Open Access Article

A CONCATENATED CONSTRUCTION OF QUANTUM ERROR-CORRECTING CODES

Anju Sharma and Vinod Kumar*
Department of Mathematics, Guru Kashi University, Bathinda, Punjab, India.

Abstract

Quantum computing stands at the forefront of technological advancement, offering the promise of solving complex problems at unprecedented speeds. This potential, however, is hindered by the inherent susceptibility of quantum information to errors stemming from decoherence and quantum noise. Quantum error-correcting codes (QECCs) have emerged as a pivotal solution to safeguard quantum data, thereby unleashing the full potential of quantum computers.

This research paper focuses on the creation of QECCs by employing a concatenated code approach, which demonstrates the ability to significantly enhance the resilience of quantum information to errors. Our study delves into the fundamental principles of quantum error correction and explores the utilization of concatenated codes as an innovative strategy for improving the fault tolerance of quantum computing systems.

Keywords: Concatenated code; Quantum error-correcting codes; Construction of QECCs.

1. Introduction

The exploration of quantum error-correcting codes has seen an extraordinary surge in growth since the pivotal realization that these codes, much like their classical counterparts, safeguard quantum information. Quantum error-correcting codes stand as a potent solution, offering an efficient defense against decoherence, a significant hurdle in quantum information processing.

The groundwork for this domain was laid when Shor revealed the first quantum error-correcting code ([13]). Subsequently, Calderbank and colleagues ([1]) pioneered constructing these codes by drawing on classical error-correcting codes. The landscape of quantum error-correcting code theory has rapidly expanded, witnessing a prolific development. Notably, numerous robust quantum error-correcting codes have emerged through the application of classical cyclic codes over finite fields F_q (where q represents a power of a prime number). These codes exhibit self-orthogonal or dual-containing properties, as showcased in references ([8]), ([4]), ([9]), ([7]), ([10]), ([15]), and ([14]). This rapid expansion and diversification in the development of quantum error-correcting codes herald a promising era in quantum information protection and manipulation.

In classical coding theory, one effective approach to creating extensive codes within limited finite fields involves the concatenation method. This technique combines codes over a sizable finite field (referred to as outer codes) having a minimum distance of D with appropriate inner codes featuring a

Received: October 04, 2023 / Revised: October 30, 2023 / Accepted: November 18, 2023 / Published: December 18, 2023
About the authors：Anju Sharma
Corresponding author- Email:

minimum distance of d. The result is the generation of linear codes over a corresponding smaller field, ensuring a minimum distance that is at least dD. The concept presented in paper [2] demonstrates the construction of LCD codes utilizing the concatenated code method. Currently, we are applying this very approach to pioneer the construction of quantum error-correcting codes - an area that has yet to be explored by anyone.

In this paper, the second section will revisit the fundamentals of coding theory. Moving to the third section, we will delve into the isometry code, a special case of Concatenated code, illustrated through various examples. The fourth section will present the Concatenated construction of quantum error-correcting codes. Finally, the last section will offer a comprehensive conclusion summarizing the key findings and implications outlined in this paper.

2. Preliminaries

In this section, we present an overview of the fundamental concepts related to quantum error-correcting codes. For a more comprehensive understanding, interested readers may refer to Huffman and Pless 2010([6]) and Ling and Xing 2004 ([11]).

A linear code is a subspace of a vector space over a finite field, typically denoted as $\mathbb{F}_q^n$, where q is the size of the finite field, and n is the code length. A linear code is defined as a linear subspace of $\mathbb{F}_q^n$.

A linear code can be uniquely described by a generator matrix. This matrix, denoted as G, has dimensions $k \times n$, where k is the dimension of the code (the number of information symbols), and n is the code length. The rows of the generator matrix span the code.

Another way to represent a linear code is through a parity-check matrix, denoted as H. The parity-check matrix has dimensions $(n-k) \times n$ and is used for error detection and correction. The rows of the parity-check matrix are orthogonal to the rows of the generator matrix.

