Title

Quantum Hierarchical Locally Recoverable Codes

ISBN

9798189272264

Author

Trivedi, Pranav

Publication Date

2028-05-01

Peer reviewed|Thesis/dissertation

Quantum Hierarchical Locally Recoverable Codes

by

Pranav Trivedi

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Venkatesan Guruswami, Chair
Professor Richard Borcherds
Professor Sylvie Corteel

Spring 2026

Quantum Hierarchical Locally Recoverable Codes

Abstract

Quantum Hierarchical Locally Recoverable Codes

by

Pranav Trivedi

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Venkatesan Guruswami, Chair

Quantum locally recoverable codes (QLRCs) have recently gained attention as a framework for achieving efficient quantum storage with local recovery capabilities. Analogous to their classical counterparts, QLRCs allow a lost qudit to be reconstructed using only a small subset of other qudits, thereby reducing the resource and operational overhead in recovery. In this work, we extend the study of QLRCs by considering (r, δ) QLRCs characterized by locality parameter r and local distance $\delta \geq 2$. We present constructions of both random and explicit (r, δ) QLRCs, including explicit families based on the quantum Tamo—Barg construction. We also present an efficient decoding algorithm for these quantum Tamo–Barg codes.

Furthermore, we introduce quantum *hierarchical* locally recoverable codes (QHLRCs), which extend local recovery to multiple hierarchical levels. For any integer $h \geq 2$, we construct both random and explicit h-level QHLRCs—the latter being h-level quantum Tamo—Barg codes—and establish a Singleton-like bound for these codes using a CSS framework built from dual-containing classical codes. These results advance the theoretical foundations of quantum erasure recovery and contribute to the design of efficient quantum storage architectures.

For my parents.

Contents

Acknowledgments

First and foremost, I am extremely grateful to my advisor, Venkat Guruswami, who has patiently guided me through my years as a doctoral student. I would like to thank my committee members and researchers with whom I have had the fortune of collaborating: Sylvie Corteel, Richard Borcherds, Ken Ribet, Rutuja Kshirsagar, Elena Berardini, and Sarvagya Upadhyay. Finally, I would like to acknowledge a special admiration for Julia Hartmann, my undergraduate advisor, who introduced me to the world of coding theory.

My graduate experience would not have been nearly as much fun if not for all the friends (you know who you are) I made along the way. From climbing to playing Mario Kart one-handed you have enabled me to enjoyably procrastinate. Lastly, I would like to thank my parents, Nina and Rajesh, for instilling the joys of mathematics in me from a young age and constantly supporting me in my continued pursuit of it.

Chapter 1

Introduction

Erasure recovery plays a central role in maintaining data reliability in classical storage systems, particularly those that are distributed across multiple physical locations or devices. In such systems, data loss can occur due to node failures, hardware errors, or network disruptions. To mitigate these failures, erasure codes are widely employed, enabling the reconstruction of lost data from the remaining intact portions. As the size and complexity of distributed systems grow, so does the need for codes that can efficiently recover data with minimal redundancy and computational overhead.

Extending these concepts to quantum systems is essential for developing robust quantum memories—an indispensable component of large-scale quantum computing and quantum communication networks. Quantum memories must not only preserve fragile quantum information over time but also allow recovery from physical qubit losses, known as erasures. Consequently, understanding and adapting erasure recovery mechanisms to the quantum setting is a foundational step toward fault-tolerant quantum information processing.

Classically, erasure recovery operates under the assumption that the location of erased symbols is known to the decoder. This is a critical simplification: once the erased positions are identified, the remaining symbols and parity constraints can be used to reconstruct the missing information efficiently. The same principle applies to quantum erasure recovery, where it is assumed that the locations of the lost qubits are known to the recovery operation. In both classical [5] and quantum [16, 17] contexts, it has been demonstrated that erasures are inherently easier to recover than general errors, since the decoder does not need to infer where errors have occurred. Furthermore, recent experiments have shown that detected errors can be converted into erasures in certain physical implementations of quantum hardware. This conversion has been demonstrated in neutral-atom systems [17, 37] and superconducting qubit architectures [35], making erasure-based quantum recovery schemes particularly practical and appealing.

In the classical regime, locally recoverable codes (LRCs), introduced in [15], have emerged as a particularly effective solution for efficient erasure recovery. The central idea behind LRCs is locality: each symbol of a codeword can be recovered by accessing only a small subset of other symbols, rather than the entire codeword. Formally, an (n, k, r) LRC over the finite field $\mathbb{F}_q$ encodes a message of k symbols into a codeword of length n such that each codeword symbol has a recovery set of at most r other symbols. The parameter r thus captures the locality of the code, representing the size of the largest subset needed for recovery. Typically, $1 \leq r \leq k$, and smaller r values indicate more efficient local recovery. Such local recovery is critical in distributed storage for efficient repair of a failed server, which is highly common. At the same time, we want the LRCs to have good (ideally near-optimal) distance, subject to the locality constraints, so that we have fault-tolerance to a larger number of failures (erasures) in the worst-case.

The notion of locality can be further generalized by introducing the (r, δ)-LRC [24], which enhances fault tolerance within each recovery group. In an (r, δ)-LRC, each local group can correct up to $\delta - 1$ erasures, allowing the system to recover even when multiple erasures occur within a single locality group. This generalization strikes a balance between local redundancy and global robustness, providing a flexible framework for erasure recovery in large-scale distributed storage systems.

Explicit constructions achieving optimal trade-offs between distance and locality have been provided by Tamo and Barg [33], whose families of LRCs meet the Singleton-like bound for local recoverability [15]. Ballentine, Barg, and Vladut [1] further demonstrated that these constructions naturally extend to the hierarchical setting.

Building upon these classical developments, quantum locally recoverable codes (QLRCs) were introduced by Golowich and Guruswami [14] to explore the notion of locality in the context of quantum error correction. QLRCs are designed so that lost or corrupted qudits can be recovered using only a small subset of other qudits, preserving the quantum analog of locality.

Subsequent research has expanded on the theory of QLRCs, including [2, 8, 9, 10, 25, 26, 27, 31, 38]. In this work, we focus on the (r, δ)-QLRCs as defined in [10]. Our contributions extend the random QLRC and (folded) quantum Tamo–Barg constructions introduced in [14] to the general (r, δ) setting. The folded variant of the explicit constructions improves the asymptotic rate and distance trade-off when compared to the unfolded explicit construction. While proving that our constructions indeed give (r, δ) QLRCs, computing the dimension and locality parameters for these codes was straightforward, but computing a bound on the minimum distance (Theorem 4.12) of these codes required manipulating the more general parameters of (r, δ). Subsequently, the distance proofs are more involved than in [14], but the constructions in [14] still arise as a special case of our framework when $\delta = 2$.

Analogous to their classical counterparts, we generalize QLRCs to quantum hierarchical locally recoverable codes (QHLRCs), characterized by a hierarchy of locality and distance parameters $((r_1, \delta_1), \ldots, (r_h, \delta_h))$ for $h \geq 2$. QHLRCs inherit the multi-tier recovery structure of HLRCs, enabling both efficient local recovery and robust multi-erasure correction. We propose a random construction of QHLRCs (Section 3.3), along with a Singleton-like bound on their minimum distance, extending the trade-off relations known for classical codes to the quantum domain. Furthermore, we present an explicit construction of quantum hierarchical Tamo–Barg codes (Chapter 5), which naturally generalize the (r, δ)-Quantum Tamo–Barg codes while introducing a hierarchical recovery structure. Finally, we also develop an efficient decoding algorithm for the quantum Tamo–Barg codes.

This unified framework bridges the gap between locality-based code design in classical and quantum settings. By generalizing locality and hierarchical recovery to quantum codes, our constructions introduce new techniques which will prove useful towards developing scalable, efficient, and fault-tolerant quantum storage and computation systems capable of addressing reliability challenges in quantum technologies. It should be noted that not all notions related to classical locality extend to the quantum setting. One such notion is that of availability, as shown in [14, Theorem 9]. Hence, hierarchy is the natural generalization of locality in the quantum setting.

1.1 Contributions of the Dissertation

The main contributions of this dissertation are as follows.

1.1.1 Quantum Locally Recoverable Codes

QLRCs were previously defined only for $\delta = 2$ in the work of Golowich–Guruswami [14]. We generalize the definition to arbitrary $\delta \geq 2$, formalize the recovery guarantees, and show how to impose (r, δ) locality constraints within the CSS framework. We give both randomized and explicit constructions and discuss their optimality.

1.1.2 Quantum Hierarchical Locally Recoverable Codes

We define and construct the first quantum analogues of hierarchical LRCs, enabling multiple layers of locality with nested repair groups. These constructions extend both the combinatorial and operational intuition of classical HLRCs into the quantum setting. We provide randomized constructions and explicit constructions based on evaluation polynomials and analyze their optimality.

1.1.3 Folded Quantum Tamo–Barg codes.

We modify the explicit QLRC construction via a common technique known as folding and derive new trade-offs for the rate and distance.

1.1.4 Decoding Quantum Tamo–Barg codes.

We present a polynomial-time decoding algorithm for quantum Tamo–Barg codes that correct arbitrary errors up to half the distance, which is optimal in the unique-decoding sense.

1.2 Organization of the Dissertation

Chapter 2 establishes background material: finite fields, polynomials, linear codes, distance and rate, puncturing and shortening, classical LRCs and Tamo–Barg codes, and quantum CSS codes. Chapter 3 introduces (r, δ) quantum LRCs, defines quantum hierarchical LRCs and constructs randomized QLRCs and QHLRCs. Chapters 4 and 5 present explicit constructions of QLRCs and QHLRCs, respectively, inspired by Tamo–Barg codes. Chapter 6 develops folded quantum Tamo–Barg codes which achieve better asymptotic rate-distance trade-offs than the unfolded counterpart. Chapter 7 presents a polynomial time decoding algorithm for the quantum Tamo–Barg codes that corrects errors up to half the distance of the code.

Chapter 2

Preliminaries

In this chapter we collect the background material needed for the rest of the dissertation. We begin with basic notions from classical coding theory such as linear codes, rate, and distance, and recall standard bounds and examples like Reed–Solomon codes. We then discuss locally recoverable codes (LRCs) and the Tamo–Barg construction, since these are the classical prototypes underlying our quantum locally recoverable code constructions. We review stabilizer and CSS quantum codes, and the operations of puncturing and shortening that will appear repeatedly in later chapters. Lastly, we present some material on field theory, algebraic number theory, and uncertainty principles.

We fix some notation that will be used throughout the dissertation. Given a positive integer t, $[t] := \{0, 1, \ldots, t-1\}$. We write $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{C}$ for the integers, rational numbers, and complex numbers, respectively. If p is a prime, we write $\mathbb{F}_p$ for the finite field with p elements. We write $\mathbb{F}_q$ for the finite field where $q = p^m$ is a power of some prime p and positive integer m. Let $\mathbb{F}_q^n$ denote the n-dimensional vector space over the field $\mathbb{F}_q$. Let $\mathbb{F}_q^*$ denote the set of nonzero elements of $\mathbb{F}_q$. The set of $m \times n$ matrices with entries in $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^{m\times n}$. The entry in the i^{th} row and j^{th} column of a matrix $A \in \mathbb{F}_q^{m\times n}$ is denoted by A_{ij}.

2.1 Classical codes and basic parameters

We begin by recalling the standard definition of a (classical) code and its basic parameters.

Definition 2.1. Let Σ be a finite alphabet. A code C of block length n over Σ is a subset $C \subseteq \Sigma^n$. Elements of C are called *codewords*.

In this dissertation we will work only over finite fields, so the alphabet Σ will be $\mathbb{F}_q$ for some prime power q.

Definition 2.2 (Linear code)**.** A *linear code* C of block length n over $\mathbb{F}_q$ is a linear subspace $C \subseteq \mathbb{F}_q^n$.

The *dimension* of C is $k := \dim_{\mathbb{F}_q} C$ and the rate of C is $R(C) = k/n$. In many applications, a codeword $c \in C \subseteq \mathbb{F}_q^n$ is transmitted over a noisy channel and the received word $y \in (\mathbb{F}_q \cup \{?\})^n$ may differ from c. We distinguish between two types of corruptions.

- An *error* at position i occurs when the symbol c_i is altered to an unknown value in $\mathbb{F}_q$.
- An *erasure* at position i occurs when the symbol c_i is lost entirely and its location is known to the decoder; we denote erasures by the symbol ?.

The *support* of an error or erasure pattern is the set of corrupted coordinates. Errors are adversarial in value, whereas erasures reveal their locations. For $x, y \in \mathbb{F}_q^n$, the Hamming distance between x and y is

$$d_H(x, y) := |\{i \in [n] : x_i \neq y_i\}|.$$

The Hamming weight of a vector $x \in \mathbb{F}_q^n$ is $w_H(x) := d_H(x, 0)$.

Definition 2.3 (Minimum distance, relative distance)**.** The *minimum distance* of a code $C \subseteq \mathbb{F}_q^n$ is

$$d(C) := \min_{\substack{x,y \in C \\ x \neq y}} d_H(x, y) \;=\; \min_{0 \neq x \in C} w_H(x).$$

The *relative distance* is $\delta(C) := d(C)/n$.

If C has block length n, dimension k, and minimum distance d, we say C is an $[n, k, d]_q$ code (or simply $[n, k, d]$ if the field size is understood).

The minimum distance of a code governs its error- and erasure-correcting capabilities.

Proposition 2.4. *Let $C \subseteq \mathbb{F}_q^n$ be a code with minimum distance d.*

1. *C can uniquely correct up to $\lfloor (d-1)/2 \rfloor$ errors.*
2. *C can uniquely correct up to $d - 1$ erasures.*
3. *More generally, C can uniquely correct any pattern of t errors and e erasures satisfying*

$$2t + e < d.$$

Proof sketch. If two distinct codewords differ in at least d positions, then they cannot both agree with the received word outside a set of size $2t + e < d$. In the erasure-only case, uniqueness follows since at most one codeword can agree with the received symbols on $n - (d - 1)$ known positions. ■

Thus, the minimum distance quantifies the global resilience of a code against symbol corruptions. In later sections, we will be interested not only in global correction guarantees, but also in the ability to correct erasures using *local* subsets of coordinates, leading to the notion of locally recoverable codes.

The dual of linear code C is $C^{\perp} = \{c \in \mathbb{F}_q^n \mid c \cdot x = 0, \forall\, x \in C\}$. In other words, it is the orthogonal complement of C.

We will usually be interested in *families* of codes of growing block length. A family $\mathcal{C} = \{C_n\}$ consists of codes $C_n \subseteq \mathbb{F}_q^n$ with $n \to \infty$. The rate and relative distance of the family are defined by

$$R(\mathcal{C}) := \liminf_{n\to\infty} \frac{\log_q |C_n|}{n}, \qquad \delta(\mathcal{C}) := \liminf_{n\to\infty} \frac{d(C_n)}{n}.$$

We say that $\mathcal{C}$ is *asymptotically good* if $R(\mathcal{C}) > 0$ and $\delta(\mathcal{C}) > 0$.

Example 1. One simple class of codes is the repetition code. For any positive integer r, the r-repetition code maps $\mathbb{F}_q^k$ to $\mathbb{F}_q^{rk}$ by repeating each vector component r times. This gives a family of codes which is defined for any block length n_i, a multiple of r. The rate of this family of codes is $1/r$ and the relative distance is r/n. For a fixed r, as $n \to \infty$, the relative distance tends to 0 so the code family is not asymptotically good. However, as we increase r, the rate will decrease and the relative distance increases.

The repetition code exhibits one of the most fundamental phenomenons of error correcting codes: the rate and distance tradeoff. A classical upper bound on the achievable tradeoff between rate and distance is the Singleton bound.

Theorem 2.5 (Singleton bound)**.** *Let C be a q-ary code of block length n and minimum distance d. Then*

$$|C| \leq q^{n-d+1}.$$

In particular, if C is linear of dimension k, then $k \leq n - d + 1$, i.e.,

$$R(C) \ \leq \ 1 - \delta(C) + \frac{1}{n}.$$

Proof sketch. Any two distinct codewords must disagree in at least d coordinates, so they cannot agree on any fixed set of $n - d + 1$ coordinates. Thus each codeword is uniquely determined by its first $n - d + 1$ symbols, giving at most q^{n-d+1} codewords in total. ■

Codes that meet the Singleton bound with equality (i.e. with $k = n - d + 1$) are called Maximum Distance Separable (MDS).

2.2 Polynomial evaluation and Reed–Solomon codes

Many of the codes we consider—both classical and quantum—are based on evaluation of low-degree polynomials over finite fields. We briefly recall this perspective here.

Evaluation codes

Let $\mathbb{F}_q[X]$ denote the polynomial ring in one variable X over the field $\mathbb{F}_q$.

Definition 2.6 (Evaluation code)**.** Fix a subset $S \subseteq \mathbb{N}$ and let

$$\mathbb{F}_q[X]^S = \left\{ \sum_{i \in S} a_i X^i \mid a_i \in \mathbb{F}_q \right\}$$

denote the $|S|$-dimensional subspace of $\mathbb{F}_q[X]$ consisting of polynomials with zero coefficients for all monomials X^i with $i \notin S$. Define the polynomial evaluation map at a set $E \subseteq \mathbb{F}_q$ as

$$\mathrm{ev}_E : \mathbb{F}_q[X]^S \to \mathbb{F}_q^{|E|}$$

by $\mathrm{ev}(f) = (f(x))_{x \in E}$. The image of $\mathrm{ev}_E(\mathbb{F}_q[X]^S)$ is a linear code with alphabet size q, block length $|E|$, and dimension $|S|$.

Note that for the code to be nontrivial, q and E must be large enough so that $q \geq |E| > |S|$. Some common choices for E are $\mathbb{F}_q$ or $\mathbb{F}_q^*$. From now on if E is not specified, we assume $E = \mathbb{F}_q^*$

Perhaps the most well-known polynomial evaluation code is the Reed-Solomon code. Let $E = \{\alpha_1, \dots, \alpha_n\}$ be distinct points in $\mathbb{F}_q$ and let $S = \{0, \dots, k-1\}$. The Reed-Solomon code is the polynomial evaluation code $C = \mathrm{ev}_E(\mathbb{F}_q[X]^S)$. By definition, C has dimension k and block length n over an alphabet of size q. We now show that Reed-Solomon codes are MDS.

Lemma 2.7. *Let $C = \mathrm{ev}_E(\mathbb{F}_q[X]^S)$ be the Reed-Solomon code as described above. Then C is an $[n, k, n-k+1]_q$ linear code.*

Proof. Linearity and $\dim C = k$ are immediate. For distance, if $0 \neq f \in \mathbb{F}_q[X]$ with $\deg f < k$, then f has at most $k-1$ zeros in $\mathbb{F}_q$. Thus its evaluation vector can have at most $k-1$ zeros among the n coordinates, so the Hamming weight is at least $n-(k-1) = n-k+1$. This shows $d(C) \geq n-k+1$, and the Singleton bound implies equality. ■

These Reed-Solomon codes will serve as a conceptual starting point for Tamo–Barg codes and their quantum analogues in later chapters.

Puncturing and shortening

Before describing Tamo–Barg codes, we introduce two standard operations on codes that will be used throughout this dissertation: puncturing and shortening.

Definition 2.8 (Puncturing)**.** Let $C \subseteq \mathbb{F}_q^n$ and let $I \subseteq [n]$ be a set of coordinates. The *puncturing* of C on I, denoted as $\pi_I(C)$ or $C|_I$, is the code in $\mathbb{F}_q^{|I|}$ obtained by restricting each codeword to the coordinates in I:

$$C|_I := \{(c_i)_{i \in I} : c \in C\}.$$

Puncturing simply deletes coordinates but does not impose any additional linear constraints. Additionally, puncturing a code can only decrease the distance. In contrast, shortening first restricts to codewords that have zeros at certain coordinates and then punctures them. Consequently, the shortening of a code can only increase the distance.

Definition 2.9 (Shortening)**.** Let $C \subseteq \mathbb{F}_q^n$ and let $I \subseteq [n]$. The *shortening* of C on I, denoted $\sigma_I(C)$ or C^I, is defined by

$$C^I := \{(c_i)_{i \in I} : c \in C,\ c_j = 0 \text{ for all } j \notin I\}.$$

If C is linear, both $\pi_I(C)$ and $\sigma_I(C)$ are linear. Furthermore, a well-known fact is $\pi_I(C)^\perp = \sigma_I(C^\perp)$ (see [21]) and by definition $\sigma_I(C) \subseteq \pi_I(C)$.

2.3 Locally recoverable codes and Tamo–Barg construction

We now turn to *locality*. In many storage and communication systems one wishes not only to correct a large number of errors globally, but also to repair individual erased symbols by accessing only a small *local* subset of other symbols. This leads to the notion of locally recoverable codes (LRCs).

Locality and (r, δ)-locality

The original notion of locality required that each coordinate can be recovered from at most r other coordinates.

Definition 2.10. A code $C \subseteq \mathbb{F}_q^n$ has *locality* r if, for every coordinate $i \in [n]$, there exists a subset $R_i \subseteq [n]$ such that $i \in R_i$ and $|R_i| \le r + 1$ and a recovery function $\phi_i : \mathbb{F}_q^{R_i \setminus \{i\}} \to \mathbb{F}_q$ such that, for every codeword $c \in C$,

$$c_i = \phi_i\left((c_j)_{j \in R_i \setminus \{i\}}\right).$$

The set R_i is called a *repair set* for coordinate i.

In the presence of multiple erasures within the same repair set, it is useful to have several linearly independent local parity checks, each supported on a slightly larger set. This motivates the (r, δ)-locality notion.

Definition 2.11. Let $\delta \ge 2$ be an integer. A linear code $C \subseteq \mathbb{F}_q^n$ has (r, δ)-*locality* if for every coordinate $i \in [n]$ there exists a subset $R_i \subseteq [n]$ with $i \in R_i$ and $|R_i| \le r + \delta - 1$ such that the punctured code $C|_{R_i}$ has minimum distance at least δ. Equivalently, the restriction $C|_{R_i}$ can correct up to $\delta - 1$ erasures within R_i.

Thus each coordinate participates in a small local code of length at most $r+\delta-1$ and distance at least δ. When $\delta = 2$, this reduces to the original locality notion: each local group provides a single parity check that can repair any single erasure in the group using at most r other symbols.

We have a generalization of the Singleton bound for LRCs that we state without proof.

Theorem 2.12 ([23])**.** *Let C be an $[n, k, d]$ linear code with (r, δ) locality. The minimum distance of C satisfies*

$$d \leq n - k + 1 - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1).$$

We already saw that Reed-Solomon codes meet the Singleton bound. We will now present a generalization of the Reed-Solomon codes which meets the Singleton-type bound for LRCs.

Tamo–Barg codes

Tamo–Barg (TB) codes ([33]) are polynomial evaluation codes with carefully chosen evaluation sets and monomial sets ensuring (r, δ)-locality.

Construction 2.13. Suppose we are given a finite field $\mathbb{F}_q$, a dimension parameter k, and recovery parameters (r, δ). Assume $r+\delta-1 \mid q-1$ and $r \mid k$. Let $\Omega \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup of size $r+\delta-1$. Let $g(X) = X^{r+\delta-1}$ and note that g is constant on each coset of Ω. Let

$$S = \bigcup_{j=1}^{\delta-1} (-j + (r+\delta-1)\mathbb{Z})$$

and

$$\ell = \left(\frac{k}{r} - 1 \right) (r+\delta-1) + r.$$

Consider the evaluation codes $A = \mathrm{ev}(\mathbb{F}_q[X]^{[\ell]})$ and $B = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\setminus S})$. Then the (r, δ) Tamo–Barg code is defined to be $C := A \cap B$.

We now prove the dimension, distance, and locality properties of this code.

Theorem 2.14 ([33])**.** *The (r, δ) Tamo–Barg code C from Construction 2.13 has block length $n = q-1$, dimension k, and distance*

$$d = n - k + 1 - \left(\frac{k}{r} - 1 \right) (\delta - 1)$$

meeting the bound from Theorem 2.12. Lastly, it is an (r, δ) LRC as defined in Definition 2.11.

Proof. The block length is $n = q-1$ since we are evaluating at all points in $\mathbb{F}_q^*$. For every group of $(r+\delta-1)$ exponents, we exclude $\delta-1$ exponents. Consequently, out of ℓ exponents, we include

$$\left(\frac{k}{r}-1\right)r + r = k$$

exponents so the dimension of the code is k. Any polynomial that we evaluate has degree at most $\ell - 1$ so the corresponding codeword has weight at least

$$n-(\ell-1) = n - \left(\frac{k}{r}-1\right)(r+\delta-1) - r + 1 = n-k+1-\left(\frac{k}{r}-1\right)(\delta-1).$$

Therefore, the distance of the (r,δ) TB code meets the Singleton-type bound for LRCs from Theorem 2.12. Lastly, we show that it satisfies (r,δ)-locality. Suppose we have a codeword $c = \mathrm{ev}(f)$ and the erased symbol is at $x \in \alpha\Omega$ for some coset $\alpha\Omega$. Restricting f to the coset $\alpha\Omega$ is a polynomial with degree at most $r-1$ and $|\alpha\Omega \setminus \{x\}| = r+\delta-2$ so f can be reconstructed from any r values in $\alpha\Omega \setminus \{x\}$. Equivalently, f can be reconstructed from r points inside $\alpha\Omega$ when $\delta - 1$ of them are erased. ■

Remark 2.15. This presentation of a Tamo–Barg code is not the most general. We evaluate at all $q-1$ points, but this can be relaxed to arbitrary n. Furthermore, the restriction of $r \mid k$ can also be dropped. For explicit details of these relaxations see [33]. Notice that if $r = k$ and $\delta = 2$, then Construction 2.13 reduces to the Reed-Solomon code.

We can extend the structure of LRCs so that the punctured subcodes are themselves LRCs. This gives a hierarchical structure to the code. An h-level Hierarchical Locally Recoverable Code (HLRC) is defined as follows:

Definition 2.16 ($((r_1,\delta_1),\ldots,(r_h,\delta_h))$-HLRCs ([30])). An $[n,k,d]$ code C has h-level hierarchical locality with locality parameters $(r_1,\delta_1),\ldots,(r_h,\delta_h)$ if, for every $1 \le i \le n$, there exists a set $I \subseteq [n]$ of cardinality at most $r_1+\delta_1-1$ such that $i \in I$ and the punctured code $C|_I$ satisfies the following:

- $\dim(C|_I) \le r_1$,
- $d(C|_I) \ge \delta_1$,
- the punctured code $C|_I$ is a code with $(h-1)$-level hierarchical locality having local parameters $(r_2,\delta_2),\ldots,(r_h,\delta_h)$.

