Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

New Quantum Codes using Monomial Matrix over Hermitian Dual-Containing Matrix Product Codes

Shivender Goswami[1], Manoj Kumar[2*], Akash Rathor[3], Ankit Chaudhary[4], R.K. Mishra[5], Kamal Upreti[6], Pratik Gupta[7]

[1,2,3,4]Department of Mathematics and Statistics, Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India

[5]Department of Applied Science and Humanities, G.L. Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India

[6]School of Sciences, Christ University, Delhi NCR Campus, Ghaziabad, Uttar Pradesh, India

[7]Department of Mathematics, D.A.V Degree College, Lucknow, Uttar Pradesh, India

Email: shivendrgoswami@gmail.com[1], sdmkg1@gmail.com[2*], akashrathor9760@gmail.com[3], aakashdhama2016@gmail.com[4], rkmsit@rediffmail.com[5], kamalupreti1989@gmail.com[6], pratikgupta1810@gmail.com[7]

[*]Corresponding author

Article History:

Received: 10-11-2024

Revised: 13-12-2024

Accepted: 26-01-2025

Abstract:

Quantum error correction (QEC) is beneficial for ensuring reliable quantum computation and communication by addressing the susceptibility of quantum states to errors from decoherence and noise. This study explores the use of Quantum Matrix Product Codes (MPCs) with an emphasis on monomial matrices and Hermitian duals to achieve efficient and robust error correction. We provide a detailed mathematical formulation of MPCs utilizing monomial matrices, emphasizing the importance of Hermitian duals in maintaining code integrity and ensuring effective error correction. The paper proposes a new criterion for utilizing the rank of the generator matrix associated with linear codes established from Hermitian dual-containing (HDC) of the MPCs. Then, using this criterion, a new set of quantum maximum-distance-separable (MDS) codes has been constructed with better code parameters and error-correction potential. For comparison purpose, different codes have been observed alongside with the obtained codes to ascertain the uniqueness and error correction capabilities.

Keywords: Linear codes, Hermitian-dual-containing, Matrix-product codes, Maximum distance separable codes, Monomial matrix.

1. Introduction

The concept of QEC is pivotal in quantum computation and communication, addressing issues like decoherence and quantum noise. Since seminal works [1,2,3], research in quantum codes has flourished, particularly in constructing effective quantum codes. The notable Hermitian construction [4] demonstrates that a linear code having parameters $[[n, 2k - n, \geq d]]_{q^2}$ can be developed from a HDC $[[n, k, d]]_{q^2}$ code. Thus, developing q^2-ary HDC codes is crucial for obtaining q-ary quantum codes [5].

A HDC code ζ is a type of linear code where its Hermitian dual code $\zeta^{\perp_H}$ meets condition given as $\zeta \supseteq \zeta^{\perp_H}$. These quantum codes, introduced in [1], are important for creating high-quality quantum codes. Much research has focused on defining and constructing HDC codes. In [6], The conditions for $\lambda-$constacyclic codes over finite fields to be

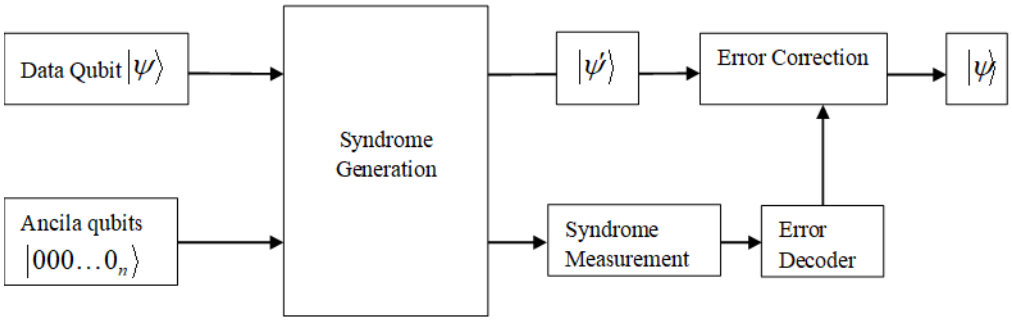

Fig. 1. Process of Quantum error correction using ancila qubits.

