda) \times \left[I_n(t_1 - t_2) + I_n(t_2 - t_1) \right]$ in (11) is even. In addition, every element of the matrix $2\lambda \times J_n$ in (11) are also even. Therefore, every element of the matrix in (11) are even. Hence,

$$H_X \times H_Z^T + H_Z \times H_X^T = 0_n \bmod 2.$$

Thus, the parity-check matrices corresponding to the HDS $(4m^2, 2m^2 - m, m^2 - m)$ where m is an even number satisfies the SIP constraint (2.4).

A. Construction of QSCs using HDS.

Firstly, we shall make a difference set from HDS parameters which is $(\mathrm{n}, \mathrm{k}, \lambda) = (4m^2, 2m^2 - m, m^2 - m)$ and must satisfy the condition $\lambda(n\text{-}1) = k(k\text{-}1)$. After proving this to be a HDS, we will construct an incidence matrix with the help of the HDS and hall polynomial. The parity-check matrix has 1 as the (i, j) entry if and only if $g_j - g_i \in D$, otherwise the element will be 0. Now, the parity-check matrix obtained must satisfy the SIP constraint (2.4) in order to hold the commutative condition for Stabilizer operators. Later, with the use of Gaussian elimination, we find linearly independent rows to construct logical operators and codeword of the stabilizer code described in equation (5) and (6) respectively.

Example 1:

The HDS parameters are $(4m^2, 2m^2 - m, m^2 - m)$. For $m = 2$, the HDS obtained is $(16, 6, 2)$. Now, we construct an abelian and non-cyclic difference set with the group denoted by $\mathrm{G} = \langle a, b \mid \mathrm{a}^8 = b^2 = 1 \rangle$ i.e., $G = \mathbb{Z}_2 \times \mathbb{Z}_8$

$$G = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),$$
$$(1,0),(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(1,7)\}$$

and $D = \{(0,0),(0,1),(0,2),(0,4),(1,1),(1,6)\}$ be a subset of the group $\mathbb{Z}_2 \times \mathbb{Z}_8$. It can be easily verified that each element of the group G can be written as difference of two elements of the subset D. Therefore, the subset D forms a Hadamard difference set with parameter $(16, 6, 2)$. Then, two shifted HDS are given as

$D + (0,3) = \{(0,3),(0,4),(0,5),(0,7),(1,1),(1,4)\}$ and

$D + (0,5) = \{(0,1),(0,5),(0,6),(0,7),(1,3),(1,6)\}$.

Therefore, the h-polynomials for $D + (0,3)$ and $D + (0,5)$ are

$h_{p_1}(x) = p_{16}^{D+(0,3)} = x^4 + x^5 + x^6 + x^8 + x^{10} + x^{13}$ and

$h_{p_2}(x) = p_{16}^{D+(0,5)} = x^2 + x^6 + x^7 + x^8 + x^{12} + x^{15}$ respectively.

As mentioned in subsection *A* of section IV, let the binary parity-check matrices using HDS be H_X and H_Z for $h_{p_1}(x)$ and $h_{p_2}(x)$ respectively, which can be easily obtained using HDS since, the parity-check matrix has 1 as the (i, j) entry if and only if $g_j - g_i \in D$, otherwise the element will be 0. So, the corresponding matrices are

$$H_X = \begin{bmatrix} 1&0&0&0&0&0&0&1&1&1&0&1&0&1&0&0\\ 0&1&0&0&0&0&0&0&1&1&1&0&1&0&1&0\\ 0&0&1&0&0&0&0&0&0&1&1&1&0&1&0&1\\ 1&0&0&1&0&0&0&0&0&0&1&1&1&0&1&0\\ 0&1&0&0&1&0&0&0&0&0&0&1&1&1&0&1\\ 1&0&1&0&0&1&0&0&0&0&0&0&1&1&1&0\\ 0&1&0&1&0&0&1&0&0&0&0&0&0&1&1&1\\ 1&0&1&0&1&0&0&1&0&0&0&0&0&0&1&1\\ 1&1&0&1&0&1&0&0&1&0&0&0&0&0&0&1\\ 1&1&1&0&1&0&1&0&0&1&0&0&0&0&0&0\\ 0&1&1&1&0&1&0&1&0&0&1&0&0&0&0&0\\ 0&0&1&1&1&0&1&0&1&0&0&1&0&0&0&0\\ 0&0&0&1&1&1&0&1&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&1&1&0&1&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&1&1&0&1&0&1&0&0&1&0\\ 0&0&0&0&0&0&1&1&1&0&1&0&1&0&0&1 \end{bmatrix}$$