The code rate, denoted as R, is the ratio of the number of information bits to the total number of codeword bits. It is given by $R = \frac{k}{n}$.

The Hamming distance between two codewords is the number of positions at which the corresponding symbols differ. It is often denoted as d. The minimum Hamming distance, $d_{\min}$, is the smallest Hamming distance between any pair of distinct codewords in the code.

The error-correcting capability of a code is measured by the number of errors it can correct. A linear code can correct up to $\left\lfloor\frac{d_{\min}-1}{2}\right\rfloor$ errors.

Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ represent two elements of the vector space F_q^n. The Euclidean inner product of vectors x and y within F_q^n is given by the expression:

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots . + x_n y_n$$

The dual code $C^{\perp}$ associated with code C is defined as the set:

$$C^{\perp} = \{x \in F_q^n : x \cdot y = 0, \forall y \in C\}$$

. A code C is termed self-orthogonal if $C^{\perp} \subseteq C$, implying that every element in $C^{\perp}$ is also in C. Moreover, a code C is self-dual if $C^{\perp} = C$, signifying that the dual code is equivalent to the original code.

The subsequent result outlines a method for constructing quantum error correcting codes by utilizing self-dual codes.

Theorem 2.1 ([5], Theorem 3). Let $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ be linear codes over F_q with $C_2^{\perp} \subseteq C_1$. Furthermore, let $d = \min\{wt(v) \colon v \in (c_1 - C_2^{\perp}) \cup (C_2 - C_1^{\perp})\} \geqslant \min\{d_1, d_2\}$. Then there exists a quantum error correcting code $C = [n, k_1 + k_2 - n, d]$. In particular, if $C_1^{\perp} \subseteq C_1$, then there exists a quantum error-correcting code $C = [n, n - 2k_1, d_1]$, where $d_1 = \min\{wt(v) : v \in (C_1 - C_1^{\perp})\}$.

3. Isometry codes

We recall the definition and basic properties of Isometry codes in this section. The Isometry codes, which are a special case of Concatenated codes, were introduced by [2].

Consider a prime power q, and let k and n be integers satisfying $2 \leqslant k \leqslant n$. The trace of an element a belonging to the field extension $\mathbb{F}q^k$ over the base field $\mathbb{F}q$ is defined as follows:

$$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) = \sum_{i=0}^{k-1} \alpha^{q^i} = a + a^q + \cdots + a^{q^{k-1}}$$

From now on, we denote $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a)$ by $\mathrm{Tr}\,(a)$. Let $\{u_1, \dots, u_k\} \subseteq \mathbb{F}_q^k$. Assume that $(u_1, \dots, u_k)$ is an ordered basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Recall that $(u_1', \dots, u_k')$ is the dual basis of $(u_1, \dots, u_k)$ if

$$\mathrm{Tr}\,(u_i u_j') = \delta_{ij} := \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

for $1 \leqslant i, j \leqslant k$. For any basis of $\mathbb{F}q^k$ over $\mathbb{F}q$, there is a unique dual basis that can be determined. A basis $(u_1, \dots, u_k)$ of $\mathbb{F}q^k$ over $\mathbb{F}q$ is termed a self-dual basis if $(u_1, \dots, u_k) = (u_1', \dots, u_k')$. It's important to note that the existence of a self-dual basis in $\mathbb{F}q^k$ over $\mathbb{F}q$ is contingent on the following conditions, as demonstrated in sources like [12]:

(i) q is even, or

(ii) q is odd and k is odd.

Definition 3.1. Consider an ordered basis $(u_1, \ldots, u_k)$ of $\mathbb{F}q^k$ over $\mathbb{F}q$. An $\mathbb{F}q$-linear map $\pi: \mathbb{F}q^k \rightarrow \mathbb{F}q^n$ is termed an isometry with respect to $(u_1, \ldots, u_k)$ if it satisfies the condition:

$$\pi(u_i) \cdot \pi(u_j') = \delta_{ij}$$

for $1 \leqslant i, j \leqslant k$, where δ_{ij} denotes the Kronecker delta and the inner product is the Euclidean inner product in $\mathbb{F}q^n$. Here, $(u_1', \ldots, u_k')$ represents the dual basis of $(u_1, \ldots, u_k)$. The set $\pi(\mathbb{F}q^k)$ is referred to as an isometry code concerning $(u1, \ldots, u_k)$.