HDC is provided and utilizing these conditions, they established several categories of quantum MDS codes. The existence of significant HDC constacyclic codes over finite fields is established in [7]. Recently, the sufficient conditions are provided for pseudo-cyclic codes to be HDC [8]. Additionally, HDC codes have been utilized on finite chain rings. These criteria are generally applicable to constacyclic codes.

Let's now introduce a criterion for an MPC relying on the rank of the generator matrix and exhibit its employment in developing quantum codes. Previous research has developed quantum codes using MPCs over finite fields where the corresponding codes need to be satisfying the condition of dual-containing. However, when the corresponding codes of MPC are not limited, the method to produce quantum codes is unclear.

Recently, exploring matrix-product codes that satisfy Euclidean or HDC conditions has emerged as a new method for constructing high-quality codes for quantum systems. For example, dual-containing matrix-product codes have been obtained from of a novel outlook to derive effective quantum codes from Reed-Muller, hyperbolic, and affine variety codes [10]. In the work [11], Zhang and Ge introduced three novel categories of MDS codes which are obtained using MPCs for Hermitian self-orthogonal codes with a length $2n$ over F_q. Later, Liu et al. proposed two techniques for constructing HDC matrix-product codes, leading to the creation of new quantum codes that surpass previously known ones in performance [12]. Song et al. [13] utilized special code chains $\zeta_1 \subset \zeta_2 \subset \zeta_3$ to develop several $3n$ length quantum codes using Hermitian MPCs of ζ_1, ζ_2 and ζ_3 over F_{r^2}, achieving distances greater than $r+1$. In this paper, we first demonstrate that any matrix-product code can be HDC. We then construct quantum codes using monomial matrices and MPCs. Notably, few quantum codes presented by proposed method are novel, and some possess larger dimensions compared to those found in existing literature. This method stands out due to its use of sophisticated algebraic structures and properties, especially the HDC property. This characteristic ensures that the constructed codes and their duals intersect trivially, which is essential for effective quantum error correction. Additionally,

the use of minimal polynomials allows for precise tuning of code parameters, resulting in highly efficient and robust quantum codes. These features make the method particularly well-suited for practical quantum computing applications, offering scalability and adaptability to different quantum architectures [14, 15]. The incorporation of these algebraic techniques enhances the performance of quantum codes and lays a strong foundation for future developments in theory of quantum error codes [16]. The organisation of the remaining paper is as follows: Section 2 covers the mathematical concepts necessary for understanding the construction of quantum codes from classical HDC codes. Section 3 outlines the proposed construction method, while section 4 provides the conditions for constructing quantum codes. Section 5 discusses the simulation results of the obtained codes, and finally section 6 gives the concluding remarks.

2. Mathematical background

Throughout this paper, take q as a prime power. Let F_{q^2} denote the finite field with q^2 number of elements and suppose $F_{q^2}^*$ denotes the set having nonzero elements from F_{q^2}. Let $a \in F_{q^2}$ be any element then $\bar{a} = a^q$ denotes the conjugate of element a. Let $M(F_{q^2}, s \times l)$ be the collection of matrices over F_{q^2} of size $s \times l$. If $A = (a_{ij}) \in M(F_{q^2}, s \times l)$ then conjugate transpose of A is denoted by $A^\dagger = (\overline{a_{ji}})$.

Consider a code $\zeta = [[n, k, d]]_{q^2}$ which is linear, is a subspace of $F_{q^2}^n$ with length n. The Singleton bound $d \leq n+1-k$, must be satisfied in order for linear code ζ to be maximum distance separable (MDS). Let's denote a q-ary quantum code Q with length n by $[[n, k, d]]_q$ which is of size q^k and minimum distance d. Then, the quantum code Q happens to be a subspace with dimension q^k of ζ^{q^n} which is the q^n-dimensional Hilbert space written as $\zeta^{q^n} \cong \zeta_q \otimes \zeta_q \otimes \cdots \otimes \zeta_q$. The quantum code Q can identify and correct at most $d-1$ and $(d-1)/2$ errors respectively. The quantum Singleton bound $2d \leq n - k + 2$ must be satisfied by the parameters of the quantum code Q. The codes attaining the bound $2d = n - k + 2$, are known as maximum distance separable (MDS) codes. We can define Hermitian inner product of two vectors $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n) \in F_{q^2}^n$ as $(x, y)_H = \sum_{i=1}^{n} x_i \overline{y_i}$. Consider a code ζ of length n which is linear and elements are from F_{q^2}, the Hermitian dual corresponding to the code ζ is written as $\zeta^{\perp_H} = \{a \in F^n_{q^2} \mid (a, b)_H = 0 \text{ for all } b \in \zeta\}$. If $\zeta \supseteq \zeta^{\perp_H}$ then code ζ is termed as HDC. Let a vector $v = (v_1, v_2, ..., v_n) \in F_{q^2}^n$, then we find $v^q = (v_1^q, v_2^q, ..., v_n^q)$. For a given subset S of $F_{q^2}^n$, S^q is defined as the set $\{v^q \mid v \in S\}$.

