# Improving Parameters of Asymptotically Good Quantum LDPC Codes via Stronger Product Expansion

Thesis by
Yiyi Cai

In Partial Fulfillment of the Requirements for the
degree of
Bachelor of Science


CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2025
Submitted June 6th, 2025

Yiyi Cai
ORCID: 0009-0003-4092-200X

# ACKNOWLEDGEMENTS

My Caltech undergraduate journey has been one of the most fulfilling and challenge experiences in my life. I will forever cherish this intellectually vibrant environment filled with passionate and dedicated people that I deeply respect.

First and foremost, none of my interests in quantum information would have flourished without John Preskill. John warmly welcomed me to his group and more broadly to the Institute of Quantum Information and Matter community in the summer of 2023. I am especially grateful for his belief in me even when I faltered, and for his unwavering encouragement, trust, and infectious optimism – reminding me to always find joy in research – all of which have been instrumental to my growth during my time at Caltech.

This thesis would not have been possible without the patient guidance of my mentor Chris Pattison, who encouraged me to pursue my interests in quantum error correction when I first mentioned them and helped conceive the project that became the heart of this work. His support has been indispensable in helping me make sense of these highly theoretical and intricate constructions, and I am deeply grateful for his clear explanations and generosity throughout. I am also thankful for Zhiyang (Sunny) He for generously taking the time to review my manuscript and offering thoughtful and constructive feedback that greatly improved the clarity and precision of this thesis. I am additionally grateful for Glen George for helping coordinate this cross-department thesis.

Within the IQIM community, I would like to thank Yu Tong and Jiaqing Jiang for introducing me to interesting problems in many-body systems and teaching me valuable techniques along the way. Their insights and creativity inspire me to keep exploring well-motivated problems with curiosity and enthusiasm during every discussion we have. I have also learned a great deal about quantum information through different perspectives from these dedicated researchers: Alexei Kitaev, Hsin-Yuan (Robert) Huang, Mehdi Soleimanifar, Robbie King, Urmila Mahadev, Jielun (Chris) Chen, Akshar Ramkumar, Matthias Caro, Haimeng Zhao, Andreas Elben, Charles ChunJun Cao, and Laura Lewis.

Outside of quantum information, I am thankful for these professors and mentors for their support during my undergraduate career: Victoria Kostina, Ali Hajimiri, Nai-Chang Yeh, Maria Spiropulu, Brad Filippone, and Glen George. I am also

grateful to my peers – too many to name – who have helped me survive Caltech through countless late-night problem sets. The collaborative and supportive spirits we have built together are something I deeply value and will always carry with me.

Finally, I would like to thank my family for their unwavering love and support throughout this journey. Their belief in me has been a constant source of strength. I am especially grateful to my parents, Ruibin Zhang and Chung-Wen Chow, for their sacrifices, encouragement, and faith in my education – none of this would have been possible without them. I carry all these lessons, memories, and relationships with me as I look ahead to the next chapter with gratitude and excitement.

# ABSTRACT

Quantum low-density parity-check (qLDPC) codes are a promising path toward scalable, fault-tolerant quantum computation. This thesis focuses on improving the relative distance of asymptotically good qLDPC codes, with a particular emphasis on quantum Tanner codes. We present a refined analysis of product expansion in tensor codes and introduce a stronger form of the expansion property that leads to improved lower bounds on code distance. Numerical results further illustrate how our method enables improved trade-offs between code parameters under practical constraints. While our analysis is framed in the quantum Tanner code setting, the techniques are broadly applicable to other constructions whose local codes are based on tensor product decompositions. Our work contributes to closing the gap between asymptotic constructions and realizable quantum codes.

# CONTENTS

# LIST OF FIGURES

*Chapter 1*

# INTRODUCTION

Quantum error correction is an essential component for scalable quantum devices. Unlike classical bits, quantum bits–or qubits–are inherently fragile and susceptible to both bit-flip and phase-flip errors due to their interactions with the environment. To combat this, quantum error-correcting codes (QECCs) embed logical qubits into higher-dimensional Hilbert spaces using carefully constructed entangled states that allow for error detection and recovery without collapsing the quantum state.

A major milestone in quantum coding theory has been the development of quantum low-density parity-check (qLDPC) codes, which seek to replicate the efficiency and scalability of their classical LDPC counterparts while satisfying the additional constraints imposed by quantum mechanics. These codes use sparse parity-check matrices to define stabilizers, enabling efficient syndrome measurement and fault-tolerant decoding. Recent advances in qLDPC constructions [PK22; LZ22; Din+23] have made it possible to achieve both linear distance and linear rate–a longstanding goal in quantum information theory.

One such class of constructions is the quantum Tanner code, derived from classical Tanner codes applied on a square complex. These codes utilize the left-right Cayley complex structure, a combinatorial object that enables two-dimensional local constraints on qubits while preserving the sparse connectivity required for scalability. The code rate and distance of quantum Tanner codes are determined by the properties of the underlying local codes placed on the rows and columns of each vertex's neighborhood.

This thesis focuses on improving the relative distance of quantum Tanner codes. While prior analyses in [LZ22; LZ23] provided a foundation for their correctness and asymptotic good rate and distance, the required parameters – particularly the length of the local code – remains impractically large, partly due to weak guarantees on the expansion behavior of the underlying code structure. To address this, we revisit and extend the notion of product expansion, which is a key property that quantifies how the weight of a codeword in the tensor product is distributed over its rows and columns. Building on the framework of [KP22], we develop a stronger form of the product expansion property by introducing a tunable, parameterized analysis that

yields significantly improved lower bounds on the expansion constant. While our analysis is carried out in the quantum Tanner code setting, the techniques developed here are broadly applicable to code constructions that use random local codes of some tensor product structure on complexes. We also provide numerical evidence that our improvements can significantly reduce the required local code length.

This thesis is structured to build a coherent narrative from foundational ideas to new theoretical contributions. Chapter 2 begins with an overview of classical error-correcting codes, introducing linear codes and LDPC codes, and culminating in the construction of expander codes. These classical tools lay the groundwork for understanding the techniques later used in the quantum setting. In Chapter 3, we transition into quantum error correction and present the stabilizer formalism and CSS codes. This chapter also introduces quantum LDPC codes by drawing parallels to their classical counterparts. Building on this foundation, Chapter 4 introduces quantum Tanner codes, a specific family of qLDPC codes constructed on square complexes with asymptotically good code parameters. We present an in-depth and self-contained analysis of the code structure, rate, and baseline distance bounds. We highlight our main contributions in Chapter 5, which is a strengthened version of the product expansion analysis, along with numerical results demonstrating the improved parameter regimes. Finally, Chapter 6 discusses the broader implications of this work and qLDPC codes, including connections to decoding, quantum computing architectures, and theoretical results such as the resolution of the NLTS conjecture.

Ultimately, this work aims to contribute to the growing body of knowledge on how to design scalable, high-performance quantum codes. While not directly implementable in current hardware, the techniques developed here provide a roadmap for what properties should be sought in future constructions—and move us one step closer to building a truly fault-tolerant quantum computer.

*Chapter 2*

# CLASSICAL ERROR CORRECTION

Classical error correction provides the foundation for quantum error correction, as many principles in quantum coding theory originate from classical coding methods. The key idea in both classical and quantum settings is to introduce redundancy to detect and correct errors while preserving as much information as possible. In the quantum world, however, additional constraints such as the need to correct both bit-flip and phase-flip errors complicate the process.

In this chapter, we introduce fundamental concepts of classical error correction and draw intuitive connections to their quantum counterparts. We discuss classical linear block codes and Low-Density Parity-Check (LDPC) codes, and provide a detailed analysis of classical expander codes, where some of the main techniques used could be adapted to the quantum setting.

During data transmission and storage, errors might arise that randomly flip bits in a message. The goal of an error-correcting code is to introduce redundancy so that errors can be detected and corrected without losing information. A classical code achieves this by encoding a $k$-bit message into an $n$-bit codeword ($n > k$), adding redundancy to facilitate the process of error correction and detection. Given a received bit-string, some dedicated decoder could estimate the most likely codeword, correcting errors introduced by potential error sources and recovering the original message.

## 2.1 Linear Codes and Parity Checks

A fundamental class of classical codes is linear block codes, where codewords form a $k$-dimensional linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$. These codes are defined by a generator matrix $G \in \mathbb{F}_q^{n \times k}$ where its $k$ columns span $\mathcal{C}$, or a parity-check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$, satisfying $\mathcal{C} = \ker(H)$, i.e. for all valid codewords $x \in \mathcal{C}$, $Hx^T = 0$. The generator $G$ can be thought of as an encoding map that encodes a message $x$ as a codeword $Gx \in \mathcal{C}$, where the codeword encompasses added redundancy to the original message that protects it against potential corruptions from error sources. By the definition of a linear code, its encoding mapping is linear, so any linear combination of its codewords is still a codeword, and the all zero vector is a codeword, i.e. $0^n \in \mathcal{C}$. The

parity-check matrix $H$ can be interpreted as the set of linear constraints that a valid codeword must satisfy, which allows errors to be detected when violations occur.

When errors occur, the received bit-string can be expressed as $y = c + e$, where $e$ represents an error vector from the set of correctable errors $\mathcal{E}$. Applying the parity-check matrix to the received word yields

$$Hy^T = H(c + e)^T = He^T = s,$$

where $s$ is the syndrome vector indicating the presence of errors. If $s = 0$, $y$ is still a valid codeword, implying no detectable errors. Otherwise, $s$ provides essential information for syndrome decoding, a process that determines the most likely error pattern and corrects it accordingly. It is important to note that in the classical world, distinct errors need to lead to distinct syndromes in order for them to be correctable, i.e. $He_1^T \neq He_2^T$ for $e_1, e_2 \in \mathcal{E}, e_1 \neq e_2$. In comparison, the quantum setting allows for distinct errors to give rise to the same syndrome, which needs to be handled differently.

The effectiveness of a linear code is characterized by three key parameters denoted $[n, k, d]$, where $n$ is the code block length (the number of bits in each codeword), $k$ is the number of logical information bits in the original message, and $d$ is the minimum distance, defined as the smallest Hamming weight (number of non-zero bits) among all nonzero codewords in $\mathcal{C}$, i.e. $d = \min_{x \in \mathcal{C} \setminus 0^n} |x|$. The minimum distance $d$ dictates the code's error detection and correction capabilities: up to $d - 1$ errors can be detected, while $\lfloor (d - 1)/2 \rfloor$ errors can be corrected. It can be shown that distinct correctable errors lead to distinct syndromes with this metric since $|e_1|, |e_2| \leq \lfloor (d - 1)/2 \rfloor$, $|e_1 + e_2| \leq d - 1 < d$, so $H(e_1 + e_2)^T \neq 0$ and $e_1 \neq e_2$ for all $e_1, e_2 \in \mathcal{E}$.

A key goal in coding theory is the construction of asymptotically good codes, which maintain favorable properties as the block length $n$ grows. A family of codes is considered *asymptotically good* if it achieves a constant rate $R = k/n$ and relative distance $\delta = d/n$ bounded away from $0$ in the limit $n \to \infty$. This ensures that the code does not degrade in performance as the code length increases, making it scalable for large communication or computational systems.

One of the simplest forms of error detection is the parity-check code, a single-check code that appends one extra parity bit to a data block to ensure that the total number of ones is even (or odd, depending on convention). For example, in an $[n, k, d] = [4, 3, 2]$

single-parity-check code, a message $(x_1, x_2, x_3)$ is encoded as $c = (x_1, x_2, x_3, p)$, where $p = x_1 + x_2 + x_3 \mod 2$. The parity-check equation for this code is given by:

$$Hc^T = (x_1 + x_2 + x_3 + p) \mod 2 = 0.$$

Here, this code can only detect single-bit errors without identifying their location, as is expected for a code with $d = 2$. More sophisticated block codes such as Hamming codes extend this idea by introducing multiple parity checks to enable error correction rather than just detection and give rise to improved code parameters $[2^r - 1, 2^r - r - 1, 3]$, for integers $r \geq 2$. These simple constructions set the foundation for more powerful coding schemes.

### 2.2 Low-Density Parity-Check (LDPC) and Expander Codes

A natural extension of simple parity-check codes is the Low-Density Parity-Check (LDPC) code [Gal62], where the parity-check matrix $H$ is sparse, meaning that each row (parity-check equation) only involves a small a small, fixed number of bits from the codeword, and each bit of the original message participates in a limited number of parity checks. This sparsity allows for various efficient iterative decoding algorithms based on message-passing techniques, and moreover, specific constructions of LDPC codes on expander graphs give asymptotically good code parameters [SS96], which is the focus of this thesis. Overall, LDPC codes have been widely adopted in modern communication systems due to their capacity-approaching performance and scalability, and we would like to extend such constructions for quantum error correction as well.

#### Expander Graphs

Expander codes are a special class of LDPC codes that leverage the combinatorial properties of expander graphs to achieve excellent error-correcting capabilities, with constant rate and linear minimum code distance in the asymptotic regime. The core idea behind expander codes is to enforce local constraints on small subsets of codeword bits while ensuring that these constraints propagate globally due to the expansion properties of the underlying graph.

As such, expander graphs are key to the constructions of asymptotically good codes for both classical and quantum codes. Specifically, expander graphs have the property where a small set of vertices has large number of neighbors, allowing error patterns to spread and become correctable. We will include some of the important properties of an expander graph that will be helpful for later constructions.

Let $\mathcal{G} = (V, E)$ be an undirected $\Delta$-regular graph on $n$ vertices. Let its adjacency matrix be $A(\mathcal{G})$, which has $n$ real-valued eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. We are primarily interested in the second-largest eigenvalue (in magnitude), denoted by $\lambda(\mathcal{G}) := \max\{|\lambda_i| : |\lambda_i| \neq \Delta\}$. The graph $\mathcal{G}$ is $\Delta$-*regular* if every vertex has degree $\Delta$, and a $\Delta$-regular graph $\mathcal{G}$ is called *Ramanujan* if $\lambda(\mathcal{G}) \leq 2\sqrt{\Delta - 1}$.

A fundamental property of expander graphs that underpins their use in coding theory is their spectral gap, characterized by its second-largest eigenvalue $\lambda(\mathcal{G})$:

**Lemma 2.2.1** (Expander Mixing Lemma)**.** *Let $\mathcal{G} = (V, E)$ be a $\Delta$-regular graph on $n$ vertices with the second-largest eigenvalue $\lambda(\mathcal{G})$. For any two subsets $S, T \subseteq V$, let $|E(S,T)| = \{(x,y) \in S \times T : (x,y) \in E(\mathcal{G})\}$ denote the number of edges connected between vertices of the two subsets where the the edges contained in intersection of the two subsets are counted twice. Then*

$$\left| |E(S,T)| - \frac{\Delta |S||T|}{|V|} \right| \leq \lambda(\mathcal{G}) \sqrt{|S||T|}. \tag{2.1}$$

Lemma 2.2.1 provides us with an approximation of the average number of edges between two sets of vertices in a $\Delta$-regular graph, which closely resembles the edge distribution in a random graph, i.e. $\frac{\Delta|S||T|}{|V|}$, where edges are distributed uniformly. Here, $\frac{\Delta}{|V|}$ represents the probability that a specific edge exists between any two vertices in a random $d$-graph, and $|S||T|$ calculates total possible pair of vertices between $S$ and T. From this bound, we can also see that the second-largest eigenvalue $\lambda$ of the graph plays a significant role in quantifying how similar the expander graph is to a random one – a smaller $\lambda$ (i.e. larger spectral gap $\Delta - \lambda$) indicates stronger connectivity in $\mathcal{G}$.