2.4 Quantum stabilizer and CSS codes

We now present the necessary background on quantum mechanics, stabilizer formalism, and the CSS construction which will be used to construct the quantum error correcting codes.

Qudits and Pauli operators

Fix a prime power $q = p^m$. A single q-level quantum system (a *qudit*) is modeled by the Hilbert space $\mathcal{H} = \mathbb{C}^q$, with computational basis $\{|0\rangle, \ldots, |q-1\rangle\}$. A general state of a qudit is given by

$$|\psi\rangle = \sum_{i=0}^{q-1} \alpha_i |i\rangle, \quad \text{where } \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{q-1} |\alpha_i|^2 = 1$$

An n-qudit system is $\mathcal{H}^{\otimes n} = (\mathbb{C}^q)^{\otimes n}$.

Elements of the dual space $\mathcal{H}^*$ are denoted by $\langle y|$ so the inner product of two vectors $|x\rangle$ and $|y\rangle$ reads $\langle x|y\rangle$ and linear operators M can be decomposed as

$$M = (M_{i,j}) = \sum_{i,j} M_{i,j} |i\rangle \langle j|.$$

Let $\omega = e^{2\pi i/p}$ be the primitive p-th root of unity and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the trace map defined by $\mathrm{tr}(z) = \sum_{i=0}^{m-1} z^{p^i}$. Quantum errors are modeled by generalized Pauli operators. For $a, b \in \mathbb{F}_q$, one defines single-qudit operators X^a and Z^b by

$$X^a = \sum_{x\in\mathbb{F}_q} |x+a\rangle \langle x|, \qquad Z^b = \sum_{x\in\mathbb{F}_q} \omega^{\mathrm{tr}(bx)} |x\rangle \langle x|$$

The X-type errors are similar to classical errors where a symbol is changed. The Z-type errors are phase change errors. We also have a quantum analogue of erasures where a qudit is affected by a depolarizing channel and the state is erased. We will mostly focus on erasures, but understanding X-type and Z-type errors is necessary for constructing quantum error correcting codes. Now consider the set of unitary operators $\mathcal{E} = \{X^a Z^b : a, b \in \mathbb{F}_q\}$ which we call the error basis. These q^2 operators form an orthogonal basis with respect to the inner product $\langle M, N\rangle = \mathrm{tr}(M^\dagger N)$ where $M^\dagger$ is the Hermitian conjugate of M. The set $\mathcal{E}$ gives rise to a group $\mathcal{P}_1 = \{\omega^i X^a Z^b : i \in [p], a, b \in \mathbb{F}_q\}$. The group properties are straightforward to verify and clearly $|\mathcal{P}| = pq^2$. The commutation relation is seen as follows:

$$\begin{aligned}
\omega^{\mathrm{tr}(ab)} X^a Z^b (X^a)^{-1} &= \omega^{\mathrm{tr}(ab)} \sum_{x\in\mathbb{F}_q} |x+a\rangle \langle x| \sum_{z\in\mathbb{F}_q} \omega^{\mathrm{tr}(bz)} |z\rangle \langle z| \sum_{y\in\mathbb{F}_q} |y\rangle \langle y+a| \\
&= \omega^{\mathrm{tr}(ab)} \sum_{z\in\mathbb{F}_q} \omega^{\mathrm{tr}(bz)} |z+a\rangle \langle z+a| \\
&= \omega^{\mathrm{tr}(ab)} \sum_{z\in\mathbb{F}_q} \omega^{\mathrm{tr}(b(z-a))} |z\rangle \langle z| \\
&= Z^b.
\end{aligned}$$

which implies

$$\omega^{\mathrm{tr}(ab)} X^a Z^b = Z^b X^a. \tag{2.1}$$

Hence, any two elements commute up to a global phase.

For the n-qudit system we take the n-fold tensor product i.e. $\mathcal{E}^{\otimes n}$ and $\mathcal{P}_n := (\mathcal{P}_1)^{\otimes n}$. In particular, now an n-qudit Pauli operator is of the form $X^a Z^b = \otimes_{i=1}^n X^{a_i} Z^{b_i}$ for $a, b \in \mathbb{F}_q^n$. The *support* of a Pauli $P = X^a Z^b$ is defined as $\text{supp}(X^a Z^b) = \{i : (a_i, b_i) \neq (0,0)\}$ and the *Hamming weight* of P is $|P| = |\text{supp}(P)|$. Equivalently, the weight is the number of tensor factors that are not I. If a K-dimensional subspace $\mathcal{Q}$ of $\mathcal{H}^{\otimes n}$ can correct all errors in $\mathcal{E}^{\otimes n}$ of weight no greater than t then $\mathcal{Q}$ is a quantum error correcting code with minimum distance $2t+1$ and is denoted as $((n, K, 2t+1))$.

Assume $s \mid n$. We denote $(\mathcal{P}_s)_{\frac{n}{s}} = \mathcal{P}_n$ and interpret as the group of length n/s strings of elements in $\mathcal{P}_s$. This structure will naturally arise when we discuss folded codes in Chapter 6.

Stabilizer codes

We will now focus on a specific class of quantum error correcting codes known as stabilizer codes. The group $\mathcal{P}_n$ has center $\langle \omega I \rangle$ so the quotient group $\overline{\mathcal{P}}_n := \mathcal{P}_n / \langle \omega I \rangle$ is isomorphic to $\mathbb{F}_q^n \times \mathbb{F}_q^n \cong \mathbb{F}_q^{2n}$. A *stabilizer group* is a subgroup $S \subseteq \mathcal{P}_n$ which is abelian and contains no nontrivial phases i.e. $S \cap \langle \omega I \rangle = \{I\}$. Elements of S are called *stabilizers*. The code space is the joint $+1$ eigenspace of all elements of S:

$$\mathcal{Q}(S) := \{|\psi\rangle \in (\mathbb{C}^q)^{\otimes n} : P\,|\psi\rangle = |\psi\rangle \text{ for all } P \in S\}.$$

If S has $n-k$ independent generators, the code encodes k logical qudits into n physical qudits so $\dim \mathcal{Q}(S) = k$. What remains is to compute the distance of $\mathcal{Q}(S)$. Recall, the weight of a Pauli operator is the number of qudits on which it acts nontrivially. The normalizer (also the centralizer) of S is $N(S) = \{P \in \mathcal{P}_n \mid PS = SP\}$ so $P \in N(S)$ if and only if it commutes with every stabilizer. Elements of $N(S) \setminus S$ are called logical operators. Given a Pauli error E, we have three cases:

- If $E \notin N(S)$, then E anticommutes with at least one stabilizer so E is a detectable error.
- If $E \in S$ then E acts trivially on the codespace.
- If $E \in N(S) \setminus S$, then E preserves the codespace, but acts nontrivially on the codespace so E is an undetectable logical error.

Therefore, we define the minimum distance of a stabilizer code as

$$d = \min\{|E| : E \in N(S) \setminus S\}.$$

The distance d is the largest integer such that every Pauli error of weight $< d$ is either detected by the stabilizers or a stabilizer itself. For a stabilizer code $\mathcal{Q}(S)$ which encodes k logical qudits into n physical qudits and has distance d, we denote it as $[[n, k, d]]_q$. We will often omit q when the field is known.

CSS codes from classical linear codes

The Calderbank–Shor–Steane (CSS) construction builds stabilizer codes from pairs of classical linear codes. Let $C_X, C_Z \subseteq \mathbb{F}_q^n$ be linear codes such that $C_Z^\perp \subseteq C_X$. Here $C_Z^\perp$ is the dual of C_Z with respect to the standard Euclidean inner product on $\mathbb{F}_q^n$. The associated stabilizer group is

$$S = \{X^a Z^b : a \in C_X^\perp, b \in C_Z^\perp\}.$$

Under the inclusion condition $C_Z^\perp \subseteq C_X$, these stabilizers commute, defining a valid stabilizer code.

Definition 2.17 (CSS code)**.** Given $C_X, C_Z \subseteq \mathbb{F}_q^n$ with $C_Z^\perp \subseteq C_X$, the *CSS code* $\mathcal{Q}$ is denoted

$$\mathcal{Q} = \mathrm{CSS}(C_X, C_Z).$$

The code encodes

$$k = \dim C_X + \dim C_Z - n$$

logical qudits into n physical qudits.

The dimension also follows from the stabilizer group as S has $\dim C_X^\perp + \dim C_Z^\perp$ generators so the dimension of $\mathcal{Q}$ is

$$\dim \mathcal{Q} = n - (\dim C_X^\perp + \dim C_Z^\perp) = \dim C_X - \dim C_Z^\perp = \dim C_X + \dim C_Z - n.$$

The distance of a CSS code decomposes into X-type and Z-type distances. The X-type logical operators correspond to $C_Z \setminus C_X^\perp$ and the Z-type logical operators correspond to $C_X \setminus C_Z^\perp$. Hence, the minimum distance is $d = \min(d_X, d_Z)$ where

$$d_X = \min\{\mathrm{wt}(v) : v \in C_Z \setminus C_X^\perp\}, \qquad d_Z = \min\{\mathrm{wt}(v) : v \in C_X \setminus C_Z^\perp\}.$$

A particularly simple and symmetric situation arises when $C_X = C_Z = C$. In this case one must have $C^\perp \subseteq C$, so C is a dual containing code. Then

$$\mathcal{Q} = \mathrm{CSS}(C, C), \qquad k = \dim C - \dim C^\perp = 2 \cdot \dim C - n,$$

and the distance is

$$d = \min\{w_H(v) : v \in C \setminus C^\perp\}.$$

All of the explicit quantum codes we construct in this dissertation are of the form $\mathrm{CSS}(C, C)$ for carefully chosen classical codes C.

2.4.1 Puncturing CSS codes

As with classical codes, there is a puncturing operation associated to quantum codes. For general stabilizer codes, puncturing is most naturally described as a shortening operation on the stabilizer group. Let $S \subseteq \mathcal{P}_n$ be a stabilizer group. If

$$P = \lambda P_1 \otimes \cdots \otimes P_n \in \mathcal{P}_n,$$

where each P_i is a single-qudit Pauli operator and λ is a phase, then for a subset $I \subseteq \{1, \ldots, n\}$ we write

$$P|_I := \lambda \bigotimes_{i \in I} P_i$$

whenever $P_j = I$ for all $j \notin I$. In other words, we only restrict P to I if P acts trivially outside I.

The puncturing of the stabilizer group S to the coordinate set I is defined by

$$S|_I := \{P|_I : P \in S,\ \mathrm{supp}(P) \subseteq I\}.$$

Thus, one first keeps only those stabilizers which act trivially on the deleted coordinates, and then restricts them to the remaining coordinates. Since S is abelian, $S|_I$ is also abelian. Moreover, $S|_I$ contains no nontrivial phase: if $P|_I$ were a nontrivial phase, then P itself would be a nontrivial phase in S, which is impossible. Hence $S|_I$ is again a valid stabilizer group, now on $|I|$ physical qudits. This is the stabilizer-code puncturing operation [18, 19].

For the constructions, we only need this operation for quantum CSS codes. Let

$$\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$$

be a CSS code, where $C_Z^\perp \subseteq C_X$. Its stabilizer group is

$$S_{\mathcal{Q}} = \{X^a Z^b : a \in C_X^\perp,\ b \in C_Z^\perp\}.$$

We define the puncturing of $\mathcal{Q}$ to the coordinate set $I \subseteq \{1, \ldots, n\}$ by puncturing the associated classical codes:

$$\mathcal{Q}|_I := \mathrm{CSS}(C_X|_I, C_Z|_I).$$

Here $C|_I = \pi_I(C)$ denotes the classical puncturing of C to the coordinates in I.

Lemma 2.18. *Let $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$ be a quantum CSS code with $C_Z^\perp \subseteq C_X$. For any subset $I \subseteq \{1, \ldots, n\}$, the punctured code*

$$\mathcal{Q}|_I := \mathrm{CSS}(C_X|_I, C_Z|_I)$$

is again a well-defined quantum CSS code. Moreover, this definition agrees with the stabilizer-code puncturing operation described above.

Proof. Let π_I denote puncturing to the coordinate set I, so that $C|_I = \pi_I(C)$. Let $\sigma_I(C)$ denote shortening to I, namely

$$\sigma_I(C) := \{c|_I : c \in C,\ c_j = 0 \text{ for all } j \notin I\}.$$

We use the standard duality relation between puncturing and shortening: $(C|_I)^\perp = \sigma_I(C^\perp)$.

First, we check the CSS orthogonality condition. Since $C_Z^\perp \subseteq C_X$, we have

$$(C_Z|_I)^\perp = \sigma_I(C_Z^\perp) \subseteq \sigma_I(C_X) \subseteq C_X|_I.$$

and by duality, we obtain $(C_X|_I)^\perp \subseteq C_Z|_I$. Therefore $C_X|_I$ and $C_Z|_I$ satisfy the CSS orthogonality conditions, so $\mathrm{CSS}(C_X|_I, C_Z|_I)$ is a well-defined quantum CSS code.

It remains to compare this definition with stabilizer puncturing. The stabilizer group of $\mathcal{Q}$ is

$$S_{\mathcal{Q}} = \{X^a Z^b : a \in C_X^\perp,\ b \in C_Z^\perp\}.$$

Its stabilizer puncturing to I is

$$S_{\mathcal{Q}}|_I = \{(X^a Z^b)|_I : a \in C_X^\perp,\ b \in C_Z^\perp,\ a_j = b_j = 0 \text{ for all } j \notin I\}.$$

Equivalently,

$$S_{\mathcal{Q}}|_I = \{X^{a'} Z^{b'} : a' \in \sigma_I(C_X^\perp),\ b' \in \sigma_I(C_Z^\perp)\}.$$

On the other hand, the stabilizer group of $\mathrm{CSS}(C_X|_I, C_Z|_I)$ is

$$\{X^{a'} Z^{b'} : a' \in (C_X|_I)^\perp,\ b' \in (C_Z|_I)^\perp\}.$$

Using $(C|_I)^\perp = \sigma_I(C^\perp)$, this becomes $\{X^{a'} Z^{b'} : a' \in \sigma_I(C_X^\perp),\ b' \in \sigma_I(C_Z^\perp)\}$, which is exactly $S_{\mathcal{Q}}|_I$. Thus, puncturing the classical codes C_X and C_Z agrees with puncturing the associated CSS stabilizer group. ■

2.5 Decoding algorithms

Here we recall a few results that are necessary to prove the efficiency of our decoding algorithm, Algorithm 1. Given a Reed-Solomon code with block length $q-1$ and rate $R = \ell/(q-1)$, there exists an efficient list decoding algorithm for the Reed-Solomon code which can be summarized in the following statement.

Theorem 2.19 ([20])**.** *The Reed-Solomon code with parameters q, ℓ has an e-list-decoding algorithm that runs in time $q^{O(1)}$ for $e = (q-1)(1-\sqrt{R})$.*

Furthermore, it is well-known that to decode a CSS code $\mathcal{Q} = CSS(C_X, C_Z)$ it is sufficient to have classical decoders for C_X, C_Z.

Proposition 2.20 ([3, 32])**.** *Let $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$ be a CSS code of block length n over $\mathbb{F}_q^s$ of size $|\mathbb{F}_q^s|$. Let $e \geq 0$ be an integer such that each permutation (α, β) of (X, Z), there exists a classical decoding algorithm Dec_α that takes as input a classical corrupted codeword $c + b$ for some $c \in C_\alpha$ and some corruption $b \in (\mathbb{F}_q^s)^n$ of Hamming weight $|b| \leq e$, and outputs some $c' \in C_\alpha$ such that $c' - c \in C_\beta^\perp$. Then $\mathcal{Q}$ has a decoding algorithm Dec that recovers from errors of weight e, so $\mathcal{Q}$ has distance $d \geq 2e+1$. Furthermore, if each Dec_α has running time $T_\alpha(n, a)$, thenDec has running time $T_X(n, a) + T_Z(n, a) + O(n^3 \operatorname{polylog} a)$.*

2.6 Field theory

Now we collect some standard field-theoretic notation and results used throughout the paper. For more details, we refer the reader to [29].

Let K be a field. A *field extension* L/K is an inclusion of fields $K \subseteq L$. It is called *finite* if L is finite-dimensional as a vector space over K. In this case, the *degree* of the extension is $[L : K] := \dim_K L$.

A field extension L/K is called *algebraic* if every element of L is a root of a nonzero polynomial with coefficients in K. An algebraic field extension L/K is called *separable* if every element of L has separable minimal polynomial (i.e. coprime to its formal derivative) over K. An algebraic field extension L/K is called *normal* if every irreducible polynomial over K that has a root in L splits into linear factors over L. An algebraic field extension which is both normal and separable is called *Galois.* We denote the Galois group of a Galois extension L/K by $\mathrm{Gal}(L/K)$.

An *algebraic closure* of K is a field $\overline{K}$ containing K such that $\overline{K}$ is algebraic over K and every nonconstant polynomial in $\overline{K}[X]$ has a root in $\overline{K}$. Equivalently, every nonconstant polynomial in $K[X]$ splits into linear factors over $\overline{K}$. Whenever an algebraic closure is needed, we fix one and denote it by $\overline{K}$.

Let L/K be a finite field extension. The *field norm* from L to K is the map

$$N_{L/K} : L \longrightarrow K$$

defined as follows. For $x \in L$, let $m_s : L \longrightarrow L$ be the K-linear map given by multiplication by x: $y \longmapsto xy$. Then

$$N_{L/K}(x) := \det_K(m_x).$$

If L/K is separable, then the norm admits the equivalent description

$$N_{L/K}(x) = \prod_{\sigma : L \hookrightarrow \overline{K}} \sigma(x),$$

where the product is over all K-embeddings of L into a fixed algebraic closure $\overline{K}$. Here a K-embedding means an injective field homomorphism that restricts to the identity on K. In particular, if L/K is Galois, then

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

When K is perfect, every finite extension of K is separable, so the embedding formula for the norm applies to all finite extensions of K.

For a positive integer n, an element ζ of a field is called an nth root of unity if $\zeta^n = 1$. It is called a *primitive* nth root of unity if n is the smallest positive integer such that $\zeta^n = 1$, or equivalently, if ζ has multiplicative order n.

The nth *cyclotomic polynomial* is the polynomial

$$\Phi_n(X) := \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(X - e^{2\pi i k/n}\right) \in \mathbb{C}[X].$$

It is a standard fact that $\Phi_n(X) \in \mathbb{Z}[X]$, and that $X^n - 1 = \prod_{d|n} \Phi_d(X)$. The degree of $\Phi_n(X)$ is $\varphi(n)$, where φ denotes Euler's totient function. We write ζ_n for a fixed primitive nth root of unity. Thus the roots of $\Phi_n(X)$ over $\mathbb{C}$ are precisely the primitive nth roots of unity.

We end this section with a definition describing the set of subspaces of a vector space and its size.

Definition 2.21. Let V be a finite-dimensional vector space over $\mathbb{F}_q$, and let $0 \le k \le \dim_{\mathbb{F}_q} V$. The *Grassmannian* of k-dimensional subspaces of V, denoted $\mathrm{Gr}_{\mathbb{F}_q}(k, V)$, is the set

$$\mathrm{Gr}_{\mathbb{F}_q}(k, V) := \{U \subseteq V : U \text{ is an } \mathbb{F}_q\text{-linear subspace and } \dim_{\mathbb{F}_q} U = k\}.$$

When $V = \mathbb{F}_q^n$, we also write $\mathrm{Gr}_{\mathbb{F}_q}(k, n) := \mathrm{Gr}_{\mathbb{F}_q}(k, \mathbb{F}_q^n)$. Since $\mathbb{F}_q$ is finite, $\mathrm{Gr}_{\mathbb{F}_q}(k, V)$ is a finite set. If $\dim_{\mathbb{F}_q} V = n$, then

$$|\mathrm{Gr}_{\mathbb{F}_q}(k, V)| = \binom{n}{k}_q := \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{k-i} - 1},$$

where $\binom{n}{k}_q$ is the Gaussian binomial coefficient.

2.7 The resultant

In this section we recall the Sylvester matrix and the resultant of two univariate polynomials. We also record the description of the resultant in terms of roots in an algebraic closure, its interpretation as a field norm in the irreducible case, and a reduction-modulo-p criterion that will be used later. For a more in-depth treatment, see [6, 12, 29]. We will use the field-theoretic notation fixed in Section 2.6.

Let K be a field, and let

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \qquad g(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0$$

be nonzero polynomials in $K[X]$ of degrees m and n, respectively.

Definition 2.22 (Sylvester matrix)**.** The *Sylvester matrix* of f and g, denoted $\mathrm{Syl}(f, g)$, is the $(m + n) \times (m + n)$ matrix obtained by writing n shifted copies of the coefficient vector of f, followed by m shifted copies of the coefficient vector of g. Explicitly,

$$\mathrm{Syl}(f, g) = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{pmatrix},$$

where the first block consists of n rows and the second block consists of m rows.

Definition 2.23 (Resultant)**.** The *resultant* of f and g is $\operatorname{Res}(f,g) := \det \operatorname{Syl}(f,g)$.

Since the entries of $\operatorname{Syl}(f,g)$ are polynomial expressions in the coefficients of f and g, the resultant is itself a polynomial expression in those coefficients, with integer coefficients. In particular, if $f, g \in \mathbb{Z}[X]$, then $\operatorname{Res}(f,g) \in \mathbb{Z}$.

Proposition 2.24 (Root formula for the resultant)**.** *Let K be a field. Let $f, g \in K[X]$ be nonzero polynomials of degrees m and n, respectively, and write*

$$f(X) = a_m \prod_{i=1}^{m} (X - \alpha_i), \qquad g(X) = b_n \prod_{j=1}^{n} (X - \beta_j)$$

in $\overline{K}[X]$, where the roots are counted with multiplicity. Then

$$\operatorname{Res}(f,g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

Equivalently,

$$\operatorname{Res}(f,g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j).$$

Proof. The equivalence of the displayed formulas follows from the fact that

$$g(\alpha_i) = b_n \prod_{j=1}^{n} (\alpha_i - \beta_j) \quad \text{and} \quad f(\beta_j) = a_m \prod_{i=1}^{m} (\beta_j - \alpha_i).$$

The agreement of these expressions with $\det \operatorname{Syl}(f,g)$ is the standard determinantal formula for the resultant. ■

The most important immediate consequence is the following.

Corollary 2.25. *Let K be a field, and let $f, g \in K[X]$ be nonzero polynomials. Then* $\operatorname{Res}(f,g) = 0$ *if and only if f and g have a common root in $\overline{K}$. Equivalently,* $\operatorname{Res}(f,g) = 0$ *if and only if f and g have a nonconstant common factor in $K[X]$.*

Proof. By Proposition 2.24,

$$\operatorname{Res}(f,g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

Since $a_m \neq 0$ and $b_n \neq 0$, this product vanishes if and only if $\alpha_i = \beta_j$ for some i, j, that is, if and only if f and g share a root in $\overline{K}$. The final equivalence is standard: two polynomials in $K[X]$ have a common root in $\overline{K}$ if and only if they have a nonconstant common factor in $K[X]$. ■

We next record the norm interpretation of the resultant in the irreducible case.

Proposition 2.26 (Resultant as a norm). *Let K be a field, let $f(X) = a_m X^m + \cdots + a_0 \in K[X]$, and $g(X) \in K[X]$, and suppose that f is irreducible and separable over K. Let α be a root of f in $\overline{K}$. Then*

$$\operatorname{Res}(f, g) = a_m^{\deg g} \, N_{K(\alpha)/K}\left(g(\alpha)\right).$$

In particular, if f is monic, then $\operatorname{Res}(f, g) = N_{K(\alpha)/K}\left(g(\alpha)\right)$.

Proof. Let $m = \deg f$ and $n = \deg g$. Write

$$f(X) = a_m \prod_{i=1}^{m} (X - \alpha_i)$$

in $\overline{K}[X]$, where $\alpha_1, \ldots, \alpha_m$ are the roots of f. Since f is irreducible and separable, these roots are distinct and are precisely the images of α under the K-embeddings $\sigma : K(\alpha) \hookrightarrow \overline{K}$. By Proposition 2.24,

$$\operatorname{Res}(f, g) = a_m^n \prod_{i=1}^{m} g(\alpha_i).$$

On the other hand, by the embedding formula for the norm,

$$N_{K(\alpha)/K}\left(g(\alpha)\right) = \prod_{\sigma : K(\alpha) \hookrightarrow \overline{K}} \sigma\left(g(\alpha)\right) = \prod_{\sigma : K(\alpha) \hookrightarrow \overline{K}} g\left(\sigma(\alpha)\right) = \prod_{i=1}^{m} g(\alpha_i).$$

Combining the two formulas gives $\operatorname{Res}(f, g) = a_m^n \, N_{K(\alpha)/K}\left(g(\alpha)\right)$. The second statement follows by setting $a_m = 1$. ■

A particularly important special case is when f is a cyclotomic polynomial.

Corollary 2.27 (Cyclotomic norm formula). *Let $n \geq 1$, let $\Phi_n(X) \in \mathbb{Z}[X]$ be the nth cyclotomic polynomial, and let $\zeta_n \in \mathbb{C}$ be a primitive nth root of unity. Then for every $A(X) \in \mathbb{Z}[X]$,*

$$\operatorname{Res}(\Phi_n(X), A(X)) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(A(\zeta_n)\right).$$

Proof. The polynomial $\Phi_n(X)$ is monic and irreducible over $\mathbb{Q}$, and ζ_n is one of its roots. Hence the formula follows immediately from Proposition 2.26. ■

We will also need the following basic reduction criterion.

Proposition 2.28. *Let $f, g \in \mathbb{Z}[X]$, and let p be a prime. If the reductions of f and g modulo p have a common root in an algebraic closure of $\mathbb{F}_p$, then $p \mid \operatorname{Res}(f, g)$.*

Equivalently, if $p \nmid \operatorname{Res}(f, g)$, then the reductions of f and g modulo p have no common root in an algebraic closure of $\mathbb{F}_p$.