Let's revisit fundamental concepts related to matrix-product codes [17],[18].

Let $A=(a_{ij})$ denote a matrix of size $s\times l$ with $s\le l$ over F_{q^2} and let $S=\{\zeta_1,\zeta_2,...,\zeta_s\}$ be a family of s linear codes with n as length of each code ζ_i having elements in F_{q^2}. The matrix-product code (MPC) generated by $\zeta_A=[\zeta_1,\zeta_2,...,\zeta_s].A$ which is a code of length nl and contains all MPCs $[c_1,c_2,...,c_s].A$ for some $c_i=(c_{1i},c_{2i},\ldots,c_{ni})^T\in\zeta_i$. Here c_i represents $n\times 1$ column vector for each $i=1,2,...,s.$ Any above defined codeword of the set $\zeta(A)$ is an $n\times l$ matrix written as

$$c=\begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1s} \\ c_{21} & c_{22} & \ldots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{ns} \end{bmatrix}.A$$

$$=\begin{bmatrix} \sum_{i=1}^{s} c_{1i}a_{i1} & \sum_{i=1}^{s} c_{1i}a_{i2} & \ldots & \sum_{i=1}^{s} c_{1i}a_{il} \\ \sum_{i=1}^{s} c_{2i}a_{i1} & \sum_{i=1}^{s} c_{2i}a_{i2} & \ldots & \sum_{i=1}^{s} c_{2i}a_{il} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{s} c_{ni}a_{i1} & \sum_{i=1}^{s} c_{ni}a_{i2} & \ldots & \sum_{i=1}^{s} c_{ni}a_{il} \end{bmatrix}$$

Consider that for each $i=1,2,...,s,$ G_i denotes the generator matrix for the linear code ζ_i then ζ_A is a classical code having the generator matrix given below

$$G_A=\begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \ldots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \ldots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \ldots & a_{sl}G_s \end{bmatrix}.$$

A matrix $A=(a_{ij})_{1\le i,j\le n}$ of size $n\times n$ is called a monomial matrix if the matrix A is non-singular and each row and column possess exactly one non-zero element.

3. Proposed Work

Denote by $A=\left(a_{ij}\right),$ an $s\times s$ matrix where entries belongs to $F^{n}{}_{q^2}$, then we designate $A^q=\left(a_{ij}{}^q\right),$ and then the condition to be HDC for a linear code is outlined below.

Theorem 1: Let ζ gives an $[n,k,d]_{q^2}$ linear code with elements from F_{q^2} and G be the generator matrix of code ζ. Then the code ζ is HDC if and only if $\rho(G(G^q)^T)\le 2k-n,$ where $\rho(A)$ is the number of linearly independent rows of the matrix A.

Proof: Let $G=\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix}$ then $G^q=\begin{bmatrix} a_1{}^q \\ a_2{}^q \\ \vdots \\ a_k{}^q \end{bmatrix}$. Let $H=\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-k} \end{bmatrix}$ be the matrix of parity-check for ζ then ζ satisfies $\zeta^{\perp} \subset \zeta^{(q)}$ if there exists vectors $(l_{11},l_{12},\ldots,l_{1k}), (l_{21},l_{22},\ldots,l_{2k}), \ldots (l_{n-k,1},l_{n-k,2},\ldots,l_{n-k,k}) \in F_{q^2}^k$ such that

$$b_1 = l_{11}a_1^q + l_{12}a_2^q + \ldots + l_{1,k}a_k^q$$
$$b_2 = l_{21}a_1^q + l_{22}a_2^q + \ldots + l_{2,k}a_k^q$$
$$\vdots$$
$$b_{n-k} = l_{n-k,1}a_1^q + l_{n-k,2}a_2^q + \ldots + l_{\mathrm{n-k},k}a_k^q$$