### Expander Codes

Expander codes can then be constructed from the $\Delta$-regular graph $\mathcal{G} = (V, E)$, where the total number of edges in $\mathcal{G}$ is given by $|E| = \Delta|V|/2$, divided by 2 to account for each edge being counted twice, one at each of its endpoints.

To define a bipartite graph suitable for constructing an error-correcting code, we consider the edge-vertex incidence graph $\mathcal{B}$, which transforms the original graph into a structured bipartite representation. The two sets of nodes in this bipartite graph correspond to the edges and vertices of $\mathcal{G}$. On one side, the variable nodes represent the edges of $\mathcal{G}$, meaning that the number of variable nodes in $\mathcal{B}$ is precisely $|E|$.

On the other side, the constraint nodes correspond to the vertices of $\mathcal{G}$, so there are $|V|$ constraints. In this bipartite structure, each variable node (edge) is connected to exactly two constraint nodes (the two endpoints of the edge in $\mathcal{G}$), while each constraint node (vertex) is connected to exactly $\Delta$ variable nodes (the edges incident to that vertex).

The next step in constructing an expander code is defining local constraints. At each constraint node, we enforce a local error-correcting code $\mathcal{C}_0$ of block length $\Delta$. This means that for each constraint node (vertex in $\mathcal{G}$), the $\Delta$ variable nodes (edges incident to that vertex) must together form a valid codeword in $\mathcal{C}_0$. The purpose of these local constraints is to ensure that small groups of variables follow predefined error-correcting patterns, which collectively enhance the global error-correction capability of the expander code. The final code, denoted as $C(\mathcal{B}, \mathcal{C}_0)$, consists of all assignments to the variable nodes that satisfy every local constraint. We will show that $C(\mathcal{B}, \mathcal{C}_0)$ can achieve minimum rate of $2r - 1$ and minimum relative distance of $\epsilon(\epsilon - \lambda/\Delta)$, where $\mathcal{C}_0$ has code parameters $[\Delta, r\Delta, \epsilon\Delta]$.

**Lemma 2.2.2** (Minimum Rate and Distance of Expander Codes, [SS96])**.** *If $\mathcal{C}_0$ is a linear code of rate $r$, block length $\Delta$, and minimum relative distance $\epsilon$, and if $\mathcal{B}$ is the edge-incidence graph of a $\Delta$-regular graph with second-largest eigenvalue $\lambda$, then the code $C(\mathcal{B}, \mathcal{C}_0)$ has the rate at least $2r - 1$ and minimum relative distance at least $\epsilon(\epsilon - \lambda/\Delta)$.*

*Proof.* Let $\mathcal{G} = (V, E)$ be a $\Delta$-regular graph from which the edge-incidence graph $\mathcal{B}$ is derived. Since $\mathcal{C}_0$ is a linear code with rate $r$, then every vertex in $V$ imposes $(1 - r)\Delta$ linear restrictions on $C(\mathcal{B}, \mathcal{C}_0)$, which totals to at most unique $(1 - r)\Delta|V|$ number of linear restrictions. The code block length is the number of variable nodes, which is $|E| = \frac{\Delta|V|}{2}$. We can then compute the rate of $C(\mathcal{B}, \mathcal{C}_0)$ as

$$r' \geq \frac{|E| - (1 - r)\Delta|V|}{|E|} \tag{2.2}$$

Substituting $|E| = \frac{\Delta|V|}{2}$, we obtian

$$r' \geq \frac{\Delta|V|/2 - (1 - r)\Delta|V|}{\Delta|V|/2} = 2r - 1 \tag{2.3}$$

To bound the minimum relative distance, we fix a nontrival codeword $c \in C(\mathcal{B}, \mathcal{C}_0)$. Denote the set:

$$P = \{e \in E : c_e = 1\}$$

as the set of edges where the corresponding bit of the codeword is nonzero. Let $S$ be the subset of vertices in $V$ that are incident to at least one edge in $P$:

$$S = \{v \in V : \exists w \in V, (v, w) \in P\}.$$

Consider the subgraph $\mathcal{G}'$ of $\mathcal{G}$ induced by $S$. The number of edges in $\mathcal{G}'$, i.e. $|E(S, S)|$, is at most $2|c|$, since each edge is counted twice (once per endpoint). Additionally, because the local code $\mathcal{C}_0$ has minimum relative distance $\epsilon$, each vertex in $S$ must be incident to at least $\epsilon\Delta$ edges in $P$, meaning

$$\epsilon\Delta|S| \leq |E(S, S)| \leq 2|c|. \tag{2.4}$$

Furthermore, we also note that the number of edges in $\mathcal{G}'$ is constrained by the expansion properties of $\mathcal{G}$. By directly applying Lemma 2.2.1 with the subset $S$ and itself, we get

$$\left| E(S, S) - \frac{\Delta|S|^2}{|V|} \right| \leq \lambda|S| \tag{2.5}$$

Combining with previous bounds, we have

$$\epsilon\Delta|S| \leq E(S, S) \leq \lambda|S| + \frac{\Delta|S|^2}{|V|} \tag{2.6}$$

Rearranging:

$$\epsilon\Delta - \lambda \leq \frac{2|c|}{\epsilon|V|}. \tag{2.7}$$

Diving both sides by $\Delta$ and simplifying, we obtain the lower bound on the relative minimum distance of $C(\mathcal{B}, \mathcal{C}_0)$:

$$\frac{|c|}{|E|} \geq \epsilon(\epsilon - \lambda/\Delta). \tag{2.8}$$

□

From this result, it becomes evident that expander codes provide a powerful framework for error correction by leveraging the expansion properties of regular graphs. These codes enforce local constraints on small subsets of variables while ensuring that errors do not remain localized due to the strong connectivity of the underlying graph.

**Tanner Codes**

A natural generalization of this idea is Tanner codes, which can be viewed as a broader framework that includes expander codes as a special case. Like expander codes, Tanner codes are constructed from a bipartite graph where constraints are

imposed on small groups of variables using a local code. However, instead of restricting the graph structure to an edge-vertex incidence graph, Tanner codes allow a more general bipartite graph construction. Given a $\Delta$-regular expander graph $\mathcal{G} = (V, E)$, we define a Tanner code by assigning local error-correcting constraints at each vertex. Each edge $e \in E$ is assigned a value in $\mathbb{F}_2$, forming a vector space $\mathbb{F}_2^E$ of edge assignments. The local view of a vertex $v$ is the restriction of $x \in \mathbb{F}_2^E$ to the edges incident to $v$, denoted as $x_v \in \mathbb{F}_2^{E(v)}$. We further introduce a binary linear local code $\mathcal{C}_0$ of length $\Delta$ (which agrees with the degree of $\mathcal{G}$) that encodes $k_0 = \rho_0 \Delta$ bits of information with minimum distance $d_0 = \delta_0 \Delta$. The Tanner code $T(\mathcal{G}, \mathcal{C}_0)$ is then defined as the set of edge assignments in $\mathbb{F}_2^E$ such that the local view $x_v$ at each vertex $v \in V$ belongs to the local code $\mathcal{C}_0$. Formally,

$$T(\mathcal{G}, \mathcal{C}_0) = \{x \in \mathbb{F}_2^E : x_v \in \mathcal{C}_0 \text{ for all } v \in V\}.$$

In other words, a Tanner code consists of all edge assignments that satisfy the constraints imposed by the local code $\mathcal{C}_0$ at each vertex.

With particular choices of a linear code and an expander graph, we can obtain asymptotically good parameters for the expander codes. Applying the results of Lemma 2.2.2, we get the code parameters for $T(\mathcal{G}, \mathcal{C}_0)$ as

$$[n, (2\rho_0 - 1)n, \delta_0(\delta_0 - \lambda(\mathcal{G})/\Delta)n].$$

Thus, we can simply choose the local code $\mathcal{C}_0$ to have rate $\rho_0 > 1/2$ and the expander graph to have the expansion property $\lambda(\mathcal{G}) < d_0$ to arrive at asymptotically good codes.

The study of LDPC and expander codes has demonstrated that structured graph-based codes can achieve excellent error-correcting capabilities with efficient decoding. By leveraging sparse parity-check constraints and the expansion properties of graphs, these codes achieve both high rate and large minimum distance, making them scalable for practical applications. The key principles that make expander codes effective—including local constraints, global propagation of errors, and spectral expansion properties—are particularly relevant when designing quantum error-correcting codes, where new challenges arise due to the nature of quantum information.

*Chapter 3*

# QUANTUM ERROR CORRECTION

Classical error correction has shown that structured codes, particularly LDPC and expander codes, provide efficient and scalable ways to protect information from noise. By enforcing local constraints while leveraging the global connectivity of a sparse graph, these codes achieve a balance between high code rate and strong minimum distance. The success of these methods in classical settings naturally raises the question: how can we adapt these principles to the quantum domain?

Unlike classical information, which is stored in discrete bits that can only experience bit-flip errors, quantum information is represented by qubits that exist in a superposition of states. This fundamental difference introduces new challenges for error correction. In addition to bit-flip errors (analogous to classical bit errors), qubits can also experience phase-flip errors, and more generally, any arbitrary quantum noise due to unwanted interactions with the environment. Compounding these challenges, quantum mechanics imposes two major constraints: (1) the no-cloning theorem, which prevents making redundant copies of quantum information, and (2) state collapse upon measurement, meaning that errors must be detected without directly measuring the quantum state.

Despite these fundamental differences, many principles from classical error correction still provide valuable insight into how quantum error correction can be designed. Classical codes introduce redundancy to detect and correct errors by adding parity-check constraints, and similarly, quantum codes introduce entanglement-assisted redundancy to protect information. However, in the quantum setting, redundancy must be carefully encoded in non-measurable subspaces rather than explicit extra bits, requiring a different mathematical framework for constructing error-correcting codes.

This chapter aims to provide an intuitive yet rigorous introduction to quantum error correction, beginning with the stabilizer formalism [Got97], a powerful framework that generalizes classical parity-check codes to the quantum setting. We first establish how stabilizer codes encode logical qubits into a higher-dimensional Hilbert space while ensuring that correctable errors move code states into distinguishable error subspaces, allowing recovery without disturbing the encoded information. Then,

we introduce Calderbank-Shor-Steane (CSS) codes [CS96; Ste96], which use the structure of classical codes to correct both bit-flip and phase-flip errors independently. CSS codes provide a direct connection between classical coding theory and quantum error correction and serve as the foundation for many quantum codes, including surface codes and quantum LDPC codes. Finally, we conclude by discussing quantum LDPC (qLDPC) codes, which extend the principles of LDPC codes to the quantum setting. These codes aim to maintain sparse parity-check constraints while achieving large code distances, making them promising candidates for scalable, fault-tolerant quantum computation. The next chapter will explore the construction of qLDPC codes, particularly focusing on the quantum Tanner code construction and their implications for fault-tolerant quantum computing.

### 3.1 Conditions for Correctable Errors

A fundamental observation in quantum error correction is that any quantum error on a single qubit can be expressed in terms of Pauli matrices, derived from the fact that the Pauli matrices $I, X, Y, Z$ form a complete basis for all $2 \times 2$ matrices. This means that any arbitrary quantum error—no matter how complex—can be decomposed into a linear combination of these four operators. Thus, instead of dealing with an infinite number of possible quantum errors, such as small rotations or general unitary transformations, we only need to consider the effects of Pauli errors. As such, because the Pauli matrices span the space of all single-qubit operations, a quantum code that can correct all single-qubit Pauli errors can also correct any arbitrary single-qubit errors, which makes the process of quantum error correction tractable.

A quantum error-correcting code (QECC) is a subspace of a larger Hilbert space that is designed to protect quantum information from errors. Formally, we define a quantum code as a subspace $\mathcal{C}$ of the physical Hilbert space $\mathcal{H}_{\text{physical}}$, where logical qubits are redundantly encoded into a larger system of physical qubits: $\mathcal{C} \subseteq \mathcal{H}$. This encoding is performed by a unitary map $U : \mathcal{H}_{\text{logical}} \to \mathcal{C}$, which takes logical states and maps them into a higher-dimensional space, often introducing entanglement across multiple qubits. For example, if the logical space consists of $k$ qubits, the physical Hilbert space consists of $n$ qubits, and the code space $\mathcal{C}$ is spanned by a set of encoded basis states $\{|\bar{x}\rangle\}_{x\in\{0,1\}^k}$, where $\bar{x}$ denotes the encoded version of the classical bit string $x$ that has been mapped to a larger Hilbert space for error protection.

When an error acts on an encoded quantum state, it alters the state's amplitude and may shift it into an orthogonal error subspace. In general, a quantum error can be represented as an operator $E$ from an error set $\mathcal{E}$, typically a subset of the Pauli group, acting on a logical state $|\psi\rangle_L$ and producing a new, potentially corrupted state $E|\Psi\rangle$. When we measure the error syndrome, we do not directly collapse the quantum state onto one specific error. Instead, the measurement process projects the state onto a subspace associated with the particular error that occurred. The probability of getting a specific syndrome corresponding to error $E$ is

$$P_{E|\psi} = \langle\psi| E^\dagger E |\psi\rangle .$$

Because quantum states must remain normalized after syndrome measurement, the erroneous state must be rescaled by a factor of $1/\sqrt{P_{E|\psi}}$ to ensure proper normalization, resulting in

$$|\psi_E\rangle = \frac{1}{\sqrt{P_{E|\psi}}} |\psi\rangle_L .$$

For a quantum code to successfully correct errors, there must exist a recovery procedure that reverses the effects of noise without disturbing the encoded quantum information. A set of errors $\mathcal{E}$ is considered correctable by a code $\mathcal{C}$ if there exists a recovery operation $Rec(\cdot)$ such that, for any error $E \in \mathcal{E}$ and any logical state $|\psi\rangle_L \in \mathcal{C}$, the original logical state can be perfectly recovered, i.e.

$$Rec(|\psi_E\rangle) = |\psi\rangle_L .$$

However, it is important to note that not all quantum codes can correct all types of errors. The Knill-Laflamme conditions [KLV00] provide a precise mathematical criterion that determines whether a code can correct a specific set of errors. These conditions state that a set of errors $\mathcal{E}$ is correctable by a quantum code with code space $\mathcal{C}$ if and only if, for all $E_i$, $E_j \in \mathcal{E}$, there exists a constant $O_{E_1,E_2}$ such that:

$$\langle\psi_i| E_i^\dagger E_j |\psi_j\rangle = O_{E_i,E_j} \langle\psi_i|\psi_j\rangle \tag{3.1}$$

for all codewords $|\psi_i\rangle, |\psi_j\rangle \in \mathcal{C}$.