Proof. Let $\overline{f}, \overline{g} \in \mathbb{F}_p[X]$ denote the reductions of f and g modulo p. Since the resultant is the determinant of the Sylvester matrix, and the entries of the Sylvester matrix are coefficients of the polynomials, reducing coefficients modulo p gives $\operatorname{Res}\big(\overline{f}, \overline{g}\big) \equiv \operatorname{Res}(f, g) \pmod p$. Indeed, the Sylvester matrix of $\overline{f}$ and $\overline{g}$ is obtained by reducing the entries of the Sylvester matrix of f and g modulo p, and determinants commute with reduction modulo p.

Now suppose that $\overline{f}$ and $\overline{g}$ have a common root in an algebraic closure of $\mathbb{F}_p$. By Corollary 2.25, this implies $\operatorname{Res}\big(\overline{f}, \overline{g}\big) = 0$ in $\mathbb{F}_p$. Therefore, $\operatorname{Res}(f, g) \equiv 0 \pmod p$, which is equivalent to p dividing $\operatorname{Res}(f, g)$. The final statement is the contrapositive. ■

For later use, let us also note the following reformulation of Proposition 2.28. If $f, g \in \mathbb{Z}[X]$ and $p \nmid \operatorname{Res}(f, g)$, then the reductions of f and g modulo p are coprime in $\mathbb{F}_p[X]$. In particular, they cannot have a common root in any extension field of $\mathbb{F}_p$.

2.8 Uncertainty principles

In this section, we recall an uncertainty principle for finite abelian groups. The first proposition is due to Meshulam [28] for finite abelian groups of arbitrary order. Meshulam's composite-order uncertainty principle generalizes the sharper prime-order uncertainty principle due to Tao [34]. We will also record a finite-field version of the composite-order uncertainty principle, valid outside finitely many characteristics and derive an immediate corollary for the finite-field version of the prime-order uncertainty principle.

Let $n \geq 2$, let $\zeta_n \in \mathbb{C}$ be a primitive nth root of unity, and let $\Omega_n := \{\zeta_n^j : j = 0, \dots, n-1\}$. Given a nonzero polynomial

$$f(X) = \sum_{i=0}^{n-1} f_i X^i \in \mathbb{C}[X] \qquad \text{with} \qquad \deg f < n,$$

we define

$$|f| := |\{\, i \in \{0, \dots, n-1\} : f_i \neq 0 \,\}|$$

and

$$|\operatorname{ev}(f)|_{\Omega_n} := |\{\, \xi \in \Omega_n : f(\xi) \neq 0 \,\}|.$$

Equivalently, if one identifies f with its coefficient vector in $\mathbb{C}^{\mathbb{Z}/n\mathbb{Z}}$, then $|f|$ is the support size of that vector and $|\operatorname{ev}(f)|_{\Omega_n}$ is the support size of its discrete Fourier transform.

Proposition 2.29 (Meshulam[28])**.** *Let $0 \neq f(X) \in \mathbb{C}[X]$ with $\deg f < n$. Let $d_1 < d_2$ be consecutive divisors of n such that $d_1 \leq |f| \leq d_2$. Then*

$$|\operatorname{ev}(f)|_{\Omega_n} \geq \frac{n}{d_1 d_2}\left(d_1 + d_2 - |f|\right).$$

Equivalently, the number of roots of f in Ω_n is at most

$$n - \frac{n}{d_1 d_2}\left(d_1 + d_2 - |f|\right).$$

Corollary 2.30. *Fix $n \geq 2$. Then there exists a nonzero integer $\mathcal{U}_n$ such that the following holds. If $\mathbb{F}_q$ is a finite field of characteristic p with $p \nmid \mathcal{U}_n$ and $n \mid (q-1)$, then every nonzero polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $< n$ satisfies*

$$|\mathrm{ev}(f)|_{\Omega_n} \geq \frac{n}{d_1 d_2} \left(d_1 + d_2 - |f|\right),$$

where $d_1 < d_2$ are the consecutive divisors of n such that $d_1 \leq |f| \leq d_2$. Equivalently, the number of roots of f in $\Omega_n \subseteq \mathbb{F}_q^*$ is at most

$$n - \frac{n}{d_1 d_2} \left(d_1 + d_2 - |f|\right).$$

Proof. For each $k \in \{1, \dots, n\}$, let $u_n(k)$ denote the Meshulam lower bound

$$u_n(k) := \frac{n}{d_1 d_2}(d_1 + d_2 - k),$$

where $d_1 < d_2$ are the consecutive divisors of n such that $d_1 \leq k \leq d_2$.

Fix k, and let $A, B \subseteq \{0, \dots, n-1\}$ be such that $|A| = k$ and $|B| < u_n(k)$. Consider the $(n - |B|) \times k$ matrix

$$V_{A,B}(X) := \left(X^{ab}\right)_{a \in B^c,\ b \in A},$$

where $B^c = \{0, \dots, n-1\} \setminus B$, and define $V_{A,B}(\zeta_n)$ by specializing $X = \zeta_n$.

We claim that $V_{A,B}(\zeta_n)$ has full column rank k. Indeed, if not, then there would exist a nonzero coefficient vector $c = (c_b)_{b \in A} \in \mathbb{C}^A$ such that $V_{A,B}(\zeta_n)c = 0$. Defining

$$f(X) := \sum_{b \in A} c_b X^b,$$

we would have $|f| = |A| = k$, and the equation $V_{A,B}(\zeta_n)c = 0$ implies $f(\zeta_n^a) = 0$ for all $a \in B^c$. Hence,

$$|\mathrm{ev}(f)|_{\Omega_n} \leq |B| < u_n(k),$$

contradicting Proposition 2.29. Thus $V_{A,B}(\zeta_n)$ has full column rank.

It follows that some $k \times k$ minor of $V_{A,B}(\zeta_n)$ is nonzero. Choose one such minor and denote the corresponding determinant polynomial by $\Delta_{A,B}(X) \in \mathbb{Z}[X]$. Then $\Delta_{A,B}(\zeta_n) \neq 0$. Since ζ_n is a root of $\Phi_n(X)$, it follows that $\Delta_{A,B}(X)$ and $\Phi_n(X)$ have no common root over $\mathbb{C}$, and therefore

$$\mathrm{Res}(\Delta_{A,B}(X), \Phi_n(X)) \neq 0.$$

Now define

$$\mathcal{U}_n := \prod_{\substack{1 \leq k \leq n \\ A,B \subseteq \{0,\dots,n-1\} \\ |A| = k,\ |B| < u_n(k)}} \mathrm{Res}(\Delta_{A,B}(X), \Phi_n(X)).$$

Since there are only finitely many pairs (A, B), this is a finite product of nonzero integers, hence $\mathcal{U}_n \neq 0$.

Now let $\mathbb{F}_q$ be a finite field of characteristic p such that $p \nmid \mathcal{U}_n$ and $n \mid (q-1)$, and let $\omega \in \mathbb{F}_q^*$ be a primitive nth root of unity. Suppose, for contradiction, that there exists a nonzero polynomial

$$f(X) = \sum_{i=0}^{n-1} f_i X^i \in \mathbb{F}_q[X] \qquad \text{with} \qquad \deg f < n$$

such that $|\mathrm{ev}(f)|_{\Omega_n} < u_n(|f|)$. Let $A := \{\, i : f_i \neq 0 \,\}$, and $B := \{\, a \in \{0,\dots,n-1\} : f(\omega^a) \neq 0 \,\}$. Then $|A| = |f|$, and by assumption

$$|B| = |\mathrm{ev}(f)|_{\Omega_n} < u_n(|f|) = u_n(|A|).$$

For every $a \in B^c$, we have

$$\sum_{b \in A} f_b \omega^{ab} = 0.$$

Thus the coefficient vector $(f_b)_{b\in A} \neq 0$ lies in the kernel of $V_{A,B}(\omega)$, so $V_{A,B}(\omega)$ does not have full column rank. Therefore every $|A| \times |A|$ minor of $V_{A,B}(\omega)$ vanishes, including the chosen one: $\Delta_{A,B}(\omega) = 0$.

Since ω is a primitive nth root of unity and $p \nmid n$, the reduction of $\Phi_n(X)$ modulo p also vanishes at ω. Hence the reductions of $\Delta_{A,B}(X)$ and $\Phi_n(X)$ have a common root in an algebraic closure of $\mathbb{F}_p$. By Proposition 2.28,

$$p \mid \mathrm{Res}(\Delta_{A,B}(X), \Phi_n(X)).$$

But this resultant is one of the factors of $\mathcal{U}_n$, so this implies $p \mid \mathcal{U}_n$, contrary to hypothesis. This contradiction proves the corollary. ∎

Corollary 2.31. *Fix a prime n. Then there exists a nonzero integer $\mathcal{U}_n'$ such that the following holds. If $\mathbb{F}_q$ is a finite field of characteristic p with $p \nmid \mathcal{U}_n'$ and $n \mid (q-1)$, then every nonzero polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $< n$ satisfies*

$$|f| + |\mathrm{ev}(f)|_{\Omega_n} \geq n + 1.$$

Equivalently,

$$|\mathrm{ev}(f)|_{\Omega_n} \geq n + 1 - |f|,$$

and the number of roots of f in Ω_n is at most $|f| - 1$.

Proof. When n is prime, the only divisors of n are 1 and n. Thus, Corollary 2.30 yields

$$|\mathrm{ev}(f)|_{\Omega_n} \geq \frac{n}{1 \cdot n}(1 + n - |f|) = n + 1 - |f|,$$

which is equivalent to the stated inequality. One may take $\mathcal{U}_n' = \mathcal{U}_n$. ∎

Remark 2.32. The prime-order finite-field uncertainty principle in Corollary 2.31 is the finite field version of the uncertainty principle proven by Tao [34]. It is also the same statement used by Golowich and Guruswami in their paper [14, Proposition 66] on quantum locally recoverable codes, where it is attributed to Goldstein–Guralnick–Isaacs [13].

This completes the preliminaries. In the next chapter we formally define quantum locally recoverable codes, extend the (r, δ) locality notion to the quantum setting, and give randomized constructions achieving good rate–distance–locality trade-offs.

Chapter 3

Quantum LRCs and HLRCs

We now define the quantum analogues of LRCs and HLRCs and present randomized constructions.

3.1 Definitions of QLRCs and QHLRCs

Before defining quantum locally recoverable codes, we recall what it means for a quantum code to correct a set of erasures. Let $\mathcal{E} = \{X^a Z^b : a, b \in \mathbb{F}_q\}$ be the single-qudit Pauli error basis introduced in Section 2.4. For a density matrix ρ on a single qudit, define the completely depolarizing channel

$$\tau(\rho) := \frac{1}{q^2} \sum_{E \in \mathcal{E}} E \rho E^\dagger$$

where $E^\dagger$ is the Hermitian dual of E. Thus τ applies each single-qudit Pauli error with equal probability. For a set of coordinates $I \subseteq \{1, \ldots, n\}$, let τ^I denote the channel on $(\mathbb{C}^q)^{\otimes n}$ which applies τ to the qudits in I and acts as the identity on the remaining qudits. Equivalently,

$$\tau^I(\rho) = \frac{1}{q^{2|I|}} \sum_{\substack{E \in \mathcal{E}^{\otimes n} \\ \mathrm{supp}(E) \subseteq I}} E \rho E^\dagger.$$

Let $\mathcal{Q} \subseteq (\mathbb{C}^q)^{\otimes n}$ be a quantum code. We say that $\mathcal{Q}$ corrects erasures at I if there exists a trace-preserving quantum operation $\mathcal{R}_{\mathcal{Q},I}$ such that

$$\mathcal{R}_{\mathcal{Q},I} \circ \tau^I(|\phi\rangle \langle\phi|) = |\phi\rangle \langle\phi|$$

for all $|\phi\rangle \in \mathcal{Q}$.

Equivalently, $\mathcal{Q}$ corrects erasures at I if it can correct every Pauli error whose support is contained in I, under the assumption that the decoder knows the erased set I. This is the usual erasure model: the locations of the errors are known, but the errors themselves are unknown.

We now impose a locality constraint on the recovery operation. The idea is that erasures on a set I should be recoverable by using only a small set of qudits J containing I.

Definition 3.1 ((I, J)-QLRC [10])**.** Let $\emptyset \neq I \subsetneq J \subseteq \{1, \ldots, n\}$. A quantum code $\mathcal{Q} \subseteq (\mathbb{C}^q)^{\otimes n}$ is said to be an (I, J)-QLRC if there exists a trace-preserving quantum operation $\mathcal{R}^J_{\mathcal{Q},I}$, acting nontrivially only on the qudits indexed by J, such that

$$\mathcal{R}^J_{\mathcal{Q},I} \circ \tau^I(|\phi\rangle \langle\phi|) = |\phi\rangle \langle\phi|$$

for all $|\phi\rangle \in \mathcal{Q}$.

Thus, if $\mathcal{Q}$ is an (I, J)-QLRC, then erasures on the coordinates in I can be recovered locally using only the qudits in J.

Definition 3.2 ((r, δ)-QLRC [10])**.** Let $r, \delta \geq 2$ be positive integers. A quantum error-correcting code $\mathcal{Q} \subseteq (\mathbb{C}^q)^{\otimes n}$ is an (r, δ)-QLRC if, for each coordinate $i \in \{1, \ldots, n\}$, there exists a set $J \subseteq \{1, \ldots, n\}$ containing i with

$$|J| \leq r + \delta - 1$$

such that, for every $I \subseteq J$ with $|I| \leq \delta - 1$, the code $\mathcal{Q}$ is an (I, J)-QLRC.

In other words, every coordinate belongs to a local recovery set J of size at most $r+\delta-1$, and any erasure pattern of size at most $\delta - 1$ inside J can be corrected using only the qudits in J. This is the quantum analogue of classical (r, δ)-locality.

The following result relates this notion of quantum locality to classical locality for dual-containing codes.

Theorem 3.3 ([10, Theorem 28])**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear code. Assume that $C^\perp \subseteq C$ and $\delta \leq d(C^\perp)$, where $d(C^\perp)$ is the minimum distance of $C^\perp$. Then $\mathcal{Q} = \mathrm{CSS}(C, C)$ is an (r, δ)-QLRC if and only if C is an (r, δ) classical LRC.*

We now extend the established (r, δ)-QLRCs to a quantum hierarchical setting, analogous to classical HLRCs. For simplicity, we first define 2-level QHLRCs.

Definition 3.4 ($((r_1, \delta_1), (r_2, \delta_2))$-QHLRC)**.** Let $r_1, \delta_1, r_2, \delta_2 \in \mathbb{Z}^+$ such that $r_1 \geq r_2$ and $\delta_1 \geq \delta_2 \geq 2$. Let $\mathcal{Q} \subseteq (\mathbb{C}^q)^{\otimes n}$ be a stabilizer quantum code. Fix two level locality parameters $(r_1, \delta_1), (r_2, \delta_2)$. We say $\mathcal{Q}$ is a $((r_1, \delta_1), (r_2, \delta_2))$-QHLRC if:

1. For every $i \in \{1, \ldots, n\}$ there exists a recovery set $J_1(i) \subseteq \{1, \ldots, n\}$ containing i with $|J_1(i)| \leq r_1 + \delta_1 - 1$ such that for all $I_1 \subseteq J_1(i)$ with $|I_1| \leq \delta_1 - 1$, $\mathcal{Q}$ is an $(I_1, J_1(i))$-QLRC. In other words, $\mathcal{Q}$ is an (r_1, δ_1)-QLRC.

2. The punctured code $\mathcal{Q}|_{J_1(i)}$ is itself an (r_2, δ_2)-QLRC.

Using Definition 3.4, we make the following observation: let $\mathcal{Q}$ be a $((r_1, \delta_1), (r_2, \delta_2))$-QHLRC. Fix a coordinate i and an erasure pattern I containing i. Let $J_1(i)$ be the corresponding recovery set. Let $J_2(i)$ be a recovery set that arises from $\mathcal{Q}|_{J_1(i)}$. If $I \subseteq J_2(i)$ and $|I| \le \delta_2 - 1$ then we can recover qudits corresponding to I using the qudits corresponding to $J_2(i) \setminus I$. Otherwise, assuming $|I| \le \delta_1 - 1$ and $I \subseteq J_1(i)$, we can recover qudits corresponding to I using the qudits corresponding to $J_1(i) \setminus I$.

Additionally, it is not too difficult to generalize the previous definition to any number of hierarchical levels.

Definition 3.5 (h-level QHLRC)**.** Let $2 \le h \in \mathbb{Z}^+$, and $r_l, \delta_l \in \mathbb{Z}^+$ for all $l \in \{1, \ldots, h\}$. Consider h level locality parameters $(r_1, \delta_1), \ldots, (r_h, \delta_h)$ with

$$r_1 \ge \cdots \ge r_h \quad \text{and} \quad \delta_1 \ge \cdots \ge \delta_h \ge 2.$$

A stabilizer quantum code $\mathcal{Q} \subseteq (\mathbb{C}^q)^{\otimes n}$ is said to be an h-level $((r_1, \delta_1), \ldots, (r_h, \delta_h))$-QHLRC if the following conditions are satisfied:

1. For every $i \in \{1, \ldots, n\}$ there exists a recovery set $J_1(i) \subseteq \{1, \ldots, n\}$ containing i with $|J_1(i)| \le r_1 + \delta_1 - 1$ such that for all $I_1 \subseteq J_1(i)$ with $|I_1| \le \delta_1 - 1$, $\mathcal{Q}$ is an $(I_1, J_1(i))$-QLRC. In other words, $\mathcal{Q}$ is an (r_1, δ_1)-QLRC.

2. The punctured code $\mathcal{Q}|_{J_1(i)}$ is an $(h-1)$-level $((r_2, \delta_2), \ldots, (r_h, \delta_h))$-QHLRC.

Note that the second condition implies that, after suitably puncturing $h - 1$ times, the resulting code is a 1-level (r_h, δ_h)-QHLRC which is simply an (r_h, δ_h)-QLRC.

We end this section by stating a Singleton-type bound for (r, δ) QLRCs.

Theorem 3.6. *Let $\mathcal{Q}$ be a QLRC of block length n, dimension k, distance d with locality parameters r, δ. Assume that for each coordinate $i \in \{1, \ldots, n\}$, there exists a recovery set $J(i)$ containing i such that $|J(i)| = r + \delta - 1$. Further assume that for all $i, j \in \{1, \ldots, n\}$ either $J(i) = J(j)$ or $J(i) \cap J(j) = \emptyset$. Then*

$$k \le \left(1 - \frac{2}{r + \delta - 1}\right) n - 2\left(d - 1 - \left\lceil \frac{d-1}{r + \delta - 2} \right\rceil\right).$$

Proof. Follows from [14, Theorem 36] by replacing r with $r + \delta - 1$. ■

3.2 Random (r, δ)-QLRCs

In this section, we construct random (r, δ)-QLRCs. We begin with a lemma that we will use repeatedly in the random constructions.

Lemma 3.7. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be distinct. For an integer $t \leq n$, consider the $t \times n$ Vandermonde matrix*

$$V_t(\alpha_1, \ldots, \alpha_n) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_n^{t-1} \end{bmatrix}.$$

Then any t columns of $V_t(\alpha_1, \ldots, \alpha_n)$ are linearly independent.

Proof. Choose any t columns, say those indexed by $j_1, \ldots, j_t$. The corresponding determinant is

$$\det\left(\alpha_{j_b}^{a-1}\right)_{1 \leq a,b \leq t} = \prod_{1 \leq u < v \leq t} (\alpha_{j_v} - \alpha_{j_u}),$$

which is nonzero because the α_i's are distinct. ■

Construction 3.8 (Random (r, δ)-QLRC)**.** We are given a block length N, locality parameter r, distance parameter $\delta \leq r$, and finite field $\mathbb{F}_q$ with $q \geq n := r + \delta - 1$. Assume that $m := N/n$ is an integer. Choose $\ell \in [N/2 - m(\delta - 1)]$. We define a random QLRC via a CSS code $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$ which is sampled as follows. Initialize G_i to be the $(\delta - 1) \times n$ Vandermonde matrix

$$G_i = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{i,1} & \alpha_{i,2} & \cdots & \alpha_{i,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i,1}^{\delta-2} & \alpha_{i,2}^{\delta-2} & \cdots & \alpha_{i,n}^{\delta-2} \end{bmatrix}$$

where for each $i = 1, \ldots, m$, every $\alpha_{i,j} \in \mathbb{F}_q$ is distinct for $j = 1, \ldots, n$. Let H_X be a block diagonal matrix comprised of m matrices:

$$H_X = \begin{bmatrix} G_1 & & & \\ & G_2 & & \\ & & \ddots & \\ & & & G_m \end{bmatrix}.$$

Let $\beta_{i,l} = \prod_{j \neq l} \frac{1}{\alpha_{i,l} - \alpha_{i,j}}$ for $l = 1, \ldots, n$ Let H_i be an $r \times n$ Vandermonde-like matrix

$$H_i = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{i,1} & \alpha_{i,2} & \cdots & \alpha_{i,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i,1}^{r-1} & \alpha_{i,2}^{r-1} & \cdots & \alpha_{i,n}^{r-1} \end{bmatrix} \cdot \begin{bmatrix} \beta_{i,1} & & & \\ & \beta_{i,2} & & \\ & & \ddots & \\ & & & \beta_{i,n} \end{bmatrix}$$

and let H_Z be the block matrix

$$H_Z = \begin{bmatrix} (H_1)_{\delta-1} & & & \\ & (H_2)_{\delta-1} & & \\ & & \ddots & \\ & & & (H_m)_{\delta-1} \end{bmatrix}$$

where $(H_i)_{\delta-1}$ means the first $\delta - 1$ rows of H_i. We then add ℓ random rows to H_X and H_Z subject to the orthogonality conditions, as follows:

1. for $i = 1, \ldots, \ell$:
   - let v be a uniformly random vector sampled from row-span$(H_Z)^\perp \setminus$ row-span(H_X)
   - append v to H_X and rename the resulting matrix as H_X i.e. $H_X = \begin{bmatrix} H_X \\ v \end{bmatrix}$
2. for $i = 1, \ldots, \ell$:
   - let v be a uniformly random vector sampled from row-span$(H_X)^\perp \setminus$ row-span(H_Z)
   - append v to H_Z and rename the resulting matrix as H_Z i.e. $H_Z = \begin{bmatrix} H_Z \\ v \end{bmatrix}$

We have sampled matrices $H_X, H_Z \in \mathbb{F}_q^{(m(\delta-1)+\ell)\times N}$ with orthogonal row spaces. Let $C_X = \ker H_X$, $C_Z = \ker H_Z$ are such that we obtain a well-defined CSS code $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$.

Lemma 3.9. *For positive integers $r \geq \delta$, let $n = r + \delta - 1$, and let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be distinct. For $l = 1, \ldots, n$ define*

$$\beta_l := \prod_{\substack{j=1 \\ j \neq l}}^{n} \frac{1}{\alpha_l - \alpha_j}.$$

Let

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\delta-2} & \alpha_2^{\delta-2} & \cdots & \alpha_n^{\delta-2} \end{bmatrix}$$

and

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \begin{bmatrix} \beta_1 & & & \\ & \beta_2 & & \\ & & \ddots & \\ & & & \beta_n \end{bmatrix}.$$

Then

$$GH^T = 0.$$

Moreover, any $\delta - 1$ columns of G are linearly independent, and any $\delta - 1$ columns of the first $\delta - 1$ rows of H are linearly independent.

Proof. The column-independence statement for G follows from Lemma 3.7. The same statement for the first $\delta - 1$ rows of H follows from Lemma 3.7 after scaling each column by the nonzero scalar β_l.

It remains to prove $GH^T = 0$. The (a,b)-entry of GH^T, where $0 \le a \le \delta - 2$ and $0 \le b \le r-1$, is

$$\sum_{l=1}^{N} \beta_l \alpha_l^{a+b}.$$

Since

$$0 \le a+b \le (\delta-2)+(r-1) = r+\delta-3 = n-2,$$

it is enough to prove that

$$\sum_{l=1}^{n} \beta_l \alpha_l^m = 0 \qquad \text{for } 0 \le m \le n-2.$$

This is the standard Lagrange interpolation identity. Indeed, let

$$L_l(X) = \prod_{\substack{j=1 \\ j \ne l}}^{n} \frac{X-\alpha_j}{\alpha_l - \alpha_j}$$

be the l-th Lagrange basis polynomial. The leading coefficient of $L_l(X)$ is β_l. For $0 \le m \le n-2$, the polynomial X^m has degree $< n-1$, so its Lagrange interpolation expansion $X^m = \sum_{l=1}^n \alpha_l^m L_l(X)$ has zero coefficient of X^{n-1} on the left-hand side. The coefficient of X^{n-1} on the right-hand side is $\sum_{l=1}^n \alpha_l^m \beta_l$. Therefore, $\sum_{l=1}^n \beta_l \alpha_l^m = 0$ for $0 \le m \le n-2$, proving $GH^T = 0$. ■

We now prove that Construction 3.8 has the desired properties of locality and good distance.

Lemma 3.10. *The random QLRC $\mathcal{Q}$ from Construction 3.8 is a QLRC of locality r and dimension $k = N - 2(m(\delta-1)+\ell)$. Furthermore, each coordinate $s \in \{1, \dots, N\}$ has recovery set $J_s = \{a(r+\delta-1)+1, \dots, a(r+\delta-1)+r+\delta-1\}$ for $a = \lceil s/(r+\delta-1) \rceil - 1$.*

Proof. First consider the deterministic local rows before the ℓ random rows are added. The matrix H_X contains, on each local group $J_a := \{a(r+\delta-1)+1, \dots, a(r+\delta-1)+r+\delta-1\}$, a copy of the $(\delta-1)\times(r+\delta-1)$ Vandermonde matrix G_a. Similarly, H_Z contains, on the same group, the first $\delta-1$ rows of the scaled Vandermonde matrix H_a.

By Lemma 3.7, any $\delta-1$ columns of G_a are linearly independent. Since the first $\delta-1$ rows of H_a are obtained from a Vandermonde matrix by nonzero column scalings, any $\delta-1$ of their columns are also linearly independent. Therefore, on every local group J_a, both the X- and Z-local parity checks can recover any erasure pattern of size at most $\delta-1$. Equivalently, the punctured local X- and Z-classical codes have local distance at least δ.

The local X- and Z-row spaces are orthogonal by Lemma 3.9. Since distinct local groups have disjoint supports, the deterministic local parts of H_X and H_Z are globally orthogonal. The additional random rows are sampled from the orthogonal complement of the current opposite row span, so after every appended row the row spans of H_X and H_Z remain orthogonal. Hence $C_X^\perp = \mathrm{rowspan}(H_X) \subseteq C_Z$ and the CSS code $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$ is well-defined.