and $n-k \le k.$

Now, $GH^T = 0$ because H is the matrix for parity-check of ζ. That is,

$$GH^T = \begin{bmatrix} a_1b_1^T & a_1b_2^T & \ldots & a_1b_{n-k}^T \\ a_2b_1^T & a_2b_2^T & \ldots & a_2b_{n-k}^T \\ \vdots & \vdots & \ddots & \vdots \\ a_kb_1^T & a_kb_2^T & \ldots & a_kb_{n-k}^T \end{bmatrix} = 0$$

The condition $\zeta^{\perp} \subset \zeta^{(q)}$ holds if and only if $(l_{11},l_{12},\ldots,l_{1k}), (l_{21},l_{22},\ldots,l_{2k}), \ldots (l_{n-k,1},l_{n-k,2},\ldots,l_{n-k,k})$ are solutions of the following system of equations with full rank,

$$\begin{cases} a_1(a_1^q)^T x_1 + a_1(a_2^q)^T x_2 + \ldots + a_1(a_k^q)^T x_k, \\ a_2(a_1^q)^T x_1 + a_2(a_2^q)^T x_2 + \ldots + a_2(a_k^q)^T x_k, \\ \vdots \\ a_k(a_1^q)^T x_1 + a_k(a_2^q)^T x_2 + \ldots + a_k(a_k^q)^T x_k, \end{cases}$$

and, $2k \ge n.$ So, the code ζ satisfies the condition for Hermitian dual-containing. Hence, if $\rho(G(G^q)^T) \le 2k-n,$ and $2k \ge n,$ then $\zeta^{\perp H} \subset \zeta.$

Now, we give some theorems which shows that the MPC is also HDC.

Let $\sigma = \begin{pmatrix} 1 & 2 & \ldots & s \\ z_1 & z_2 & \ldots & z_s \end{pmatrix}$ be a permutation on s symbols and P_σ be the corresponding permutation matrix where z_i^{th} row of the identity matrix I_s is placed at the i^{th} row of P_σ, for $i = 1, 2, ..., s.$

Theorem 2: Let $[n,k_i,d_i]_{q^2}$ be linear codes denoted by ζ_i with the condition $\zeta_i^{\perp H} \subseteq \zeta_i$, i.e., ζ_i is HDC for every $i = 1,2,\ldots,s.$ Denote by $A \in M(F_{q^2}, s \times s),$ a non-singular matrix with the property that

AA^* is a monomial matrix for some permutation σ, then the set of MPC $\zeta_A = [\zeta_1, \zeta_2, \ldots, \zeta_s].A$ is a Hermitian dual-containing code with parameters $[sn, \sum_{i=1}^{s} k_i, \geq d]_{q^2}$ where $d_i = \min\{D_i(A)d_i\}$.

Proof: With respect to the permutation σ, the matrix AA^* is given to be a monomial matrix therefore, there exists an $s \times s$ diagonal matrix $D = diag(d_{11}, d_{22}, \ldots, d_{ss})$ where $d_{ii} \neq 0$, such that

$$AA^* = DP_\sigma$$

$$\Rightarrow AA^* = DP_\sigma$$

$$\Rightarrow A = (DP_\sigma)(A^*)^{-1}$$

$$\Rightarrow A^{-1} = (DP_\sigma(A^*)^{-1})^{-1}$$

$$\Rightarrow A^{-1} = A^* P_\sigma^{-1} D^{-1}$$

$$\Rightarrow A^{-1} = A^* P_\sigma^T D^{-1}$$

$$\Rightarrow (A^{-1})^* = (A^* P_\sigma^T D^{-1})^*$$

$$\Rightarrow (A^{-1})^* = (D^{-1})^* (P_\sigma^T)^* (A^*)^*$$

$$\Rightarrow (A^{-1})^* = (D^{-1})^* P_\sigma A,$$

Using the lemma [11,19], it gives

$$([\zeta_1, \zeta_2, ..., \zeta_s].A)^{\perp H} = [\zeta_1^{\perp H}, \zeta_2^{\perp H}, ..., \zeta_s^{\perp H}].(D^{-1})^* P_\sigma A.$$