This means that when an error acts on a quantum state, it does not scramble logical information. Instead, errors must act in a way that only scales the inner product between codewords, ensuring that the code space remains distinguishable even after errors occur. This allows the syndrome measurement process to extract information

about the error without collapsing the encoded quantum state. Intuitively, different logical states must remain identifiable even after errors act. If errors were to mix different logical states unpredictably, error correction would be impossible.

This condition also implies that errors $E_i, E_j$ act identically within the code space up to a global scaling factor, meaning they cannot be distinguished by syndrome measurement alone. Some errors may act differently on physical qubits but produce the same effect on the logical states, thus yielding the same error syndrome. This is a fundamental property of quantum error correction: rather than identifying specific errors, the goal is to correct equivalence classes of errors, where two errors are equivalent if they produce the same logical transformation on the code space.

This insight fundamentally changes how quantum codes are designed. Instead of assigning a unique syndrome to every possible error, quantum codes ensure that errors affecting physical qubits can be grouped into equivalence classes, with each class corresponding to a distinct correctable syndrome.

### 3.2 The Stabilizer Formalism

The stabilizer formalism is one of the most powerful mathematical frameworks for efficiently managing these equivalence classes and enforcing the structure needed for error correction. Instead of defining a quantum code by explicitly listing its codewords, the stabilizer formalism describes the code as the simultaneous $+1$ eigenspace of a set of carefully chosen operators. These operators, known as stabilizers, form a commuting subgroup of the Pauli group and impose constraints that give rise to error detectability and correctability.

At the core of the stabilizer formalism is the Pauli group $\mathcal{P}_n$ on $n$ qubits. The Pauli group consists of all $n$-qubit operators that are tensor products of single-qubit Pauli matrices:

$$\mathcal{P} = \{\pm I, \pm X, \pm Y, \pm Z\}.$$

For multiple qubits, the $n$-qubit Pauli group $\mathcal{P}_n$ is defined as:

$$\mathcal{P}_n = \{P_1 \otimes P_2 \otimes \cdots \otimes P_n | P_i \in \mathcal{P}\}.$$

These operators either commute or anti-commute with each other, a key feature that makes them useful for error detection.

A stabilizer code is defined by a stabilizer group $\mathcal{S}$, which is an abelian (commutative) subgroup of the Pauli group that does not contain $-I$. The stabilizer group consists

of $2^{n-k}$ independent stabilizer generators, where the code encodes $k$ logical qubits in $n$ physical qubits, and each stabilizer $S_i$ satisfies:

$$S_i \left|\psi\right\rangle = \left|\psi\right\rangle, \forall S_i \in \mathcal{S}, \left|\psi\right\rangle \in \mathcal{C}.$$

Thus, valid codewords of the stabilizer code $\mathcal{C}(\mathcal{S})$ are the simultaneous eigenstates of all stabilizers with eigenvalue $+1$. Here, errors in a stabilizer code are detected through syndrome measurement. Each stabilizer generator $S_i$ acts as a parity-check operator, where if the code state is error-free, the measurement returns $+1$ for all stabilizers; if an error $E$ occurs, it may anti-commute with some stabilizers, flipping their eigenvalue to $-1$. The syndrome $s(E)$ is a binary vector indicating which stabilizers detect an error:

$$s(E) = (s_1, s_2..., s_{n-k}), \text{ where } s_i = \begin{cases} 0, \text{ if } S_i E = E S_i \\ 1, \text{ if } S_i E = -E S_i. \end{cases}$$

Here, different error equivalence classes correspond to different syndromes, allowing us to determine how to correct the system without directly measuring the logical qubits.

Errors in a quantum stabilizer code can be classified into three distinct types based on their relationship with the stabilizer group. The first type consists of errors $E \in \mathcal{P}_n$ that anticommute with one or more stabilizer generators. These errors are detectable because they flip the eigenvalue of the affected stabilizers from $+1$ to $-1$ and produce a nontrivial syndrome that allows the error to be identified and corrected. Since syndrome measurements reveal which stabilizers have changed, the decoder can infer the most likely error and apply a correction without disturbing the encoded quantum information.

If the error is an element of the stabilizer group itself, i.e. $E \in \mathcal{S}$, then they act trivially on the code space because stabilizer operators define the space of valid code states. Applying a stabilizer to a valid codeword leaves it unchanged, meaning such errors have no observable effect on the encoded logical qubits. Since stabilizer errors do not alter the syndrome or the logical state, they are automatically corrected by the structure of the code.

The third type of errors are errors that commute with all stabilizers but act as logical operators on the code space. These errors do not change the stabilizer measurements but modify logical qubits, meaning they cannot be detected through syndrome extraction and are thus uncorrectable. The smallest weight of such a Pauli error

$E \in \mathcal{P}_n - \mathcal{S}$ that commutes with all stabilizers but acts as a nontrivial logical operation on the encoded qubits is considered as the code distance of stabilizer codes. Since these errors remain undetectable within the stabilizer framework, they accumulate over time and must be minimized for fault-tolerant quantum computation.

### 3.3 CSS Codes

While the stabilizer formalism provides a general framework for constructing quantum codes, certain families of stabilizer codes exhibit additional structures that simplify the encoding and decoding processes. One particularly important subclass is the Calderbank-Shor-Steane (CSS) codes, which leverage the fact that bit-flip ($X$-type) and phase-flip ($Z$-type) can be corrected independently. The key insight behind CSS codes is that classical parity-check matrices can be adapted to construct stabilizer generators consisting entirely of either $X$-type or $Z$-type Pauli operators, thereby simplifying both encoding and decoding procedures. This structure makes CSS codes one of the most practical and widely used families of quantum error-correcting codes.

Specifically, a CSS code is constructed from two classical codes, $C_X$ and $C_Z$, with code parameters $[n, k_X, d_X]$ and $[n, k_Z, d_Z]$ respectively. The idea is to use the parity checks of $C_X$ to correct phase-flip $Z$ errors and the parity checks of $C_Z$ to correct bit-flip errors $X$. Since phase errors behave like bit errors in the Hadamard basis ($HZH = X$), the structure of CSS codes allows independent correction of both error types. The stabilizer group of a CSS code is generated by two sets of stabilizer operators: $X$-type stabilizers and $Z$-type stabilizers, corresponding to generators of the form: $X^{h_X}, Z^{h_Z}$ for $h_X \in C_X^{\perp}, h_Z \in C_Z^{\perp}$ respectively. Here, $C_Z^{\perp}$ is the dual code of $C_Z$, which consists of all binary vectors orthogonal to every codeword in $C_Z$ under the standard inner product over $\mathbb{F}_2$:

$$C_Z^{\perp} = \{v \in \mathbb{F}_2 | v \cdot w = 0, \forall w \in C_Z\},$$

and the same applies for $C_X^{\perp}$, which consists of all parity-check constraints for $C_X$. Overall, the $X$-stabilizers enforce the parity checks from $C_X$ to detect $Z$ errors, and vice versa for $Z$-stabilizers.

To ensure that the stabilizer group forms a valid quantum code, these operators must satisfy the stabilizer commutativity condition, meaning that all $X$-type and $Z$-type stabilizers must commute with each other, i.e.

$$X^{h_X} Z^{h_Z} = (-1)^{\langle h_X, h_Z \rangle} Z^{h_Z} X^{h_X},$$

where $\langle h_X, h_Z \rangle = \sum_{i=1}^{n} h_{X,i} h_{Z,i} \mod 2$ is the binary inner product. We then need to enforce the condition $\langle h_X, h_Z \rangle = 0$, which is equivalent to the following dual containment condition:

$$C_X^{\perp} \subseteq C_Z, C_Z^{\perp} \subseteq C_X.$$

This condition guarantees that the stabilizers commute and defines a valid CSS code.

The logical codewords in CSS codes are constructed as superpositions of cosets of one classical code within another. More specifically, for every $c_Z \in C_Z$, the code logical basis states of the CSS code $\mathcal{Q}$ are formed as uniform superpositions over cosets of $C_X^{\perp}$ within $C_Z$:

$$\mathcal{Q} := \text{Span} \left\{ \frac{1}{\sqrt{|C_X^{\perp}|}} \sum_{h_X \in C_X^{\perp}} |c_Z + h_X\rangle \right\}.$$

Such an encoding procedure expresses that each quantum codeword is constructed from classical codewords in $C_Z$ but includes a sum over cosets of $C_X^{\perp}$ to ensure that the quantum state remains protected against both bit-flip and phase-flip errors.

The number of logical qubits encoded is equivalent to the number of degrees of freedom remaining after imposing stabilizer constraints, and in the case of CSS codes,

$$k = \dim(C_X) - \dim(C_Z^{\perp}).$$

The distance of a CSS code is determined by the minimum weight of an undetectable logical error, meaning an error that commutes with all stabilizers but acts non-trivially on the logical subspace. To analyze this, we separately consider bit-flip $X$ and phase-flip $Z$ errors. A bit-flip error $X^e$ on $n$ qubits, where $e \in \{0,1\}^n$, is detectable if it produces a nonzero syndrome when measured against the $Z$-type stabilizers. The syndrome of $X^e$ is given by the inner product $\langle h_Z, e \rangle \mod 2$, where $h_Z \in C_Z^{\perp}$, meaning that $X^e$ is undetectable if and only if $e \in C_Z$. It is important to note that in the stabilizer construction, if the error $e \in C_X^{\perp}$, $X^e$ acts trivially on all codewords in $\mathcal{Q}$, i.e. $X^e |\psi\rangle_L = |\psi\rangle_L$. As such, the smallest nontrivial bit-flip error that is undetectable is given by the minimum weight of any element in $C_Z$ that is not already in $C_X^{\perp}$. We then define the quantity $d_Z$ as the smallest non-trivial bit-flip errors that we cannot detect:

$$d_Z = \min_{e \in C_Z \setminus C_X^{\perp}} |e|.$$

Similarly, phase-flip $Z$ errors are detectable using the $X$-stabilizers defined by $C_X^{\perp}$, and the smallest undetectable $Z$ error corresponds to an element in $C_X$ not in $C_Z^{\perp}$,

leading to

$$d_X = \min_{e \in C_X \setminus C_Z^\perp} |e|.$$

The overall distance of the CSS code $\mathcal{Q}$ is

$$d = \min(d_X, d_Z).$$

We denote the resulting quantum code parameters by $[\![n, k, d]\!]$, and the CSS code $\mathcal{Q}(C_X, C_Z)$ has the code parameters $[\![n, k_X + k_Z - n, \min(d_X, d_Z)]\!]$. Similar to classical codes, we would like to construct asymptotically good quantum codes, where $k \sim \mathcal{O}(n)$ and $d \sim \mathcal{O}(n)$.

### 3.4 Quantum LDPC Codes

Quantum low-density parity-check (LDPC) codes are a subclass of CSS codes that combine the structure of stabilizer codes with the sparsity and efficient decoding properties of classical LDPC codes. Just as classical LDPC codes use sparse parity-check matrices to enable efficient syndrome decoding, quantum LDPC codes employ sparse check matrices $H_X$ and $H_Z$ to define stabilizers with low-weight constraints. The goal is to achieve high-distance, high-rate quantum codes that are both scalable and efficiently decodable, suitable for fault-tolerant quantum computation.

Historically, the earliest example of a quantum LDPC code was the toric code [Kit03], which provided a foundational framework for topological error correction but suffered from a low number of logical qubits, encoding only a constant number while achieving a distance of $\mathcal{O}(\sqrt{n})$. The development of hypergraph product codes [TZ13; BH14] marked a significant improvement, allowing for a linear number of logical qubits while maintaining a $\mathcal{O}(\sqrt{n})$ distance scaling. Subsequent constructions such as fibre bundle codes [HHO21], lifted product codes [PK21a], and balanced product codes [BE21] introduced algebraic and topological methods to push distance scaling beyond $\sqrt{n}$, achieving sublinear improvements with scalings like $\tilde{\Omega}(n^{3/5})$, $\tilde{\Omega}(n^{1-\alpha/2})$, and $\Omega(n^{3/5})$, respectively. Despite these advances, breaking past the $\sqrt{n}$ barrier proved difficult, as balancing the trade-offs between rate, distance, and sparsity required new mathematical techniques.

Notably, both lifted product (LP) and balanced product (BP) codes use highly similar and often interchangeable techniques. The LP framework in particular played a pivotal role in paving the way toward asymptotically good constructions. Indeed, recent breakthroughs constructions [PK22; LZ22; Din+23] have broken this barrier and achieved both linear rate and linear distance. Despite their differences, these

constructions share several key properties that were crucial in achieving both linear rate and linear distance. Similar to classical LDPC codes, they rely on expander graph structures, which provide strong local connectivity properties while maintaining a robust global code distance. These constructions also enforce some variants of local-to-global properties, which allows small-scale constraints imposed by local stabilizer checks to effectively extend to global error suppression.

In the next chapters, we will explore how quantum Tanner codes [LZ22] achieve both linear rate and linear distance, and investigate methods to improve their relative distance.

*Chapter 4*

# QUANTUM TANNER CODE CONSTRUCTION

Quantum Tanner codes are derived from classical Tanner codes defined on a square complex. By placing qubits on the faces of the square complex and enforcing local parity constraints at the vertices, quantum Tanner codes achieve good asymptotic performance while offering a conceptually simpler foundation than previous constructions based on chain complexes or homological products. In this chapter, we will present the construction of quantum Tanner codes, the conditions needed for local codes, and an analysis of the code parameters.

## 4.1 Left-Right Cayley Complex

At the heart of the quantum Tanner code construction lies a square complex known as the left-right Cayley complex, first presented in [Din+22]. This combinatorial object is derived from a finite group $G$ and two symmetric generating sets $A, B \subset G$, each closed under inversion $A^{-1} = A, B^{-1} = B$ and of size $\Delta$. The vertex set of the complex is bipartitioned as $V = V_0 \cup V_1$, where each part is identified as a copy of $G$: specifically, $V_0 = G \times \{0\}, V_1 = G \times \{1\}$. Edges in the complex are separated into two types: an $A$-edge connects $(g, 0)$ to $(ag, 1)$ for each $a \in A$, and a $B$-edge connects $(g, 0)$ to $(gb, 1)$ for each $b \in B$. We use $E_A$ to denote the set of $A$-edges and $E_B$ for the set of $B$-edges. Squares in this complex are defined as the 4-tuples

$$\{(g, 0), (ag, 1), (gb, 1), (agb, 0)\},$$

where diagonally opposite vertices belong to the same part of the partition, i.e. $(g, 0), (agb, 0) \in V_0$ and $(ag, 1), (gb, 1) \in V_1$. The collection of such squares form the set $\mathcal{Q}$, and each square can be viewed as a qubit in the quantum code.

To ensure the structure is well-behaved, the complex must satisfy the *Total No-Conjugacy* (TNC) condition: for all $g \in G, a \in A, b \in B$, we require that $ag \neq gb$. This guarantees that squares are non-degenerate and that each vertex has a well-defined local neighborhood isomorphic to a grid.