Remark 3.2. It's important to note that an isometry code $\pi(\mathbb{F}_{q^k})$ concerning $(u_1, \ldots, u_k)$ forms a linear $[n, k]$ code over $\mathbb{F}_q$. This arises from the linear independence of $\pi(u_1), \pi(u_2), \ldots, \pi(u_k)$ over $\mathbb{F}_q$: Assuming $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_q$ such that $\alpha_1 \pi(u_1) + \alpha_2 \pi(u_2) + \cdots + \alpha_k \pi(u_k) = 0$, multiplying both sides by the vector $\pi(u_1')$ yields:

$$\alpha_1 \pi(u_1') \cdot \pi(u_1) + \alpha_2 \pi(u_1') \cdot \pi(u_2) + \cdots + \alpha_k \pi(u_1') \cdot \pi(u_k) = \alpha_1 = 0$$

Similarly, it can be concluded that $\alpha_2 = \alpha_3 = \cdots = \alpha_k = 0$, which demonstrates that the dimension of $\pi(\mathbb{F}_{q^k})$ is k over $\mathbb{F}_q$.

Next, we provide some simple examples.

Example 3.3. When $k = n$ and $(u_1, \ldots, u_k)$ represents a self-dual basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, the mapping

$$\begin{aligned} \pi: \mathbb{F}_{q^k} &\rightarrow \mathbb{F}_q^k \\ v &\longmapsto \pi(v) = \left(\operatorname{Tr}(u_1 v), \operatorname{Tr}(u_2 v), \ldots, \operatorname{Tr}(u_k v)\right) \end{aligned}$$

This mapping is evidently an isometry concerning $(u_1, \ldots, u_k)$. The resulting isometry code $\pi(\mathbb{F}_{q^k})$ constitutes a linear $[k, k, 1]$ code over $\mathbb{F}_q$.

Example 3.4. In the paper referenced as [2], the authors have verified the following outcomes using MAGMA computations:

- When $k = 2, n = 3$, and $q = 2$, there exist 6 unique isometries $\pi: \mathbb{F}q^2 \rightarrow \mathbb{F}q^3$ for each basis (e_1, e_2) of $\mathbb{F}q^2$ over $\mathbb{F}q$.
- For $k = 2, n = 4$, and $q = 2$, there are 32 distinct isometries $\pi: \mathbb{F}q^2 \rightarrow \mathbb{F}q^4$ corresponding to each basis (e_1, e_2) of $\mathbb{F}q^2$ over $\mathbb{F}q$.
- In the case of $k = 3, n = 4$, and $q = 2$, there exist 48 distinct isometries $\pi: \mathbb{F}q^3 \rightarrow \mathbb{F}q^4$ for every basis (e_1, e_2, e_3) of $\mathbb{F}q^3$ over $\mathbb{F}q$.

- When $k = 2, n = 2$, and $q = 3$, there is no isometry $\pi: \mathbb{F}q^2 \to \mathbb{F}q^2$ for any basis (e_1, e_2) of $\mathbb{F}q^2$ over $\mathbb{F}q$.
- For $k = 2, n = 3$, and $q = 3$, there exist 24 distinct isometries $\pi: \mathbb{F}q^2 \to \mathbb{F}q^3$ corresponding to each basis (e_1, e_2) of $\mathbb{F}q^2$ over $\mathbb{F}q$.
- When $k = 2, n = 4$, and $q = 3$, there are 288 unique isometries $\pi: \mathbb{F}q^2 \to \mathbb{F}q^4$ for every basis (e_1, e_2) of $\mathbb{F}q^2$ over $\mathbb{F}q$.