It is well known that $\zeta_i^{\perp H}$ is linear, so $d_{ii}^{-q}\zeta_i^{\perp H} = \zeta_i^{\perp H}$ for every $i = 1, 2, ..., s$. From the theorem 3 and $[\zeta_1^{\perp H}, \zeta_2^{\perp H}, ..., \zeta_s^{\perp H}].P_\sigma = [\zeta_{z_1}^{\perp H}, \zeta_{z_2}^{\perp H}, ..., \zeta_{z_s}^{\perp H}]$,

$$[\zeta_1^{\perp H}, \zeta_2^{\perp H}, ..., \zeta_s^{\perp H}].(D^{-1})^* P_\sigma A = [d_{11}^{-q}\zeta_1^{\perp H}, d_{22}^{-q}\zeta_2^{\perp H}, \ldots, d_{ss}^{-q}\zeta_s^{\perp H}].P_\sigma A$$

$$= [\zeta_1^{\perp H}, \zeta_2^{\perp H}, ..., \zeta_s^{\perp H}].P_\sigma A$$

$$= [\zeta_{z_1}^{\perp H}, \zeta_{z_2}^{\perp H}, ..., \zeta_{z_s}^{\perp H}].A$$

$$\subseteq [\zeta_1, \zeta_2, ..., \zeta_s].A).$$

Hence, the linear code together with the MPC satisfies the condition for Hermitian dual-containing. Through the use of lemma [17], the code's parameters are $[sn, \sum_{i=1}^{s} k_i, \geq d]_{q^2}$, here $d_i = \min\{D_i(A)d_i\}$.

4. Codes obtained from MPC utilizing HPC codes for quantum system.

Quantum codes are crucial for both quantum communication and computation. From the time of noteworthy discoveries cited in [2] and [3], the field of quantum information and error correction has advanced rapidly. Recently, the focus has been on constructing MDS codes, which are central to quantum coding theory. These quantum MDS codes are developed utilizing the Hermitian codes together with quantum Singleton bound. To obtain quantum MDS codes, it's necessary to identify the MDS codes over F_{q^2} that satisfy $\zeta^{\perp H} \subseteq \zeta$. This approach has led to the creation of several new category of MDS codes for quantum system. For instance, Guardia [20] constructed quantum codes utilizing cyclic codes, while Kai and Zhu gave negacyclic codes which aided in developing new categories of quantum MDS codes. Inspired by the work referenced in [6], Kai et al. introduced many quantum MDS codes from constacyclic codes with advanced parameters. Let's review some foundational idea and consequence of quantum codes. For additional details, refer to [21].

Let $V_n = \zeta^{q^n} = \zeta^q \otimes \zeta^q \otimes ... \otimes \zeta^q$ (n-times) denote the Hilbert space. Suppose that $|x\rangle$ ket vector belongs to orthonormal basis of the code ζ^{q^n}, here the elements x belongs to F_q. Then the orthonormal basis of V_n is defined as

$$\{|c\rangle = |c_1 c_2 ... c_n\rangle\}$$

$$= \{|c_1\rangle \otimes |c_2\rangle \otimes ... \otimes |c_n\rangle : \mathrm{c} = (c_1, c_2, ..., \mathrm{c}_n) \in F_n^q\}\}$$

Let $a, b \in F_q$ be any two elements and $\omega = \exp(2\pi i/p)$ denote the primitive p^{th} root of unity. First define tr as the trace map from $F_q \to F_p$. Then unitary error operators $X(a)$ and $Z(b)$ in ζ^q are defined by $X(a)|x\rangle = |x+a\rangle$ and $Z(b)|x\rangle = \omega^{tr(bx)}|x\rangle$ respectively. For $a = (a_1, a_2, ..., a_n) \in F_n^q$ we define $X(a) = X(a_1) \otimes X(a_2) \otimes ... \otimes X(a_n)$ and $Z(a) = Z(a_1) \otimes Z(a_2) \otimes ... \otimes Z(a_n)$ to be the error operators. The error basis for complex vector space ζ^{q^n} is $E_n = \{X(a)Z(b) | a, b \in F_n^q\}$ and $G_n = \{\omega^c X(a)Z(b) | a, b \in F_n^q, c \in F_p\}$ is the error group associated with E_n.