For each vertex $v \in V$ (either in $V_0$ or $V_1$), we define its $Q$-neighborhood, denoted $Q(v)$, as the set of all squares $q \in \mathcal{Q}$ incident to $v$. Since every square is defined as a 4-tuple of group-labeled vertices, each vertex appears in precisely $\Delta^2$ squares,

i.e. its $Q$-neighborhood contains $\Delta^2$ squares. Without loss of generality, for a vertex $v \in V_0$, its $Q$-neighborhood is a bijection with the Cartesian product $A \times B$:

$$(a, b) \in A \times B \leftrightarrow q = \{v, (ag, 1), (gb, 1), (agb, 0)\} \in \mathcal{Q}.$$

This means we can view $Q(v)$ as a $\Delta \times \Delta$ matrix, where each row is indexed by $a \in A$ and each column by $b \in B$. This grid-like structure of each vertex's neighborhood allows us to apply structured, two-dimensional local constraints in a natural way. In particular, each row of the grid corresponds to a fixed $a \in A$ and varies over all $b \in B$, and each column corresponds to a fixed $b \in B$ and varies over $a \in A$, meaning that any constraints imposed on a row or column extend naturally to neighboring vertices in the complex. When two vertices share a row or column — which happens naturally in this complex due to the way squares overlap — they also share some of their constraints. This shared structure is particularly useful for defining parity-check conditions in quantum codes, as it allows local constraints to propagate globally through the complex.

Note that the square complex $\mathcal{Q}$ naturally induces two graphs, where we restrict the vertex set in $\mathcal{Q}$ to $V_0$ and $V_1$ respectively. When restricted to $V_0$, every square is incident to only two vertices, and the set of squares can be seen as a set of edges on $V_0$. We then define the graph $\mathcal{G}_0^{\square}(V_0, \mathcal{Q})$ with vertex set $V_0$ and with edges given by the set of squares shared between vertices in $V_0$, and similar for $\mathcal{G}_1^{\square}(V_1, \mathcal{Q})$. These graphs connect vertices in $V_0$ (and $V_1$) that share common squares, and we will use them as structures that support local constraints, which then lead to CSS codes.

### 4.2 Local Codes on the Square Complex

Since each $Q$-neighborhood is naturally structured as a grid, a tensor product code aligns perfectly with this structure. We first choose two classical codes $C_A, C_B$, both of length $\Delta$, then construct the tensor product code $C_A \otimes C_B$, which consists of all $\Delta \times \Delta$ matrices where each row belongs to $C_A$ and each column belongs to $C_B$. The parity check of a tensor code, i.e. $(C_A \otimes C_B)^{\perp}$, can be thought of as a codespace where every column of the codeword is in $C_A^{\perp}$ or every row of the codeword is in $C_B^{\perp}$, written as $(C_A \otimes C_B)^{\perp} = C_A^{\perp} \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^{\perp}$, and similarly, $(C_A^{\perp} \otimes C_B^{\perp})^{\perp} = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$. We construct two classical Tanner codes using graphs $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$ with local constraints enforced by the codewords of tensor codes $C_A \otimes C_B$ and $C_A^{\perp} \otimes C_B^{\perp}$, respectively. We will show that the following classical Tanner codes satisfy the CSS code properties:

$$\mathcal{C}_0 = T(\mathcal{G}_0^{\square}, (C_A \otimes C_B)^{\perp}), \mathcal{C}_1 = T(\mathcal{G}_1^{\square}, (C_A^{\perp} \otimes C_B^{\perp})^{\perp}).$$

**Proposition 4.2.1.** *$\mathcal{C}_0, \mathcal{C}_1$ forms a CSS code.*

*Proof.* Consider a vertex $v \in V_0$ and $u \in V_1$. At the $Q$-neighborhood of $v$, there are some parity checks $h_X \in C_A \otimes C_B$ enforced by the local code $(C_A \otimes C_B)^\perp$. Similarly, $Q(u)$ contains parity check $h_Z \in C_A^\perp \otimes C_B^\perp$ by construction. We will show that these parity checks commute, i.e. $h_X \cdot h_Z = 0$. In the trivial case where the $Q$-neighborhoods of the two vertices do not share any squares, i.e. $Q(v) \cap Q(u) = \varnothing$, $h_X \cdot h_Z = 0$ since each of the parity checks is only non-zero on its corresponding $Q$-neighborhood. In the case where their $Q$-neighborhood intersects on some $\Delta$ number of squares, we know that they must share an $A$-edge, which means that $h_X \in C_B$ and $h_Z \in C_B^\perp$, so $h_X \cdot h_Z = 0$. This completes the proof that $\mathcal{C}_0$ and $\mathcal{C}_1$ form a CSS code. □

### 4.3 Code Rate

The rate of a CSS code is determined by the rates of the underlying classical codes used in the Tanner construction. We pick $C_A$ and $C_B$ to have code parameters $[\Delta, \rho\Delta, \delta\Delta]$ and $[\Delta, (1-\rho)\Delta, \delta\Delta]$, respectively, for some $\rho \in [0, 1]$.

In the square complex, we have $|V| = 2|G|$ vertices and $|\mathcal{Q}| = |G||A||B|/2 = |G|\Delta^2/2$ number of squares, which gives us $n = |G|\Delta^2/2$ block length for the quantum Tanner code. We first count the number of constraints placed by $C_A \otimes C_B$, which is the parity check for $(C_A \otimes C_B)^\perp$, for a given vertex in $\mathcal{G}_0^\square$:

$$\dim(C_A \otimes C_B) = \dim(C_A)\dim(C_B) = \rho\Delta(1-\rho)\Delta = \rho(1-\rho)\Delta^2.$$

Similarly, there are at most $\dim(C_A^\perp \otimes C_B^\perp) = \rho(1-\rho)\Delta^2$ constraints placed by the local code $(C_A^\perp \otimes C_B^\perp)^\perp$ per vertex in $\mathcal{G}_1^\square$. The total number of constraints in the Cayley complex is at most $2 \cdot |G| \cdot \rho(1-\rho)\Delta^2 = 4|G|\rho(1-\rho)\Delta^2$. The number of encoded qubits, which is the number of independent checks subtracted from the number of physical qubits, is then

$$k \geq |G|\Delta^2/2 - 2|G|\Delta^2\rho(1-\rho) = (2\rho-1)^2 n.$$

Thus, the number of logical qubits is linear in $n$, which gives us the desired constant rate. We note that each parity check involves one $Q$-neighborhood, which has size $\Delta^2$. Moreover, each qubit (which lives on the squares) is part of at most $2\rho(1-\rho)\Delta^2$ parity checks. As long as $\Delta$ is constant, the quantum Tanner codes have constant check weights.

## 4.4 Code Distance

The goal of this thesis is to improve the relative distance of the quantum Tanner codes. Although the current construction achieves a desirable constant relative distance, the constant is too small for the code to be useful in any practical setting. We present a construction that combines the left-right Cayley complex with local codes that are robustly testable, and we will explicitly derive the distance bound that will be improved upon in a later chapter.

### Robustly Testable Codes

Because of the unique structure of tensor product codes, for $x \in C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp$, we can decompose it into $x = c + r$, where $c \in C_A^\perp \otimes \mathbb{F}_2^B$ and $r \in \mathbb{F}_2^A \otimes C_B^\perp$. Intuitively, it would be desirable to have the property that when we add $c$ and $r$ together, the Hamming weight of the sum $x$ doesn't differ significantly from the Hamming weight of $c$ and $r$ individually. In this way, $|x| \approx |c| + |r|$, and any lower bounds on $|c|$ and $|r|$ will allow us to arrive at an expression for the distance of the code.

This intuition can be extended to a robustness property called $\kappa$-product expansion [KP22], stated as following:

**Definition 4.4.1.** *A code $C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp$ is called $\kappa$-product expanding if for any codeword $x$ with its decomposition $x = r + c$ for $c \in C_A^\perp \otimes \mathbb{F}_2^B$ and $r \in \mathbb{F}_2^A \otimes C_B^\perp$,*

$$|x| \geq \kappa\Delta(\|c\| + \|r\|)$$

*for some constant $\kappa$ that is independent of the code length $\Delta$.*

Here, the norm $\|c\|$ denotes the number of non-zero columns of $c$ (equivalent to the number of non-zero codewords in $C_A^\perp$) that are supported by $c$. The same argument applies to $\|r\|$ with respect to rows of $r$.

Such property does not hold generally since whenever $c$ and $r$ share many non-zero entries, $|x|$ would be much smaller than $|c| + |r|$. The question becomes when would this product expansion property hold? Ultimately, randomly selected codes $C_A$ and $C_B$ are sufficient, as shown in [KP22] and summarized in Theorem 4.4.2. We can then use this relation to derive a linear lower bound for the distance of the quantum code!

**Theorem 4.4.2.** *For a pair of codes $C_A = [\Delta, \rho\Delta]$ and $C_B = [\Delta, (1-\rho)\Delta]$ sampled uniformly at random, the code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is $\kappa$-product-expanding with*

*high probability as* $\Delta \to \infty$ *with*

$$\kappa = \frac{1}{2} \min \left( \frac{1}{4} H_2^{-1}(\rho/8)^2, H_2^{-1}(\rho/8)^2 \right),$$

*where* $H_2^{-1}$ *is the inverse of the binary entropy function given by*

$$H_2(x) := -x \log_2(x) - (1-x) \log_2(1-x).$$

In Chapter 5, we will provide in-depth analysis of an improved version of this theorem.

**Decomposition of a Codeword**

We wish to bound the Hamming weight of codeword $x \in \mathcal{C}_1 \backslash \mathcal{C}_0^\perp$, which can be achieved by first obtaining the minimal representation of $x$, then using the product expansion property to relate the Hamming weight of $x$ and its norm. We choose $C_A, C_B$ as well as their dual codes to have at least distance $\delta\Delta$ for some non-zero constant $\delta$.

Here, $x$ lives on the graph $\mathcal{G}_1^\square$ and needs to satisfy the local constraint

$$(C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B.$$

For each vertex $v$ in $V_0 \cup V_1$, we examine its $Q$-neighborhood $Q(v)$, where the restriction of $x$ to $Q(v)$, denoted as $x_v$, can be written as:

$$x_v = c_v + r_v,$$

where $c_v \in C_A \otimes \mathbb{F}_2^B$ is the column component of $x_v$, and $r_v \in \mathbb{F}_2^A \otimes C_B$ is the row component of $x_v$. Within each Q-neighborhood, the codeword decomposes into row and column contributions. Using our prior definition of the norm $\|\cdot\|$, $\|c_v\|$ ($\|r_v\|$) is simply the number of non-zero columns (rows) in $c_v$ ($r_v$), and since the distance of $C_A$ and $C_B$ are $\delta\Delta$, for every non-zero column, there must be at least $\delta\Delta$ non-zero bits. We could then relate the Hamming weight and norm as following:

$$|c_v| \geq \delta\Delta \|c_v\|, |r_v| \geq \delta\Delta \|r_v\|.$$

We define the norm of $x$ as

$$\|x\| := \sum_{v \in V_1} (\|c_v\| + \|r_v\|).$$

We could then relate the norm and Hamming weight of $x$ via the product-expansion property:

**Lemma 4.4.3.** *If $x \in \mathcal{C}_1 \backslash \mathcal{C}_0^\perp$ and the choices of local codes used for $\mathcal{C}_0$ and $\mathcal{C}_1$ have $\kappa$-product-expanding property, then*

$$|x| \geq \frac{\kappa\Delta}{2}\|x\|.$$

*Proof.* Consider the decomposition $x_v = c_v + r_v$ for $v \in V_1$, we know that from product expansion,

$$|c_v + r_v| \geq \kappa\Delta(\|c_v\| + \|r_v\|).$$

Summing over all vertices in $V_1$, we obtain

$$\sum_{v \in V_1} |x_{Q(v)}| \geq \kappa\Delta \sum_{v \in V_1} (\|c_v\| + \|r_v\|) = \kappa\Delta\|x\|.$$

However, each square (qubit) double appears in exactly two $Q$-neighborhood, so the sum $\sum_{v \in V_1} |x_{Q(v)}|$ double-counts each nonzero entry of $x$:

$$\sum_{v \in V_1} |x_{Q(v)}| = 2|x|.$$

Combining both bounds, we arrive at

$$|x| \geq \frac{\kappa\Delta}{2}\|x\|.$$

□

**Exceptional and Ordinary Vertices**

We first define the active set $S_i$ as the set of vertices in $V_i$ where the restriction of $x$ to the $Q$-neighborhood is nonzero:

$$S_i = \left\{ v' \in V_i : \left( \sum_{v \in V_i} c_v + r_v \right)_{Q(v')} \neq 0 \right\}.$$

Since we are interested in the minimum weight of $x$, we can bound the size of this set by

$$|S_1| \leq \sum_{v \in V_1} \|c_v\| + \|r_v\|.$$

To further classify the contributions of different vertices, we define a threshold of $\alpha\Delta$, where $\alpha$ is a fixed constant dependent on the minimum distance of the local codes. A vertex $v \in V_1$ is said to be exceptional if the total number of nonzero rows

and columns in its $Q$-neighborhood exceeds this threshold, and ordinary otherwise. Formally, we define the sets:

$$S_i^e = \{v \in V_i : \|c_v\| + \|r_v\| \geq \alpha\Delta\}$$
$$S_i^o = \{v \in V_i : \|c_v\| + \|r_v\| < \alpha\Delta\}$$

Thus, every active vertex belongs to either the exceptional or ordinary set, and we express this partition as

$$S_i = S_i^e \cup S_i^o.$$

This classification allows us to distinguish between high-weight regions, where weight propagation is concentrated, and low-weight regions, where contributions are more localized. We will use this distinction to analyze how weight spreads across the Cayley graphs and to bound the minimum distance of the quantum Tanner code.

First, we note that $\mathcal{G}_0^\square$ and $\mathcal{G}_1^\square$ are Ramanujan graphs:

**Lemma 4.4.4.** *If $\mathcal{G}_A = (V = V_0 \cup V_1, E_A)$ and $\mathcal{G}_B = (V = V_0 \cup V_1, E_B)$ are Ramanujan graphs, then*

$$\lambda(\mathcal{G}_0^\square) \leq 4\Delta, \lambda(\mathcal{G}_1^\square) \leq 4\Delta.$$

*Proof.* Let $M_A$ and $M_B$ be the adjacency matrices of the bipartite Ramanujan graphs $\mathcal{G}_A$ and $\mathcal{G}_B$, with nontrivial eigenvalues bounded by $2\sqrt{\Delta}$. Since $M_A$ and $M_B$ commute, the eigenvalues of $M_A M_B$ are products of eigenvalues of $M_A$ and $M_B$, and thus are bounded by $4\Delta$. The graph $\mathcal{G}^\square$ defined by $M_A M_B$ splits into two components: $\mathcal{G}_0^\square$ and $\mathcal{G}_1^\square$. Each inherits the spectral bound $\lambda \leq 4\Delta$. □

We will then show in Lemma 4.4.5 that if the set $S_i$ is small enough to begin with, then the number of exceptional vertices is simply a small fraction of $|S_i|$, on the order of $\mathcal{O}(1/\Delta^2)$:

**Lemma 4.4.5.** *If $|S_i|/|V_i| \leq \frac{\kappa\alpha}{2}$,*

$$|S_i^e| \leq \frac{64}{\kappa^2\alpha^2\Delta^2}|S_i|$$

*Proof.* Without loss of generality, consider $v \in S_1^e$. By definition, the number of nonzero rows and columns in $Q(v)$ satisfies

$$\|c_v\| + \|r_v\| \geq \alpha\Delta.$$

Applying the product expansion property of the Tanner graph, we get

$$|x_{Q(v)}| \geq \kappa\Delta(\|c_v\| + \|r_v\|) \geq \kappa\alpha\Delta^2.$$

Thus, each exceptional vertex has degree of at least $\kappa\alpha\Delta^2$, which means it contributes at least $\kappa\alpha\Delta^2$ weight to $x$.