Above, all examples provide a guarantee of the existence of isometric codes.

4. A Concatenated Construction of Quantum error-correcting codes

This section meticulously outlines a construction method for self-orthogonal codes employing the isometric code. It then proceeds to offer results that demonstrate the creation of quantum error-correcting codes by utilizing the construction of these self-orthogonal codes. The link between the isometric code and the subsequent development of quantum error-correcting codes underscores a significant breakthrough in the application of self-orthogonal dual codes within the realm of quantum computing, paving the way for more robust and efficient error-correction strategies in quantum information processing. In the paper by Carlet et al. [2], the authors provided a similar proof demonstrating the construction of linear complementary dual (LCD) codes over small fields.

Consider integers $2 \leqslant k \leqslant n$ and a finite field $\mathbb{F}q$. Let $\pi: \mathbb{F}q^k \to \mathbb{F}q^n$ be an isometry concerning a basis $(u1, \dots, u_k)$ of $\mathbb{F}q^k$ over $\mathbb{F}q$. Assume that $\pi(\mathbb{F}q^k)$ forms an $\mathbb{F}q$-linear code characterized by a length of n, dimension of k, and minimum distance of d.

Consider a linear code $C \subseteq \mathbb{F}q^{k^S}$ over $\mathbb{F}q^k$ with parameters $[s, t, d(C)]$. Let $\pi^{\otimes s}$ represent the $\mathbb{F}_q$-linear map defined as follows:

$$\pi^{\otimes s}: \mathbb{F}_{q^k}^S \to \mathbb{F}_q^{ns}$$

$$(a_1, a_2, \dots, a_s) \longmapsto [\pi(a_1), \pi(a_2), \dots, \pi(a_s)]$$

Here, $\mathbb{F}q^{ns}$ is associated with $n \times s$ matrices over $\mathbb{F}q$, and $\pi(\alpha_i)$ refers to the i-th column, which has a length of s over $\mathbb{F}_q$.

Theorem 4.1. Suppose C represents a self-orthogonal dual code over $\mathbb{F}q^k$ characterized by parameters $[s, t, d(C)]$. In such a scenario, $\pi^{\otimes s}(C)$ transforms into a self-orthogonal dual code over $\mathbb{F}q$ with parameters $[sn, tk, \geqslant d(C)d]$.

Proof. Utilizing certain methodologies from Chen-Ling-Xing as described in [3], consider $A = \pi(\mathbb{F}q^k)$ and $A^\perp$, its corresponding dual in $\mathbb{F}q^n$. It's worth noting that A represents a linear $[n, k]q$ code, while $A^\perp$ denotes a linear $[n, n-k]q$ code. For $1 \leqslant i \leqslant s$, define $A_i = A$ and $A_i^\perp = A^\perp$. Note that

$$A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp} \subseteq \mathbb{F}_q^{sn}$$

is an $\mathbb{F}_q$--linear code with parameters $[sn, s(n-k)]_q$. We note that $\pi^{\otimes s}(\mathbb{F}_{q^k}) \perp (A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp})$ trivially as

$$[\pi(x_1), \pi(x_2), \dots, \pi(x_s)] \cdot [y_1, y_2, \dots, y_s] = \pi(x_1) \cdot y_1 + \pi(x_2) \cdot y_2 + \cdots + \pi(x_s) \cdot y_s = 0$$

if $\pi(x_1) \perp y_1, \pi(x_2) \perp y_2, \dots, \pi(x_s) \perp y_s$. Hence,
$\pi^{\otimes s}(C) \perp (A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp})$.