The local recovery sets are precisely the groups J_a. Thus $\mathcal{Q}$ is an (r,δ)-QLRC. Finally, each of H_X and H_Z has $m(\delta-1)+\ell$ rows. The Vandermonde local rows are linearly independent across disjoint supports, and the random rows are sampled outside the current row span, so the rank of each matrix is $m(\delta-1)+\ell$. Therefore $\dim C_X = \dim C_Z = N-(m(\delta-1)+\ell)$, and the CSS dimension is

$$k = \dim C_X + \dim C_Z - N = N - 2(m(\delta-1)+\ell).$$

The condition $\ell \in [N/2 - m(\delta-1)]$ ensures this dimension is positive. ∎

Now we bound the distance of the random (r,δ)-QLRCs that we constructed.

Proposition 3.11. *For sufficiently large N, given any $\rho,\epsilon > 0$, the distance $d(\mathcal{Q})$ of a random (r,δ)-QLRC $\mathcal{Q}$ from Construction 3.8 with parameters, N, r, δ, and $N/2 - m(\delta-1) > \ell \geq (H_q^{(\delta)}(\rho)+2\epsilon)N$ (if one exists) over the alphabet $\mathbb{F}_q$ satisfies*

$$\Pr[d(\mathcal{Q}) \geq \rho N] > 1 - 2q^{-\epsilon N}, \tag{3.1}$$

where for $w = |y| \in \mathbb{F}_q^N \setminus \{0\}$,

$$H_q^{(\delta)}(\rho) = \limsup_{N\to\infty} \frac{1}{N}\log_q\left(\sum_{w\leq \rho N} \mathcal{N}^{(\delta)}(N,w)(q-1)^w\right) \tag{3.2}$$

and

$$\mathcal{N}^{(\delta)}(N,w) = \sum_{s=1}^{\lfloor w/\delta \rfloor}\binom{m}{s}\sum_{\substack{w_1+\cdots+w_s=w\\ w_i\geq\delta}}\prod_{i=1}^{s}\binom{r+\delta-1}{w_i} \tag{3.3}$$

and the $\limsup$ *is taken over N divisible by $r+\delta-1$.*

Proof. Fix a nonzero vector $y \in \mathbb{F}_q^N$. Let $H_Z^{(i)}$ denote the matrix after the ith iteration of step 2 in Construction 3.8. If $y \in C_Z \setminus C_X^\perp$ then for $0 \leq i \leq \ell-1$, $y \in \ker H_Z^{(i)}$ and $y \in \ker H_Z^{(i+1)}$. Since $y \notin C_X^\perp$, exactly $1/q$-fraction of the vectors in C_X are orthogonal to y. It follows if $y \in \ker H_Z^{(i)}$ then less than $1/q$-fraction of the vectors in $C_X \setminus \text{row-span}(H_Z^{(i)})$ are orthogonal to y. Formally,

$$\Pr\Big[y \in \ker H_Z^{(i+1)} \setminus C_X^\perp \mid y \in \ker H_Z^{(i)} \setminus C_X^\perp\Big] < \frac{1}{q}.$$

Hence,

$$\begin{aligned}\Pr\big[y \in C_Z \setminus C_X^\perp\big] &= \Pr\big[y \notin C_X^\perp\big] \cdot \Pr\Big[y \in \ker H_Z^{(0)} \mid y \notin C_X^\perp\Big] \\ &\quad \cdot \prod_{i=0}^{\ell-1}\Pr\Big[y \in \ker H_Z^{(i+1)} \setminus C_X^\perp \mid y \in \ker H_Z^{(i)} \setminus C_X^\perp\Big] \\ &< q^{-\ell}.\end{aligned}$$

We now explain why the union bound only needs to count supports appearing in $\mathcal{N}^{(\delta)}(N, w)$. Let $y \in C_Z \setminus C_X^{\perp}$ be a nonzero vector. Since $y \in C_Z = \ker H_Z$, it satisfies all local Z-checks. Consider any local group J_a. If $0 < |\operatorname{supp}(y) \cap J_a| < \delta$, then the restriction of the local Z-check matrix to these nonzero coordinates has full column rank by Lemma 3.7. Hence the only vector supported on those coordinates and satisfying the local checks is the zero vector, a contradiction. Therefore every nonempty local block of $\operatorname{supp}(y)$ has size at least δ. Thus the possible supports of y of weight w are counted by $\mathcal{N}^{(\delta)}(N, w)$. The same argument applies to vectors in $C_X \setminus C_Z^{\perp}$.

Applying the union bound over all $y \in \mathbb{F}_q^N$ such that $|y| \leq \rho N$ gives

$$\begin{aligned}
\Pr\big[\exists\, y \in C_Z \setminus C_X^{\perp}, |y| \leq \rho N\big] &< q^{-\ell} \sum_{w \leq \rho N} \mathcal{N}^{(\delta)}(N, w)(q-1)^w \\
&\leq q^{-\ell} q^{(H_q^{(\delta)}(\rho)+\epsilon)N} \\
&\leq q^{-\epsilon N}
\end{aligned}$$

for sufficiently large N and by symmetry

$$\Pr\big[\exists\, y \in C_X \setminus C_Z^{\perp}, |y| \leq \rho N\big] < q^{-\epsilon N}.$$

Therefore,

$$\Pr[d(\mathcal{Q}) \leq \rho N] < 2q^{-\epsilon N},$$

as desired. ■

Remark 3.12. The proof of Proposition 40 from [14] works for Proposition 3.11, but gives a weaker estimate because it over counts the number of low-weight codewords. It would require ℓ more random rows to drive the union bound to zero so existence/distance threshold and rate-vs-distance tradeoff will be worse.

3.3 Random $((r_1, \delta_1), \ldots, (r_h, \delta_h))$-QHLRCs

Now we move on to constructing random h-level quantum hierarchical LRCs. The main difference from the one-level construction is that the deterministic local X and Z checks must be chosen recursively so that nested local checks remain mutually orthogonal.

3.3.1 Constructing a random QHLRC

Definition 3.13. Let J be a finite set of coordinates, let $U \subseteq \mathbb{F}_q^J$ be a row space, and let a, s be positive integers. For $E \subseteq J$, define

$$\mathbb{F}_q^J[E] = \{x \in \mathbb{F}_q^J \mid \operatorname{supp}(x) \subseteq E\}.$$

We say that U has the (a, s)-strong local MDS property on J if:

1. for every $E \subseteq J$ with $|E| \leq a$, $\operatorname{rank}(U|_E) = |E|$;
2. for every $E \subseteq J$ with $|E| \leq s$, $U \cap \mathbb{F}_q^J[E] = \{0\}$.

Equivalently, the second condition says that the restriction map

$$\pi_{J\setminus E} : U \to \mathbb{F}_q^{J\setminus E}$$

is injective for every $E \subseteq J$ with $|E| \leq s$. It is also equivalent to $\operatorname{rank}(U^{\perp}|_E) = |E|$ for $|E| \leq s$.

Construction 3.14 (h-level QHLRC)**.** Suppose we are given a block length N, locality and distance parameters $(r_1, \delta_1), (r_2, \delta_2), \ldots, (r_h, \delta_h)$ such that $r_1 \geq \cdots \geq r_h$ and $\delta_1 \geq \cdots \geq \delta_h \geq 2$, and a finite field $\mathbb{F}_q$, with q sufficiently large. Let $n_l := r_l + \delta_l - 1$ and suppose $\delta_1 \leq n_h/2$. Further assume that $m_l := N/n_l$ is an integer for $l = 1, \ldots, h$ and $n_h \mid n_{h-1} \mid \cdots \mid n_1 \mid N$.

We will set some notation for the construction. For a level-l block where $b = 0, \ldots, m_l - 1$, write $J_{l,b} := \{bn_l + 1, bn_l + 2, \ldots, (b+1)n_l\}$. Thus level-$(l+1)$ blocks refine level-l blocks. We first construct deterministic local row spaces $U^{\mathrm{loc}}, V^{\mathrm{loc}} \subseteq \mathbb{F}_q^N$ which will become the local parts of H_X and H_Z.

Bottom level. For each level-h block $J_{h,b}$, choose n_h distinct field elements $\alpha_{b,1}, \ldots, \alpha_{b,n_h} \in \mathbb{F}_q$. Let $U_{h,b} \subseteq \mathbb{F}_q^{J_{h,b}}$ be the row space of the $(\delta_h - 1) \times n_h$ Vandermonde matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{b,1} & \alpha_{b,2} & \cdots & \alpha_{b,n_h} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{b,1}^{\delta_h-2} & \alpha_{b,2}^{\delta_h-2} & \cdots & \alpha_{b,n_h}^{\delta_h-2} \end{bmatrix}.$$

Let

$$\eta_{b,t} := \prod_{\substack{u=1 \\ u\neq t}}^{n_h} \frac{1}{\alpha_{b,t} - \alpha_{b,u}}.$$

Let $V_{h,b} \subseteq \mathbb{F}_q^{J_{h,b}}$ be the row space of the scaled Vandermonde matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{b,1} & \alpha_{b,2} & \cdots & \alpha_{b,n_h} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{b,1}^{\delta_h-2} & \alpha_{b,2}^{\delta_h-2} & \cdots & \alpha_{b,n_h}^{\delta_h-2} \end{bmatrix} \begin{bmatrix} \eta_{b,1} & & & \\ & \eta_{b,2} & & \\ & & \ddots & \\ & & & \eta_{b,n_h} \end{bmatrix}.$$

By Lemma 3.9, the Vandermonde space generated by degrees $0, \ldots, \delta_h - 2$ is orthogonal to the full scaled dual Vandermonde space generated by degrees $0, \ldots, r_h - 1$. Since $V_{h,b}$ is contained in this scaled dual space, we have $U_{h,b} \perp V_{h,b}$.

Moreover, both $U_{h,b}$ and $V_{h,b}$ have the $(\delta_h - 1, \delta_1 - 1)$-strong local MDS property on $J_{h,b}$. Indeed, the Vandermonde property gives

$$\operatorname{rank}(U_{h,b}|_E) = \operatorname{rank}(V_{h,b}|_E) = |E| \qquad (|E| \le \delta_h - 1).$$

Also, each of $U_{h,b}$ and $V_{h,b}$ is a scaled generalized Reed–Solomon row space of dimension $\delta_h - 1$ and length n_h, hence has minimum distance

$$n_h - (\delta_h - 1) + 1 = r_h + 1 > \delta_1 - 1 \iff n_h > \delta_1 + \delta_h - 3.$$

Since $\delta_h \le \delta_1 \le n_h/2$, we have $n_h \ge 2\delta_1 > \delta_1 + \delta_h - 3$. Therefore neither row space has a nonzero word supported on at most $\delta_1 - 1$ coordinates.

Higher levels. Suppose that for all levels $u > l$ we have already constructed local X- and Z-row spaces supported on level-u blocks, and that within each level-$(l+1)$ block the accumulated X- and Z-spaces are orthogonal.

Fix a level-l block $J_{l,b}$. Let $U_{>l,b}$ be the sum of all previously constructed X-row spaces supported inside $J_{l,b}$, and let $V_{>l,b}$ be the analogous sum of previously constructed Z-row spaces. By induction, $U_{>l,b} \perp V_{>l,b}$.

Set $\Delta_l := \delta_l - \delta_{l+1}$. Choose a Δ_l-dimensional subspace $U_{l,b}^+ \subseteq V_{>l,b}^\perp$ such that

$$\dim(U_{>l,b} + U_{l,b}^+) = \dim U_{>l,b} + \Delta_l,$$

and such that $U_{>l,b} + U_{l,b}^+$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property on $J_{l,b}$. Then choose a Δ_l-dimensional subspace $V_{l,b}^+ \subseteq (U_{>l,b} + U_{l,b}^+)^\perp$ such that

$$\dim(V_{>l,b} + V_{l,b}^+) = \dim V_{>l,b} + \Delta_l,$$

and such that $V_{>l,b} + V_{l,b}^+$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property on $J_{l,b}$.

The existence of such $U_{l,b}^+, V_{l,b}^+$ follows from Theorem 3.20 which is proved at the end of the section.

We perform an exhaustive search over the relevant finite Grassmannian (Definition 2.21) which gives a deterministic finite procedure. Enumerate all $U_{l,b}^+ \in \mathrm{Gr}_{\mathbb{F}_q}(\Delta_l, V_{>l,b}^\perp)$ and choose one such that $U_{l,b}^+ \cap U_{>l,b} = \{0\}$ and $U_{l,b}^+ + U_{>l,b}$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property. Then enumerate all $V_{l,b}^+ \in \mathrm{Gr}_{\mathbb{F}_q}(\Delta_l, (U_{>l,b} + U_{l,b}^+)^\perp)$ and choose one such that $V_{l,b}^+ \cap V_{>l,b} = \{0\}$ and $V_{l,b}^+ + V_{>l,b}$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property.

After performing this for every level-l block and every $l = h-1, \dots, 1$, let U^{loc} be the span of all constructed X-local spaces and let V^{loc} be the span of all constructed Z-local spaces. These spaces are all constructed deterministically.

By construction, $U^{\mathrm{loc}} \perp V^{\mathrm{loc}}$. Let

$$M := m_h(\delta_h - 1) + \sum_{l=1}^{h-1} m_l(\delta_l - \delta_{l+1}),$$

then $\dim U^{\mathrm{loc}} = \dim V^{\mathrm{loc}} = M$. Choose bases of U^{loc} and V^{loc}, and use them as the initial rows of H_X and H_Z, respectively.

Finally, choose an integer $\ell < N/2 - M$. We then add ℓ random rows to H_X and H_Z subject to the orthogonality conditions, as follows:

1. for $i = 1, \ldots, \ell$:
   - let v be a uniformly random vector sampled from $\text{row-span}(H_Z)^{\perp} \setminus \text{row-span}(H_X)$
   - append v to H_X and rename the resulting matrix as H_X i.e. $H_X = \begin{bmatrix} H_X \\ v \end{bmatrix}$
2. for $i = 1, \ldots, \ell$:
   - let v be a uniformly random vector sampled from $\text{row-span}(H_X)^{\perp} \setminus \text{row-span}(H_Z)$
   - append v to H_Z and rename the resulting matrix as H_Z i.e. $H_Z = \begin{bmatrix} H_Z \\ v \end{bmatrix}$

We have sampled matrices $H_X, H_Z \in \mathbb{F}_q^{(M+\ell)\times N}$ with orthogonal row spaces. Let $C_X = \ker H_X$, $C_Z = \ker H_Z$ and obtain a well-defined CSS code $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$.

3.3.2 Dimension, locality, and distance

We will begin with computing the dimension and proving the locality properties of the quantum HLRC $\mathcal{Q}$.

Lemma 3.15. *The random QHLRC $\mathcal{Q}$ from Construction 3.14 is a quantum HLRC of hierarchical locality $(r_1, \delta_1), \ldots, (r_h, \delta_h)$ and dimension $k = N - 2(M + \ell)$ where*

$$M = m_h(\delta_h - 1) + \sum_{l=1}^{h-1} m_l(\delta_l - \delta_{l+1}). \tag{3.4}$$

Proof. Since $r_1, \ldots, r_h$ and $\delta_1, \ldots, \delta_h$ are decreasing sequences, $m_1, \ldots, m_h$ is a increasing sequence. Therefore,

$$m_h(\delta_h - 1) + \sum_{l=1}^{h-1} m_l(\delta_l - \delta_{l+1}) \leq m_h(\delta_1 - 1) \tag{3.5}$$

and

$$m_h(\delta_1 - 1) < N/2 \iff \delta_1 - 1 < n_h/2. \tag{3.6}$$

The latter inequality is enforced in Construction 3.14. By construction, the deterministic local X-row space has dimension

$$M = m_h(\delta_h - 1) + \sum_{l=1}^{h-1} m_l(\delta_l - \delta_{l+1}),$$

and the same is true for the deterministic local Z-row space. Each random global row is chosen outside the current row span, so it increases rank by one. Hence, $\operatorname{rank} H_X = \operatorname{rank} H_Z = M + \ell$. Therefore, $\dim C_X = \dim C_Z = N - (M + \ell)$, and the CSS dimension is

$$k = \dim C_X + \dim C_Z - N = N - 2(M + \ell).$$

It remains to prove hierarchical locality. Fix a level l block $J_{l,b}$. By construction, the X-local row space supported in $J_{l,b}$ has the $\delta_l - 1$ local MDS property:

$$\operatorname{rank}(U|_E) = |E| \qquad \text{for every } E \subseteq J_{l,b},\ |E| \le \delta_l - 1.$$

Thus any $\delta_l - 1$ erasures in $J_{l,b}$ can be recovered using X-type local checks supported inside $J_{l,b}$. The same statement holds for the Z-local row space.

Since $n_h \mid n_{h-1} \mid \cdots \mid n_1$, each level-$(l+1)$ block is contained in a level-l block. Therefore the punctured code on a level-l block inherits the lower-level repair structure from the blocks contained inside it. Hence the code is an h-level QHLRC with locality parameters $((r_1, \delta_1), \ldots, (r_h, \delta_h))$. ■

We now count the possible supports of logical operators compatible with the hierarchical local checks. Define

$$B_h(z) = \sum_{t=\delta_h}^{n_h} \binom{n_h}{t} z^t.$$

For $l = h-1, \ldots, 1$, define recursively

$$B_l(z) = \sum_{t=\delta_l}^{n_l} [z^t]\,(1 + B_{l+1}(z))^{n_l/n_{l+1}}\, z^t.$$

Finally, define

$$\mathcal{N}^{(\boldsymbol{\delta})}(N, w) = [z^w](1 + B_1(z))^{N/n_1}. \tag{3.7}$$

When $h = 1$, (3.7) recovers (3.3):

$$N^{(\delta_1)}(N, w) = [z^w]\left(1 + \sum_{t=\delta_1}^{n_1} \binom{n_1}{t} z^t\right)^{N/n_1} = \sum_{s=1}^{\lfloor w/\delta_1 \rfloor} \binom{m_1}{s} \sum_{\substack{w_1 + \cdots + w_s = w \\ w_i \ge \delta_1}} \prod_{i=1}^{s} \binom{n_1}{w_i}.$$

Lemma 3.16. *Let $y \in C_Z \setminus C_X^\perp$ or $y \in C_X \setminus C_Z^\perp$. If $y \neq 0$, then for every level-l block $J_{l,b}$, either $\operatorname{supp}(y) \cap J_{l,b} = \emptyset$, or $|\operatorname{supp}(y) \cap J_{l,b}| \ge \delta_l$. Consequently, the number of possible supports of such vectors of weight w is at most $\mathcal{N}^{(\boldsymbol{\delta})}(N, w)$.*

Proof. We prove the statement for $y \in C_Z \setminus C_X^\perp$; the other case is identical. Since $y \in C_Z = \ker H_Z$, the vector y satisfies all deterministic local Z-checks.

Fix a level-l block $J_{l,b}$. Let $E = \operatorname{supp}(y) \cap J_{l,b}$ and suppose $0 < |E| \le \delta_l - 1$. The local Z-row space supported in $J_{l,b}$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property, so

$$\operatorname{rank}(V|_E) = |E|.$$

Thus, the only vector supported on E and satisfying all these local checks is the zero vector. This contradicts the definition of E. Therefore every nonempty intersection with $J_{l,b}$ has size at least δ_l.

The recursive generating function counts exactly such supports. At the bottom level, a nonempty level-h block must have weight at least δ_h, so its generating function is

$$B_h(z) = \sum_{t=\delta_h}^{n_h} \binom{n_h}{t} z^t.$$

A level-l block consists of n_l/n_{l+1} level-$(l+1)$ blocks. Each child block is either empty or has a support counted by $B_{l+1}(z)$. Hence the generating function before imposing the level-l threshold is

$$(1 + B_{l+1}(z))^{n_l/n_{l+1}}.$$

However, we only want the nonempty configurations which also meet the threshold of δ_l. For $l = 1, \ldots, h-1$ define

$$B_l(z) = \sum_{t=\delta_l}^{n_l} [z^t](1 + B_{l+1}(z))^{\frac{n_l}{n_{l+1}}} \cdot z^t$$

where $[z^t]f(z)$ is the coefficient of z^t in $f(z)$. This recursively defines $B_{h-1}, \ldots, B_1$. At the top level, the whole length N consists of N/n_1 level-1 blocks, each either empty or counted by $B_1(z)$. Therefore the number of admissible supports of weight w is

$$[z^w](1 + B_1(z))^{N/n_1} = \mathcal{N}^{(\boldsymbol{\delta})}(N, w),$$

as desired. ■

We use the number of admissible supports to define an entropy-like function and give a probabilistic argument for the distance bound.

Proposition 3.17. *For all sufficiently large N, given any $\rho, \epsilon > 0$, the distance $d(\mathcal{Q})$ of a random h-level QHLRC $\mathcal{Q}$ from Construction 3.14 with parameters N, $(r_l, \delta_l)_{l=1,\ldots,h}$, and $N/2 - M > \ell \geq (H_q^{(\boldsymbol{\delta})}(\rho) + 2\epsilon)N$ (if one exists) over the alphabet $\mathbb{F}_q$ satisfies*

$$\Pr[d(\mathcal{Q}) \geq \rho N] > 1 - 2q^{-\epsilon N}. \tag{3.8}$$

where

$$H_q^{(\boldsymbol{\delta})}(\rho) = \limsup_{N \to \infty} \frac{1}{N} \log_q \left(\sum_{w \leq \rho N} \mathcal{N}^{(\boldsymbol{\delta})}(N, w)(q-1)^w \right). \tag{3.9}$$

and the $\limsup$ *is taken over N divisible by n_1.*

Proof. Fix a nonzero vector $y \in \mathbb{F}_q^N$. Let $H_Z^{(i)}$ denote the matrix after the ith iteration of step 2 in Construction 3.14. If $y \in C_Z \setminus C_X^{\perp}$ then for $0 \leq i \leq \ell - 1$, $y \in \ker H_Z^{(i)}$ and $y \in \ker H_Z^{(i+1)}$. Since $y \notin C_X^{\perp}$, exactly $1/q$-fraction of the vectors in C_X are orthogonal to y.

It follows if $y \in \ker H_Z^{(i)}$ then less than $1/q$-fraction of the vectors in $C_X \setminus \text{row-span}(H_Z^{(i)})$ are orthogonal to y. Formally,

$$\Pr\Big[y \in \ker H_Z^{(i+1)} \setminus C_X^{\perp} \mid y \in \ker H_Z^{(i)} \setminus C_X^{\perp}\Big] < \frac{1}{q}.$$

Hence,

$$\begin{aligned}\Pr\big[y \in C_Z \setminus C_X^{\perp}\big] &= \Pr\big[y \notin C_X^{\perp}\big] \cdot \Pr\Big[y \in \ker H_Z^{(0)} \mid y \notin C_X^{\perp}\Big] \\ &\quad \cdot \prod_{i=0}^{\ell-1} \Pr\Big[y \in \ker H_Z^{(i+1)} \setminus C_X^{\perp} \mid y \in \ker H_Z^{(i)} \setminus C_X^{\perp}\Big] \\ &< q^{-\ell}.\end{aligned}$$

Now union bound over all possible supports of weight $w \le \rho N$. By Lemma 3.16, any logical vector of weight w has one of at most $\mathcal{N}^{(\boldsymbol{\delta})}(N, w)$ admissible supports. For each support of size w, there are at most $(q-1)^w$ nonzero vectors supported on it. Therefore, applying the union bound over all $y \in \mathbb{F}_q^N$ with weight, w at most ρN gives

$$\begin{aligned}\Pr\big[\exists\, y \in C_Z \setminus C_X^{\perp}, |y| \le \rho N\big] &< q^{-\ell} \sum_{w \le \rho N} \mathcal{N}^{(\boldsymbol{\delta})}(N, w)(q-1)^w \\ &\le q^{-\ell} q^{(H_q^{(\boldsymbol{\delta})}(\rho)+\epsilon)N} \\ &\le q^{-\epsilon N}\end{aligned}$$

for sufficiently large N and by symmetry

$$\Pr\big[\exists\, y \in C_X \setminus C_Z^{\perp}, |y| \le \rho N\big] < q^{-\epsilon N}.$$

Therefore,

$$\Pr[d(\mathcal{Q}) \le \rho N] < 2q^{-\epsilon N},$$

as desired. ∎

Remark 3.18. In the hierarchical setting, for the most general setting, we are given locality and distance parameters $(r_1, \delta_1), \dots, (r_h, \delta_h)$ such that $r_1 \ge \cdots \ge r_h \ge 1$ and $\delta_1 \ge \cdots \ge \delta_h \ge 2$. We imposed the restriction $n_h \mid n_{h-1} \mid \cdots \mid n_1 \mid N$ so the groups nest. We want each level to meaningfully correct additional erasures so if there is some $1 \le l \le h-1$ such that $\delta_l = \delta_{l+1}$ then level l does not correct any more erasures that level $l+1$. In the parity check view, we would not be adding additional parity checks corresponding to level l because $\delta_l - \delta_{l+1} = 0$. Consequently, it is reasonable to assume $\delta_1 > \cdots > \delta_h \ge 2$. Suppose there is some $1 \le l \le h-1$ such that $r_l = r_{l+1}$. We have

$$r_l + \delta_l - 1 = r_{l+1} + \delta_{l+1} - 1 + (\delta_l - \delta_{l+1})$$

and by the divisibility condition $r_{l+1} + \delta_{l+1} - 1 \mid r_l + \delta_l - 1$ so $r_{l+1} + \delta_{l+1} - 1 \mid \delta_l - \delta_{l+1}$ which is a contradiction. Therefore, we may also assume $r_1 > \cdots > r_h$.

Lastly, we prove a Singleton-like bound for CSS codes constructed from a dual-containing classical HLRC.

Proposition 3.19. *Consider a classical h-level $((r_1, \delta_1), \ldots, (r_h, \delta_h))$-HLRC C such that $C^{\perp} \subseteq C$ and $d(C^{\perp}) \geq \delta_1$. Then $\dim C = (N+k)/2$ and $\mathcal{Q} = \mathrm{CSS}(C, C)$ is an $[[N, k, \geq d(C)]]$ quantum h-level HLRC satisfying*

$$k + 2d(C) \leq N + 2 - 2\sum_{l=1}^{h-1}\left(\left\lceil \frac{N+k}{2r_l} \right\rceil - 1\right)(\delta_l - \delta_{l+1}) - 2\left(\left\lceil \frac{N+k}{2r_h} \right\rceil - 1\right)(\delta_h - 1) \quad (3.10)$$

When $h = 1$, this recovers the same bound as [10, Theorem 30].