We can also apply the Expander Mixing Lemma 2.2.1 to arrive at an upper bound in terms of $|S_1^e|$:

$$|E(S_1^e, S_1)| \leq \frac{\Delta^2}{|V_1|}|S_1^e||S_1| + \lambda(\mathcal{G}_1^{\square})\sqrt{|S_1^e||S_1|}$$

By Lemma 4.4.4, we have that $\lambda(\mathcal{G}_1^{\square}) \leq 4\Delta$. Combining both bounds, we arrive at

$$\kappa\alpha\Delta^2|S_1^e| \leq \frac{\Delta^2}{|V_1|}|S_1^e||S_1| + 4\Delta\sqrt{|S_1^e||S_1|}. \tag{4.1}$$

Solving the above inequality with the assumption that $|S_1|/|V_1| \leq \frac{\kappa\alpha}{2}$, we arrive at the desired bound

$$|S_1^e| \leq \frac{64}{\kappa^2\alpha^2\Delta^2}|S_1|. \tag{4.2}$$

□

Here, since the number of exceptional vertices is limited, we focus on describing the behavior of the code mostly through the ordinary vertices. Although ordinary vertices contribute only limited local weight, the rows and columns they activate must necessarily appear in other $Q$-neighborhoods as well, due to the overlapping structure of the square complex. We then introduce a set $T$, defined as the set of vertices in $V_0$ whose $Q$-neighborhood shares a nonzero row or column with that of an ordinary vertex—i.e., a vertex in $S_1^o$:

$$T := \{v \in V_0 : \exists w \in S_1^o \text{ such that } x_{Q(v)} \text{ and } x_{Q(w)} \text{ share a nonzero row or column}\}.$$

Now, we construct a bipartite graph between $S_1^o \subset V_1$ and $T \subset V_0$ with an edge $w \sim v$ if their local views share a nonzero row or column. This bipartite structure captures how support from the local view of $x$ propagates across the square complex. Our goal is to show that this propagation is limited — specifically, that the size of $T$ cannot be too large in terms of the size of $|S_1|$, under a mild sparsity assumption.

**Lemma 4.4.6.** *If* $|S_0| \leq \frac{\delta}{4}|V_1|$,

$$|T| \leq \frac{64}{\delta^2\Delta}|S_1|.$$

*Proof.* Let $v \in T \subset V_0$. By definition of $T$, its $Q$-neighborhood shares at least one nonzero column with the local view of some vertex $w \in S_1^o$. Since $w$ is ordinary, the number of rows or columns in its local view is limited to at most $\alpha\Delta$. However, for each column, say $c_w$, the local codeword structure ensures weight of at least $\delta\Delta$. Here, the "residual weight" in each shared row/column must come from $v \in T$. Thus, every vertex $v \in T$ must carry at least $\delta\Delta - \alpha\Delta$ nonzero entries in its local view, giving us

$$|E(S_1^o, T)| \geq (\delta\Delta - \alpha\Delta) \cdot |T|.$$

We can then apply an upper bound by applying the Expander Mixing Lemma 2.2.1, arriving at

$$|E(S_1^o, T)| \leq \frac{\Delta}{|V_1|}|S_1^o||T| + 2\sqrt{\Delta}\sqrt{|S_1^o||T|}.$$

Combining both bounds, we have that

$$(\delta\Delta - \alpha\Delta)|T| \leq \frac{\Delta}{|V_1|}|S_1^o||T| + 2\sqrt{\Delta}\sqrt{|S_1^o||T|}.$$

Rearranging, we arrive at the desired bound for $|T|$. □

**Lemma 4.4.7.** *For any codeword $x \in \mathcal{C}_1 \backslash \mathcal{C}_0^\perp$, where $\Delta \geq \frac{128(1-\alpha)}{\alpha^2\kappa^2(\delta^2-128\alpha)}$ and $\alpha < \frac{\delta^2}{128}$,*

$$||x|| \geq \frac{\alpha\kappa n}{2\Delta^2}.$$

*Proof.* Assume, for the sake of contradiction, that $||x|| < \frac{\alpha\kappa n}{2\Delta^2}$. Let $S_i \subseteq V_i$ denote the set of active vertices in $V_i$, for $i \in [0, 1]$, i.e., whose $Q$-neighborhood intersect the support of $x$. We know that each $v \in S_i$ must contribute at least 1 to the norm $||x||$, because either $c_v$ or $r_v$ must be nonzero. This gives us $|S_i| \leq ||x|| \leq \frac{\alpha\kappa n}{2\Delta^2}$. Since each vertex $v \in V_i$ is incident to exactly $\Delta^2$ squares, then $|V_i| = \frac{n}{\Delta^2}$. This gives us $|S_i| \leq \frac{\alpha\kappa}{2}|V_i|$, which satisfies the assumption needed for Lemma 4.4.5 that gives us an upper bound on the number of exceptional vertices:

$$|S_i^e| \leq \frac{64}{\alpha^2\kappa^2\Delta^2}|S_i|. \tag{4.3}$$

Then, the number of ordinary vertices can be bounded by $|S_i^o| \geq (1 - \frac{64}{\alpha^2\kappa^2\Delta^2})|S_i| := \beta|S_i|$. Without loss of generality, assume that at least half of the ordinary vertices in $S_1^o$ contribute a nonzero column in their local view. Define the set of ordinary columns:

$$C_1 := \{(c_v)_i : \text{column } i \text{ is nonzero in } c_v, v \in S_1^o\}$$

so that $|C_1| \geq \frac{1}{2}|S_1^o| \geq \frac{\beta}{2}|S_1|$. Now consider the set $T \subseteq V_0$ of vertices $V_0$ whose $Q$-neighborhoods intersect with a row or column of a $Q$-neighborhood of some vertex in $S_1^o$. By enforcing $\delta \geq 2\alpha\kappa$, we can directly apply Lemma 4.4.6 and obtain

$$|T| \leq \frac{64}{\delta^2 \Delta}|S_1|. \tag{4.4}$$

Now, we consider the average value of $\|c_v\| + \|r_v\|$ over $v \in T$ and place an upper bound and lower bound accordingly. For the lower bound, we have that

$$\frac{1}{T}\sum_{v\in T}(||c_v|| + ||r_v||) \geq \frac{1}{T}\sum_{v\in T}||c_v|| \geq \frac{\beta\delta^2\Delta}{128}. \tag{4.5}$$

For the upper bound, let $p$ denote the fraction of exceptional vertices in $T$. Since the $Q$-neighborhood $Q(v)$ contains $\Delta$ squares, $\|c_v\| + \|r_v\|$ is at most $\Delta$. For ordinary vertices, we have that $\|c_v\| + \|r_v\| < \alpha\Delta$ by construction. We can then upper bound the average:

$$\operatorname*{avg}_{v\in T}(||c_v|| + ||r_v||) \leq p\Delta + (1-p)\alpha\Delta. \tag{4.6}$$

Combining the two bounds, we obtain a lower bound of the proportion of exceptional vertices $p$:

$$p \geq \frac{\frac{\delta^2\beta}{128} - \alpha}{1-\alpha}. \tag{4.7}$$

Now, we use this to lower bound the number of exceptional vertices in $V_0$. Since $T$ includes all vertices in $V_0$ whose $Q$-neighborhoods overlap with ordinary columns, and each such vertex touches at most $\Delta$ columns, the minimal size of $T$ occurs when ordinary columns are maximally packed, i.e.

$$|T| \geq \frac{\beta}{2\Delta}|S_1|. \tag{4.8}$$

Therefore, the number of exceptional vertices in $V_0$ is at least:

$$|S_0^e| \geq p|T| \geq \frac{\beta}{2\Delta}\frac{\delta^2\beta - 128\alpha}{128(1-\alpha)}|S_1|. \tag{4.9}$$

Without loss of generality assume $|S_1| \geq |S_0|$, we then arrive at the final bound

$$\frac{\beta}{2\Delta}\frac{\delta^2\beta - 128\alpha}{128(1-\alpha)}|S_0| \leq |S_0^e| \leq \frac{64}{\alpha^2\kappa^2\Delta^2}|S_0|. \tag{4.10}$$

To reach a contradiction, we need to have that $\Delta \geq \frac{128(1-\alpha)}{\alpha^2\kappa^2(\delta^2-128\alpha)}$, which completes the proof. □

**Corollary 4.4.8.** *The minimum relative distance of quantum Tanner codes is* $\frac{\alpha\kappa^2\delta^2 n}{4\Delta^2}$.

*Proof.* Combining results from Lemma 4.4.3 and Lemma 4.4.7, we arrive at the minimum distance of $|x| \geq \frac{\alpha\kappa^2\delta^2 n}{4\Delta}$. □

We note that the analytical bound on $\Delta$, while theoretically sound, becomes astronomically large when the expansion constant $\kappa$ is small. For instance, if $\kappa \sim 10^5$, even with carefully chosen $\alpha$ and moderate $\delta$, the bound forces $\Delta$ to exceed $10^{19}$. Such a value is far beyond any practical degree achievable in code constructions. Given the current status of known families of codes and graphs, where $\kappa$ tends to be small, we underscore the fundamental limitation of quantum Tanner codes: under the current analysis, they are provably impossible to implement in practice.

This limitation drives the need to improve the expansion parameter $\kappa$, which we explore in the next chapter. There, we analyze new constructions that yield better expansion and allow us to consider codes with smaller $\Delta$. Although the lower bound above on $\Delta$ remains formally unsatisfied, the analysis is important for closing the gap between asymptotic guarantees and realizable code parameters.

*Chapter 5*

# STRONGER PRODUCT EXPANSION

To construct quantum LDPC codes with large minimum distance, it is not sufficient for the component classical codes to individually have good parameters. We must also control how these codes behave under tensor product operations. Thus, a key challenge is that even when the component classical codes have large distance, their tensor product may admit low-weight codewords, often arising from the additive structure of tensor products. For instance, a codeword in the dual tensor product code $C_1 \boxplus C_2 := C_1 \otimes \mathbb{F}_q^{\Delta} + \mathbb{F}_q^{\Delta} \otimes C_2$ might be formed by combining only a few columns from $C_1$ and a few rows from $C_2$, resulting in a sparse matrix.

To prevent this, [KP22] presented a useful structural guarantee – product expansion property – which asserts that any codeword in $C_1 \boxplus C_2$ must be "spread out" across many rows and columns in any decomposition. We include the specific definition of the property below:

**Definition 5.0.1** ($\kappa$-Product Expansion)**.** *We say a collection of linear codes $\mathcal{C} = (\mathcal{C}_i)_{i\in[2]}$ of linear codes $\mathcal{C}_i \subseteq \mathbb{F}_q^{\Delta_i}$ is $\kappa$-product-expanding if every codeword $c \in \mathcal{C}_1 \boxplus \mathcal{C}_2 = \mathcal{C}_1 \otimes \mathbb{F}_q^{\Delta_2} + \mathbb{F}_q^{\Delta_1} \otimes \mathcal{C}_2$ can be represented as a sum $c = c_1 + c_2$ for $c_1 \in \mathcal{C}_1 \otimes \mathbb{F}_q^{\Delta_2}$ and $c_2 \in \mathbb{F}_q^{\Delta_1} \otimes \mathcal{C}_2$, with the following property:*

$$\kappa(\Delta_1||c_1|| + \Delta_2||c_2||) \leq |c|,$$

*where $||c_1||$ denotes the number of columns in the support of $c_1$, $||c_2||$ denotes the number of rows in the support of $c_2$.*

We note that $\mathcal{C}$ here denotes a collection of linear codes, not to be confused with the Tanner code $\mathcal{C}$ used earlier. The individual codes in the collections $C_1 \in \mathcal{C}_1, C_2 \in \mathcal{C}_2$ correspond to the local codes $C_A, C_B$ used in the previous chapter.

In this chapter, we revisit and refine the central arguments of [KP22]. While previous works established the existence of this property with high probability for random codes, the bounds they provided were too loose for practical applications. We significantly strengthen these results by explicitly tracking tunable parameters in the analysis. By doing so, we demonstrate strictly better guarantees on the product-expansion factor $\kappa$ for randomly sampled codes to exhibit such properties.

Specifically, when applied to the setting of quantum Tanner codes, we numerically observe some improvements for $\kappa$. We present the numerical results in Section 5.3.

Notably, the relative distance of the asymptotically good qLDPC constructions in [LZ22] is quadratic in $\kappa$ by Corollary 4.4.8. Other asymptotically good constructions [PK22; Din+23] use similar expansion properties for their local codes and could be adapted to the $\kappa$-product expansion presented in this chapter. As such, our results lead to stronger guarantees for the minimum distance of quantum codes constructed from random classical codes with the product-expansion property, bringing these codes one step closer towards practical implementation.

We summarize the main probabilistic guarantee we establish in this chapter: the tensor product of two random linear codes satisfies the product-expansion property with high probability. We state this result informally below:

**Theorem 5.0.2** (Informal version of Theorem 5.2.7)**.** *For any $R_1, R_2 \in (0,1)$, there exists $\kappa > 0$ such that the dual tensor code $\mathcal{C}_1 \boxplus \mathcal{C}_2$ for two random codes $\mathcal{C}_1, \mathcal{C}_2$ of dimensions $k_i = R_i\Delta$ is $\kappa$-product-expanding with high probability as $\Delta \to \infty$.*

The remainder of this chapter is devoted to analyzing when and why this expansion property holds for random tensor codes. Many of the foundational tools in our analysis are adapted from the framework developed in [KP22]. For results that we do not modify, we cite them directly and omit the proofs for clarity. Readers interested in full technical details may refer to the original paper.