Moreover, $\pi(\mathbb{F}_{q^k}) \cap A^{\perp} = \{0\}$. Indeed, let $\alpha \in \mathbb{F}_{q^k}$ with $\pi(\alpha) \perp A$, or equivalently

$$\pi(\alpha) \cdot \pi(u_i) = 0$$

for $1 \leqslant i \leqslant k$. Let $(u_1', u_2', \dots, u_k')$ be the dual basis for the basis $(u_1, u_2, \dots, u_k)$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Let $\alpha = y_1 u_1' + \cdots + y_k u_k'$ with $y_1, \dots, y_k \in \mathbb{F}_q$. Then by (1) we have

$$(\pi(u_1')y_1 + \pi(u_2')y_2 + \cdots + \pi(u_k')y_k) \cdot \pi(u_1) = 0$$

which implies that $y_1 = 0$ as π is an isometry and hence $\pi(u_i') \cdot \pi(u_1) = \delta_{1i}$. Similarly, $y_2 = \cdots = y_k = 0$ and hence $\alpha = 0$. Therefore, $\pi^{\otimes s}\left(\mathbb{F}_{q^k}^s\right) \cap (A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp}) = \{0\}$ and in particular

$$\pi^{\otimes s}(C^{\perp}) \cap (A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp}) = \{0\}.$$

To show that $\pi^{\otimes s}(C)$ is self dual code, we observe that it is enough to prove

$$\pi^{\otimes s}(C^{\perp}) \perp \pi^{\otimes s}(C)$$

Indeed, the dimension of the dual of $\pi^{\otimes s}(C)$ is

$$sn - tk = \dim\left(\pi^{\otimes s}(C^{\perp})\right) + \dim(A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp})$$

as $\dim\left(\pi^{\otimes s}(C^{\perp})\right) = k(s-t)$ and $\dim(A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp}) = s(n-k)$. Using (1), (3) and (4), we conclude that the dual of $\pi^{\otimes s}(C)$ is $(A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp}) \oplus \pi^{\otimes s}(C^{\perp})$.

As $\pi^{\otimes s}(C) \cap (A_1^{\perp} \times A_2^{\perp} \times \cdots \times A_s^{\perp}) = \{0\}$ and $C^{\perp} \subseteq C$, we conclude that $\pi^{\otimes s}(C)$ is self dual code. Indeed, if $\underline{a} \in \pi^{\otimes s}(C)^{\perp} = \pi^{\otimes s}(C^{\perp})$, then there exists $\underline{\alpha} \in C^{\perp}$ such that $\underline{a} = \pi^{\otimes s}(\underline{\alpha})$. As C is self dual code we obtain that $\underline{\alpha} \in C$ and hence $\underline{a} \in \pi^{\otimes s}(C)$.

Now we prove (4). Let $(a_1, \dots, a_s) \in \mathbb{F}_{q^k}^s$ and $(b_1, \dots, b_s) \in \mathbb{F}_{q^k}^s$ such that $(a_1, \dots, a_s) \cdot (b_1, \dots, b_s) = 0$. For $1 \leqslant l \leqslant s$ and $1 \leqslant i, j \leqslant k$, let $\alpha_l^i, \beta_l^j \in \mathbb{F}_q$ such that

$$a_l = \sum_{i=1}^{k} \alpha_l^i u_i \text{ and } b_l = \sum_{j=1}^{k} \beta_l^j u_j'$$

Hence, we have that

$$\sum_{l=1}^{s} \sum_{i=1}^{k} \sum_{j=1}^{k} \alpha_l^i \beta_l^j u_i u_j' = 0$$

Taking the trace of both sides, we obtain that

$$\sum_{l=1}^{s} \sum_{i=1}^{k} \alpha_l^i \beta_l^i = 0$$

as Tr $\left(e_i e_j'\right) = \delta_{ij}$ for $1 \leqslant i, j \leqslant k$. We will show that

$$\pi^{\otimes s}(a_1, \dots, a_s) \cdot \pi^{\otimes s}(b_1, \dots, b_s) = \sum_{l=1}^{s} \pi(a_l) \cdot \pi(b_l) = 0$$

which implies (4). We have $\pi(a_l) = \sum_{i=1}^{k} \alpha_l^i \pi(e_i)$ and $\pi(b_l) = \sum_{j=1}^{k} \beta_l^j \pi\left(e_j'\right)$ for $1 \leqslant l \leqslant s$. Hence