and,

$$H_Z = \begin{bmatrix} 0&0&1&0&0&1&0&0&0&1&1&1&0&0&0&1\\ 1&0&0&1&0&0&1&0&0&0&1&1&1&0&0&0\\ 0&1&0&0&1&0&0&1&0&0&0&1&1&1&0&0\\ 0&0&1&0&0&1&0&0&1&0&0&0&1&1&1&0\\ 0&0&0&1&0&0&1&0&0&1&0&0&0&1&1&1\\ 1&0&0&0&1&0&0&1&0&0&1&0&0&0&1&1\\ 1&1&0&0&0&1&0&0&1&0&0&1&0&0&0&1\\ 1&1&1&0&0&0&1&0&0&1&0&0&1&0&0&0\\ 0&1&1&1&0&0&0&1&0&0&1&0&0&1&0&0\\ 0&0&1&1&1&0&0&0&1&0&0&1&0&0&1&0\\ 0&0&0&1&1&1&0&0&0&1&0&0&1&0&0&1\\ 1&0&0&0&1&1&1&0&0&0&1&0&0&1&0&0\\ 0&1&0&0&0&1&1&1&0&0&0&1&0&0&1&0\\ 0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&1\\ 1&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0\\ 0&1&0&0&1&0&0&0&1&1&1&0&0&0&1&0 \end{bmatrix}$$

The parity check matrix is given as

$$H = \left[H_X \,|\, H_Z \right] \qquad (12)$$

It can be easily seen that $H_X \times {H_Z}^T + H_Z \times {H_X}^T = 0_{16}$. Therefore, the parity-check matrices H_X and H_Z satisfies the SIP constraint. The sixteen stabilizer operators related to the sixteen rows in (8) are given as

$$\partial_1 = XIZIIZIXXYZYIXIZ\ ;$$
$$\partial_2 = ZXIZIIZIXXYZYIXI\ ;$$
$$\partial_3 = IZXIZIIZIXXYZYIX\ ;$$
$$\partial_4 = XIZXIZIIZIXXYZYI\ ;$$
$$\partial_5 = IXIZXIZIIZIXXYZY\ ;$$
$$\partial_6 = YIXIZXIZIIZIXXYZ\ ;$$
$$\partial_7 = ZYIXIZXIZIIZIXXY\ ;$$
$$\partial_8 = YZYIXIZXIZIIZIXX\ ;$$
$$\partial_9 = XYZYIXIZXIZIIZIX\ ;$$
$$\partial_{10} = XXYZYIXIZXIZIIZI\ ;$$
$$\partial_{11} = IXXYZYIXIZXIZIIZ\ ;$$
$$\partial_{12} = ZIXXYZYIXIZXIZII\ ;$$
$$\partial_{13} = IZIXXYZYIXIZXIZI\ ;$$
$$\partial_{14} = IIZIXXYZYIXIZXIZ\ ;$$
$$\partial_{15} = ZIIZIXXYZYIXIZXI\ ;$$
$$\partial_{16} = IZIIZIXXYZYIXIZX\ ;$$

In all these sixteen generators, there are only ten linearly independent operators which are

$$\partial_1 = XIZIIZIXXYZYIXIZ\ ;$$
$$\partial_2 = ZXIZIIZIXXYZYIXI\ ;$$
$$\partial_3 = IZXIZIIZIXXYZYIX\ ;$$
$$\partial_4 = XIZXIZIIZIXXYZYI\ ;$$
$$\partial_5 = IXIZXIZIIZIXXYZY\ ;$$
$$\partial_6 = YIXIZXIZIIZIXXYZ\ ;$$
$$\partial_7 = ZYIXIZXIZIIZIXXY\ ;$$
$$\partial_8 = YZYIXIZXIZIIZIXX\ ;$$
$$\partial_9 = XYZYIXIZXIZIIZIX\ ;$$
$$\partial_{10} = XXYZYIXIZXIZIIZI\ ;$$

Other stabilizer operators can be formed by using these linearly independent operators $\partial_1, \partial_2, \partial_3, \partial_4, \partial_5, \partial_6, \partial_7, \partial_8, \partial_9, \partial_{10}$. Therefore, the stabilizer group is,

$$S = \left\{ \partial_1, \partial_2, \partial_3, \partial_4, \partial_5, \partial_6, \partial_7, \partial_8, \partial_9, \partial_{10}, \partial_{11}, \partial_{12}, \partial_{13}, \partial_{14}, \partial_{15}, \partial_{16} \right\}$$

And it is generated by

$$S = \left\langle \partial_1, \partial_2, \partial_3, \partial_4, \partial_5, \partial_6, \partial_7, \partial_8, \partial_9, \partial_{10} \right\rangle$$