## 5.1 Sparse Resistance Property

To analyze the structure of low-weight codewords in tensor codes, we introduce a key technical tool known as the sparse resistance property. This property captures the idea that random subspaces are unlikely to overlap with sparse, low-dimensional subspaces. We will first present the relevant definitions:

**Definition 5.1.1** (Sparseness)**.** *We say a vector $v \in \mathbb{F}_q^\Delta$ is $\alpha$-sparse if $|v| \leq \alpha\Delta$. We say a subspace $V \subseteq \mathbb{F}_q^\Delta$ is $\alpha$-sparse if it can be spanned by $\alpha$-sparse vectors.*

**Definition 5.1.2** (Sparse Resistance Property)**.** *Let $U \subseteq \mathbb{F}_q^\Delta$. We say that $U$ satisfies the sparse resistance property if for every $\alpha$-sparsely generated subspace $V \subseteq \mathbb{F}_q^\Delta$, where $\alpha \in (0,1]$, we have some $\beta(\alpha) \in (0,1)$ such that*

$$\dim(U \cap V) \leq \beta \cdot \dim(V).$$

This property ensures that a subspace $U \subseteq \mathbb{F}_q^\Delta$ cannot have too much overlap with any subspace that is generated by sparse vectors. Intuitively, it implies that codewords in $U$ must be sufficiently spread out and cannot be well-approximated by linear combinations of sparse vectors. This will be crucial in Section 5.2, where we argue that low-weight codewords in the tensor product code must vanish over large submatrices, which is one of the key properties that leads to the strong expansion guarantees.

We will first show that for random codes, the sparse resistance property holds with high probability. We will use the following lemma that bounds the probability of a fixed subspace intersecting with a random subspace from [KP22] directly:

**Lemma 5.1.3.** *For a subspace $V \subseteq \mathbb{F}_q^n$ of dimension $v$ and a random subspace $U \in \mathbb{F}_q^n$ of dimension $u$,*

$$\Pr[\dim(U \cap V) \geq k] \leq 4q^{-k(n+k-v-u)}.$$

The above lemma will be used to bound the probability that sparse resistance property holds for random subspaces below:

**Lemma 5.1.4.** *Let $\epsilon \in (0,1), r \geq R \cdot \Delta$ for $\Delta \in \mathbb{N}$. A random $(\Delta - r)$-dimensional subspace $U \subseteq \mathbb{F}_q^\Delta$ satisfies the sparse resistance property with high probability. More specifically, for any $\beta \in (0,1)$, $\gamma \in (0,1)$, and $\alpha$-sparsely generated subspace $V \subseteq \mathbb{F}_q^\Delta$, we have that*

$$\dim(U \cap V) \leq \beta \cdot \dim(V),$$

*with probability at least $1 - 4\frac{q^{\beta^2(\gamma-1)r}}{1-q^{\beta^2(\gamma-1)r}}$, where $\alpha := H_q^{-1}(\gamma\beta^2 R)$.*

*Proof.* We fix a $\alpha$-sparsely generated subspace $V \subseteq \mathbb{F}_q^\Delta$ of dimension $m$, for some $m \in [1, r]$. First, we estimate the probability that a fixed $\alpha$-sparse subspace $V$ has $\dim(U \cap V) > \beta m$, where $U$ is a random $(\Delta - r)$-dimensional subspace of $\mathbb{F}_q^\Delta$. Applying Lemma 5.1.3 with $k \leftarrow \lceil \beta m \rceil$, $n \leftarrow \Delta$, $v \leftarrow m$, $u \leftarrow \Delta - r$, we obtain

$$\begin{aligned} \Pr_U[\dim(U \cap V) \geq \lceil \beta m \rceil] &\leq 4q^{-\lceil \beta m \rceil(\Delta + \lceil \beta m \rceil - m - (\Delta - r))} \\ &\leq 4q^{-\beta m(r-(1-\beta)m)} \\ &\leq 4q^{-\beta^2 mr}, \end{aligned} \tag{5.1}$$

where the last inequality holds since $m \leq r$.

Next, we will estimate the number of $\alpha$-sparsely generated subspaces $V$ of dimension

$m$. Let $S(\Delta, \alpha) := \{x \in \mathbb{F}_q^\Delta : |x| \leq \alpha\Delta\}$ denote the set of $\alpha$-sparse vectors. The size of the set can be bounded as following:

$$|S(\Delta, \alpha)| \leq \sum_{i=0}^{\lfloor \alpha\Delta \rfloor} \binom{\Delta}{i} (q-1)^i \leq q^{\Delta \cdot H_q(\alpha)}. \tag{5.2}$$

where the first inequality counts the number of supports of weight $i$ and values in $(q-1)^i$, and the second follows from the entropy upper bound on binomial coefficients. Since a basis for $V$ consists of $m$ such vectors, we obtain

$$|S(\Delta, \alpha)|^m \leq q^{m\Delta H_q(\alpha)} \tag{5.3}$$

We now apply a union bound over all such subspaces $V \in \mathcal{V}_m$, where $\mathcal{V}_m$ denotes the collection of $\alpha$-sparsely generated subspaces of dimension $m$. Then:

$$\begin{aligned} \Pr_U[\exists V \in \mathcal{V}_m \text{ such that } \dim(U \cap V) \geq \beta m] &\leq \sum_{V \in \mathcal{V}_m} \Pr_U[\dim(U \cap V) \geq \beta m] \\ &< q^{m\Delta H_q(\alpha)} \cdot 4q^{-\beta^2 mr} \\ &= 4q^{m\Delta H_q(\alpha) - \beta^2 mr} \\ &\leq 4q^{\beta^2 mr(\gamma - 1)} \end{aligned} \tag{5.4}$$

To ensure this probability is exponentially decaying, we require $H_q(\alpha) < \beta^2 R$ where $R \leq r/\Delta$. As such, we fix $\gamma \in (0, 1)$ such that $\alpha := H_q^{-1}(\gamma\beta^2 R)$.

Lastly, we sum over all dimensions $m \in [1, r]$ to upper bound the total failure probability. From 5.4, we have:

$$\begin{aligned} \Pr[\text{Sparse Resistance fails for some } V \text{ of dim } m \leq r] &\leq \sum_{m=1}^{r} 4q^{-m(\beta^2 r - \Delta H_q(\alpha))} \\ &= \sum_{m=1}^{r} 4q^{-m\beta^2 r(1-\gamma)} \\ &= 4\sum_{m=1}^{r} \left(q^{-\beta^2 r(1-\gamma)}\right)^m \\ &< \frac{4q^{-\beta^2 r(1-\gamma)}}{1 - q^{-\beta^2 r(1-\gamma)}}. \end{aligned} \tag{5.5}$$

This quantity is exponentially small in $r$, so with high probability, the random subspace $U \subseteq \mathbb{F}_q^\Delta$ satisfies the sparse resistance property for all $\alpha$-sparsely generated subspaces of dimension at most $r$. $\square$

In the context of random tensor codes, this justifies our assumption that the component codes $\mathcal{C}_1, \mathcal{C}_2$, chosen independently at random, will typically possess the structural robustness needed to resist alignment with sparse subspaces. This property will be fundamental in the analysis of low-rank codewords in the following sections, where it allows us to derive large zero rectangles and ultimately prove strong expansion guarantees.

## 5.2 Low-Weight Codewords

In this section, we will analyze the structural implications of a low-weight in the code $\mathcal{C}_1 \boxplus \mathcal{C}_2$. In particular, we show that codewords of low-weight, low-rank that satisfy the sparse resistance property must vanish on a large submatrix–a so-called *zero rectangle*.

**Definition 5.2.1** (Zero Rectangle)**.** *A matrix $x \in \mathbb{F}_q^{\Delta \times \Delta}$ has a* zero rectangle $A \times B$ *for $A, B \subseteq [\Delta]$, if $x_{i,j} = 0$ for all $i \in A$, $j \in B$. That is, the submatrix $x|_{A \times B}$, denoted as $x(A, B)$, is identically zero.*

We show the existence of such a large zero rectangle (i.e. $|A|, |B|$ has nontrivial lower bounds) for low-weight, low-rank codewords below, and that this structural sparsity can be used to bound their rank and, ultimately, control their contribution to the global code. The following lemmas show how zero rectangles arise naturally when analyzing low-rank codewords. Firstly, we cite a result stating that for any low-rank codeword in the dual tensor code and any choice of index subsets $A_1, A_2$, one can construct a new codeword whose support lies entirely within those subsets and which preserves the rank structure.

**Lemma 5.2.2** (Support Restriction with Rank Preservation, [KP22])**.** *For linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{\Delta}$, codeword $x \in \mathcal{C}_1 \boxplus \mathcal{C}_2$, and subsets $A_1, A_2 \subseteq [\Delta]$, there exists $x' \in \mathcal{C}_1 \boxplus \mathcal{C}_2$ such that $x'(A_1, A_2) = x(A_1, A_2)$ and rank$(x') =$ rank$(x(A_1, A_2))$.*

We also note that the rank of a dual tensor codeword can be related to the intersection of the row and column spaces of the component codes as following.

**Lemma 5.2.3** ([KP22])**.** *For linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{\Delta}$ and codeword $x \in \mathcal{C}_1 \boxplus \mathcal{C}_2$,*

$$\textit{rank}(x) \leq \textit{dim}(C \cap \mathcal{C}_1) + \textit{dim}(R \cap \mathcal{C}_2),$$

*where we denote use $R$ and $C$ to denote the row and column space of $x$, respectively.*

**Lemma 5.2.4** (Large Zero Rectangle Exists)**.** *Let $C_1, C_2 \subseteq \mathbb{F}_q^{\Delta}$ be linear codes of dimensions $\Delta - r_1$ and $\Delta - r_2$ respectively and satisfy the sparse resistance property. For each code $C_i$, fix a parameter $\beta_i \in (0,1)$ for $i \in [2]$ such that $\beta_1 + \beta_2 < 1$, and define $\alpha_i := H_q^{-1}(\gamma_i \beta_i^2 \frac{r_i}{\Delta})$ for $i \in (0,1)$. Let $x \in C_1 \boxplus C_2 \subseteq \mathbb{F}_q^{\Delta \times \Delta}$ be a codeword such that $|x| \leq c_1 c_2 \alpha_1 \alpha_2 \Delta^2$ and rank$(x) \leq r := \min(r_1, r_2)$ for $c_i \in (0, \frac{1}{2}]$. Then $d(C_i) > \alpha_i \Delta$, and the codeword $x$ has a zero rectangle $A \times B \subseteq [\Delta] \times [\Delta]$, where:*

$$|A| \geq \Delta - \frac{|x|}{c_2 \alpha_2 \Delta}, \qquad |B| \geq \Delta - \frac{|x|}{c_1 \alpha_1 \Delta}.$$

*Proof.* We begin by noting that for any vector $v \in \mathbb{F}_q^{\Delta}$ with $|v| \leq \alpha_i \Delta$, the span $V := \langle v \rangle$ is an $\alpha_i$-sparse 1-dimensional subspace. By the sparse resistance property, $\dim(C_i \cap V) \leq \beta_i < 1$, so $v \notin C_i$, and hence $d(C_i) > \alpha_i \Delta$.

Let $x \in C_1 \boxplus C_2$ be a codeword of weight $|x| \leq c_1 c_2 \alpha_1 \alpha_2 \Delta^2$ with rank $\leq r$. Define:

$$A := \{i \in [\Delta] : \text{row } i \text{ has weight } \leq c_2 \alpha_2 \Delta\},$$
$$B := \{j \in [\Delta] : \text{column } j \text{ has weight } \leq c_1 \alpha_1 \Delta\},$$

and let $\bar{A} := [\Delta] \setminus A, \bar{B} := [\Delta] \setminus B$. Then:

$$|x| \geq \max\left(|\bar{A}| \cdot c_2 \alpha_2 \Delta,\ |\bar{B}| \cdot c_1 \alpha_1 \Delta\right).$$

Using the weight upper bound on $x$, we conclude

$$|\bar{A}| \leq \frac{|x|}{c_2 \alpha_2 \Delta}, \qquad |\bar{B}| \leq \frac{|x|}{c_1 \alpha_1 \Delta}.$$

Since $c_i \leq 1/2$, $c_i \alpha_i \Delta < d(C_i)$, and we obtain

$$|A| \geq \Delta - \frac{|x|}{c_2 \alpha_2 \Delta} > \Delta - d(\mathcal{C}_1), \qquad |B| \geq \Delta - \frac{|x|}{c_1 \alpha_1 \Delta} > n - d(\mathcal{C}_2). \tag{5.5}$$

Lastly, we will proceed by contradiction to show that $x(A, B)$ is a zero rectangle. Assume that $x|_{A \times B} \neq 0$. By Lemma 5.2.2, there exists a codeword $x' \in \mathcal{C}_1 \boxplus \mathcal{C}_2$ such that $x'(A, B) = x(A, B)$, and all rows of $x'$ are spanned by rows of $x'(A, \cdot)$, all columns of $x'$ are spanned by columns of $x'(\cdot, B)$.

We consider the space of the rows of $x'$, and note that for $i \in A$

$$|x'(i, \cdot)| \leq |x'(i, B)| + |\bar{B}| = |x(i, B)| + |\bar{B}| \leq 2 c_2 \alpha_2 \Delta \leq \alpha_2 \Delta. \tag{5.6}$$

Thus, the row space of $x'$, denoted by $R$, is $\alpha_2$-sparse. Similarly, the column space of $x'$, denoted by $C$, is $\alpha_1$-sparse. We can then apply the sparse resistance property for

the codes $\mathcal{C}_1, \mathcal{C}_2$. Since $rank(x) < r := \min(r_1, r_2)$, the dimensions of the row and column spans of $x'$, namely $\dim(R)$ and $\dim(C)$, are each less than $r$, so the sparse resistance bounds are valid:

$$\dim(\mathcal{C}_1 \cap C) \leq \beta_1 \dim(C), \dim(\mathcal{C}_2 \cap R) \leq \beta_2 \dim(R).$$

Applying Lemma 5.2.3, we arrive at

$$\text{rank}(x') \leq \dim(\mathcal{C}_1 \cap C) + \dim(\mathcal{C}_2 \cap R) \leq (\beta_1 + \beta_2) \cdot \text{rank}(x'). \tag{5.7}$$

Since $\beta_1 + \beta_2 < 1$, we arrive at a contradiction. □

A codeword in $\mathcal{C}_1 \boxplus \mathcal{C}_2$ with a large zero rectangle yields useful properties for decomposing it into a sum of a few rows from $\mathcal{C}_2$ and a few columns from $\mathcal{C}_1$. We cite the relevant property below:

**Lemma 5.2.5** (Zero Rectangle Decomposition, [KP22])**.** *Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{\Delta}$ be two linear codes. For a codeword $x \in \mathcal{C}_1 \boxplus \mathcal{C}_2$ and subsets $A_1, A_2 \subseteq [\Delta]$ such that $\Delta - |A_i| \leq d(\mathcal{C}_i)$, $i \in [2]$, and $x(A_1, A_2) = 0$, then $x$ can be represented as a sum of $\Delta - |A_1|$ rows from $\mathcal{C}_2$ and $\Delta - |A_2|$ columns from $\mathcal{C}_1$.*

Before we proceed to proving the main result, we note that among low-weight codewords, high-rank codewords are undesirable since we would no longer be able to apply Lemma 5.2.4 to obtain a large rectangle. As such, we cite the result that the probability that a fixed matrix $x$ of large rank lies in the dual tensor product of two random linear codes is low:

**Lemma 5.2.6** (High-Rank Codewords, [KP22])**.** *Let $x \in \mathbb{F}_q^{\Delta \times \Delta}$ matrix of rank $\geq \min(r_1, r_2)$. Then the probability that $x \in \mathcal{C}_1 \boxplus \mathcal{C}_2$ for a pair of linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{\Delta}$ of dimensions $k_1 = \Delta - r_1$ and $k_2 = \Delta - r_2$ is at most $5q^{-r_1 r_2}$.*

We now have all the groundwork needed to show that, with high probability, the dual tensor product of two random linear codes satisfies the $\kappa$-product-expansion property for an explicitly stated parameter $\kappa > 0$.