Theorem 3 [10]: Let $[n, k, d]_{q^2}$ is a linear code denoted by ζ and suppose its generator matrix is G. Then a quantum code $[[n, 2k-n, \geq d]]_q$, exists if $\rho(G(G^q)^T) \leq 2k-n$, and $2k \geq n$.

Theorem 4: If A denote a monomial matrix of size n with non-zero elements $a_0, a_1, \ldots, a_{n-1} \in F_q$, then there exist a permutation $\sigma \in S_n$ such that $A = diag(a_0, a_1, \ldots, a_{n-1})P_\sigma$ where P_σ is the matrix with respect to the permutation σ.

Proof: Let $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ z_1 & z_2 & \ldots & z_n \end{pmatrix}$ be any permutation on S_n, then we can obtain a permutation matrix P_σ for σ as

$$P_\sigma = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}$$

where i^{th} row of the identity matrix goes to the z_i^{th} row of the $n \times n$ identity matrix.

Now, let

$$D = \begin{pmatrix} d_{11} & 0 & 0 & 0 \\ 0 & d_{22} & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & d_{nn} \end{pmatrix}$$

be a diagonal matrix with $d_{ii} \in F_q^*$ ($d_{ii} \neq 0$ for each i).

To construct a monomial matrix from the permutation σ and diagonal matrix D, multiplying D and P_σ, we get

$$A = DP_\sigma$$

$$= \begin{pmatrix} d_{11} & 0 & 0 & 0 \\ 0 & d_{22} & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & d_{nn} \end{pmatrix} \times \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}$$

$= \begin{pmatrix} d_{11} \\ d_{22} \\ \vdots \\ d_{nn} \end{pmatrix}$ where each d_{ii} occurs in some order.

Hence, the matrix A defined above is a monomial matrix.

Example 1: Let ζ denote an $[n,k,d]_{q^2}$ linear code with length 13 where elements belongs to the field F_{5^2} having generator matrix G. The trace function is define as $tr(bx) = (bx) + (bx)^5$

$$G=\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{10} & \omega^{12} & \omega^{19} & \omega^{6} \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{20} & \omega^{4} & \omega^{23} & \omega^{2} \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{5} & \omega & \omega^{12} & \omega^{13} \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^{15} & \omega^{18} & \omega^{16} & \omega^{9} \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & \omega^{5} & \omega^{10} & \omega^{15} \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega^{9} & \omega^{6} & \omega^{18} & \omega^{15} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \omega^{13} & \omega^{12} & \omega & \omega^{5} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^{2} & \omega^{23} & \omega^{4} & \omega^{20} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^{6} & \omega^{19} & \omega^{12} & \omega^{10}
\end{bmatrix}$$

Since we can easily that the rank of $(G(G^5)^T)$ is 5, which is less than or equal to $2\times 9-13$. By Theorem 4, a code having parameter $[[13,5,5]]_5$ and satisfying MDS condition is found.

Example 2: Let ζ denote a linear $[n,k,d]_{q^2}$ code with $n=17$ over the field F_{7^2} having generator matrix G. The trace function is define as $tr(bx)=(bx)+(bx)^7$

$$G=\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{37} & \omega^{15} & \omega^{14} & \omega^{61} \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{56} & \omega^{30} & \omega^{19} & \omega^{77} \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{42} & \omega^{45} & \omega^{48} & \omega^{51} \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{76} & \omega^{60} & \omega^{20} & \omega^{64} \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{41} & \omega^{75} & \omega^{79} & \omega^{26} \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{3} & \omega^{9} & \omega^{15} & \omega^{21} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{61} & \omega^{24} & \omega^{24} & \omega^{61} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^{21} & \omega^{15} & \omega^{9} & \omega^{3} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \omega^{26} & \omega^{79} & \omega^{75} & \omega^{41} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega^{64} & \omega^{20} & \omega^{60} & \omega^{76} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \omega^{51} & \omega^{48} & \omega^{45} & \omega^{42} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^{77} & \omega^{19} & \omega^{30} & \omega^{56} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^{61} & \omega^{14} & \omega^{15} & \omega^{37}
\end{bmatrix}$$

Since $\rho(G(G^7)^T)=9\le 2\times 13-17$, Using the Theorem 5, a quantum MDS code with parameters $[[17,9,5]]_7$ is found. For comparison, the obtained quantum code has good and new parameters than in [12]. Other quantum codes such as $[[11,5,4]]_3$, $[[18,12,4]]_7$ and $[[64,56,3]]_9$ are also obtained.