Using equation (3), the matrix H can be transformed into its standard form

$$H = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&0\\ 0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&1&0\\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&1\\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0\\ 0&1&0&1&0&0&1&0&0&0&0&0&0&1&1&1&1&1&0\\ 1&0&1&0&1&0&0&1&0&0&0&0&0&0&1&1&1&1&1\\ 1&1&0&1&0&1&0&0&1&0&0&0&0&0&0&1&0&1&1\\ 1&1&1&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&1\\ 0&1&1&1&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0\\ 1&0&1&0&0&1&0&0&0&0&0&0&1&1&1&0&1&0&0 \end{bmatrix}$$

$$\cdots \begin{bmatrix} 0&0&1&1&1&1&0&1&0&1&1&0&1\\ 0&0&0&1&1&1&1&0&1&0&1&1&0\\ 0&0&1&1&0&0&1&0&0&0&1&1&0\\ 0&0&0&1&1&0&0&1&0&0&0&1&1\\ 1&0&0&0&1&1&0&0&1&0&0&0&1\\ 0&1&0&0&0&1&1&0&0&1&0&0&0\\ 0&0&1&0&0&0&1&1&0&0&1&0&0\\ 1&0&0&1&0&0&0&1&1&0&0&1&0\\ 1&1&1&1&0&1&0&1&1&0&1&0&0\\ 0&1&1&1&1&0&1&0&1&1&0&1&0\\ 0&0&1&0&0&1&0&0&1&0&0&0&1\\ 0&0&0&1&0&0&1&0&0&1&0&0&0\\ 1&0&0&0&1&0&0&1&0&0&1&0&0\\ 1&1&0&0&0&1&0&0&1&0&0&1&0\\ 1&1&1&0&0&0&1&0&0&1&0&0&1\\ 0&1&0&0&1&0&0&1&0&0&0&1&1 \end{bmatrix}_{16\times 32}$$

and its logical operators $\bar{X}$ and $\bar{Z}$ can be obtained by using the method of Gaussian elimination defined in (5).

$$\bar{X}=\begin{bmatrix}
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

$$\cdots\begin{bmatrix}
1&0&0&1&1&1&0&0&0&0&0&0&0\\
0&1&0&0&1&1&1&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}_{10\times 32},$$

$$\bar{Z}=\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

$$\cdots\begin{bmatrix}
0&0&0&0&0&1&0&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&1&0&1&0&0&0&0&0&1&0\\
0&0&0&0&1&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}_{10\times 32}$$

where $\bar{X}_i$ and $\bar{Z}_i$ are the corresponding row vectors of the logical operator $\bar{X}$ and $\bar{Z}$ respectively, given as

$$\bar{X}_1 = ZIIZIIZZZIXIIIII$$
$$\bar{X}_2 = IZIIZIIZZZIXIIII$$
$$\bar{X}_3 = ZIIIIZIIIZIIXIII$$
$$\bar{X}_4 = ZZZIIIZIZIIIIXII$$
$$\bar{X}_5 = IZZZIIIZIZIIIIXI$$
$$\bar{X}_6 = ZIIZZIIIIIIIIIX$$

and,

$$\bar{Z}_1 = ZIZIIIIIZIZIIIII$$
$$\bar{Z}_2 = IZIZIIIIIIIZIIII$$
$$\bar{Z}_3 = ZIIIZIIIZIIIZIII$$
$$\bar{Z}_4 = IZIIIZIIIZIIIZII$$
$$\bar{Z}_5 = ZIIIIIZIZIIIIIZI$$
$$\bar{Z}_6 = IZIIIIIZIZIIIIIZ$$

The codewords of the QSC $[[16,6]]$ are described as,

$$\left|c_1c_2c_3c_4c_5c_6\right\rangle = \frac{1}{\sqrt{2^{10}}}\times\left(\prod_{i=1}^{10}\left(I+\partial_i\right)\right)\times$$
$$\bar{X}_1^{c_1}\times\bar{X}_2^{c_2}\times\bar{X}_3^{c_3}\times\bar{X}_4^{c_4}\times\bar{X}_5^{c_5}\times\bar{X}_6^{c_6}\left|0_10_{2\ldots}0_{16}\right\rangle$$

where $\prod_{i=1}^{10}\left(I+\partial_i\right)=\sum_{o\in S}\partial$ and $c_i\in\{0,1\}$.

From the smallest weight of the operators in $N(S)/S$, the minimum distance $d_{\min}$ of the $[[16,6]]$ code is calculated. Among the logical operators, the smallest weight is $\bar{Z}_2\times IIIIIIIIIIIIII$ as $W\left(\bar{Z}_2\times IIIIIIIIIIIIII\right)=3$, so Therefore, the QSC from the DS with parameters $(16,6,2)$ is $[[16,6,3]]$.