Proof. Denote the parameters of C as $[N, k', d(C)]$. By the classical HLRC Singleton-like bound [30, Theorem 3.1] , we have

$$d(C) \leq N - k' + 1 - \sum_{l=1}^{h-1}\left(\left\lceil \frac{k'}{r_l} \right\rceil - 1\right)(\delta_l - \delta_{l+1}) - \left(\left\lceil \frac{k'}{r_h} \right\rceil - 1\right)(\delta_h - 1). \quad (3.11)$$

We know by the CSS construction that $k = k' + k' - N$ so $k' = (N + k)/2$. Plugging this into the above bound, we have

$$d(C) \leq N - \frac{N+k}{2} + 1 - \sum_{l=1}^{h-1}\left(\left\lceil \frac{N+k}{2r_l} \right\rceil - 1\right)(\delta_l - \delta_{l+1}) - \left(\left\lceil \frac{N+k}{2r_h} \right\rceil - 1\right)(\delta_h - 1)$$

and upon rearranging we get

$$\frac{N+k}{2} + d(C) \leq N + 1 - \sum_{l=1}^{h-1}\left(\left\lceil \frac{N+k}{2r_l} \right\rceil - 1\right)(\delta_l - \delta_{l+1}) - \left(\left\lceil \frac{N+k}{2r_h} \right\rceil - 1\right)(\delta_h - 1)$$
$$k + 2d(C) \leq N + 2 - 2\sum_{l=1}^{h-1}\left(\left\lceil \frac{N+k}{2r_l} \right\rceil - 1\right)(\delta_l - \delta_{l+1}) - 2\left(\left\lceil \frac{N+k}{2r_h} \right\rceil - 1\right)(\delta_h - 1),$$

as desired. ∎

3.3.3 Existence of subspaces

We now prove the existence of the desired $U^{+}_{l,b}, V^{+}_{l,b}$ used in Construction 3.14. The proof is quite technical so we first present two inequalities and use them to justify the existence of the desired subspaces.

Theorem 3.20. *Let J be a level-l block of length n_l, and set $\Delta_l := \delta_l - \delta_{l+1}$. Suppose that inside J we have already constructed lower-level row spaces $U_{>l}, V_{>l} \subseteq \mathbb{F}_q^J$ such that*

$$U_{>l} \perp V_{>l} \quad \textit{and} \quad \dim U_{>l} = \dim V_{>l}.$$

Further suppose both $U_{>l}$ and $V_{>l}$ have the $(\delta_{l+1}-1,\delta_1-1)$-strong local MDS property on every level-$(l+1)$ child block inside J. More specifically, suppose that J is partitioned into level-$(l+1)$ child blocks

$$J = \bigsqcup_i J_i,$$

and that

$$U_{>l} = \bigoplus_i U_i, \qquad V_{>l} = \bigoplus_i V_i,$$

where $U_i, V_i \subseteq \mathbb{F}_q^{J_i}$, extended by zero outside J_i, satisfy $U_i \perp V_i$ and both U_i and V_i have the $(\delta_{l+1}-1,\delta_1-1)$-strong local MDS property on J_i. Assume q is sufficiently large. Then there exists a Δ_l-dimensional subspace $U_l^+ \subseteq V_{>l}^\perp$ such that

$$\dim(U_{>l}+U_l^+) = \dim U_{>l} + \Delta_l,$$

and $U_{>l-1} := U_{>l} + U_l^+$ has the (δ_l-1,δ_1-1)-strong local MDS property on J.

After choosing such a U_l^+, there exists a Δ_l-dimensional subspace $V_l^+ \subseteq (U_{>l}+U_l^+)^\perp$ such that

$$\dim(V_{>l}+V_l^+) = \dim V_{>l} + \Delta_l,$$

and $V_{>l-1} := V_{>l}+V_l^+$ has the (δ_l-1,δ_1-1)-strong local MDS property on J. Consequently,

$$U_{>l-1} \perp V_{>l-1} \quad \textit{and} \quad \dim U_{>l-1} = \dim V_{>l-1}.$$

Proof. We first record two consequences of the inductive hypotheses.

Rank-Deficiency Bound: Let $E \subseteq J$ such that $|E| \le \delta_l - 1$. Decompose E among the level-$(l+1)$ child blocks:

$$E = \bigsqcup_i E_i.$$

By the level-$(l+1)$ strong local MDS property,

$$\operatorname{rank}(U_{>l}|_{E_i}) \ge \min\{|E_i|, \delta_{l+1}-1\}$$

which implies

$$\operatorname{rank}(U_{>l}|_E) \ge \sum_i \min\{|E_i|, \delta_{l+1}-1\}.$$

Hence,

$$|E| - \operatorname{rank}(U_{>l}|_E) \le \sum_i (|E_i| - \delta_{l+1}+1)_+.$$

where $y_+ = \max\{y, 0\}$. If the right-hand side is nonzero, then

$$\sum_i (|E_i| - \delta_{l+1}+1)_+ \le |E| - \delta_{l+1} + 1 \le \delta_l - 1 - \delta_{l+1} + 1 = \Delta_l.$$

If it is zero, the same inequality is immediate. Thus, $|E| - \operatorname{rank}(U_{>l}|_E) \le \Delta_l$. The same argument gives $|E| - \operatorname{rank}(V_{>l}|_E) \le \Delta_l$.

Dimension Margin Inequality: By hypothesis, $D := \dim U_{>l} = \dim V_{>l}$. Inside a level-$l$ block, the accumulated lower-level dimension is

$$D = \frac{n_l}{n_h}(\delta_h - 1) + \sum_{u=l+1}^{h-1} \frac{n_l}{n_u}(\delta_u - \delta_{u+1})$$

and dividing by n_l, we get

$$\frac{D}{n_l} = \frac{\delta_h - 1}{n_h} + \sum_{u=l+1}^{h-1} \frac{\delta_u - \delta_{u+1}}{n_u} \leq \frac{\delta_{l+1} - 1}{n_h}.$$

Thus,

$$n_l - 2D \geq n_l \left(1 - \frac{2(\delta_{l+1} - 1)}{n_h}\right) = \frac{n_l}{n_h}\left(n_h - 2(\delta_{l+1} - 1)\right). \tag{3.12}$$

Decompose J among the level-$(l+1)$ child blocks:

$$J = \bigsqcup_i J_i,$$

then $V_{>l}$ decomposes as a direct sum over the J_i:

$$V_{>l} = \bigoplus_i V_i$$

where each $V_i \subseteq \mathbb{F}_q^{J_i}$. By induction hypothesis, each V_i has the $(\delta_{l+1} - 1, \delta_1 - 1)$-strong local MDS property on J_i. Hence, for every $E_i \subseteq J_i$, with $|E_i| \leq \delta_1 - 1$, we have $V_i \cap \mathbb{F}_q^J[E_i] = \{0\}$. Now take any subset $E \subseteq J$ with $|E| \leq \delta_1 - 1$ and write $E_i = E \cap J_i$, then $|E_i| \leq \delta_1 - 1$. Suppose $v \in V_{>l} \cap \mathbb{F}_q^J[E]$. We can decompose $v = \sum_i v_i$ for $v_i \in V_i$. Since v is supported inside E, each component is supported inside E_i. Thus,

$$v_i \in V_i \cap \mathbb{F}_q^J[E_i],$$

but $|E_i| \leq \delta_1 - 1$ so $v_i = 0$. Hence, $v = 0$ and $V_{>l} \cap \mathbb{F}_q^J[E] = \{0\}$,

Recall by the hypotheses of the construction, $n_h \mid n_l$ and $\delta_1 - 1 < n_h/2$. For every $E \subseteq J$ with $|E| \leq \delta_1 - 1$, let

$$\pi_{J \setminus E} : \mathbb{F}_q^J \to \mathbb{F}_q^{J \setminus E}$$

be the coordinate projection. Since $V_{>l} \cap \mathbb{F}_q^J[E] = \{0\}$ for $|E| \leq \delta_1 - 1$, we have

$$\begin{aligned}
\dim \pi_{J \setminus E}(V_{>l}^{\perp}) &= \dim V_{>l}^{\perp} - \dim \ker(\pi_{J \setminus E}|_{V_{>l}^{\perp}}) \\
&= n_l - D - \dim(V_{>l}^{\perp} \cap \mathbb{F}_q^J[E]) \\
&= n_l - D - \dim \ker(V_{>l}|_E) \\
&= n_l - D - |E| + \operatorname{rank}(V_{>l}|_E).
\end{aligned}$$

Also, since $U_{>l} \cap \mathbb{F}_q^J[E] = \{0\}$,

$$\dim \pi_{J\setminus E}(U_{>l}) = \dim U_{>l} - \dim \ker(\pi_{J\setminus E}|_{U_{>l}}) = D - \dim(U_{>l} \cap \mathbb{F}_q^J[E]) = D.$$

Therefore,

$$\dim \pi_{J\setminus E}(V_{>l}^{\perp}) - \dim \pi_{J\setminus E}(U_{>l}) = n_l - 2D - |E| + \operatorname{rank}(V_{>l}|_E).$$

By the level-$l+1$ strong local MDS property,

$$\operatorname{rank}(V_{>l}|_E) \geq \min\{|E|, \delta_{l+1} - 1\}$$

so

$$|E| - \operatorname{rank}(V_{>l}|_E) \leq \delta_1 - 1 - \delta_{l+1} + 1 = \delta_1 - \delta_{l+1}$$

and

$$\dim \pi_{J\setminus E}(V_{>l}^{\perp}) - \dim \pi_{J\setminus E}(U_{>l}) \geq n_l - 2D - \delta_1 + \delta_{l+1}.$$

By (3.12),

$$n_l - 2D \geq \frac{n_l}{n_h}\left(n_h - 2(\delta_{l+1} - 1)\right) \geq n_h - 2(\delta_{l+1} - 1)$$

and

$$n_h - 2(\delta_{l+1} - 1) = n_h - 2(\delta_1 - 1) + 2(\delta_1 - \delta_{l+1}) \geq 2(\delta_1 - \delta_{l+1}) \geq \delta_1 + \delta_l - 2\delta_{l+1}$$

Consequently,

$$\dim \pi_{J\setminus E}(V_{>l}^{\perp}) - \dim \pi_{J\setminus E}(U_{>l}) \geq \delta_l - \delta_{l+1} = \Delta_l.$$

The same argument, with $U_{>l}$ and $V_{>l}$ interchanged, gives

$$\dim \pi_{J\setminus E}(U_{>l}^{\perp}) - \dim \pi_{J\setminus E}(V_{>l}) \geq \Delta_l.$$

Existence: We prove the existence of U_l^+; the reasoning for V_l^+ is identical after U_l^+ has been chosen. We choose U_l^+ from the Grassmannian $\mathrm{Gr}_{\mathbb{F}_q}(\Delta_l, V_{>l}^{\perp})$. Equivalently, after fixing a basis of $V_{>l}^{\perp}$, we may parameterize an ordered Δ_l-tuple of vectors in $V_{>l}^{\perp}$ by a matrix of variables

$$W \in \mathbb{F}_q^{\Delta_l \times \dim V_{>l}^{\perp}}.$$

We impose three types of conditions.

First, we require $U_l^+ \cap U_{>l} = \{0\}$. This is equivalent to

$$\dim(U_{>l} + U_l^+) = \dim U_{>l} + \Delta_l,$$

and is the nonvanishing of some $(D + \Delta_l) \times (D + \Delta_l)$ minor in the coordinates W. Such a determinant polynomial is not identically zero because

$$\dim(V_{>l}^{\perp}/U_{>l}) = n_l - 2D \geq \Delta_l.$$

Hence there exist $w_1, \dots, w_{\Delta_l} \in V_{>l}^{\perp}$ whose images are linearly independent modulo $U_{>l}$. For this choice, the matrix obtained by adjoining the w_i's to a fixed basis of $U_{>l}$ has rank $\dim U_{>l} + \Delta_l$. Therefore at least one full-rank minor of that matrix is nonzero at this choice, and the corresponding minor polynomial is not identically zero.

Second, for every $E \subseteq J$ with $|E| \le \delta_l - 1$, we require

$$\operatorname{rank}((U_{>l} + U_l^+)|_E) = |E|.$$

The rank-deficiency bound proved above says that at most Δ_l new directions are needed on E. Since $V_{>l}$ has no nonzero word supported on E, the restriction $(V_{>l}^{\perp})|_E$ has full rank $|E|$. The vectors from $V_{>l}^{\perp}$ can complete the rank of $U_{>l}|_E$. Hence, for each fixed E, at least one $|E| \times |E|$ minor of the restricted matrix is a nonzero polynomial in the entries of W.

Third, for every $E \subseteq J$ with $|E| \le \delta_1 - 1$, we require

$$(U_{>l} + U_l^+) \cap \mathbb{F}_q^J[E] = \{0\}.$$

Equivalently, restriction to $J \setminus E$ is injective on $U_{>l} + U_l^+$, i.e.

$$\operatorname{rank}((U_{>l} + U_l^+)|_{J\setminus E}) = \dim(U_{>l} + U_l^+).$$

The dimension margin inequality above says that inside $\pi_{J\setminus E}(V_{>l}^{\perp})$ there are at least Δ_l dimensions available modulo $\pi_{J\setminus E}(U_{>l})$. Thus, the injectivity condition is also the nonvanishing of a suitable maximal minor.

Thus all required conditions are finitely many polynomial nonvanishing conditions in the entries of W. Let $F(W)$ be the product of one nonzero polynomial for each condition. Then F is a nonzero polynomial. By the Schwartz–Zippel lemma,

$$\Pr[F(W) = 0] \le \frac{\deg F}{q}$$

where the probability is over random choices of entries of W. Therefore, for $q > \deg F$, there exists a choice of entries of W such that $F(W) \neq 0$. The span of the Δ_l chosen vectors in $V_{>l}^{\perp}$ is the desired subspace U_l^+.

Now set $U_{>l-1} := U_{>l} + U_l^+$. By construction, $U_{>l-1}$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property and $\dim U_{>l-1} = D + \Delta_l$. We now choose V_l^+ from $\operatorname{Gr}_{\mathbb{F}_q}(\Delta_l, U_{>l-1}^{\perp})$. The rank-deficiency bound for $V_{>l}$ was already proved:

$$|E| - \operatorname{rank}(V_{>l}|_E) \le \Delta_l \qquad (|E| \le \delta_l - 1).$$

Also, since $U_{>l-1}$ has no nonzero word supported on a set of size at most $\delta_1 - 1$, the restriction of $U_{>l-1}^{\perp}$ to any such E has full rank. It remains to check the dimension margin inequality. For $|E| \le \delta_1 - 1$, we have

$$\begin{aligned}
\dim \pi_{J\setminus E}(U_{>l-1}^{\perp}) &= \dim U_{>l-1}^{\perp} - \dim \ker(\pi_{J\setminus E}|_{U_{>l-1}^{\perp}}) \\
&= n_l - D - \Delta_l - \dim(U_{>l-1}^{\perp} \cap \mathbb{F}_q^J[E])
\end{aligned}$$

$$= n_l - D - \Delta_l - \dim\ker(U_{>l-1}|_E)$$
$$= n_l - D - \Delta_l - |E| + \mathrm{rank}(U_{>l-1}|_E)$$

and since $V_{>l} \cap \mathbb{F}_q^J[E] = \{0\}$

$$\dim \pi_{J\setminus E}(U_{>l-1}^{\perp}) - \dim \pi_{J\setminus E}(V_{>l}) = n_l - (D + \Delta_l) - D - |E| + \mathrm{rank}(U_{>l-1}|_E).$$

Since $U_{>l-1}$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property, for every $E \subseteq J$ with $|E| \leq \delta_1 - 1$, we have

$$\mathrm{rank}(U_{>l-1}|_E) \geq \min\{|E|, \delta_l - 1\}$$

so

$$|E| - \mathrm{rank}(U_{>l-1}|_E) \leq \delta_1 - 1 - (\delta_l - 1) = \delta_1 - \delta_l.$$

Therefore,

$$\dim \pi_{J\setminus E}(U_{>l-1}^{\perp}) - \dim \pi_{J\setminus E}(V_{>l}) \geq n_l - 2D - \Delta_l - (\delta_1 - \delta_l).$$

Using

$$n_l - 2D \geq \delta_1 + \delta_l - 2\delta_{l+1},$$

we get

$$n_l - 2D - \Delta_l - (\delta_1 - \delta_l) \geq \delta_l - \delta_{l+1} = \Delta_l.$$

Thus, the same Schwartz–Zippel argument produces a subspace $V_l^+ \subseteq U_{>l-1}^{\perp}$ such that $V_l^+ \cap V_{>l} = \{0\}$ and $V_{>l-1} := V_{>l} + V_l^+$ has the $(\delta_l - 1, \delta_1 - 1)$-strong local MDS property.

Finally, $U_l^+ \subseteq V_{>l}^{\perp}$ and $V_l^+ \subseteq U_{>l-1}^{\perp} = (U_{>l} + U_l^+)^{\perp}$, so by construction,

$$U_{>l-1} \perp V_{>l-1} \quad \text{and} \quad \dim U_{>l-1} = \dim V_{>l-1}.$$

This proves the theorem. ■

Chapter 4

Quantum Tamo–Barg Codes

We now use the intuition of the randomized constructions from Section 3.2 and Section 3.3 to give an explicit construction of a QLRC which builds upon classical Tamo–Barg codes.

Here we extend the quantum Tamo–Barg code definition in [14] to a (r, δ) quantum Tamo–Barg (QTB) code. Our parameters are adjusted to match the convention of classical (r, δ) Tamo–Barg code constructions presented in [33].

Definition 4.1 ((r, δ) quantum Tamo–Barg code)**.** Let p be a prime number and m be a positive integer, and $q = p^m$. Given an integer $\delta \geq 2$, a locality parameter $r \geq \delta$ such that $(r + \delta - 1)|(q - 1)$, and an integer $\ell \in [q]$, the (r, δ) quantum Tamo–Barg code is defined to be the CSS code $\mathcal{Q} = \mathrm{CSS}(C, C)$ with $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$, where

$$\begin{aligned} S = \{i \in [\ell] \mid i \not\equiv -j \bmod (r + \delta - 1) \text{ for any } j \in \{1, \ldots, \delta - 1\}\} \\ \cup \{i \in [q - 1] \mid i \equiv j \bmod (r + \delta - 1) \text{ for some } j \in \{1, \ldots, \delta - 1\}\}. \end{aligned}$$

In what follows, we will require this lemma [14, Lemma 54] which we restate without proof. Consider classical codes A_X, A_Z, B_X, B_Z in $\mathbb{F}_q^n$ such that $A_X^\perp \subseteq A_Z$ and $B_X^\perp \subseteq B_Z$.

Lemma 4.2. *For CSS codes $\mathcal{A} = \mathrm{CSS}(A_X, A_Z)$ and $\mathcal{B} = \mathrm{CSS}(B_X, B_Z)$ of block length n over $\mathbb{F}_q$, there exists a CSS code $\mathcal{Q} = \mathrm{CSS}(C_X, C_Z)$ given by*

$$C_X = (A_X \cap B_X) + B_Z^\perp \tag{4.1}$$

$$C_Z = (A_Z \cap B_Z) + B_X^\perp, \tag{4.2}$$

so that

$$C_X^\perp = (A_X^\perp \cap B_Z) + B_X^\perp \tag{4.3}$$

$$C_Z^\perp = (A_Z^\perp \cap B_X) + B_Z^\perp. \tag{4.4}$$

Consider the following sets:

$$S_+ = \bigcup_{j=1}^{\delta-1} (j + (r + \delta - 1)\mathbb{Z}),$$

$$S_- = \bigcup_{j=1}^{\delta-1}(-j + (r+\delta-1)\mathbb{Z}).$$

Then

$$S = ([\ell] \cap ([q-1] \setminus S_-)) \cup ([q-1] \cap S_+) = ([\ell] \setminus S_-) \cup ([q-1] \cap S_+).$$

We construct the (r, δ) quantum Tamo–Barg codes as follows:

Lemma 4.3. *For integers $r \geq \delta \geq 2$ such that $(r+\delta-1)|(q-1)$, and $\ell \in [q]$, let*

$$A = \mathrm{ev}(\mathbb{F}_q[X]^{[\ell]}), \tag{4.5}$$

$$B = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\setminus S_-}). \tag{4.6}$$

Then $A \cap B$ is a (r, δ) TB code. Furthermore,

$$A^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-\ell]\setminus\{0\}}) \text{ and} \tag{4.7}$$

$$B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+}) \subseteq B. \tag{4.8}$$

If $\ell \geq q/2$, then $A^\perp \subseteq A$. Letting $C = (A \cap B) + B^\perp$, we obtain that $\mathrm{CSS}(C, C)$ is a QTB code with

$$C^\perp = (A^\perp \cap B) + B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^T) \subseteq C \tag{4.9}$$

where

$$T = (([q-\ell] \setminus \{0\}) \cap ([q-1] \setminus S_-)) \cup ([q-1] \cap S_+). \tag{4.10}$$

Proof. We first prove the equality in (4.7) by dimension counting. Notice that $\dim A = \ell$, so $\dim A^\perp = q - 1 - \ell$. Since $\dim \mathrm{ev}(\mathbb{F}_q[X]^{[q-\ell]\setminus\{0\}}) = q - \ell - 1$, it suffices to prove $\mathrm{ev}(\mathbb{F}_q[X]^{[q-\ell]\setminus\{0\}}) \subseteq A^\perp$. To that end, by choosing a monomial basis for $\mathbb{F}_q[X]^{[\ell]}$ and $\mathbb{F}_q[X]^{[q-\ell]\setminus\{0\}}$, it is sufficient to prove $\mathrm{ev}(X^i) \cdot \mathrm{ev}(X^s) = 0$ for every $i \in [\ell]$ and $s \in [q-\ell] \setminus \{0\}$. We have $\mathrm{ev}(X^i) \cdot \mathrm{ev}(X^s) = \sum_{\alpha \in \mathbb{F}_q^*} \alpha^{i+s} = 0$ for $i + s \not\equiv 0 \mod q-1$.

To see this last result, let ω_{q-1} be a generator for $\mathbb{F}_q^*$. Then $\alpha = \omega_{q-1}^j$ for some j. Therefore,

$$\sum_{\alpha \in \mathbb{F}_q^*} \alpha^{i+s} = \sum_{j=1}^{q-1} \omega_{q-1}^{j(i+s)} = \sum_{j=1}^{q-1} (\omega_{q-1}^{(i+s)})^j = \frac{(\omega_{q-1}^{i+s})^q - \omega_{q-1}^{i+s}}{\omega_{q-1}^{i+s} - 1} = \frac{\omega_{q-1}^{i+s} - \omega_{q-1}^{i+s}}{\omega_{q-1}^{i+s} - 1} = 0$$

because $i + s \not\equiv 0 \pmod{q-1}$ so the denominator is not zero.

Now we prove the equality in (4.8). It is straightforward to see that

$$\dim B = q - 1 - \frac{q-1}{r+\delta-1}(\delta - 1)$$

then

$$\dim B^\perp = \frac{q-1}{r+\delta-1}(\delta-1).$$

Notice, $\dim \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+}) = \dim B^\perp$ so it suffices to prove

$$\mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+}) \subseteq B^\perp.$$

Choose a monomial basis for $\mathbb{F}_q[X]^{[q-1]\setminus S_-}$ and $\mathbb{F}_q[X]^{[q-1]\cap S_+}$. For all $i \in [q-1] \setminus S_-$ and $s \in [q-1] \cap S_+$, we have $\mathrm{ev}(X^i) \cdot \mathrm{ev}(X^s) = \sum_{\alpha \in \mathbb{F}_q^*} \alpha^{i+s} = 0$ for $i + s \not\equiv 0 \mod q-1$.

The inclusion $B^\perp \subseteq B$ follows from

$$\begin{aligned} \delta \le r &\iff \delta - 1 < \frac{r+\delta-1}{2} \\ &\implies S_- \cap S_+ = \emptyset \end{aligned}$$

and the remaining arguments follow immediately using Lemma 4.2. ■

We now compute the dimension of the (r, δ) quantum Tamo–Barg code defined in Definition 4.1.

Lemma 4.4. *The (r, δ) quantum Tamo–Barg code $\mathcal{Q} = \mathrm{CSS}(C, C)$ with parameters q, r, ℓ, δ as defined in Definition 4.1 has dimension*

$$\begin{aligned} k &= 1 + |\{q - \ell \le i \le \ell - 1 : i \notin (S_+ \cup S_-)\}| \\ &= 1 + (2\ell - q)\left(1 - \frac{2(\delta-1)}{r+\delta-1}\right) + \epsilon \end{aligned}$$

for some $\epsilon \in [-2(\delta-1), 2(\delta-1)]$.

Proof. Recall $S \subseteq [q-1]$ as defined in Definition 4.1, $T \subseteq S$ as defined in Lemma 4.3 such that $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$ and $C^\perp = \mathrm{ev}(\mathbb{F}_q[X]^T)$. Then, the dimension of $\mathcal{Q}$ can be computed as follows:

$$\begin{aligned} \dim(\mathcal{Q}) &= \dim(C) - \dim(C^\perp) \\ &= |S \setminus T| \\ &= |\{0\} \cup \{q - \ell \le i \le \ell - 1 : i \notin (S_+ \cup S_-)\}| \,. \end{aligned}$$

which proves the first equality. For the second equality, we inspect

$$\{q - \ell \le i \le \ell - 1 : i \notin (S_+ \cup S_-)\}.$$

If $(r + \delta - 1) \mid (2\ell - q)$ then this set has size exactly

$$(2\ell - q)\left(1 - \frac{2(\delta-1)}{r+\delta-1}\right)$$

because we exclude $2(\delta - 1)$ elements in every block of $(r + \delta - 1)$. Note, this exclusion will leave a nontrivial number of elements precisely because

$$2(\delta - 1) < r + \delta - 1 \iff \delta - 1 < r \iff \delta \le r.$$

If $(r+\delta-1) \nmid (2\ell - q)$, we differ from

$$(2\ell - q)\left(1 - \frac{2(\delta-1)}{r+\delta-1}\right)$$

by at most $2(\delta - 1)$ in absolute value and the second equality follows. ∎

We need to show that the code, $\mathcal{Q} = \mathrm{CSS}(C, C)$ defined in Definition 4.1 is an (r, δ)-QLRC. By Theorem 3.3, it suffices to show that $C^\perp$ contains low-weight parity checks whose supports cover all $q-1$ code components. As defined in Lemma 4.3, $B^\perp \subseteq C^\perp$ so it suffices to show that $B^\perp$ contains low-weight parity checks. The result is summarized in Lemma 4.5.