$$\sum_{l=1}^{s} \pi(a_l) \cdot \pi(b_l) = \sum_{l=1}^{s} \sum_{i=1}^{k} \sum_{j=1}^{k} \alpha_l^i \beta_l^j \pi(u_i) \cdot \pi\left(u_j'\right) = \sum_{l=1}^{s} \sum_{i=1}^{k} \alpha_l^i \beta_l^i$$

which follows from the isometry property that $\pi(u_i) \cdot \pi\left(u_j'\right) = \delta_{ij}$ for $1 \leqslant i, j \leqslant k$. Using (5) and (6), we complete the proof.

The following result showcases the Concatenated construction of quantum error-correcting codes through the utilization of self-dual codes.

Theorem 4.2. If C is a self-orthogonal code over $\mathbb{F}_{q^k}$ with parameters $[s, t, d(C)]$, then there exists a quantum error-correcting code over $\mathbb{F}_q$ with parameters $[sn, sn - 2tk, d_1]$, where $d_1 = \min\{wt(v) \colon v \in (C^{\perp} - C)\}$.

Certainly, by leveraging Theorem 2.1 and Theorem 4.1, one can establish the theorem mentioned earlier.

5. Conclusion

In summary, this paper delves into the foundational understanding of Concatenated codes, elucidating their definition and presenting the construction of a self-dual code through their application. Building upon this groundwork, the paper explores the innovative Concatenated construction of quantum error-correcting codes by leveraging the created self-dual code. This progression showcases the potential for implementing Concatenated codes in quantum error correction, opening doors to enhanced error-detection and correction mechanisms in quantum computing. The intricate interplay between Concatenated codes and quantum error correction techniques signifies a promising avenue for future advancements in error-correcting code development in quantum computing.

6. References

[1] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. Sloane. Quantum error correction via codes over gf (4). IEEE Transactions on Information Theory, 44(4):1369-1387, 1998.

[2] C. Carlet, C. Güneri, F. Özbudak, and P. Solé. A new concatenated type construction for lcd codes and isometry codes. Discrete Mathematics, 341(3):830-835, 2018.

[3] H. Chen, S. Ling, and C. Xing. Asymptotically good quantum codes exceeding the ashikhmin-litsyn-tsfasman bound. IEEE Transactions on Information Theory, 47(5):2055-2058, 2001.

[4] K. Feng, S. Ling, and C. Xing. Asymptotic bounds on quantum codes from algebraic geometry codes. IEEE transactions on information theory, 52(3):986-991, 2006.

[5] M. Grassl, T. Beth, and M. Roetteler. On optimal quantum codes. International Journal of Quantum Information, 2(01):55-64, 2004.

[6] W. C. Huffman and V. Pless. Fundamentals of error-correcting codes. Cambridge university press, 2010.

[7] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. IEEE transactions on information theory, 52(11):4892-4914, 2006.

[8] A. Klappenecker and P. K. Sarvepalli. Clifford code constructions of operator quantum error-correcting codes. IEEE transactions on information theory, 54(12):5760-5765, 2008.

[9] G. G. La Guardia and R. Palazzo Jr. Constructions of new families of nonbinary css codes. Discrete mathematics, 310(21):2935-2945, 2010.

[10] R. Li and X. Li. Binary construction of quantum codes of minimum distance three and four. IEEE Transactions on Information Theory, 50(6):13311335,2004.

[11] S. Ling and C. Xing. Coding theory: a first course. Cambridge University Press, 2004.

[12] G. Seroussi and A. Lempel. Factorization of symmetric matrices and trace orthogonal bases in finite fields. SIAM Journal on Computing, 9(4):758767,1980.

[13] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. Physical review A, 52(4):R2493, 1995.

[14] A. M. Steane. Simple quantum error-correcting codes. Physical Review A, 54(6):4741, 1996.

[15] X.-K. Xu, J. Zhang, and M. Small. Rich-club connectivity dominates assortativity and transitivity of complex networks. Physical Review E, 82(4):046117, 2010.