V. PERFORMANCE AND COMPARISON

In this section, the results for the simulation of the constructed HDS codes are provided. The qubit error rate (QBER) which refers to the probability that a single quantum bit, or qubit, undergoes an error during a quantum computation or quantum communication process. This error can result from various sources, such as environmental noise, imperfect gates, or interactions with nearby qubits [48],[49],[50]. Classical cyclic codes are typically decoded with the help of majority-logic decoder to decrease the decoding complexity, which is a hard-decision decoding algorithm. Since, the HDS codes are constructed by CPM, majority-logic decoding [51],[52] is being performed on the proposed codes in Qiskit. The program uses the QASM simulator backend to run the quantum circuit. It adds a depolarizing error channel to simulate noise in the system. This decoding method is implemented for simulation-speed issues for the relative performances of the codes. Simulations is performed on the depolarizing channel which creates the X, Y and Z errors simultaneously with same probability $f/3$. In this simulation, to further decrease the complexity of the decoder side, an approximation of marginal flip probability $2f/3$ has been executed on each received qubit. On the basis of the proposed construction of HDS code, the performance of the constructed code is observed with 1000 shots. The relative performance of the HDS code $[[16,6,3]]$ is calculated as a function of block length, see Fig. 3. QBER is remarkably low as the size of the block decreases. One of the possible reasons for this is that the distance property of the QSCs obtained from DS is unrelated to the block size of the code, but is related to the size of the difference set. For comparison, we see that parameter constraint for DS in the proposed construction are different from [53]. Since,

$2p-1 \cong p-1 (\mathrm{mod}\, 2)$, where p is even. HDS used in the proposed construction cannot be obtained from [53], because $4p-1$ must be a prime number.

Additionally, for the purpose of comparison, we integrated existed quantum code with length 16, i.e., $[[16,6,4]]$ from [54] and $[[16,10,3]]$ from [15] into our decoder with depolarizing probability '$p=0.4$'. The key observation from Fig. 4 is that the performance of the proposed code $[[16,6,3]]$ is comparable with our closely related $[[16,6,4]]$ quantum code. Here, $[[16,6,4]]$ provides the highest error correction capability but require more physical qubits, $[[16,6,3]]$ offers moderate error correction with fewer physical qubits required and $[[16,10,3]]$ maximizes the encoding rate but sacrifices error correction capabilities.

TABLE 2. Comparison of the proposed method with Xie et al. [53]

Xie et al.'s construction	Proposed construction
Difference set with parameters $(4p-1, 2p-1, p-1)$ are utilized, where p is even and $4p-1$ is prime.	Difference set with parameters $\left(4m^2, 2m^2-m, m^2-m\right)$, $m \in \mathbb{Z}^+$ are utilized.
Difference sets are cyclic in nature.	Difference sets are non-cyclic in nature.
Length of the QSCs must be a prime number.	Length of the QSCs does not need to be a prime number.
Less number of QSCs covered.	Large number of QSCs covered with greater length.
Ex.- $[[7,3,1]]$ and $[[23,11,5]]$	Ex.- $[[16,6,3]]$ and $[[36,15,6]]$

VI. CONCLUSION

A non-cyclic QSC is proposed handling a new construction method in which HDSs over binary operation is utilised. These codes, which were developed using the general SIP condition in place of the unique CSS type, offer a variety of rates and lengths. The condition of a DS to satisfy the SIP constraint is identical to determine an HDS with parameter $\left(4m^2, 2m^2-m, m^2-m\right), m \in \mathbb{Z}^+$. QSC $[[16,6,3]]$ acquired from the proposed construction with HDS $(16,6,2)$ for practical application. The construction method yields dimensions for larger length of QSCs and illustrates enhanced error correction. The results of the performance indicate that the suggested codes are more capable of rectification and can accommodate a variety of dimensions. Quantum stabilizer codes originating from non-cyclic HDS are at the forefront of quantum information theory, presenting both challenges and remarkable capabilities. The difficulties lie in effectively managing error correction overhead, countering the effects of decoherence and noise, ensuring scalability, and addressing experimental obstacles. Correcting errors in quantum systems often demands extra qubits and computational resources, while environmental factors like decoherence and noise pose threats to the reliability of quantum computations. Moreover, as quantum computers expand in size, achieving fault tolerance and reliability becomes increasingly complex, requiring scalable error correction methods and precise experimental setups. However, alongside these challenges come notable advantages. Stabilizer codes derived from non-cyclic HDS provide enhanced error correction capabilities, empowering fault-tolerant quantum computing architectures resilient to environmental disturbances. They also fortify the security of quantum communication protocols, safeguarding the confidentiality and integrity of transmitted quantum data. Furthermore, these codes pave the way for novel avenues in quantum information processing, facilitating advancements in quantum computation, communication, and cryptography. Despite the obstacles, leveraging the unique capabilities of these codes holds the promise of revolutionizing quantum technologies, unlocking their full potential for practical applications.

VII. FUTURE WORK

An extension to this work can be to find the QSCs over quasi difference sets and to find the orthogonal codes of the above codes with different applications of these codes. Moreover, QSCs from HDS could focus on optimizing algorithms for code design, improving experimental realization techniques, exploring hybrid error correction schemes.