Lemma 4.5. *Consider the code $B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+})$ as defined in Lemma 4.3. Let $\Omega_{r+\delta-1} = \{x \in \mathbb{F}_q^* : x^{r+\delta-1} = 1\}$ be the subgroup of $(r+\delta-1)$th roots of unity. Then a function $f : \mathbb{F}_q^* \to \mathbb{F}_q$ lies in $B^\perp$ if and only if for every coset $\alpha\Omega_{r+\delta-1}$ for some $\alpha \in \mathbb{F}_q^*$, there exists a polynomial $P_\alpha(X) \in \mathbb{F}_q[X]$ with $\deg P_\alpha \le \delta - 1$ and no constant term such that*

$$f(\alpha\omega) = P_\alpha(\omega)$$

for all $\omega \in \Omega_{r+\delta-1}$.

Before we prove the lemma, we make some observations about the statement. Since P_α has no constant term, $P_\alpha(0) = 0$. An equivalent formulation would be to say that f lies in $B^\perp$ if and only if f is a piecewise polynomial in ω of degree $\le \delta - 1$ on each coset $\alpha\Omega_{r+\delta-1}$ and that polynomial has no constant term.

Proof. By dimension counting, it suffices to show the forward direction.

($\Longrightarrow$) Let $n := r + \delta - 1$. Fix $f(X) = \sum_{i\in[q-1]} f_i X^i$ with $\mathrm{ev}(f) \in B^\perp$. By definition, f_i for $i \notin [q-1] \cap S_+$ must be zero. Grouping terms by residues modulo n, we can write

$$f(X) = \sum_{j=1}^{\delta-1} X^j F_j(X^n)$$

where $F_j \in \mathbb{F}_q[Y]$ is a polynomial. Fix a coset $\alpha\Omega_n$. For any $x \in \alpha\Omega_n$, we can write $x = \alpha\omega$ for some $\omega \in \Omega_n$. Since $\omega^n = 1$, we have

$$f(x) = f(\alpha\omega) = \sum_{j=1}^{\delta-1} (\alpha\omega)^j F_j((\alpha\omega)^n) = \sum_{j=1}^{\delta-1} (\alpha\omega)^j F_j(\alpha^n) = \sum_{j=1}^{\delta-1} (\alpha^j F_j(\alpha^n))\omega^j.$$

The final sum is a polynomial in ω of degree $\le \delta - 1$ and no constant term. Therefore, we can define P_α to be

$$P_\alpha(X) = \sum_{j=1}^{\delta-1} (\alpha^j F_j(\alpha^n)) X^j$$

and it is clear that $\deg P_\alpha \le \delta - 1$, P_α has no constant term, and $f(\alpha\omega) = P_\alpha(\omega)$ for all $\omega \in \Omega_{r+\delta-1}$.

∎

Corollary 4.6. *The (r,δ)-QTB code defined in Definition 4.1 is a QLRC with locality r such that $\delta - 1$ erasures are corrected by each local repair group.*

Proof. By Theorem 3.3, it is sufficient to show that C is classically (r,δ)-locally recoverable. Let $n := r + \delta - 1$ and fix $\alpha\Omega_n$. By Lemma 4.3, we know $C^\perp \supseteq B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+})$ and Lemma 4.5 implies that $B^\perp$ contains the $\delta - 1$ functions

$$f_{\alpha,j}(x) = \begin{cases} x^j, & x \in \alpha\Omega_n \\ 0, & x \notin \alpha\Omega_n \end{cases}$$

for $j = 1, \ldots, \delta - 1$. These are linearly independent. Their restriction to $\alpha\Omega_n$ forms a $(\delta - 1) \times n$ Vandermonde-type matrix

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\delta-1} & x_2^{\delta-1} & \cdots & x_n^{\delta-1} \end{bmatrix}.$$

Hence, any $\delta - 1$ columns are linearly independent so $d(C|_{\alpha\Omega_n}) \geq \delta$. Since $|\alpha\Omega_n| = r + \delta - 1$, this shows C is an (r,δ)-LRC.

Additionally, since puncturing can only decrease the distance and $C^\perp \subseteq C$, we have the following

$$d(C^\perp) \geq d(C) \geq d(C|_{\alpha\Omega_n}) \geq \delta.$$

Therefore, by Theorem 3.3, $\mathcal{Q} = \mathrm{CSS}(C, C)$ is an (r,δ)-QLRC. ■

4.1 Non-vanishing theorem

It remains to compute a lower bound on the distance of the (r,δ)-QTB. For the distance bound, we will need the following theorem on the number of roots of unity at which a particular polynomial vanishes. In order to prove this theorem, we rely on proving a particular combinatorial fact on homogeneous symmetric polynomials (Lemma 4.17) which, to the best of our knowledge, does not appear in the current literature and may be of independent interest.

Theorem 4.7. *Let $r \geq \delta \geq 3$ and let $n = r + \delta - 1$. Let $\zeta \in \mathbb{C}$ be a primitive nth root of unity. For each $b \in \{\delta - 1, \ldots, n - 1\}$, let*

$$Q_b(Y) = Y^b + \sum_{t=0}^{\delta-2} v_t Y^t$$

be a polynomial satisfying $Q_b(\zeta^t) = 0$ for $t = 0, \ldots, \delta - 2$. Then $Q_b(\zeta^s) \neq 0$ for any $s \in \{\delta - 1, \ldots, n - 1\}$. In other words, $Q_b(\zeta^s) = 0 \iff s = 0, \ldots, \delta - 2$.

Proof. Fix $s, b \in \{\delta-1, \ldots, n-1\}$. Consider the $\delta \times \delta$ matrix $M_{s,b} = (\zeta^{ac})_{a \in R, c \in C}$ where $R = \{0, 1, \ldots, \delta-2, s\}$ and $C = \{0, 1, \ldots, \delta-2, b\}$. More explicitly,

$$M_{s,b} = \begin{bmatrix} \zeta^{0\cdot 0} & \zeta^{0\cdot 1} & \cdots & \zeta^{0\cdot(\delta-2)} & \zeta^{0\cdot b} \\ \zeta^{1\cdot 0} & \zeta^{1\cdot 1} & \cdots & \zeta^{1\cdot(\delta-2)} & \zeta^{1\cdot b} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \zeta^{s\cdot 0} & \zeta^{s\cdot 1} & \cdots & \zeta^{s\cdot(\delta-2)} & \zeta^{s\cdot b} \end{bmatrix}.$$

Replacing the last column Y^b, by $Q_b(Y) = Y^b + \sum_{t=0}^{\delta-2} v_t Y^t$ does not change the determinant because we are only performing column operations. By hypothesis, $Q_b(\zeta^t) = 0$ for $t = 0, \ldots, \delta-2$. Hence, the last column is $[0, \ldots, 0, Q_b(\zeta^s)]^T$. Therefore, $\det M_{s,b} = \det(\zeta^{a,c})_{0 \le a,c \le \delta-2} \cdot Q_b(\zeta^s)$.

Let $x_1 = \zeta^0, x_2 = \zeta^1, \ldots, x_{\delta-1} = \zeta^{\delta-2}, x_\delta = \zeta^s$. Then,

$$Q_b(\zeta^s) = \frac{\det M_{s,b}}{\det(\zeta^{a,b})_{0 \le a,b \le \delta-2}} \tag{4.11}$$

$$= \frac{\begin{vmatrix} x_1^b & x_2^b & \cdots & x_\delta^b \\ x_1^{\delta-2} & x_2^{\delta-2} & \cdots & x_\delta^{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_\delta \\ 1 & 1 & \cdots & 1 \end{vmatrix}}{\begin{vmatrix} x_1^{\delta-2} & x_2^{\delta-2} & \cdots & x_{\delta-1}^{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_{\delta-1} \\ 1 & 1 & \cdots & 1 \end{vmatrix}} \tag{4.12}$$

$$= \frac{\begin{vmatrix} x_1^b & x_2^b & \cdots & x_\delta^b \\ x_1^{\delta-2} & x_2^{\delta-2} & \cdots & x_\delta^{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_\delta \\ 1 & 1 & \cdots & 1 \end{vmatrix}}{\begin{vmatrix} x_1^{\delta-1} & x_2^{\delta-1} & \cdots & x_\delta^{\delta-1} \\ x_1^{\delta-2} & x_2^{\delta-2} & \cdots & x_\delta^{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_{\delta-1} \\ 1 & 1 & \cdots & 1 \end{vmatrix}} \cdot \frac{\begin{vmatrix} x_1^{\delta-1} & x_2^{\delta-1} & \cdots & x_\delta^{\delta-1} \\ x_1^{\delta-2} & x_2^{\delta-2} & \cdots & x_\delta^{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_{\delta-1} \\ 1 & 1 & \cdots & 1 \end{vmatrix}}{\begin{vmatrix} x_1^{\delta-2} & x_2^{\delta-2} & \cdots & x_{\delta-1}^{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_{\delta-1} \\ 1 & 1 & \cdots & 1 \end{vmatrix}} \tag{4.13}$$

$$= s_{\lambda=(b-\delta+1,0,\ldots,0)}(x_1, \ldots, x_\delta) \cdot \prod_{t=0}^{\delta-2}(x_\delta - x_{t+1}) \tag{4.14}$$

$$= \begin{vmatrix} h_{b-(\delta-1)} & h_{b-(\delta-2)} & \cdots & h_b \\ h_{-1} & h_0 & \cdots & h_{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_{-(\delta-1)} & h_{-(\delta-2)} & \cdots & h_0 \end{vmatrix} \cdot \prod_{t=0}^{\delta-2}(x_\delta - x_{t+1}) \tag{4.15}$$

$$= \begin{vmatrix} h_{b-(\delta-1)} & h_{b-(\delta-2)} & \cdots & h_b \\ 0 & 1 & \cdots & h_{\delta-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{vmatrix} \cdot \prod_{t=0}^{\delta-2}(x_\delta - x_{t+1}) \tag{4.16}$$

$$= h_{b-\delta+1}(x_1, \dots, x_\delta) \cdot \prod_{t=0}^{\delta-2}(x_\delta - x_{t+1}) \tag{4.17}$$

$$= h_{b-\delta+1}(1, \dots, \zeta^{\delta-2}, \zeta^s) \cdot \prod_{t=0}^{\delta-2}(\zeta^s - \zeta^t). \tag{4.18}$$

Here, $s_\lambda(x_1, \dots, x_\delta)$ is the Schur polynomial over the partition λ and $h_{b-\delta+1}$ is the complete homogeneous symmetric polynomial of degree $b - \delta + 1$. Equation (4.12) follows from (4.11) because the determinant is unchanged under column swaps and transposition. The first term in (4.14) follows from (4.13) by Jacobi's bialternant formula for Schur polynomials (also a special case of Weyl character formula)[4, 22] and the second term follows from taking a quotient of two Vandermonde determinants. Equation (4.15) follows from (4.14) by the Jacobi-Trudi formula [22, 36]. For $s \in \{\delta - 1, \dots, n - 1\}$, $\zeta^s - \zeta^t \neq 0$ for all $t = 0, \dots, \delta - 2$. Hence, $Q_b(\zeta^s) \neq 0$ if and only if $h_{b-\delta+1}(1, \zeta, \dots, \zeta^{\delta-2}, \zeta^s) \neq 0$ which follows from Lemma 4.17. ■

Remark 4.8. Theorem 4.7 is not true in the case of $\delta = 2$. Consider the following example. Let $\delta = 2$ then $n = r + 1$. We must choose $b \in \{1, \dots, r\}$. $Q_b(Y) = Y^b + v_0$ and $Q_b(1) = 0$ so $v_0 = -1$ and $Q_b(Y) = Y^b - 1$. Now for $s \in \{1, \dots, r\}$, $Q_b(\zeta^s) = 0$ if $\zeta^{sb} = 1$. Let $r = 3$ so $n = 4$ and choose $b = s = 2$ then $Q_2(\zeta^2) = \zeta^4 - 1 = 0$.

Hence, if s is chosen such that $n \mid sb$, then ζ^s is a root. If $\delta = 2$ and we strengthen the hypothesis of Theorem 4.7 to choosing b such that $\gcd(b, r + 1) = 1$, then the claim will follow. For more details on where the proof particularly breaks see Remark 4.18.

Theorem 4.7 is over $\mathbb{C}$, but we need results over finite fields so we present the following reduction. In particular, the same result will hold over finite fields once we exclude finitely many prime characteristics.

Corollary 4.9. *Fix integers $r \geq \delta \geq 3$, and set $n = r + \delta - 1$. For each*

$$m \in \{0, \dots, r - 1\} \qquad \textit{and} \qquad s \in \{\delta - 1, \dots, n - 1\},$$

define

$$A_{m,s}(X) := h_m(1, X, X^2, \dots, X^{\delta-2}, X^s) \in \mathbb{Z}[X].$$

Let $\Phi_n(X) \in \mathbb{Z}[X]$ denote the nth cyclotomic polynomial, and define

$$\mathcal{M}_{r,\delta} := \prod_{m=0}^{r-1} \prod_{s=\delta-1}^{n-1} \operatorname{Res}(\Phi_n(X), A_{m,s}(X)) \in \mathbb{Z}.$$

Then $\mathcal{M}_{r,\delta} \neq 0$. Consequently, if $\mathbb{F}_q$ is a finite field of characteristic p such that $p \nmid \mathcal{M}_{r,\delta}$ and $n \mid (q-1)$, then for every primitive nth root of unity $\omega \in \mathbb{F}_q$, every $b \in \{\delta-1, \ldots, n-1\}$, and every $s \in \{\delta-1, \ldots, n-1\}$, the polynomial

$$Q_b(Y) = Y^b + \sum_{t=0}^{\delta-2} v_t Y^t$$

satisfying $Q_b(\omega^t) = 0$ for $t = 0, \ldots, \delta-2$ also satisfies $Q_b(\omega^s) \neq 0$. In particular, for fixed r and δ, the conclusion of Theorem 4.7 holds over every finite field of characteristic outside a finite set of primes.

Proof. Let $\zeta \in \mathbb{C}$ be a primitive nth root of unity. By Lemma 4.17, for every

$$m \in \{0, \ldots, r-1\}, \qquad s \in \{\delta-1, \ldots, n-1\},$$

we have

$$A_{m,s}(\zeta) = h_m(1, \zeta, \zeta^2, \ldots, \zeta^{\delta-2}, \zeta^s) \neq 0.$$

Lemma 4.17 applies to every primitive n-th root η. Hence, $A_{m,s}(\eta) \neq 0$ for every root η of Φ_n, so $A_{m,s}$ and Φ_n have no common root in $\mathbb{C}$. Therefore, they are coprime in $\mathbb{Q}[X]$ and

$$\operatorname{Res}(\Phi_n(X), A_{m,s}(X)) \neq 0$$

for every such pair (m, s). Thus $\mathcal{M}_{r,\delta} \neq 0$.

Now let $\mathbb{F}_q$ be a finite field of characteristic p such that $p \nmid M_{r,\delta}$ and $n \mid (q-1)$, and let $\omega \in \mathbb{F}_q$ be a primitive nth root of unity. Fix

$$b \in \{\delta-1, \ldots, n-1\}, \qquad s \in \{\delta-1, \ldots, n-1\},$$

and let $m = b - \delta + 1$. Suppose, for contradiction, $Q_b(\omega^s) = 0$.

By the same determinant/Jacobi–Trudi computation used in the proof of Theorem 4.7—which is purely algebraic and therefore valid over any field containing a primitive nth root of unity—we have

$$Q_b(\omega^s) = 0 \implies A_{m,s}(\omega) = 0,$$

because

$$\prod_{t=0}^{\delta-2} (\omega^s - \omega^t) \neq 0$$

in any field containing a primitive n-th root of unity. Hence, $A_{m,s}(\omega) = 0 \in \mathbb{F}_q$ so ω is a root of the reduction $\overline{A_{m,s}}(X) \in \mathbb{F}_p[X]$.

We next show that ω is also a root of the reduction of $\Phi_n(X)$ modulo p. Since $n \mid (q-1)$, we have $p \nmid n$. Reducing the factorization

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

modulo p, we obtain in $\mathbb{F}_p[X]$

$$X^n - 1 = \prod_{d \mid n} \overline{\Phi_d}(X).$$

Now $\omega^n = 1$, so ω is a root of $X^n - 1$. Moreover, because ω has exact multiplicative order n, it is not a root of $X^d - 1$ for any proper divisor $d \mid n$. Since every root of $\overline{\Phi_d}(X)$ is also a root of $X^d - 1$, it follows that ω cannot be a root of $\overline{\Phi_d}(X)$ for any proper divisor $d < n$. Therefore, ω must be a root of $\overline{\Phi_n}(X)$.

Thus, ω is a common root of the reductions modulo p of $A_{m,s}(X)$ and $\Phi_n(X)$. By Proposition 2.28,

$$p \mid \operatorname{Res}(\Phi_n(X), A_{m,s}(X))\,.$$

But $\operatorname{Res}(\Phi_n(X), A_{m,s}(X))$ is one of the factors of $\mathcal{M}_{r,\delta}$, so this forces $p \mid \mathcal{M}_{r,\delta}$, contrary to hypothesis. Therefore, our assumption was false, and we conclude that

$$Q_b(\omega^s) \neq 0 \qquad (s = \delta - 1, \ldots, n-1).$$

This proves the corollary. ■

Remark 4.10. As noted in Remark 4.8, Theorem 4.7 does not hold for $\delta = 2$ without the additional hypothesis of $\gcd(b, r+1) = 1$. However, that additional assumption is all that is necessary even in the finite field setting. More formally, if $\delta = 2$, then $Q_b(Y) = Y^b - 1$ so its roots among the nth roots of unity are

$$\omega^0, \omega^{\frac{n}{\gcd(b,n)}}, \omega^{\frac{2n}{\gcd(b,n)}}, \ldots, \omega^{\frac{(\gcd(b,n)-1)n}{\gcd(b,n)}}.$$

There are exactly $\gcd(b, n)$ roots so we must impose $\gcd(b, r+1) = 1$.

Let $b \in \{1, \ldots, n-1\}$, $s \in \{1, \ldots, n-1\}$, and set $m = b - 1$. We claim, if $\gcd(b, n) = 1$, then

$$\operatorname{Res}(\Phi_n(X), h_m(1, X^s)) = 1.$$

Since

$$h_m(1, X^s) = 1 + X^s + \cdots + X^{ms} = 1 + X^s + \cdots + X^{(b-1)s},$$

and $\Phi_n(X)$ is monic with roots ζ_n^a for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have

$$\operatorname{Res}(\Phi_n(X), h_m(1, X^s)) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(1 + \zeta_n^{as} + \cdots + \zeta_n^{(b-1)as}\right).$$

Because $1 \leq s \leq n-1$, we have $\zeta_n^{as} \neq 1$, so

$$1 + \zeta_n^{as} + \cdots + \zeta_n^{(b-1)as} = \frac{1 - \zeta_n^{asb}}{1 - \zeta_n^{as}}.$$

Thus

$$\operatorname{Res}(\Phi_n(X), h_m(1, X^s)) = \frac{\prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}(1-\zeta_n^{asb})}{\prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}(1-\zeta_n^{as})}.$$

Since $\gcd(b, n) = 1$, multiplication by b permutes $(\mathbb{Z}/n\mathbb{Z})^\times$, so the numerator and denominator are equal. Therefore the resultant is 1 and it follows that $\mathcal{M}_{r,2} = 1$ so there are no characteristics p which we need to exclude.

In [14], the authors chose $r + 1$ to be prime which is stronger than necessary because with $r + 1$ prime, $\gcd(b, r + 1) = 1$ is immediate.

We now give an example of a pair of values r, δ for which there exists a prime characteristic p such that $Q_b(\omega^s) = 0$ for some $b \in \{\delta - 1, \dots, n - 1\}$ and some $s \in \{\delta - 1, \dots, n - 1\}$.

Example 2. Let $\delta = 3$ and $r = 9$. Then $n = 11$. Let $q = 23$ so $n \mid (q - 1)$ and let $\omega = 2$ be the primitive 11th root of unity in $\mathbb{F}_q$. Let $b = 4$ and $s = 5$.

By definition,

$$Q_4(Y) = Y^4 + v_1Y + v_0$$

and $Q_4(1) = Q_4(\omega) = 0$. Solving for v_1 and v_0, we obtain $Q_4(Y) = Y^4 + 8Y + 14$. Now substituting $\omega^5 = 2^5 = 9$, we get

$$Q_4(9) = 9^4 + 72 + 14 = 81^2 + 17 = 12^2 + 17 = 161 = 0 \in \mathbb{F}_{23}.$$

Hence, for characteristic $p = 23$, there exists $b \in \{\delta-1, \dots, n-1\}$ and $s \in \{\delta-1, \dots, n-1\}$ such that $Q_b(\omega^s) = 0$.

Now we show that 23 is the only such characteristic for these values of r and δ. We need to compute $\mathcal{M}_{9,3}$. Since $n = 11$ is prime, $\Phi_{11}(X) = X^{10} + X^9 + \cdots + 1$ and $A_{m,s}(X) = h_m(1, X, X^s)$ so by Corollary 2.27,

$$\operatorname{Res}(\Phi_n(X), A_{m,s}(X)) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(A_{m,s}(\zeta_n)\right).$$

Using SageMath, of the 81 pairs (m, s) with $0 \le m \le 8$ and $2 \le s \le 10$, 36 pairs had a resultant of 23 and the remaining 45 pairs had a resultant of 1. The 36 pairs are (m, s) for

$$m \in \{1, 2, 3, 5, 6, 7\}, \qquad s \in \{3, 4, 5, 7, 8, 9\}.$$

We will compute

$$\operatorname{Res}(\Phi_{11}(X), A_{2,5}(X)) = N_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}}\left(A_{2,5}(\zeta_{11})\right)$$

to show the computation for one of the 81 pairs with the others proceeding similarly.

Let $\zeta = \zeta_{11}$. Then

$$\alpha = A_{2,5}(\zeta) = 1 + \zeta + \zeta^2 + \zeta^5 + \zeta^6 + \zeta^{10} \in \mathbb{Q}(\zeta)$$

and

$$\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^\times = \{1, \dots, 10\}.$$

For each $a \in \{1, \ldots, 10\}$, the corresponding automorphism is $\sigma_a : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ where $\sigma_a(\zeta) = \zeta^a$ so the conjugates of α are exactly

$$\alpha_a := \sigma_a(\alpha) = A_{2,5}(\zeta^a) = 1 + \zeta^a + \zeta^{2a} + \zeta^{5a} + \zeta^{6a} + \zeta^{10a}.$$

Thus,

$$N_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}}\left(A_{2,5}(\zeta_{11})\right) = \prod_{a=1}^{10} \alpha_a = 23.$$

One could also see this by computing the minimal polynomial of α, $\prod_{a=1}^{10}(X - \alpha_a)$, and noting that the constant of this polynomial is exactly the norm.

4.2 Bound on the minimum distance of (r, δ) Quantum Tamo–Barg codes

We begin with a small lemma whose properties we will use when proving a bound on the minimum distance of the code.

Lemma 4.11. *Let $r \geq \delta \geq 2$, set $n = r + \delta - 1$, and define*

$$\psi(t) := (r - t)_+ \left(n - (\delta - 1)t\right)_+, \qquad y_+ := \max\{y, 0\}.$$

Then ψ is nonincreasing and convex on $[0, \infty)$.

Proof. Set

$$a := \delta - 1, \qquad T := \min\left\{r, \frac{n}{a}\right\}.$$

Then $\psi(t) > 0$ precisely for $0 \leq t < T$, and on this interval

$$\psi(t) = (r - t)(n - at) = rn - (n + ar)t + at^2.$$

Hence,

$$\psi'(t) = -(n + ar) + 2at, \qquad \psi''(t) = 2a > 0.$$

Thus, ψ' is strictly increasing on $[0, T)$, so ψ is convex on $[0, T)$.

For $t \geq T$, at least one of the two factors $(r - t)_+$ and $(n - at)_+$ is zero, so $\psi(t) = 0$. Thus, ψ is constant on $[T, \infty)$, and its right derivative at T is $\psi'_+(T) = 0$. We now check that the derivative does not jump downward at T. The left derivative is

$$\psi'_-(T) = -(n + ar) + 2aT.$$

There are two cases. If $T = r$, then $r \leq n/a$, equivalently $ar \leq n$. Hence,

$$\psi'_-(T) = \psi'_-(r) = -(n + ar) + 2ar = ar - n \leq 0.$$

If $T = n/a$, then $n/a \le r$, equivalently $n \le ar$. Hence,

$$\psi'_-(T) = \psi'_-\left(\frac{n}{a}\right) = -(n+ar) + 2n = n - ar \le 0.$$

Therefore, in both cases,

$$\psi'_-(T) \le 0 = \psi'_+(T)$$

so the derivative is nondecreasing through the clipping point. Since ψ' is increasing on $[0,T)$ and is equal to 0 on $[T,\infty)$, the derivative is nondecreasing on all of $[0,\infty)$. Therefore ψ is convex on $[0,\infty)$.

We now show that ψ is nonincreasing. Since ψ' is increasing on $[0,T)$ and $\psi'_-(T) \le 0$, we have $\psi'(t) \le 0$ for all $0 \le t < T$. For $t \ge T$, $\psi(t) = 0$ is constant. Hence ψ is nonincreasing on $[0,\infty)$. ■

Theorem 4.12. *Consider (r,δ)-QTB code $\mathcal{Q} = \mathrm{CSS}(C,C)$ defined in Definition 4.1. If $\delta \ge 3$, assume $\mathrm{char}(\mathbb{F}_q) \nmid \mathcal{M}_{r,\delta}$ or if $\delta = 2$, assume $r+1$ is prime. Then $\mathcal{Q}$ has distance at least*

$$\frac{q-1}{2}\left(\frac{1}{\delta-1} + \frac{r}{r+\delta-1} - \sqrt{\left(\frac{r}{r+\delta-1} - \frac{1}{\delta-1}\right)^2 + \frac{4r}{(\delta-1)(r+\delta-1)}\cdot\frac{\ell-1}{q-1}}\right). \tag{4.19}$$

Proof. Fix an arbitrary $\mathrm{ev}(f(X)) \in C \setminus C^\perp$. Since $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$ for

$$S = ([\ell] \setminus S_-) \cup ([q-1] \cap S_+)$$

we may write $f(X) = g(X) + h(X)$ where $g(X) \in \mathbb{F}_q[X]^{[\ell]\setminus(S_-\cup S_+)}$ and $h(X) \in \mathbb{F}_q[X]^{[q-1]\cap S_+}$. By Lemma 4.5, h is piecewise of degree at most $\delta-1$. Since $\mathrm{ev}(h) \in C^\perp$ and $\mathrm{ev}(f) \notin C^\perp$ we must have $g \neq 0$.