5. Results and Comparison

Utilizing HDC, MPC and minimal polynomials with the HDC property has resulted in the development of the $[[13,5,5]]_5$ and $[[17,9,5]]_7$ quantum codes. These newly constructed codes demonstrate superior

error correction capabilities, offering a practical balance of rates and lengths suitable for implementation in quantum computing systems. The underlying algebraic structures and properties not only enhance the current performance but also lay the foundation for upcoming improvements in quantum error correction technology. The newly developed quantum codes, characterized by improved parameters such as distance, rate, and length, are explicitly adapted for practical quantum computing implementation. The use of advanced algebraic structures and properties in their construction not only boosts their performance but also lays a robust groundwork for future advancements in quantum coding theory [22,23]. In quantum codes obtained using the proposed construction method, the parameters are better because we have encoded a greater number of physical qubits increasing the rate of the codes have a larger minimum distance of these codes. A larger minimum distance enables the code to identify and fix a greater number of errors. This is essential because quantum systems are extremely vulnerable to various types of noise and errors, including bit-flips, phase-flips, and their combinations. Fault-tolerant quantum computation necessitates maintaining error rates below a specific threshold. Codes with larger minimum distances generally possess higher error thresholds, enhancing their suitability for practical quantum computing applications. Although codes with larger minimum distances often need more physical qubits for encoding, they decrease the overhead required for repeated error correction cycles, resulting in more efficient resource utilization in large-scale quantum systems.

Table 1. Comparison of various codes obtained from the proposed method and [24].

Proposed Quantum Codes	Existing Codes from [24]
$[[11,5,4]]_3$	$[[11,1,4]]_3$
$[[13,5,5]]_5$	$[[13,9,3]]_5$
$[[17,9,5]]_7$	$[[17,13,3]]_7$
$[[18,12,4]]_7$	$[[18,10,4]]_7$

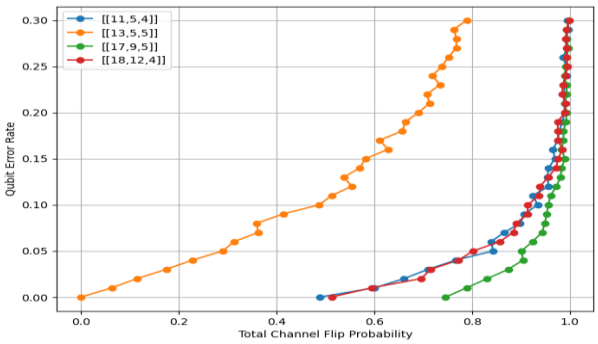

Fig. 2 Comparison of various codes obtained with different parameters

From the Fig. 2, it is evident that the codes constructed exhibits better error correction proficiency. These codes have a lower qubit error rate with respect to the total channel flip probability with varying depolarizing probability under consideration. Also, the codes constructed from the proposed method have better parameters than [24]. The analysis explored a range of qubit error rates from 0 to 0.3, reflecting practical error rates in current quantum hardware. This selection aimed to cover both standard and challenging operational conditions for quantum systems. At lower error rates, the

$[[17,9,5]]_7$ code showed a notable ability to mitigate errors, maintaining a low total channel flip probability (TCFP). This performance suggests that the code effectively corrected errors introduced by depolarizing noise, thereby preserving the state of logical qubits. As the qubit error rate increased, the TCFP exhibited a linear rise, indicating the growing difficulty in keeping qubits error-free. Despite this rise, the code's error correction remained effective at moderate error rates, highlighting its reliability under typical conditions found in quantum hardware. However, when the error rate approached 0.3, the TCFP escalated sharply. This increase marked the point where the error-correcting capabilities of the codes began to diminish, struggling to handle the higher frequency of errors. This observation underscores the limitations of the code at elevated noise levels, pointing to the need for further optimization or alternative strategies to manage such extreme conditions more effectively. https://github.com/ShivenderGoswami/Quantum-MPCs

6. Conclusion

The method of establishing quantum codes using HDC together with MPC and minimal polynomials with the HDC property has led to significant advancements. The resulting codes, such as the $[[13,5,5]]_5$ and $[[17,9,5]]_7$ codes, feature excellent parameters in terms of distance, rate, and length, making them highly suitable for practical quantum computing applications. These codes exhibit robust error correction capabilities, making them resilient to various forms of quantum noise and errors. Additionally, the integration of specific algebraic structures and properties enhances their performance and establishes a strong foundation for ongoing research and development in quantum coding theory. This innovative approach opens new pathways for the creation of more efficient and reliable quantum codes, advancing the field of quantum information science.