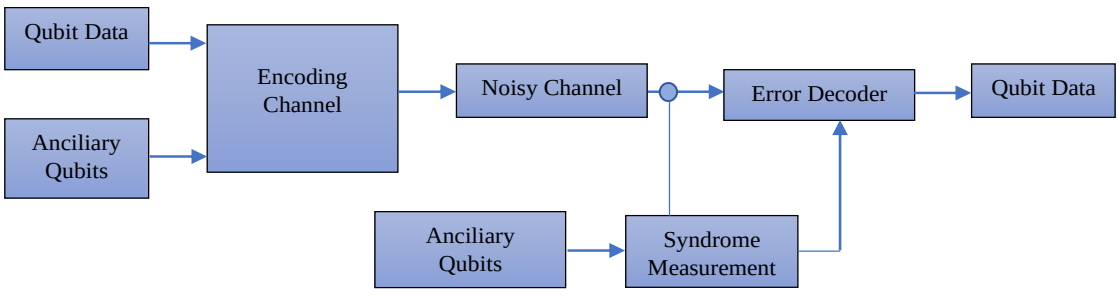

Fig. 1. Process of Quantum error correction.

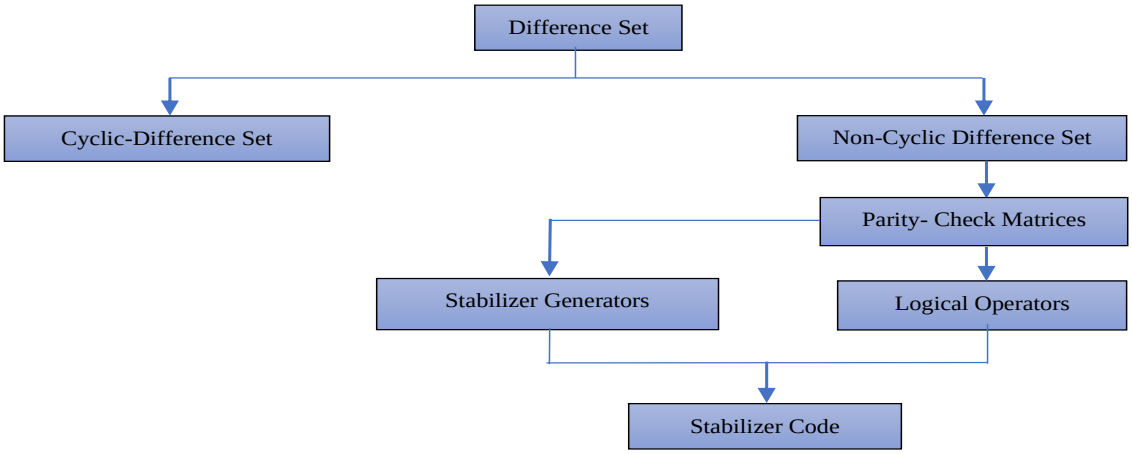

Fig. 2. Flowchart of the Proposed Method

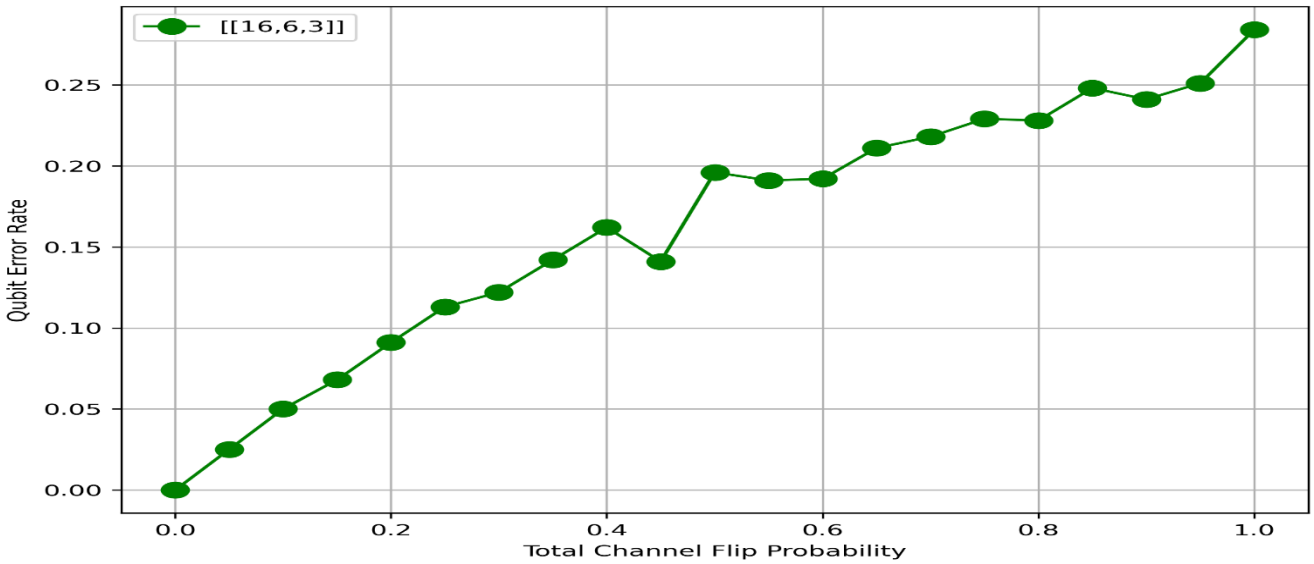

Fig. 3. Performance of HDS code obtained from the proposed method

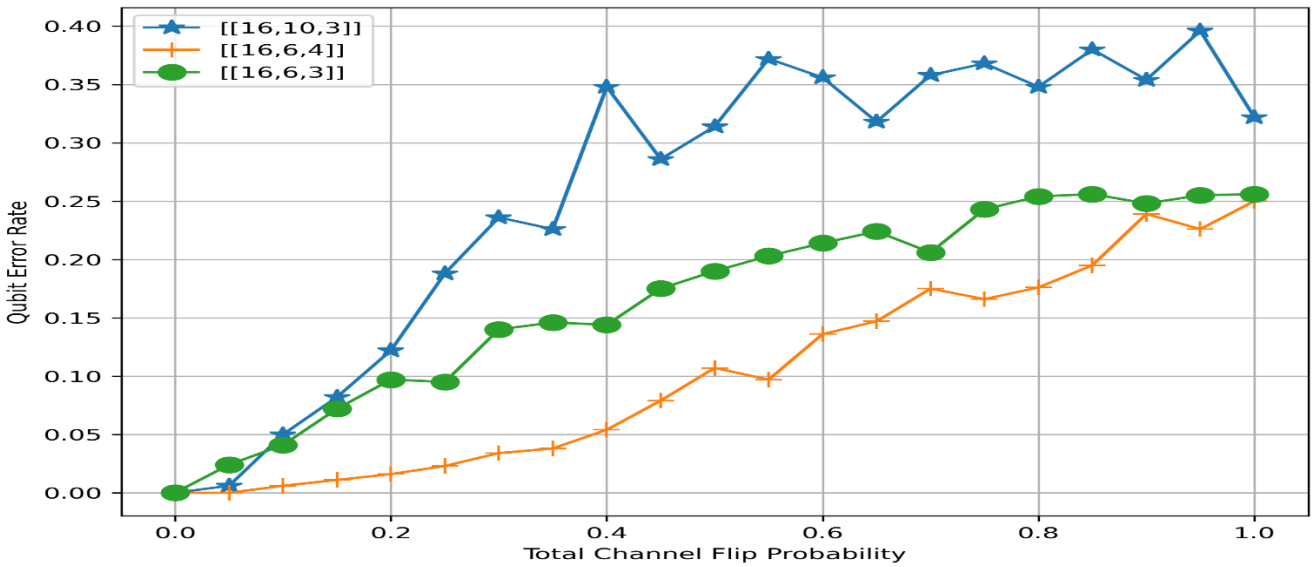

Fig. 4. Comparison of different quantum stabilizer codes with depolarizing probability $p = 0.4$

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134.

[2] D. M. Nguyen and S. Kim, "Quantum key distribution protocol based on modified generalization of Deutsch-Jozsa algorithm in d-level quantum system," *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 71-82, 2019.

[3] A. Rathor, M. Kumar, R. K. Mishra, S. Goswami, and A. Chaudhary, "Enhanced Performance of Isogenies Over Huff Curve for Post Quantum Cryptography," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 6, pp. 445-457, 2023.

[4] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, p. R2493, 1995.

[5] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, p. 793, 1996.

[6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, p. 1098, 1996.