Let $n = r+\delta-1$. Choose integers $\Gamma_i = \{0,1,\ldots,\delta-2,i\}$ that are distinct modulo n so $i \in \{\delta-1,\ldots,n-1\}$. There are exactly r such Γ_is. Then for a fixed $\omega \in \Omega_n$, we construct the Vandermonde-type matrix

$$V_i = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{\delta-2} & \omega^i \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{\delta-2} & \omega^{(\delta-2)2} & \cdots & \omega^{(\delta-2)(\delta-2)} & \omega^{(\delta-2)i} \end{bmatrix}.$$

Clearly $\mathrm{rank}(V_i) = \delta-1$ so there is a nontrivial vector $v_i = (v_{i,0},\ldots,v_{i,\delta-2},v_{i,\delta-1})$ such that $V_i v_i = 0$. If $v_{i,\delta-1} = 0$, then the first $\delta-1$ columns of V_i would be linearly dependent, but the first $\delta-1$ columns of V_i form a Vandermonde matrix. Hence, $v_{i,\delta-1} \neq 0$ and by normalizing, we may assume $v_{i,\delta-1} = 1$. Consider the polynomial

$$Q_i(Y) = Y^i + \sum_{t=0}^{\delta-2} v_{i,t} Y^t.$$

By construction, $Q_i(\omega^\gamma) = 0$ for $\gamma = 0, \dots, \delta - 2$. Let $\alpha\Omega_n \in \mathbb{F}_q^*/\Omega_n$. For a coset element $x \in \alpha\Omega_n$,

$$\omega^{-i}(\omega^i x)^j + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}(\omega^t x)^j = x^j \left(\omega^{(j-1)i} + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{(j-1)t}\right) = x^j Q_i(\omega^{j-1}) = 0$$

for $j = 1, \dots, \delta - 1$. It follows, for all $x \in \mathbb{F}_q^*$,

$$\omega^{-i}h(\omega^i x) + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}h(\omega^t x) = 0.$$

Define

$$g_i^{(1)}(X) = \omega^{-i}g(\omega^i X) + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}g(\omega^t X).$$

Note that $\deg g_i^{(1)} \leq \deg g \leq \ell - 1$. Additionally, if $x \in \mathbb{F}_q^*$, is such that $f(\omega^\gamma x) = 0$ for all $\gamma \in \Gamma_i$, then

$$0 = \omega^{-i}f(\omega^i x) + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}f(\omega^t x) = g_i^{(1)}(x) + \omega^{-i}h(\omega^i x) + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}h(\omega^t x) = g_i^{(1)}(x).$$

Hence, any $x \in \mathbb{F}_q^*$ such that $f(\omega^\gamma x) = 0$ for all $\gamma \in \Gamma_i$, is a root of $g_i^{(1)}(X)$.

We define

$$G(X) = \prod_{i=\delta-1}^{n-1} g_i^{(1)}(X),$$

which has degree at most $r(\ell - 1)$. It remains to show that $G \neq 0$ for which it suffices to show that each $g_i^{(1)} \neq 0$. Fix $i \in \{\delta - 1, \dots, n - 1\}$. Writing $g(X) = \sum_{j \in [\ell] \setminus (S_- \cup S_+)} g_j X^j$, we see that

$$\begin{aligned} g_i^{(1)}(X) &= \sum_{j \in [\ell] \setminus (S_- \cup S_+)} g_j \left(\omega^{-i}(\omega^i X)^j + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}(\omega^t X)^j\right) \\ &= \sum_{j \in [\ell] \setminus (S_- \cup S_+)} g_j \left(\omega^{(j-1)i} + \sum_{t=0}^{\delta-2} v_{i,t}\omega^{(j-1)t}\right) X^j \\ &= \sum_{j \in [\ell] \setminus (S_- \cup S_+)} g_j Q_i(\omega^{j-1}) X^j. \end{aligned}$$

Since $j \notin S_+$, by Corollary 4.9 (and Remark 4.10 if $\delta = 2$), $Q_i(\omega^{j-1}) \neq 0$ so $g_i^{(1)}(X) \neq 0$. Since i was arbitrary, $G \neq 0$.

We now bound the number of roots of G in terms of the number of roots of f. Fix a coset $A = \alpha\Omega_n$ and let $|\mathrm{ev}(f)|_A$ denote the Hamming weight of the restriction of $\mathrm{ev}(f)$ to A. Let

$$N_A = |\{x \in A \mid f(x) = f(\omega x) = \cdots = f(\omega^{\delta-2}x) = 0\}|$$

so N_A counts the number of starting points of a consecutive block of $\delta-1$ zeros. For a fixed $x \in A$ which is counted by N_A, $g_i^{(1)}(x)$ vanishes precisely when $f(\omega^i x) = 0$. Each nonzero position blocks at most $\delta-1$ possible starts of a $(\delta-1)$-zero block so

$$N_A \geq (n-(\delta-1)|\mathrm{ev}(f)|_A)_+.$$

Now fix an $x \in A$ counted by N_A. Then

$$f(x) = f(\omega x) = \cdots = f(\omega^{\delta-2}x) = 0.$$

For an allowed value $i \in \{\delta-1, \ldots, n-1\}$, the polynomial $g_i^{(1)}$ vanishes at x whenever $f(\omega^i x) = 0$. Among the r allowed values of i, at least $(r-|\mathrm{ev}(f)|_A)_+$ satisfy this condition, since there are only $|\mathrm{ev}(f)|_A$ nonzero positions in the coset A. Therefore the total root multiplicity contribution from the coset A is at least

$$(r-|\mathrm{ev}(f)|_A)_+ N_A \geq (r-|\mathrm{ev}(f)|_A)_+(n-(\delta-1)|\mathrm{ev}(f)|_A)_+ = \psi(|\mathrm{ev}(f)|_A).$$

Summing over all cosets, we obtain

$$|\{\text{roots of } G \text{ in } \mathbb{F}_q^*, \text{ counted with multiplicity}\}| \geq \sum_{A \in \mathbb{F}_q^*/\Omega_n} \psi(|\mathrm{ev}(f)|_A).$$

By the convexity of ψ as proven in Lemma 4.11, Jensen's inequality gives

$$\sum_{A \in \mathbb{F}_q^*/\Omega_n} \psi(|\mathrm{ev}(f)|_A) \geq \frac{q-1}{n}\psi\left(\frac{n|\mathrm{ev}(f)|}{q-1}\right).$$

Since G is nonzero and $\deg G \leq r(\ell-1)$, we get

$$\frac{q-1}{n}\psi\left(\frac{n|\mathrm{ev}(f)|}{q-1}\right) \leq r(\ell-1) \iff \psi\left(\frac{n|\mathrm{ev}(f)|}{q-1}\right) \leq rn\frac{\ell-1}{q-1}.$$

By Lemma 4.11, the function ψ is nonincreasing on $[0,\infty)$. Moreover, on the interval where $\psi(t) > 0$, it is given by

$$\psi(t) = (r-t)(n-(\delta-1)t).$$

Let y be the smaller solution of

$$(r-y)(n-(\delta-1)y) = rn\frac{\ell-1}{q-1}.$$

Then $\psi(t) > rn\frac{\ell-1}{q-1}$ for $0 \leq t < y$, while $\psi(t) \leq rn\frac{\ell-1}{q-1}$ for $t \geq y$. Since

$$\psi\left(\frac{n|\mathrm{ev}(f)|}{q-1}\right) \leq rn\frac{\ell-1}{q-1},$$

we conclude that
$$\frac{n|\mathrm{ev}(f)|}{q-1} \geq y.$$
Let
$$\lambda := \frac{\ell - 1}{q-1}.$$
Solving the quadratic in terms of y, substituting, and rearranging gives
$$|\mathrm{ev}(f)| \geq \frac{q-1}{n} \cdot \frac{n + (\delta-1)r - \sqrt{(n+(\delta-1)r)^2 - 4(\delta-1)rn\left(1 - \frac{\ell-1}{q-1}\right)}}{2(\delta-1)}.$$
Simplifying, we obtain
$$|\mathrm{ev}(f)| \geq \frac{q-1}{2}\left(\frac{1}{\delta-1} + \frac{r}{n} - \sqrt{\left(\frac{r}{n} - \frac{1}{\delta-1}\right)^2 + \frac{4r}{(\delta-1)n} \cdot \frac{\ell-1}{q-1}}\right)$$
and substituting $n = r + \delta - 1$ gives (4.19), as desired. ■

We make some important remarks regarding the relation of (4.19) to the bound presented in [14, Theorem 62] and illustrate the necessity of Theorem 4.7 and Corollary 4.9.

Remark 4.13. Setting $\delta = 2$ in (4.19) and shifting $r + 1$ to r recovers the exact bound presented in [14, Theorem 62].

Remark 4.14. Since we require Corollary 4.9 and Remark 4.10 to hold for (r, δ), we must first fix δ, then r, and then compute $\mathcal{M}_{r,\delta}$. After which we choose q, a prime power such that $(r + \delta - 1) \mid (q-1)$ and $\mathrm{char}(\mathbb{F}_q) \nmid \mathcal{M}_{r,\delta}$. There are finitely many characteristics to exclude and, by Dirichlet's theorem on arithmetic progressions [7], there are infinitely many primes of the form $p \equiv 1 \pmod{r + \delta - 1}$. Hence, there are infinitely many prime powers q such that $(r + \delta - 1) \mid (q-1)$ and $\mathrm{char}(\mathbb{F}_q) \nmid \mathcal{M}_{r,\delta}$. In particular, one may take $q = p$ for infinitely many such primes.

Remark 4.15. There is a shorter proof of Corollary 4.9 in the case that $n = r + \delta - 1$ is prime and Corollary 2.31 holds over $\mathbb{F}_q$. Indeed, for
$$Q_b(Y) = Y^b + \sum_{t=0}^{\delta-2} v_t Y^t,$$
we have $|Q_b| \leq \delta$. Hence, by Corollary 2.31,
$$|\mathrm{ev}(Q_b)|_{\Omega_n} \geq n + 1 - \delta = r,$$
so the number of roots of Q_b in Ω_n is at most $n - r = \delta - 1$. Since Q_b was constructed to vanish at ω^t for $t = 0, \ldots, \delta - 2$ it follows that these are its only roots in Ω_n.

However, this argument is insufficient for our purposes for two reasons. First, it requires n to be prime, whereas Theorem 4.7 and Corollary 4.9 hold for arbitrary $n = r + \delta - 1$, outside finitely many characteristics. Second, the composite-order uncertainty principle from Corollary 2.30 is generally too weak to recover the same conclusion. Indeed, if $d_1 < d_2$ are the consecutive divisors of n such that $d_1 \leq |Q_b| \leq d_2$, then it yields only

$$|\mathrm{ev}(Q_b)|_{\Omega_n} \geq \frac{n}{d_1 d_2}\left(d_1 + d_2 - |Q_b|\right),$$

which in general does not imply that the number of roots of Q_b in Ω_n is at most $\delta - 1$.

This distinction becomes especially important in the hierarchical setting. In order to derive a distance bound which meaningfully utilizes each level, one would like to apply the analogue of Corollary 4.9 at each level l, with $n_l = r_l + \delta_l - 1$. Using Corollary 2.31 would, therefore, force one to assume that each n_l is prime, which is prohibitively restrictive. In particular, once n_1 is prime, the hierarchy necessarily collapses to one level. By contrast, Corollary 4.9 avoids any primality assumption on the n_l, and for this reason is better suited to the hierarchical constructions developed later.

We obtain the asymptotic distance of (r, δ) QTBs as an immediate corollary of Theorem 4.12:

Corollary 4.16. *Given $\delta \geq 2$, for every $r \geq \delta$ and every $0 < R < (r - \delta + 1)/(r + \delta - 1)$, there exists an explicit family of QLRCs of locality (r, δ) and rate $\geq R$, and relative distance at least*

$$\frac{1}{2}\left(\frac{1}{\delta - 1} + \frac{r}{r + \delta - 1} - \sqrt{\left(\frac{r}{r+\delta-1} - \frac{1}{\delta-1}\right)^2 + \frac{2r}{(\delta-1)(r+\delta-1)}\left(1 + R\frac{r+\delta-1}{r-\delta+1}\right)}\right). \tag{4.20}$$

Proof. By Lemma 4.4, the dimension of $\mathcal{Q}$ is

$$k = 1 + (2\ell - q)\left(1 - \frac{2(\delta-1)}{r+\delta-1}\right) + \epsilon$$

for some $\epsilon \in [-2(\delta - 1), 2(\delta - 1)]$. Let $k = R(q - 1)$. Then

$$\frac{R(q-1) - 1 - \epsilon}{1 - \frac{2(\delta-1)}{r+\delta-1}} = 2\ell - 2 - q + 2 = 2(\ell - 1) - (q - 2).$$

Dividing by $(q - 1)$,

$$\frac{R - \frac{1+\epsilon}{q-1}}{1 - \frac{2(\delta-1)}{r+\delta-1}} = 2\left(\frac{\ell-1}{q-1}\right) - \frac{q-2}{q-1} \implies \frac{\ell-1}{q-1} = \frac{\frac{q-2}{q-1} + \frac{R - \frac{1+\epsilon}{q-1}}{1 - \frac{2(\delta-1)}{r+\delta-1}}}{2}$$

and

$$\begin{aligned}\frac{\ell-1}{q-1} &= \frac{\frac{q-2}{q-1}+\frac{R-\frac{1+\epsilon}{q-1}}{1-\frac{2(\delta-1)}{r+\delta-1}}}{2} \\ &= \frac{1}{2}-\frac{1}{2(q-1)}\left(1+(1+\epsilon)\frac{r+\delta-1}{r-\delta+1}\right)+\frac{R}{2}\cdot\frac{r+\delta-1}{r-\delta+1}. \end{aligned} \tag{4.21}$$

Hence, the relative distance is at least

$$\frac{1}{2}\Bigg(\frac{1}{\delta-1}+\frac{r}{r+\delta-1} \\ -\sqrt{\left(\frac{r}{r+\delta-1}-\frac{1}{\delta-1}\right)^2+\frac{2r}{(\delta-1)(r+\delta-1)}\cdot\left(1+R\frac{r+\delta-1}{r-\delta+1}\right)}\Bigg)$$

as $q\to\infty$. ■

Note that for fixed $\delta \geq 2$, as $r\to\infty$, (4.20) tends to

$$\frac{1}{2}\left(1+\frac{1}{\delta-1}-\sqrt{\left(1-\frac{1}{\delta-1}\right)^2+\frac{2(1+R)}{\delta-1}}\right)=\frac{1}{2}\left(\frac{\delta}{\delta-1}-\sqrt{\left(\frac{\delta-2}{\delta-1}\right)^2+\frac{2(1+R)}{\delta-1}}\right).$$

4.3 Non-vanishing of complete homogeneous symmetric polynomial

In this section, we present the technical lemma used to conclude the non-vanishing of Q_b in Theorem 4.7.

Lemma 4.17. *Let $d \geq 3$ and let $n \geq 2d-1$. Let $\zeta \in \mathbb{C}$ be a primitive nth root of unity and write $h_t(x_1,\ldots,x_d)$ for the complete homogeneous symmetric polynomial of degree t in d variables. Then, for every $0 \leq t \leq n-d$ and $d-1 \leq s \leq n-1$, we have*

$$h_t(1,\zeta,\ldots,\zeta^{d-2},\zeta^s)\neq 0.$$

Proof. It suffices to prove the result for $\zeta = e^{2\pi i/n}$ as any other primitive nth root of unity is obtained from this one by a Galois automorphism of $\mathbb{Q}(\zeta)$, and such automorphisms preserve non-vanishing.

Set $W=(1,\zeta,\ldots,\zeta^{\delta-2})$ and fix $s\in\{d-1,\ldots,n-1\}$. Define

$$F_s(T)=\sum_{j\geq 0}h_j(W,\zeta^s)T^j.$$

Using the generating function for complete homogeneous symmetric polynomials and the identity

$$\prod_{j=0}^{n-1}(1-\zeta^j T) = 1 - T^n,$$

we get

$$F_s(T) = \frac{1}{(1-\zeta^s T)\prod_{u=0}^{d-2}(1-\zeta^u T)} = \frac{\prod_{\substack{u=d-1 \\ u\neq s}}^{n-1}(1-\zeta^u T)}{1-T^n}$$

The numerator has degree $(n-1)-(d-2)-1 = n-d < n$. Hence, for every $0 \le j \le n-d$, the coefficient of T^j is unaffected by the factor $(1-T^n)^{-1}$, and therefore

$$h_j(W,\zeta^s) = [T^j] \prod_{\substack{u=d-1 \\ u\neq s}}^{n-1}(1-\zeta^u T).$$

Writing

$$\prod_{\substack{u=d-1 \\ u\neq s}}^{n-1}(1-\zeta^u T) = \sum_{j=0}^{n-d} c_j(s) T^j,$$

it follows that $c_j(s) = h_j(W,\zeta^s)$.

We next record a symmetry of the coefficients $c_j(s)$. Let $\Lambda_s = (\zeta^{d-1},\ldots,\widehat{\zeta^s},\ldots,\zeta^{n-1})$ be the vector of length $n-d$ comprised of the consecutive roots $\zeta^{d-1},\ldots,\zeta^{n-1}$, but excluding ζ^s. Since

$$\prod_{\lambda\in\Lambda_s}(1-\lambda T) = \sum_{j=0}^{n-d}(-1)^j e_j(\Lambda_s) T^j,$$

we have

$$c_j(s) = (-1)^j e_j(\Lambda_s)$$

where e_j is the elementary symmetric polynomial. Because every $\lambda \in \Lambda_s$ satisfies $|\lambda| = 1$, we have $\lambda^{-1} = \overline{\lambda}$, and hence

$$e_{n-d-j}(\Lambda_s) = e_{n-d}(\Lambda_s)\, e_j(\Lambda_s^{-1}) = e_{n-d}(\Lambda_s)\, \overline{e_j(\Lambda_s)}.$$

Therefore

$$c_{n-d-j}(s) = (-1)^{n-d-j} e_{n-d-j}(\Lambda_s) = (-1)^{n-d} e_{n-d}(\Lambda_s)\, \overline{c_j(s)}.$$

In particular,

$$c_{n-d-j}(s) = 0 \iff c_j(s) = 0$$

because

$$e_{n-d}(\Lambda_s) = \prod_{\lambda \in \Lambda_s} \lambda = \prod_{\substack{u=d-1 \\ u \neq s}}^{n-1} \zeta^u = \zeta^{\sum_{u=d-1, u\neq s}^{n-1} u} \neq 0.$$

Since $c_j(s) = h_j(W, \zeta^s)$, it follows that

$$h_{n-d-j}(W, \zeta^s) = 0 \iff h_j(W, \zeta^s) = 0.$$

Thus, it suffices to prove that the polynomial $h_t(W, \zeta^s) \neq 0$ for

$$0 \leq t \leq \left\lfloor \frac{n-d}{2} \right\rfloor.$$

Fix such a t. If $t = 0$, then $h_0(W, \zeta^s) = 1$ so there is nothing to prove. Hence, assume $t \geq 1$ and consider the polynomial

$$f_t(Y) := h_t(W, Y) = h_t(1, \zeta, \ldots, \zeta^{d-2}, Y).$$

By the defining recurrence for complete homogeneous symmetric polynomials,

$$f_t(Y) = \sum_{u=0}^{t} h_{t-u}(W)\, Y^u.$$

Additionally, by definition

$$h_j(W) = h_j(1, \ldots, \zeta^{d-2}) = \sum_{a_0 + \cdots + a_{d-2} = j} (1)^{a_0} (\zeta)^{a_1} \cdots (\zeta^{d-2})^{a_{d-2}},$$

but we can also interpret this combinatorially. We have $d-1$ objects, labeled $0, \ldots, d-2$ and we choose a_0 copies of 0, a_1 copies of 1, …, a_{d-2} copies of $d-2$ so in total we have

$$j = a_0 + a_1 + \cdots + a_{d-2}$$

objects. Hence, we have j objects each of size at most $d-2$ and this is the standard interpretation of the Gaussian binomial

$$\binom{j+d-2}{j}_\zeta.$$

Now we can simplify the Gaussian binomial by substituting $\zeta = e^{2\pi i/n}$:

$$\begin{aligned} \binom{j+d-2}{j}_\zeta &= \prod_{k=1}^{j} \frac{1-\zeta^{d-2+k}}{1-\zeta^k} \\ &= \prod_{k=1}^{j} \frac{1-(e^{2\pi i/n})^{d-2+k}}{1-(e^{2\pi i/n})^k} \end{aligned}$$

$$
\begin{aligned}
&= \zeta^{\frac{j(d-2)}{2}} \prod_{k=1}^{j} \frac{\sin\left(\frac{\pi(d-2+k)}{n}\right)}{\sin\left(\frac{\pi k}{n}\right)} \\
&= \zeta^{\frac{j(d-2)}{2}} \frac{\prod_{k=d-1}^{d-2+j} \sin\left(\frac{\pi k}{n}\right)}{\prod_{k=1}^{j} \sin\left(\frac{\pi k}{n}\right)} \\
&= \zeta^{\frac{j(d-2)}{2}} \frac{\prod_{k=1}^{d-2+j} \sin\left(\frac{\pi k}{n}\right)}{\prod_{k=1}^{j} \sin\left(\frac{\pi k}{n}\right) \prod_{k=1}^{d-2} \sin\left(\frac{\pi k}{n}\right)} \\
&= \zeta^{\frac{j(d-2)}{2}} \prod_{k=1}^{d-2} \frac{\sin\left(\frac{\pi(j+k)}{n}\right)}{\sin\left(\frac{\pi k}{n}\right)}
\end{aligned}
$$

and get

$$h_j(W) = \zeta^{\frac{j(d-2)}{2}} \rho_j$$

for

$$\rho_j = \prod_{k=1}^{d-2} \frac{\sin\left(\frac{\pi(j+k)}{n}\right)}{\sin\left(\frac{\pi k}{n}\right)}.$$

The coefficient $\rho_j > 0$ because $0 \le j \le n-d$ and $1 \le j+k \le n-d+d-2 \le n-2$ so both sine terms in each fraction are positive.

Substituting this expression into $f_t(Y)$ gives

$$f_t(Y) = \sum_{u=0}^{t} h_{t-u}(W)\, Y^u = \sum_{u=0}^{m} \zeta^{\frac{(t-u)(d-2)}{2}} \rho_{t-u}\, Y^u = \zeta^{\frac{t(d-2)}{2}} \rho_t \sum_{u=0}^{m} \zeta^{\frac{-u(d-2)}{2}} \frac{\rho_{t-u}}{\rho_t}\, Y^u.$$

Let

$$P_t(z) := \sum_{u=0}^{t} p_u z^u, \qquad p_u := \frac{\rho_{t-u}}{\rho_t}$$

so

$$f_t(Y) = \zeta^{\frac{t(d-2)}{2}} \rho_t P_t(\zeta^{-\frac{d-2}{2}} Y).$$

Thus the zeros of $f_t(x)$ are exactly the zeros of $P_t(z)$, rotated by the unit scalar $\zeta^{(d-2)/2}$.

We now show that the coefficients of P_t are strictly decreasing positive reals. Indeed,

$$\frac{\rho_{j+1}}{\rho_j} = \frac{\sin\left(\frac{\pi(j+d-1)}{n}\right)}{\sin\left(\frac{\pi(j+1)}{n}\right)}$$

by telescoping. If $0 \le j \le t-1$, then

$$2j + d \le 2t + d - 2$$

and since $t \le \lfloor (n-d)/2 \rfloor$, we have

$$2t + d - 2 \le n - 2 < n.$$

Therefore,

$$0 < \frac{(2j+d)\pi}{2n} < \frac{\pi}{2},$$

and using

$$\sin A - \sin B = 2\cos\left(\frac{A+B}{2}\right)\sin\left(\frac{A-B}{2}\right),$$

with

$$A = \frac{\pi(j+d-1)}{n}, \qquad B = \frac{\pi(j+1)}{n},$$

we obtain

$$\sin\left(\frac{\pi(j+d-1)}{n}\right) - \sin\left(\frac{\pi(j+1)}{n}\right) = 2\cos\left(\frac{\pi(2j+d)}{2n}\right)\sin\left(\frac{\pi(d-2)}{2n}\right) > 0.$$

Hence, $\rho_{j+1} > \rho_j$ for $0 \le j \le t-1$. It follows that

$$\rho_t > \rho_{t-1} > \cdots > \rho_0 > 0$$

and dividing by ρ_t, since $p_u = \rho_{t-u}/\rho_t$, we obtain

$$1 = p_0 > p_1 > \cdots > p_t > 0.$$

Now apply the Eneström–Kakeya theorem [11, Theorem 4] to $P_t(z)$. Since every p_u is a positive real and $1 = p_0 > p_1 > \cdots > p_t > 0$, every zero z^* of P_t satisfies

$$|z^*| \ge \min_{0\le u\le t-1} \frac{p_u}{p_{u+1}} = \min_{0\le u\le t-1} \frac{\rho_{t-u}}{\rho_{t-(u+1)}} = \min_{1\le u\le t} \frac{\rho_u}{\rho_{u-1}} > 1.$$

Thus every zero of P_t lies strictly outside the unit disk. Since

$$f_t(Y) = \zeta^{\frac{t(d-2)}{2}} \rho_t P_t(\zeta^{-\frac{d-2}{2}} Y)$$

the same is true for $f_t(Y)$: if z^* is a zero of P_m, then $\zeta^{(d-2)/2} z^*$ is a zero of f_m and

$$|\zeta^{(d-2)/2} z^*| = |\zeta|^{\frac{d-2}{2}} |z^*| = |z^*| > 1.$$

Since $|\zeta^s| = 1$, ζ^s cannot be a zero of f_m. Hence

$$h_t(W, \zeta^s) = f_t(\zeta^s) \ne 0$$

for $0 \le m \le \lfloor (n-d)/2 \rfloor$ and $d-1 \le s \le n-1$. By the symmetry

$$h_{n-d-t}(W, \zeta^s) \ne 0 \iff h_t(W, \zeta^s) \ne 0,$$

for $0 \le t \le \lfloor (n-d)/2 \rfloor$, this extends to all $0 \le t \le n-d$. Therefore, $h_t(W, \zeta^s) \ne 0$ for $0 \le t \le n-d$ and $d-1 \le s \le n-1$. Since

$$h_{n-d+t}(1, \zeta, \ldots, \zeta^{d-2}, \zeta^s) = h_t(W, \zeta^s)$$

we conclude $h_{n-d+t}(1, \zeta, \ldots, \zeta^{d-2}, \zeta^s) \ne 0$, as desired. ■

Remark 4.18. Lemma 4.17 is not true if $d = 2$. Let $d = 2$ and suppose $n = 6$ and $t = 2$. Then,

$$h_2(1, \zeta^s) = 1 + \zeta^s + \zeta^{2s} = \frac{\zeta^{3s} - 1}{\zeta^s - 1}$$

and for $s = 2$, this quantity is zero.