**Theorem 5.2.7.** *For every $\epsilon_1 \in (0,1), \epsilon_2 \in (0,1)$, set $r_1 \geq \epsilon_1 \Delta$ and $r_2 \geq \epsilon_2 \Delta$.*

*Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{\Delta}$ be independently chosen random linear codes of dimensions at most $\Delta - r_1$ and $\Delta - r_2$ respectively. Then, $\mathcal{C}_1 \boxplus \mathcal{C}_2$ is $\kappa$-product expanding for*

$$\kappa = \frac{1}{2} \min\left(c_1 c_2 \alpha_1 \alpha_2, H_q^{-1}\left(d\frac{r_1 r_2}{4}\right)\right)$$

*with probability at least*

$$1 - 5q^{\frac{1}{4}(d-1)r_1r_2} - 4\frac{q^{-\beta_1^2(1-\gamma_1)r_1}}{1-q^{-\beta_1^2(1-\gamma_1)r_1}} - 4\frac{q^{-\beta_2^2(1-\gamma_2)r_2}}{1-q^{-\beta_2^2(1-\gamma_2)r_2}},$$

*subject to the following constraints for each* $i \in \{1,2\}$ :
$\beta_i \in (0,1), \quad \beta_1+\beta_2 < 1, \quad \gamma_i \in (0,1), \quad \alpha_i := H_q^{-1}\left(\gamma_i\beta_i^2\frac{r_i}{\Delta}\right),$
$d \in (0,1), \quad c_i \in \left(0, \frac{1}{2}\right], \quad$ *and* $r_i \geq \frac{1}{\beta_i^2(1-\gamma_i)}$

*Proof.* Let $x \in \mathcal{C}_1 \boxplus \mathcal{C}_2$ be a nonzero codeword. We analyze the cases based on the Hamming weight $|x|$ and rank of $x$, and show that $\mathcal{C}_1 \boxplus \mathcal{C}_2$ satisfies $\kappa$-product expansion property with high probability. We consider the following two good cases, where product expansion holds, and two bad cases, where product expansion may fail.

Firstly, for any high weight codeword where $|x| \geq 2\kappa\Delta^2$, product expansion holds. Indeed, we can see that for any decomposition $x = c_1 + c_2$ for some $c_1 \in \mathcal{C}_1 \otimes \mathbb{F}_q^{\Delta}$ and $c_1 \in \mathbb{F}_q^{\Delta} \otimes \mathcal{C}_2$, we have

$$\kappa n(||c_1|| + ||c_2||) \leq \kappa\Delta \cdot 2\Delta = \kappa \cdot 2\Delta^2. \tag{5.8}$$

Next, we consider low-weight, low-rank codewords with sparse resistance property. More specifically, assume $|x| < 2\kappa\Delta^2$ and $rank(x) < r := \min(r_1, r_2)$. If the code pair satisfies sparse resistance property and $\kappa \leq \frac{1}{2}c_1c_2\alpha_1\alpha_2$, by Lemma 5.2.4, the codeword $x$ has a zero rectangle at $A_1 \times A_2$, for subsets $A_1, A_2 \subseteq [\Delta]$ with $|A_1| \geq \frac{|x|}{c_2\alpha_2\Delta}$, $|A_2| \geq \frac{|x|}{c_1\alpha_1\Delta}$, and $d(\mathcal{C}_i) > \alpha_i\Delta$. Then, applying Lemma 5.2.5, $x$ can be represented as a sum of $\Delta - |A_1|$ rows from $\mathcal{C}_2$ and $\Delta - |A_2|$ columns from $\mathcal{C}_1$. We then obtain the bound that

$$\kappa\Delta((\Delta - |A_1|) + (\Delta - |A_2|)) \leq \kappa\Delta\left(\frac{|x|}{c_2\alpha_2\Delta} + \frac{|x|}{c_1\alpha_1\Delta}\right) \leq |x|, \tag{5.9}$$

satisfying the product expansion property.

Now, we consider the undesirable cases where the codewords are low-weight and high-rank, and when product expansion does not hold. We will show that each of these events occurs with low probability. Firstly, we will bound the probability of low-weight, high-rank codewords, and more specifically, the probability of getting a random pair $(\mathcal{C}_1, \mathcal{C}_2)$ such that there exists $x \in \mathcal{C}_1 \boxplus \mathcal{C}_2$ of weight $|x| \leq 2\rho\Delta^2$ and of rank $rk(x) \geq r$. For each such $x$, Lemma 5.2.6 implies that

$$\Pr_{\mathcal{C}_1,\mathcal{C}_2}[x \in \mathcal{C}_1 \boxplus \mathcal{C}_2] \leq 5q^{-r_1r_2}. \tag{5.10}$$

We apply a union bound to get all possible codewords of weight $\leq 2\rho\Delta^2$:

$$\begin{aligned}\Pr_{\mathcal{C}_1,\mathcal{C}_2}[x \in \mathcal{C}_1 \boxplus \mathcal{C}_2 : |x| \leq 2\kappa\Delta^2, \text{rank}(x) \geq r] &\leq \sum_{i=0}^{\lfloor 2\rho n^2 \rfloor} \binom{\Delta^2}{i} (q-1)^i \cdot 5q^{-\frac{1}{4}r_1 r_2} \\ &\leq q^{H_q(2\kappa)\Delta^2} \cdot 5q^{-\frac{1}{4}r_1 r_2} \\ &= 5q^{\frac{1}{4}(d-1)r_1 r_2},\end{aligned} \tag{5.11}$$

where the last equality comes from the choice of $\kappa$ where $\kappa = \frac{1}{2}H_q^{-1}\left(\frac{d}{4}r_1 r_2\right)$ for $d \in (0,1)$.

Lastly, we will show that the probability of either $\mathcal{C}_1$ or $\mathcal{C}_2$ not having the sparse resistance property is low as well. From Lemma 5.1.4, we have that the probability $\mathcal{C}_i$ does not satisfy the property is no more than $4\frac{q^{-\beta_i^2(1-\gamma_i)r_i}}{1-q^{-\beta_i^2(1-\gamma_i)r_i}}$. Note that $q^{-\beta_i^2(1-\gamma_i)r_i} \leq \frac{1}{2}$ for $r_i \geq \frac{1}{\beta_i^2(1-\gamma_i)}$ and for $q \geq 2$, so we have $\frac{q^{-\beta_i^2(1-\gamma_i)r_i}}{1-q^{-\beta_i^2(1-\gamma_i)r_i}} \leq 2q^{-\beta_i^2(1-\gamma_i)r_i}$. This completes the proof. □

Theorem 5.2.7 above guarantees that, with high probability, a randomly sampled pair of classical linear codes satisfies the $\kappa$-product-expansion property, provided their dimensions are chosen appropriately. In the context of quantum Tanner codes, we require that this expansion property hold for both the pair $(\mathcal{C}_1, \mathcal{C}_2)$ as well as its dual $(\mathcal{C}_1^\perp, \mathcal{C}_2^\perp)$, given that the code rate for the code $\mathcal{C}_1$ is complement to that of $\mathcal{C}_2$. The following corollary formalizes this observation, showing that when the expansion success probability exceeds $\frac{1}{2}$, the product expansion property necessarily holds for both the original and dual code pairs with positive probability.

**Corollary 5.2.8.** *Let $\mathcal{C}_1, \mathcal{C}_2$ be independently chosen random linear codes of dimension $\Delta - r_1$ and $\Delta - r_2$ respectively, where $r_2 := \Delta - r_1$. Let $\mathcal{C}_1^\perp$, $\mathcal{C}_2^\perp \subseteq \mathbb{F}_q^\Delta$ denote their duals. Fix parameters $\alpha_i, \beta_i, \gamma_i, \epsilon_i, c_i, r_i, d$ for $i \in [2]$ such that they satisfy the conditions stated in Theorem 5.2.7. Then, with probability $> 0$, the code $\mathcal{C}_1 \boxplus \mathcal{C}_2$ as well as the dual $\mathcal{C}_1^\perp \boxplus \mathcal{C}_2^\perp$ are both $\kappa$-product expanding for some $\kappa > 0$.*

*Proof.* By Theorem 5.2.7, we know that $\mathcal{C}_1 \boxplus \mathcal{C}_2$ is $\kappa$-product expanding with probability at least $1/2 + \delta$ for some $\delta > 0$ and $\kappa > 0$. Now observe that the dual codes $\mathcal{C}_1^\perp, \mathcal{C}_2^\perp \subseteq \mathbb{F}_q^\Delta$ have dimensions $r_1, r_2$ and are also uniformly random among all linear codes of their respective dimensions, since the dual of a uniformly random linear code is uniformly random among codes of complementary dimension. Moreover, the parameters $\beta_i, \gamma_i, \epsilon_i, c_i, r_i,$ and $d$ still satisfy that conditions of Theorem 5.2.7 when

applied to the dual codes. Therefore, by symmetry, the probability that $\mathcal{C}_1^\perp \boxplus \mathcal{C}_2^\perp$ is $\kappa$-product expanding is at least $1/2 + \delta$ as well. Using the union bound,

$$\begin{aligned}\Pr[\mathcal{C}_1 \boxplus \mathcal{C}_2 \text{ and } \mathcal{C}_1^\perp \boxplus \mathcal{C}_2^\perp \text{ are both } \kappa\text{-product expanding}] &\geq \left(\frac{1}{2} + \delta\right) + \left(\frac{1}{2} + \delta\right) - 1 \\ &= 2\delta,\end{aligned}$$

which is strictly positive. This proves that the probability of both code pairs being $\kappa$-product expanding is nonzero.

□

### 5.3 Numerical Improvements of Product-Expansion Bounds

In this section, we examine the effectiveness of our refined product-expansion analysis by numerically evaluating the product expansion parameter $\kappa$ under both the original bounds presented in [KP22] and our optimized approach. We assess how $\kappa$ varies with respect to varying quantum Tanner code rates and local code lengths $\Delta$, using a success criterion based on the probability that a randomly sampled pair of classical codes $(\mathcal{C}_1, \mathcal{C}_2)$ satisfies the product-expansion property. Specifically, we require this probability to be at least $0.51$. This threshold is crucial: if expansion holds for a random pair of codes with probability strictly greater than $1/2$, then by Corollary 5.2.8, it also holds for their duals with strictly positive probability. This allows us to guarantee simultaneous $\kappa$-product expansion for both $\mathcal{C}_1 \boxplus \mathcal{C}_2$ and its dual $\mathcal{C}_1^\perp \boxplus \mathcal{C}_2^\perp$.

Figure 5.1 presents the product expansion parameter $\kappa$ as a function of the quantum Tanner code rate, for a fixed local code length $\Delta = 100$. While this choice of $\Delta$ serves as a valuable proof of concept for demonstrating the improvements achieved by our method, we note that it may not satisfy the theoretical constraint $\Delta \geq \frac{128(1-\alpha)}{\alpha^2\kappa^2(\delta^2-128\alpha)}$ required for the distance bound in Corollary 4.4.8 to hold. Nevertheless, we use this local block length to illustrate the substantial improvements our approach provides over existing bounds.

Under the construction in [KP22], the expansion guarantee fails to meet the $0.51$ success threshold beyond an extremely narrow range, becoming invalid around quantum code rate $R \approx 0.04$. In contrast, our refined bounds maintain validity over a range of meaningful quantum code rates $R \in (0, \frac{1}{2}]$. Beyond the validity range, the magnitude of $\kappa$ itself is substantially improved. For the same local code size, our bounds yield values of $\kappa$ around one order of magnitude larger than prior bounds.

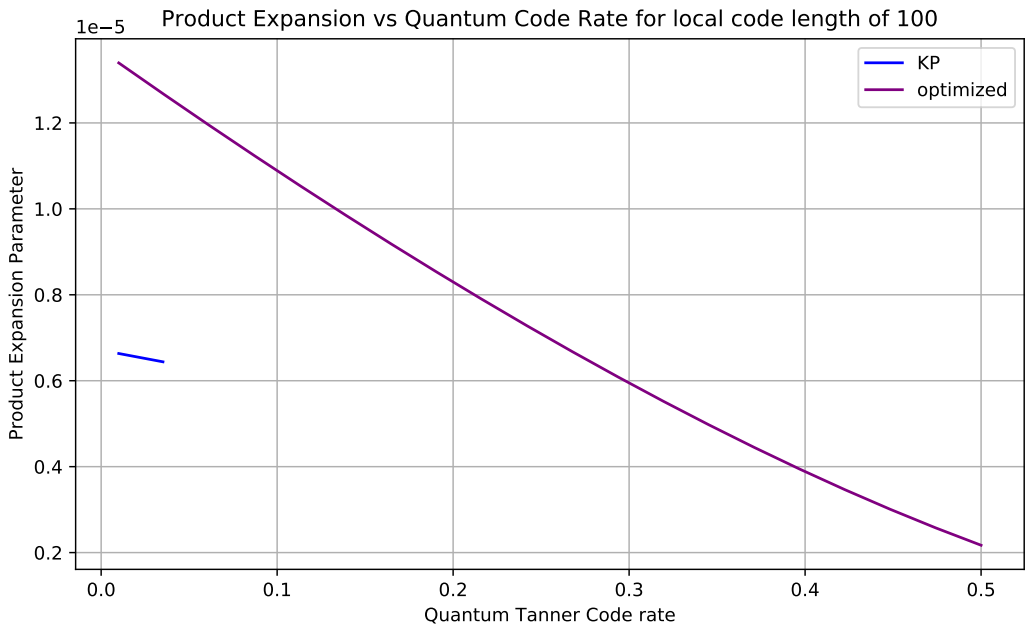


Figure 5.1: Comparison of the product expansion parameter $\kappa$ as a function of the quantum Tanner code rate, for local code length $\Delta = 100$ over the field $\mathbb{F}_2$. The blue curve (“KP") represents the theoretical lower bound from [KP22], while the purple curve (“optimized") corresponds to the improved bounds obtained via our tighter analysis.

In Figure 5.2, we explore the dependence on local code length $\Delta$ for several fixed rates, again as a proof of concept without enforcing the minimum length of the local code $\Delta$. The goal is to determine how large $\Delta$ must be to achieve expansion with high probability at a given code rate. The results again demonstrate the advantage of our method. Under the parameters used in [KP22], $\kappa$ remains nearly constant in $\Delta$, requiring local code lengths of $\sim 100$ to achieve meaningful expansion parameters. In contrast, our optimized bounds show that $\kappa$ increases significantly with $\Delta$, achieving robust product expansion even for local code lengths as small as $60 - 100$. This has important physical implications – in a quantum system, smaller $\Delta$ translates to lower check weight, simpler stabilizer circuits, and reduces hardware overhead.