[7] M. Cao and J. Cui, "Construction of new quantum codes via Hermitian dual-containing matrix-product codes," *Quantum Information Processing*, vol. 19, pp. 1-26, 2020.

[8] H. Song, R. Li, Y. Liu, and G. Guo, "New quantum codes from matrix-product codes over small fields," *Quantum Information Processing*, vol. 19, pp. 1-22, 2020.

[9] K. Noh and C. Chamberland, "Fault-tolerant bosonic quantum error correction with the surface–Gottesman-Kitaev-Preskill code," *Physical Review A*, vol. 101, p. 012316, 2020.

[10] I. Convy, H. Liao, S. Zhang, S. Patel, W. Livingston, H. N. Nguyen, et al., "Machine learning for continuous quantum error correction on superconducting qubits," *New Journal of Physics*, 2022.

[11] S. Borah, B. Sarma, M. Kewming, F. Quijandria, G. J. Milburn, and J. Twamley, "Measurement-based estimator scheme for continuous quantum error correction," *Quantum Information Processing*, vol. 19, pp. 1-22, 2020.

[12] T. Matsuura, S. Yamano, Y. Kuramochi, T. Sasaki, and M. Koashi, "Refined finite-size analysis of binary-modulation continuous-variable quantum key distribution," *Quantum Information Processing*, vol. 19, pp. 1-22, 2020.

[13] S. Ball, "Some constructions of quantum MDS codes," *Designs, Codes and Cryptography*, vol. 89, pp. 811-821, 2021.