References

[1] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF (4). IEEE Trans. Inf. Theory 44(4), 1369–1387 (1998)
[2] Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A 52, 2493– 2496 (1995)
[3] Steane, A.M.: Multiple-particle interference and quantum error correction. Proc. R. Soc. Lond. Ser. A 452, 2551–2577 (1996)
[4] Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory 47(7), 3065– 3072 (2001)
[5] Grassl, M., Beth, T., Rötteler, M.: On optimal quantum codes. Int. J. Quantum Inf. 2(1), 55–64 (2004)
[6] Kai, X., Zhu, S., Li, P.: IEEE Trans. Inf. Theory 60(4), 2080 (2014)
[7] Chen, B., Ling, S., Zhang, G.: IEEE Trans. Inform. Theory 61(3), 1474 (2015)
[8] Li, S., Xiong, M., Ge, G.: IEEE Trans. Inform. Theory 64(4), 1703 (2016)
[9] Liu, X. S., Liu, H.: Quantum Inf. Process 16, 240 (2017). doi: 10.1007/s11128-017- 1695-7
[10] Galindo, C., Hernando, F., Ruano, D.: New quantum codes from evaluation and matrix-product codes. Finite Fields Appl. 36, 98–120 (2015)
[11] Zhang, T., Ge, G.: Quantum codes from Generalized Reed-Solomon codes and matrix-product codes, arxiv:1508.00978v1 (2015)
[12] Liu, X., Hu, P.: New quantum codes from two linear codes. Quantum Inf Process 19, 78 (2020)
[13] Song, H., Li, R., Wang, J., Lv, J.: Construction of new matrix-product codes and their applications. IEEE Access (2019).
[14] Rathor, A., Kumar, M., Mishra, R.K., Goswami, S., Chaudhary, A.: Enhanced Performance of Isogenies Over Huff Curve for Post Quantum Cryptography. International Journal of Intelligent Engineering and Systems, 16(6), 445-457 (2023)

[15] Kumar, M. Gupta, M. K., Mishra, R.K., Dubey, S.S., Kumar, A., 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, 694, 373-389 (2020)

[16] Hardeep, Kumar, M., Mishra, R. K.: Sharing of information using bi-qutrit quantum states based on bivariate quantum gates. Journal of Xi'an Shiyou University, Natural Sciences Edition, 64(12), 91-101 (2021)

[17] Blackmore, T., Norton, G.H.: Matrix-product codes over Fq. Appl. Algebra Eng. Commun. Comput. 12, 477–500 (2001)

[18] Hernando, F., Lally, K., Ruano, D.: Construction and decoding of matrix-product codes from nested codes. Appl. Algebra Eng. Commun. Comput. 20(5–6), 497–507 (2009)

[19] Liu, X., Dinh, H.Q., Liu, H., Yu, L.: On new quantum codes from matrix product codes. Cryptogr. Commun. 10, 579–589 (2018)

[20] La Guardia, G.G.: IEEE Trans. Inf. Theory 57(8), 5551 (2011)

[21] Aly, S. A., Klappenecker, A., Sarvepalli, P. K.: IEEE Trans. Inf. Theory 53, 1183 (2007)

[22] Goswami, S., Kumar, M., Mishra, R.K., Rathor, A.: A Novel and Efficient Stabilizer Codes Over Non- Cyclic Hadamard Difference Sets for Quantum System. IAENG International Journal of Applied Mathematics, 54(7), 1416-1426 (2024)

[23] Rathor, A., Kumar, M., Mishra, R.K., Goswami, S.: Complete Analysis of Isogeny on Hessian Curve. IAENG International Journal of Computer Science, 51(7), 906-917 (2024)

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