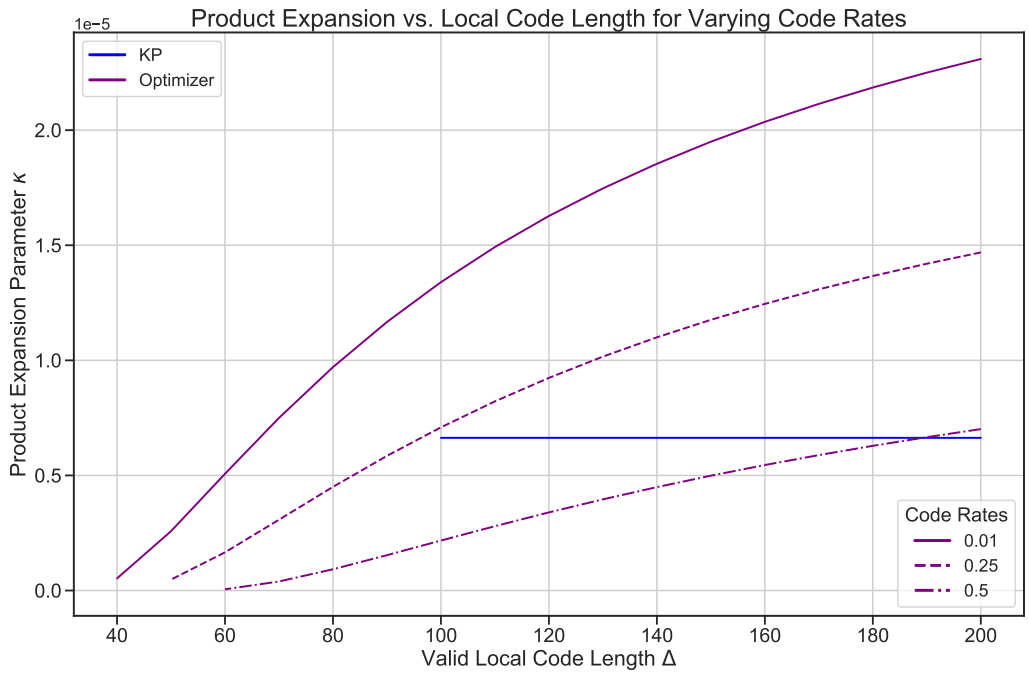


Figure 5.2: Comparison of the product expansion parameter $\kappa$ as a function of local code length $\Delta$, of varying quantum Tanner code rates. Each curve represents a fixed quantum code rate ($R = 0.01, 0.25, 0.5$). The blue segments ("KP") indicate the lower bounds from [KP22] with a quantum code rate fo $0.01$, which remain nearly constant as $\Delta$ increases. The purple curves ("optimized") show the improved expansion parameters achieved through our analysis. Notably, our method yields robust product-expansion even at moderate local code sizes.

To address the theoretical requirement for $\Delta$, we present in Figure 5.3 results in a more realistic setting with the local code length $\Delta$ on the order of $10^{19}$. While the improvement of $\kappa$ in this setting isn't as substantial as smaller values of $\Delta$ shown in Figure 5.1 and 5.2, we note that when the bound $\Delta \geq \frac{128(1-\alpha)}{\alpha^2\kappa^2(\delta^2-128\alpha)}$ is satisfied, the relative distance of the quantum Tanner codes scales linearly in $\kappa^6$. Thus, the resulting improvements in the code distance are amplified significantly.

While the constructions and bounds discussed in this section are still largely theoretical, they offer important analytical insight into the behavior of random tensor product codes. In particular, our refined product expansion analysis highlights what parameter regimes—such as larger $\kappa$ or stronger sparse resistance—are desirable when designing qLDPC codes.

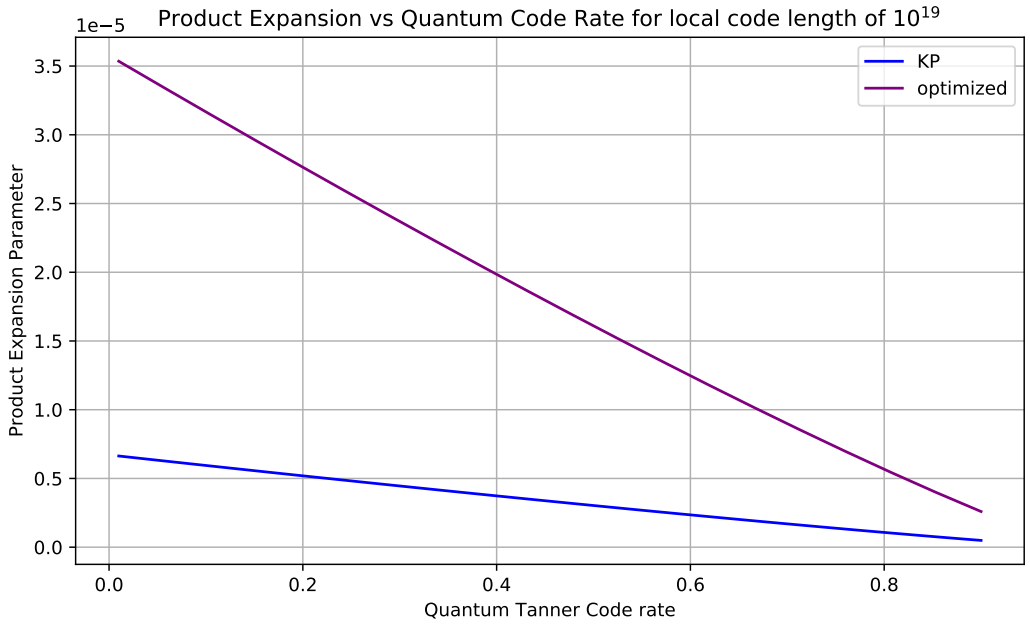


Figure 5.3: Comparison of the product expansion parameter $\kappa$ as a function of quantum Tanner code rate, for local code length $\Delta = 10^{19}$. This choice of $\Delta$ here is large enough such that the distance scaling of the code can provably hold. We choose the parameters $\delta = 0.5$ and $\alpha = \frac{\delta^2}{256}$.

In future implementations, it is unlikely that product expansion will be verified directly; instead, one will likely choose small, random local codes on Cayley complexes of specific groups. Our analysis provides guidance on what properties to expect or target in such codes. In this way, the quantum Tanner code serves not as an immediately practical proposal, but as a conceptual testbed for studying the expansion behavior that underpins all known asymptotically good qLDPC codes.

*Chapter 6*

# CONCLUSION AND OUTLOOK

In this thesis, we focused on improving the relative distance of quantum Tanner codes by strengthening the product-expansion guarantees in the underlying classical tensor code structure. By introducing a more refined probabilistic analysis that explicitly tracks tunable parameters, we demonstrated significantly tighter bounds on the product expansion parameter $\kappa$, with high-probability guarantees. These improvements yield shorter local code lengths and improved expansion parameters, which deepen our understanding of expansion in random tensor codes and support the design of constructions with lower local code complexity and a broader range of quantum rates. However, we must address some of the fundamental limitations that emerge from our analysis. The bound on the local code size $\Delta$ remains too large for near-term implementation, and quantum Tanner codes themselves are unlikely to be deployed directly in practice. Nonetheless, the analytical tools developed here can inform future constructions that do use random local codes on structured group complexes.

While the immediate focus of this thesis has been on quantum Tanner codes, the insights developed here have broader implications. Many recent breakthroughs in quantum LDPC codes, including lifted product codes [PK21b; PK22; Din+23], balanced product codes [BE21], and fiber bundle codes [HHO21], rely on analogous local-to-global amplification mechanisms, often via tensor products or fibered code families. These constructions similarly require robust spreading of support across the code structure to ensure high distance, and thus their performance also hinges on expansion-type properties. The analytical techniques developed in this work, especially the improved bounds for the product expansion property, could therefore potentially be adapted to strengthen distance bounds in these other frameworks as well.

In particular, we note that the other two asymptotically good qLDPC constructions [PK22; Din+23] both rely on the probabilistic argument that random local codes achieve global properties with high probability. The version of product expansion presented in [KP22] could likely be applied to these two constructions, and our analysis would similarly be applied to strengthen the corresponding code parameters.

While the current theoretical requirement for the number of physical qubits needed for these codes is astronomical, we note that the lifted product (LP) construction in particular has already led to many practical constructions for near-term devices. For instance, [PK21b] developed an efficient decoding algorithm tailored to lifted product codes and demonstrated their applicability in fault-tolerant settings. More recently, [Xu+24] demonstrates the applicability of LP codes for quantum memory in near-term neutral atom arrays, and a family of qLDPC codes, the bivariate bicycle codes [Bra+24], has been proposed for fault-tolerant quantum memory within the reach of near-term quantum processors as well.

Another active area of development involves decoding. These asymptotically good codes are only useful if they can be decoded efficiently and accurately. Various decoders [GPT23; LZ23] have been proposed for quantum Tanner codes, and a recent work [Gu+24] has shown that the decoder proposed in [LZ23] satisfies the powerful single-shot decoding property: it requires only one round of syndrome measurement to recover from noise. Notably, the ideas behind these decoders are not restricted to Tanner codes and are expected to generalize to other constructions, including the lifted product code in [PK22]. In addition, the [Din+23] construction introduced its own decoding algorithm tailored to its specific structure.

However, decoding alone does not suffice. To build a full-fledged quantum computer based on qLDPC codes, one must not only protect and store quantum information but also perform logical operations fault-tolerantly. [Got13] first pioneered qLDPC-based fault-tolerant computation using gate teleportation, and has since been substantially optimized. For example, [NP24] streamlines resource usage in the asymptotic regime. Recently, an alternative paradigm has been proposed in the form of the extractor architecture [He+25] which replaces teleportation with code surgery and achieves significant improvements in spatial overhead compared to traditional surface-code-based computers. These proposals are the current leading approaches to realizing a qLDPC-based quantum computer.

Furthermore, the development of asymptotically good quantum LDPC codes has also had profound theoretical consequences beyond error correction. Notably, it enabled the resolution of the No Low-Energy Trivial States (NLTS) conjecture [ABN23], which asks whether there exist local Hamiltonians whose low-energy states cannot be prepared by shallow quantum circuits. This was a key open problem in quantum complexity theory and a critical step toward the quantum PCP conjecture [AAV13].

Lastly, we hope this work encourages continued exploration of how local code

structures can give rise to robust global properties. As the field shifts from establishing existence to achieving efficient and physically realizable architectures, understanding and optimizing these local building blocks will be key to constructing quantum codes that are not only theoretically sound, but ultimately scalable and adaptable to emerging quantum hardware platforms.

# BIBLIOGRAPHY


[PK22] Pavel Panteleev and Gleb Kalachev. "Asymptotically good quantum and locally testable classical LDPC codes." In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. 2022, pp. 375–388.

[LZ22] Anthony Leverrier and Gilles Zémor. "Quantum tanner codes." In: *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2022, pp. 872–883.

[Din+23] Irit Dinur et al. "Good quantum LDPC codes with linear time decoders." In: *Proceedings of the 55th annual ACM symposium on theory of computing*. 2023, pp. 905–918.

[LZ23] Anthony Leverrier and Gilles Zémor. "Decoding quantum Tanner codes." In: *IEEE Transactions on Information Theory* 69.8 (2023), pp. 5100–5115.

[KP22] Gleb Kalachev and Pavel Panteleev. "Two-sided robustly testable codes." In: *arXiv preprint arXiv:2206.09973* (2022).

[Gal62] Robert Gallager. "Low-density parity-check codes." In: *IRE Transactions on information theory* 8.1 (1962), pp. 21–28.

[SS96] Michael Sipser and Daniel A Spielman. "Expander codes." In: *IEEE transactions on Information Theory* 42.6 (1996), pp. 1710–1722.

[Got97] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[CS96] A Robert Calderbank and Peter W Shor. "Good quantum error-correcting codes exist." In: *Physical Review A* 54.2 (1996), p. 1098.

[Ste96] Andrew M Steane. "Error correcting codes in quantum theory." In: *Physical Review Letters* 77.5 (1996), p. 793.

[KLV00] Emanuel Knill, Raymond Laflamme, and Lorenza Viola. "Theory of quantum error correction for general noise." In: *Physical Review Letters* 84.11 (2000), p. 2525.

[Kit03] A Yu Kitaev. "Fault-tolerant quantum computation by anyons." In: *Annals of physics* 303.1 (2003), pp. 2–30.

[TZ13] Jean-Pierre Tillich and Gilles Zémor. "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength." In: *IEEE Transactions on Information Theory* 60.2 (2013), pp. 1193–1202.

[BH14] Sergey Bravyi and Matthew B Hastings. "Homological product codes." In: *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*. 2014, pp. 273–282.

[HHO21] Matthew B Hastings, Jeongwan Haah, and Ryan O'Donnell. "Fiber bundle codes: breaking the n 1/2 polylog (n) barrier for quantum ldpc codes." In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 2021, pp. 1276–1288.

[PK21a] Pavel Panteleev and Gleb Kalachev. "Quantum LDPC codes with almost linear minimum distance." In: *IEEE Transactions on Information Theory* 68.1 (2021), pp. 213–229.

[BE21] Nikolas P Breuckmann and Jens N Eberhardt. "Balanced product quantum codes." In: *IEEE Transactions on Information Theory* 67.10 (2021), pp. 6653–6674.

[Din+22] Irit Dinur et al. "Locally testable codes with constant rate, distance, and locality." In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. 2022, pp. 357–374.

[PK21b] Pavel Panteleev and Gleb Kalachev. "Degenerate quantum LDPC codes with good finite length performance." In: *Quantum* 5 (2021), p. 585.

[Xu+24] Qian Xu et al. "Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays." In: *Nature Physics* 20.7 (2024), pp. 1084–1090.

[Bra+24] Sergey Bravyi et al. "High-threshold and low-overhead fault-tolerant quantum memory." In: *Nature* 627.8005 (2024), pp. 778–782.

[GPT23] Shouzhen Gu, Christopher A Pattison, and Eugene Tang. "An efficient decoder for a linear distance quantum LDPC code." In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 919–932.

[Gu+24] Shouzhen Gu et al. "Single-shot decoding of good quantum LDPC codes." In: *Communications in Mathematical Physics* 405.3 (2024), p. 85.

[Got13] Daniel Gottesman. "Fault-tolerant quantum computation with constant overhead." In: *arXiv preprint arXiv:1310.2984* (2013).

[NP24] Quynh T Nguyen and Christopher A Pattison. "Quantum fault tolerance with constant-space and logarithmic-time overheads." In: *arXiv preprint arXiv:2411.03632* (2024).

[He+25] Zhiyang He et al. "Extractors: QLDPC Architectures for Efficient Pauli-Based Computation." In: *arXiv preprint arXiv:2503.10390* (2025).

[ABN23] Anurag Anshu, Nikolas P Breuckmann, and Chinmay Nirkhe. "NLTS Hamiltonians from good quantum codes." In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1090–1096.

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. “Guest column: the quantum PCP conjecture.” In: *Acm sigact news* 44.2 (2013), pp. 47–79.