[14] H. Liu and X. Liu, "Constructions of quantum MDS codes," *Quantum Information Processing*, vol. 20, pp. 1-13, 2021.

[15] D. Gottesman, "Stabilizer codes and quantum error correction," Doctoral dissertation, California Institute of Technology, 1997.

[16] D. M. Nguyen and S. Kim, "Minimal-entanglement entanglement-assisted quantum error correction codes from modified circulant matrices," *Symmetry*, vol. 9, p. 122, 2017.

[17] Zhongfeng Li, Yingxin Wei, and Lidong Wang, "Active Event-Triggered Fault-Tolerant Control Design for Switched Pure-Feedback Nonlinear Systems," Engineering Letters, vol. 31, no.3, pp896-905, 2023

[18] D. M. Nguyen and S. Kim, "Construction and complement circuit of a quantum stabilizer code with length 7," in *Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2016, pp. 332-336.

[19] M. Grassl and T. Beth, "Quantum BCH codes," in *Proceedings X. International Symposium on Theoretical Electrical Engineering*, Magdeburg, 1999, pp. 207-212. arXiv preprint quant-ph/9910060, 1999.

[20] M. Grassl, W. Geiselmann, and T. Beth, "Quantum reed—solomon codes," in *International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer, 1999, pp. 231-244.

[21] Yung-Ning Cheng, and Kou-Huang Chen, "Study for Contradictory Pairwise Comparison Matrices," IAENG International Journal of Applied Mathematics, vol. 53, no.3, pp1138-1147, 2023

[22] A. A. De Almeida and R. Palazzo, "A concatenated [(4, 1, 3)] quantum convolutional code," *Information Theory Workshop, IEEE*, 2004, pp. 28-33.

[23] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, pp. 865-880, 2007.

[24] Ren Guo-Xi, "Research on a Convolutional Neural Network Method for Modulation Waveform Classification," IAENG International Journal of Computer Science, vol. 50, no.3, pp875-882, 2023

[25] M. S. Postol, "A proposed quantum low density parity check code," arXiv preprint quant-ph/0108131, 2001.

[26] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, pp. 2315-2330, 2004.

[27] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low-density generator matrix over different quantum channels," in *4th International Symposium on Turbo Codes & Related Topics; 6th International ITG-Conference on Source and Channel Coding*, 2006, pp. 1-6.

[28] T. Camara, H. Ollivier, and J. P. Tillich, "Constructions and performance of classes of quantum LDPC codes," arXiv preprint quant-ph/0502086.

[29] V. Aggarwal and A. R. Calderbank, "Boolean functions, projection operators, and quantum error correcting codes," *IEEE Transactions on Information Theory*, vol. 54, pp. 1700-1707, 2008.

[30] Mohammad Ivan Azis, "A Computational Study on Unsteady Anisotropic Helmholtz Type Equation of Quadratically Varying Coefficients," IAENG International Journal of Applied Mathematics, vol. 53, no.3, pp826-832, 2023

[31] M. Ashraf, N. Khan, and G. Mohammad, "Quantum codes from constacyclic codes over a semi-local ring," *Reports on Mathematical Physics*, vol. 90, pp. 271-284, 2022.

[32] C. Galindo, F. Hernando, H. Martín-Cruz, and D. Ruano, "Stabilizer quantum codes defined by trace-depending polynomials," *Finite Fields and Their Applications*, vol. 87, p. 102138, 2023.

[33] C. Galindo and F. Hernando, "On the generalization of the construction of quantum codes from Hermitian self-orthogonal codes," *Designs, Codes and Cryptography*, vol. 90, pp. 1103-1112, 2022.

[34] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, pp. 2315-2330, 2004.

[35] L. D. Baumert, Cyclic difference sets, vol. 182, Springer, 2006.

[36] I. Anderson, Combinatorial designs: construction methods, John Wiley & Sons, 1990.

[37] T. Beth, D. Jungnickel, and H. Lenz, Design Theory: Vol. 1, Cambridge University Press, 1999.

[38] K. W. Smith, "Non-abelian Hadamard difference sets," *Journal of Combinatorial Theory*, Series A, vol. 70, 1995, pp. 144-156.

[39] J. F. Dillon, "Variations on a scheme of McFarland for noncyclic difference sets," *Journal of Combinatorial Theory*, Series A, vol. 40, pp. 9-21, 1985.

[40] E. S. Lander, Symmetric designs: an algebraic approach, Cambridge University Press, Vol. 74, 1983.

[41] E. F. Assmus Jr and C. J. Salwach, "The (16, 16, 2) designs," *International Journal of Mathematics and Mathematical Sciences*, vol. 2, pp. 261-281, 1979.

[42] R. E. Kibler, "A summary of noncyclic difference sets, k< 20," *Journal of Combinatorial Theory*, Series A, vol. 25, pp. 62-67, 1978.

[43] N. D. R. Mishu, F. I. Meem, A. E. Ridwan, M. M. Rahman, and M. M. Mary, "Quantum error correction using quantum convolutional neural network," Doctoral dissertation, Brac University, 2021.

[44] M. Cao and F. Wei, "Construction of some new entanglement-assisted quantum error-correcting codes of large lengths," *Discrete Mathematics*, vol. 347, no. 6, p. 113969, 2024.

[45] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A*, vol. 54, p. 1844, 1996.

[46] Hardeep, M. Kumar, and R. K. Mishra, "Sharing of information using bi-qutrit quantum states based on bivariate quantum gates," *Journal of Xi'an Shiyou University*, Natural Sciences Edition, vol. 64, no. 12, pp. 91-101, 2021.

[47] M. Kumar, M. K. Gupta, R. K. Mishra, S. S. Dubey, A. Kumar, and Hardeep, "Security Analysis of a Threshold Quantum State Sharing Scheme of an Arbitrary Single-Qutrit Based on Lagrange Interpolation Method," in Evolving Technologies for Computing, *Communication and Smart World*, Lecture Notes in Electrical Engineering, vol. 694, pp. 373-389, 2020.

[48] Septia Devi Prihastuti Yasmirullah, Bambang Widjanarko Otok, Jerry Dwi Trijoyo Purnomo, and Dedy Dwi Prastyo, "Parameter Estimation of Spatial Error Model -Multivariate Adaptive Generalized Poisson Regression Spline," Engineering Letters, vol. 31, no.3, pp1265-1272, 2023

[49] Q. Guo, Y. Y. Zhao, M. Grassl, X. Nie, G. Y. Xiang, T. Xin, Z. Q. Yin, and B. Zeng, "Testing a quantum error-correcting code on various platforms," *Science Bulletin*, vol. 66, no. 1, pp. 29-35, 2021.
[50] M. Khairudin, R. Mahaputra, M. Luthfi Hakim, Asri Widowati, B Rahmatullah, and A. A. M. Faudzi, "Choosing the Quality of Two Dimension Objects by Comparing Edge Detection Methods and Error Analysis," IAENG International Journal of Computer Science, vol. 50, no.3, pp960-969, 2023
[51] W. Ryan and S. Lin, Channel codes: classical and modern, Cambridge University Press, 2009.
[52] S. Lin and D. J. Costello Jr, Error control coding, Library of Congress, 1983.
[53] Y. Xie, J. Yuan, and R. Malaney, "Quantum stabilizer codes from difference sets," in *IEEE International Symposium on Information Theory, IEEE, 2013*, pp. 524-528.
[54] P. Hu and X. Liu, "Quantum error-correcting codes from the quantum construction X," *Quantum Information Processing*, vol. 22, no. 10, p. 366, 2023.

Shivender Goswami is a candidate of Ph.D. degree at Gurukula Kangri University. He obtained his B.Sc. (Hons.) degree in Mathematics from University of Delhi in 2016. Then he received his degree of Master of Science in Mathematics from Chaudhary Charan Singh University, Meerut in 2018. Besides, he qualified the NET (National Eligibility Test) in 2019. His research direction is Quantum error correction codes.

Manoj Kumar is an associate professor & Head of the department of Mathematics and Statistics, at Gurukula Kangri University. He obtained his B. Sc. Degree in Physics, Chemistry and Mathematics from Chaudhary Charan Singh University in 1998. Then he received M.Sc. degree in Mathematics from Chaudhary Charan Singh University in 2000. Besides, he qualified the CSIR-NET (National Eligibility Test) in 2001. Later in 2002, he completed his degree of Master of Philosophy in Mathematics from Chaudhary Charan Singh University. Further, he was awarded for the Ph.D. Degree in Mathematics by Chaudhary Charan Singh University in 2007. He has more than 20 years of teaching as well as research experience. His areas of research interest are Cryptography and Network Security, Elliptic Curve Cryptography, Quantum Cryptography and Isogeny Based Cryptography. He has been published more than 25 research papers in his research fields.

R.K. Mishra is a Professor & Head of the department in Applied Science and Humanities at GL Bajaj Institute of Technology & Management. He obtained his B.Sc. degree in Physics, Chemistry and Mathematics from MJP Rohilkhand University in 1991. Then he received his M.Sc. degree in Mathematics from MJP Rohilkhand University in 1993. Besides, he awarded his Ph.D. degree in Mathematics from MJP Rohilkhand University in 1998. He has more than 30 years of teaching as well as research experience. His major areas of research interest are Cryptography and Network Security and Approximation Theory. He has been published more than 30 research papers in these research areas.

Akash Rathor is a candidate of Ph.D. degree at Gurukula Kangri University. He obtained his B.Sc. degree in Physics, Chemistry and Mathematics from Gurukula Kangri University in 2016. Then he received his M.Sc. degree in Mathematics from Gurukula Kangri University in 2018. Besides, he qualified the CSIR-UGC NET (National Eligibility Test) in 2019. His research direction is isogeny-based cryptography.