The proof particularly breaks when we define ρ_j. For $d = 2$, all $\rho_j = 1$ so all $p_u = 1$ and $P_t(z) = 1 + z + \cdots + z^t$. Since, all the coefficients of P_t are equal to 1, every root of P_t has modulus 1 by Eneström-Kakeya. In our setting, all the roots of P_t are the nontrivial $(t+1)$th roots of unity. Therefore, if s is chosen such that $n \mid s(t+1)$, ζ^s is a root.

In the case of $d = 2$, if we strengthen the hypothesis of Lemma 4.17 to choosing t such that $\gcd(t + 1, n) = 1$, then the claim will follow.

Chapter 5

Hierarchical Quantum Tamo–Barg Codes

We extend the work in Chapter 4 to the hierarchical setting by modifying the underlying classical Tamo–Barg code and endowing it with hierarchical structure.

We now extend the (r, δ) quantum Tamo–Barg code to an h-level quantum hierarchical LRC. Let $r_l, \delta_l \in \mathbb{Z}^+$ for $l = 1, \ldots, h$. Consider the following sets

$$S_{l,+} = \bigcup_{j_l=1}^{\delta_l - 1} (j_l + (r_l + \delta_l - 1)\mathbb{Z})$$
$$S_{l,-} = \bigcup_{j_l=1}^{\delta_l - 1} (-j_l + (r_l + \delta_l - 1)\mathbb{Z})$$

and define

$$S_+ = \bigcup_{l=1}^{h} S_{l,+} \quad \text{and} \quad S_- = \bigcup_{l=1}^{h} S_{l,-}.$$

Definition 5.1 (h-level quantum Tamo–Barg code)**.** Given a prime p and $m \in \mathbb{Z}^+$, let $q = p^m$. Given locality and distance parameters $(r_l, \delta_l)_{l=1,\ldots,h}$ such that

$$r_1 \geq \cdots \geq r_h \geq \delta_1 \geq \cdots \geq \delta_h \geq 2$$

and $n_h \mid n_{h-1} \mid \cdots \mid n_1 \mid (q-1)$ where $n_l := r_l + \delta_l - 1$, and an integer $\ell \in [q]$, the h-level quantum Tamo–Barg code is defined to be the CSS code $\mathcal{Q} = \mathrm{CSS}(C, C)$ with $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$ for

$$S = ([\ell] \cap ([q-1] \setminus S_-)) \cup ([q-1] \cap S_+). \tag{5.1}$$

An immediate consequence from the definition of the sets $S_{l,+}$ and $S_{l,-}$ and Definition 5.1 is the disjointness of the sets.

Lemma 5.2. *Suppose we are given locality and distance parameters $(r_l, \delta_l)_{l=1,\ldots,h}$ such that*

$$r_1 \geq \cdots \geq r_h \geq \delta_1 \geq \cdots \geq \delta_h \geq 2$$

and $r_{l+1} + \delta_{l+1} - 1 \mid r_l + \delta_l - 1$ for $l = 1, \ldots, h-1$ and $r_1 + \delta_1 - 1 \mid q - 1$. Then for $1 \leq u \leq v \leq h$, $S_{u,+} \cap S_{v,-} = \emptyset = S_{u,-} \cap S_{v,+}$.

Proof. We break the proof into cases.

1. Suppose $u = v$. $|S_{u,+}| = |S_{u,-}| = \delta_u - 1$. Since

$$2(\delta_u - 1) < r_u + \delta_u - 1 \iff \delta_u - 1 < r_u$$

is satisfied by hypothesis, $S_{u,+} \cap S_{u,-} = \emptyset$.

2. Suppose $u < v$. By hypothesis, $r_u \geq r_v \geq \delta_u \geq \delta_v$ and $r_v + \delta_v - 1 \mid r_u + \delta_u - 1$. Fix $s \in S_{v,-}$ so $s \equiv -j_v \mod (r_v + \delta_v - 1)$. For the sake of contradiction, suppose $s \in S_{u,+}$. Then $s \equiv j_u \mod (r_u + \delta_u - 1)$. Since $r_v + \delta_v - 1 \mid r_u + \delta_u - 1$, $s \equiv j_u \mod r_v + \delta_v - 1$. Hence, $r_v + \delta_v - 1 \mid j_u + j_v$ and $j_u + j_v \geq 2$ so $j_u + j_v$ is a nonzero multiple of $r_v + \delta_v - 1$. However, $j_u + j_v \leq \delta_u + \delta_v - 2$ and

$$\delta_u + \delta_v - 2 < r_v + \delta_v - 1 \iff \delta_u - 1 < r_v \iff \delta_u \leq r_v$$

which is a contradiction.

Now fix $s \in S_{v,+}$ and suppose for the sake of contradiction that $s \in S_{u,-}$. By similar reasoning, $s \equiv j_v \mod (r_v + \delta_v - 1)$ and $s \equiv -j_u \mod (r_v + \delta_v - 1)$. Again $r_v + \delta_v - 1 \mid j_u + j_v$ so we have a contradiction.

Thus, $1 \leq u \leq v \leq h$, $S_{u,+} \cap S_{v,-} = \emptyset = S_{u,-} \cap S_{v,+}$. ■

We now present the hierarchical analogue of Lemma 4.3. For $l = 1, \ldots, h$, define

$$B_l := \mathrm{ev}(\mathbb{F}_q[X]^{[q-1] \setminus S_{l,-}}), \qquad B_l^\perp := \mathrm{ev}(\mathbb{F}_q[X]^{[q-1] \cap S_{l,+}}).$$

Then

$$B = \bigcap_{l=1}^{h} B_l = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1] \setminus S_-}).$$

Moreover, since the dual of an intersection is the sum of the duals,

$$B^\perp = \left(\bigcap_{l=1}^{h} B_l \right)^\perp = \sum_{l=1}^{h} B_l^\perp.$$

Equivalently, because the spaces $B_l^\perp$ are monomial evaluation spaces,

$$B^\perp = \sum_{l=1}^{h} \mathrm{ev}(\mathbb{F}_q[X]^{[q-1] \cap S_{l,+}}) = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1] \cap S_+}).$$

Lemma 5.3. *For $q, (r_l, \delta_l)_{l=1,\dots,h}$, and ℓ as defined in Definition 5.1 let*

$$A = \mathrm{ev}(\mathbb{F}_q[X]^{[\ell]}), \tag{5.2}$$

$$B = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\setminus S_-}). \tag{5.3}$$

Then $A \cap B$ is an h-level TB code. Furthermore,

$$A^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-\ell]\setminus\{0\}}) \text{ and} \tag{5.4}$$

$$B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+}) \subseteq B. \tag{5.5}$$

If $\ell \geq q/2$, then $A^\perp \subseteq A$. Letting $C = (A \cap B) + B^\perp$, we obtain that $\mathrm{CSS}(C, C)$ is an h-level QTB code with

$$C^\perp = (A^\perp \cap B) + B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^T) \subseteq C \tag{5.6}$$

where

$$T = (([q-\ell] \setminus \{0\}) \cap ([q-1] \setminus S_-)) \cup ([q-1] \cap S_+). \tag{5.7}$$

Proof. It suffices to show $B^\perp \subseteq B$ because the remaining claims follow from Lemma 4.3. By Lemma 5.2, we have $S_{u,+} \cap S_{v,-} = \emptyset$ for all $1 \leq u, v \leq h$. Hence $S_+ \cap S_- = \emptyset$. Thus every exponent in $[q-1] \cap S_+$ lies in $[q-1] \setminus S_-$, and so

$$B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+}) \subseteq \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\setminus S_-}) = B.$$

■

We now compute the dimension of the h-level quantum Tamo–Barg code defined in Definition 5.1.

Lemma 5.4. *The h-level quantum Tamo–Barg code $\mathcal{Q} = \mathrm{CSS}(C, C)$ with parameters q, ℓ, $(r_l, \delta_l)_{l=1,\dots,h}$ as defined in Definition 5.1 has dimension*

$$\begin{aligned} k &= 1 + |\{q-\ell \leq i \leq \ell-1 : i \notin (S_+ \cup S_-)\}| \\ &= 1 + (2\ell - q)\left(1 - 2\sum_{l=1}^{h-1} \frac{\delta_l - \delta_{l+1}}{r_l + \delta_l - 1} - 2\frac{\delta_h - 1}{r_h + \delta_h - 1}\right) + \epsilon \end{aligned}$$

for some

$$\epsilon \in \left[-2\sum_{l=1}^{h-1}(\delta_l - \delta_{l+1}) - 2(\delta_h - 1), 2\sum_{l=1}^{h-1}(\delta_l - \delta_{l+1}) + 2(\delta_h - 1)\right].$$

Proof. We use a similar counting argument as in the proof of Lemma 4.4. Recall $S \subseteq [q-1]$ as defined in Definition 5.1, $T \subseteq S$ as defined in Lemma 5.3 such that $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$ and $C^\perp = \mathrm{ev}(\mathbb{F}_q[X]^T)$. Then, dimension of $\mathcal{Q}$ can be computed as follows:

$$\begin{aligned} \dim(\mathcal{Q}) &= \dim(C) - \dim(C^\perp) \\ &= |S \setminus T| \end{aligned}$$

$$= |\{0\} \cup \{q-\ell \le i \le \ell-1 : i \notin (S_+ \cup S_-)\}| \,.$$

which proves the first equality. For the second equality, we inspect

$$\{q-\ell \le i \le \ell-1 : i \notin (S_+ \cup S_-)\}.$$

If $(r_1+\delta_1-1) \mid (2\ell-q)$ then this set has size exactly

$$(2\ell-q)\left(1-2\sum_{l=1}^{h-1}\frac{\delta_l-\delta_{l+1}}{r_l+\delta_l-1}-2\frac{\delta_h-1}{r_h+\delta_h-1}\right)$$

because we exclude $2(\delta_h-1)$ elements in every block of size $(r_h+\delta_h-1)$ and as we move up the layers, we exclude another $2(\delta_l-\delta_{l+1})$ elements in every block of size of $(r_l+\delta_l-1)$ for $l=1,\ldots,h-1$. Note, this exclusion will leave a nontrivial number of elements precisely because

$$2(\delta_h-1) < r_h+\delta_h-1 \iff \delta_h-1 < r_h \iff \delta_h \le r_h$$

and

$$2(\delta_l-\delta_{l+1}) < r_l+\delta_l-1 \iff (\delta_l-1)-2(\delta_{l+1}-1) < r_l \iff \delta_l \le r_l+2(\delta_{l+1}-1)$$

which is satisfied by the assumption on $(r_l,\delta_l)_{l=1,\ldots,h}$. If $(r_1+\delta_1-1)\nmid(2\ell-q)$, we differ from

$$(2\ell-q)\left(1-2\sum_{l=1}^{h-1}\frac{\delta_l-\delta_{l+1}}{r_l+\delta_l-1}-2\frac{\delta_h-1}{r_h+\delta_h-1}\right)$$

by at most $2\sum_{l=1}^{h-1}(\delta_l-\delta_{l+1})+2(\delta_h-1)$ in absolute value and the second equality follows. ■

We give a small example to illustrate the sizes of $[q-1]\cap S_+$ and $[q-1]\cap S_-$ which appear in the proof of Lemma 5.4.

Example 3. Let $q=49$ and let $(21,4),(10,3),(5,2)$ be the locality and distance parameters. It is easy to see that

$$r_1 \ge r_2 \ge r_3 \ge \delta_1 \ge \delta_2 \ge \delta_3 \ge 2$$

and

$$\begin{aligned} r_3+\delta_3-1 &= 6\\ r_2+\delta_2-1 &= 12\\ r_1+\delta_1-1 &= 24\end{aligned}$$

so the divisibility condition follows. Now we compute $[q-1]\cap S_+$ and $[q-1]\cap S_-$. The constituent sets are

$$[q-1]\cap S_{1,-} = \bigcup_{j_1=1}^{3}(-j_1+24\mathbb{Z}) = \{21,\underline{22,\boxed{23}},45,\underline{46,\boxed{47}}\}$$

$$[q-1] \cap S_{1,+} = \bigcup_{j_1=1}^{3} (j_1 + 24\mathbb{Z}) = \{\underline{\boxed{1}, 2}, 3, \underline{\boxed{25}, 26}, 27\}$$

$$[q-1] \cap S_{2,-} = \bigcup_{j_2=1}^{2} (-j_2 + 12\mathbb{Z}) = \{10, \boxed{11}, \underline{22, \boxed{23}}, 34, \boxed{35}, \underline{46, \boxed{47}}\}$$

$$[q-1] \cap S_{2,+} = \bigcup_{j_2=1}^{2} (j_2 + 12\mathbb{Z}) = \{\underline{\boxed{1}, 2}, \boxed{13}, 14, \underline{\boxed{25}, 26}, \boxed{37}, 38\}$$

$$[q-1] \cap S_{3,-} = \bigcup_{j_3=1}^{1} (-j_3 + 6\mathbb{Z}) = \{5, \boxed{11}, 17, \boxed{23}, 29, \boxed{35}, 41, \boxed{47}\}$$

$$[q-1] \cap S_{3,+} = \bigcup_{j_3=1}^{1} (j_3 + 6\mathbb{Z}) = \{\boxed{1}, 7, \boxed{13}, 19, \boxed{25}, 31, \boxed{37}, 43\}$$

so

$$|[q-1] \cap S_+| = \left| \bigcup_{l=1}^{3} [q-1] \cap S_{l,+} \right| = 2 + 4 + 8 = \frac{48}{24}(4-3) + \frac{48}{12}(3-2) + \frac{48}{6}(2-1)$$

and an analogous statement holds for $[q-1] \cap S_-$. Thus,

$$[q-1] \cap (S_- \cup S_+) = 2\left(\frac{\delta_1 - \delta_2}{r_1 + \delta_1 - 1} + \frac{\delta_2 - \delta_3}{r_2 + \delta_2 - 1} + \frac{\delta_3 - 1}{r_3 + \delta_3 - 1}\right).$$

This example effectively showcases why in level l, we only contribute an extra $(\delta_l - \delta_{l+1})$ elements per length $r_l + \delta_l - 1$ blocks as $\delta_{l+1} - 1$ of the $\delta_l - 1$ elements have already been accounted for from levels $l+1, \ldots, h$.

We now exhibit the hierarchical locality of the code $\mathcal{Q} = \mathrm{CSS}(C, C)$ as defined in Definition 5.1 by stating and proving statement similar to Lemma 4.5 and Corollary 4.6.

Lemma 5.5. *Let $B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+})$ be as in Lemma 5.3. If $f \in B^\perp$, then f can be written as*

$$f = f_1 + \cdots + f_h, \qquad f_l \in B_l^\perp.$$

For each level l, each $f_l \in B_l^\perp$ has the following local description: for every coset $\alpha\Omega_{n_l}$, there exists a polynomial $P_{\alpha,l}(X) \in \mathbb{F}_q[X]$ with

$$\deg P_{\alpha,l} \le \delta_l - 1, \qquad P_{\alpha,l}(0) = 0,$$

such that

$$f_l(\alpha\omega) = P_{\alpha,l}(\omega) \qquad \text{for all } \omega \in \Omega_{n_l}.$$

The converse is also true.

It follows immediately that each level l contributes at most $\delta_l - 1$ independent local parity checks per level-l coset. Additionally, this lemma reduces to Lemma 4.5 when $h = 1$.

Proof. By dimension counting, it suffices to show the forward direction.

($\implies$) The equality

$$B^\perp = \sum_{l=1}^{h} B_l^\perp$$

was shown in Lemma 5.3. Hence every $f \in B^\perp$ can be written as $f = f_1 + \cdots + f_h$ with $f_l \in B_l^\perp$.

The final statement is exactly the one-level description of $B_l^\perp$ from Lemma 4.5, applied with parameters (r_l, δ_l) and $n_l = r_l + \delta_l - 1$. ∎

Corollary 5.6. *The h-level $(r_l, \delta_l)_{l=1,\dots,h}$ quantum Tamo–Barg code in Definition 5.1 is an h-level $((r_1, \delta_1), \dots, (r_h, \delta_h))$-QHLRC.*

Proof. Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be the code from Definition 5.1, and for each l write $n_l := r_l + \delta_l - 1$.

We prove by induction on l that for every level-$(l-1)$ repair group A_{l-1}, the punctured code $\mathcal{Q}|_{A_{l-1}}$ is an $(h-l+1)$-level $((r_l, \delta_l), \dots, (r_h, \delta_h))$-QHLRC. Here, for $l = 1$, we interpret $A_0 = \{1, \dots, q-1\}$ and $\mathcal{Q}|_{A_0} = \mathcal{Q}$.

Base step: $l = h$**.** Fix a level-$(h-1)$ repair group A_{h-1}. Inside A_{h-1}, the level-h repair groups are precisely the cosets $A_h = \alpha\Omega_{n_h} \subseteq A_{h-1}$.

By Lemma 5.3, we have $C^\perp \supseteq B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+})$, and by Lemma 5.5, for each $j = 1, \dots, \delta_h - 1$, the code $B_h^\perp \subseteq B^\perp$ contains the function

$$f_{\alpha,h,j}(x) = \begin{cases} x^j, & x \in A_h, \\ 0, & x \notin A_h. \end{cases}$$

Restricting to the coordinates in A_h, these give $\delta_h - 1$ checks in $(C|_{A_h})^\perp$. Writing $A_h = \{x_1, \dots, x_{n_h}\}$, we obtain a Vandermonde-type matrix

$$H_{A_h} = \begin{bmatrix} x_1 & x_2 & \cdots & x_{n_h} \\ x_1^2 & x_2^2 & \cdots & x_{n_h}^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\delta_h-1} & x_2^{\delta_h-1} & \cdots & x_{n_h}^{\delta_h-1} \end{bmatrix}.$$

After scaling the ith column by x_i^{-1}, this becomes a Vandermonde matrix, so any $\delta_h - 1$ columns are linearly independent. Hence, $d(C|_{A_h}) \geq \delta_h$ and

$$d(C|_{A_{h-1}}^\perp) \geq d(C|_{A_{h-1}}) \geq d((C|_{A_{h-1}})|_{A_h}) = d(C|_{A_h}) \geq \delta_h.$$

Therefore, by Theorem 3.3, $\mathcal{Q}|_{A_{h-1}} = \mathrm{CSS}(C|_{A_{h-1}}, C|_{A_{h-1}})$ is an (r_h, δ_h)-QLRC. This proves the base case.

Induction step. Assume $1 \le l < h$, and assume that for every level-l repair group A_l, the punctured code $\mathcal{Q}|_{A_l}$ is an $(h-l)$-level $((r_{l+1}, \delta_{l+1}), \ldots, (r_h, \delta_h))$-QHLRC.

Now fix a level-$(l-1)$ repair group A_{l-1}. Inside A_{l-1}, the level-l repair groups are the cosets $A_l = \alpha\Omega_{n_l} \subseteq A_{l-1}$. By Lemma 5.5, for each such A_l and each $j = 1, \ldots, \delta_l - 1$, the code $B_l^\perp \subseteq B^\perp \subseteq C^\perp$ contains the function

$$f_{\alpha,l,j}(x) = \begin{cases} x^j, & x \in A_l, \\ 0, & x \notin A_l. \end{cases}$$

Restricting to A_l, these give $\delta_l - 1$ checks in $(C|_{A_l})^\perp$. As in the base case, their parity-check matrix is Vandermonde after column scaling, so any $\delta_l - 1$ columns are linearly independent and therefore $d(C|_{A_l}) \ge \delta_l$. By the same reasoning as before $d(C|_{A_{l-1}}^\perp) \ge \delta_l$ so by Theorem 3.3, $\mathcal{Q}|_{A_{l-1}}$ is an (r_l, δ_l)-QLRC.

Moreover, by the induction hypothesis, for every such level-l repair group A_l, the punctured code $\mathcal{Q}|_{A_l}$ is an $(h-l)$-level $((r_{l+1}, \delta_{l+1}), \ldots, (r_h, \delta_h))$-QHLRC. Therefore, $\mathcal{Q}|_{A_{l-1}}$ satisfies the two conditions of Definition 3.5 with top-level locality parameters (r_l, δ_l). Hence, $\mathcal{Q}|_{A_{l-1}}$ is an $(h-l+1)$-level $((r_l, \delta_l), \ldots, (r_h, \delta_h))$-QHLRC.

Finally, taking $l = 1$ and $A_0 = \{1, \ldots, q-1\}$, we conclude that $\mathcal{Q}$ is indeed an h-level $((r_1, \delta_1), \ldots, (r_h, \delta_h))$-QHLRC. ■

5.1 Bound on the minimum distance of hierarchical Quantum Tamo–Barg codes

We finish our analysis of the quantum Tamo–Barg HLRC by proving a distance bound using Theorem 4.12. For clarity, we will first derive a distance bound for the case $h = 2$. The general h derivation will naturally follow, but the notation will become quite heavy. Recall Lemma 4.11 whose properties we will use repeatedly in the distance proofs.

Lemma 4.11. *Let $r \ge \delta \ge 2$, set $n = r + \delta - 1$, and define*

$$\psi(t) := (r-t)_+ \left(n - (\delta-1)t\right)_+, \qquad y_+ := \max\{y, 0\}.$$

Then ψ is nonincreasing and convex on $[0, \infty)$.

5.1.1 Two-level bound

Now we present the distance bound of the 2-level hierarchical QTB code. The proof proceeds by iterating the one-level root-counting argument. At the bottom level, for each admissible shift i_2, we apply a Q-operator to f and obtain a transformed polynomial $g_{i_2}^{(2)}$. The Q_b-nonvanishing theorem guarantees that these transforms are nonzero on the nondual part of f, while the defining vanishing of Q_b forces $g_{i_2}^{(2)}$ to vanish whenever f has a suitable block of $\delta_2 - 1$ zeros in a bottom-level repair group together with one additional zero.

We then apply the same idea at the top level. For each admissible top-level shift i_1, we apply a level-1 Q-operator to $g^{(2)}_{i_2}$, producing $g^{(1)}_{i_1,i_2}$. Taking the product over all choices of i_1 and i_2 gives a nonzero polynomial G, whose degree is at most $r_1 r_2(\ell-1)$. Thus, an upper bound on the number of roots of G comes from its degree.

The lower bound on the number of roots is obtained by counting zero incidences level by level. Inside each bottom coset B, if w_B is the weight of f on B, the bottom-level argument contributes at least

$$\psi_2(w_B) = (r_2 - w_B)_+ \left(n_2 - (\delta_2 - 1)w_B\right)_+$$

zero incidences. Averaging these incidences over the bottom cosets inside a fixed top coset gives an upper bound on the average weight of the transforms $g^{(2)}_{i_2}$ on that top coset. The top-level root-counting argument then contributes

$$\psi_1(t) = (r_1 - t)_+ \left(n_1 - (\delta_1 - 1)t\right)_+$$

roots as a function of this averaged weight. Finally, Jensen's inequality is used twice, once across the choices of i_2 and once across the top cosets, to express the resulting lower bound only in terms of the total weight $|\mathrm{ev}(f)|$. Comparing this lower bound with $\deg G \le r_1 r_2(\ell-1)$ yields the desired distance estimate.

Theorem 5.7 (Two-level hierarchical QTB distance bound)**.** *Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be a two-level hierarchical QTB code with parameters $(r_1, \delta_1), (r_2, \delta_2)$ and set*

$$n_1 := r_1 + \delta_1 - 1, \qquad n_2 := r_2 + \delta_2 - 1.$$

Assume $n_2 \mid n_1 \mid (q-1)$. Assume also that Corollary 4.9 holds at both levels; concretely, for every level $l = 1, 2$, either $\delta_l \ge 3$ and $\mathrm{char}(\mathbb{F}_q) \nmid \mathcal{M}_{r_l,\delta_l}$, or $\delta_l = 2$ and $n_l = r_l + 1$ is prime.

For $l = 1, 2$, define

$$\psi_l(t) := (r_l - t)_+ \left(n_l - (\delta_l - 1)t\right)_+ .$$

Define

$$\Theta_2(t) := \frac{q-1}{n_1}\, r_2\, \psi_1\left(n_1 - \frac{n_1}{r_2 n_2}\psi_2(t)\right), \qquad 0 \le t \le n_2.$$

Let

$$\tau_2 := \inf\left\{t \in [0, n_2] : \Theta_2(t) \le r_1 r_2(\ell-1)\right\}.$$

Then

$$d(\mathcal{Q}) \ge \frac{q-1}{n_2}\tau_2.$$

Equivalently, every nonzero codeword $\mathrm{ev}(f) \in C \setminus C^{\perp}$ of weight

$$w := |\mathrm{ev}(f)|$$

satisfies

$$r_1 r_2(\ell-1) \ge \frac{q-1}{n_1}\, r_2\, \psi_1\left(n_1 - \frac{n_1}{r_2 n_2}\psi_2\left(\frac{n_2}{q-1}w\right)\right).$$

Proof. Fix $\mathrm{ev}(f) \in C \setminus C^{\perp}$. We decompose

$$f = g + P_1 + P_2,$$

where g is supported outside $S_{1,+} \cup S_{2,+}$, P_2 is supported on $S_{2,+}$, and P_1 is supported on $S_{1,+} \setminus S_{2,+}$. Since $\mathrm{ev}(f) \notin C^{\perp}$, we have $g \neq 0$.

For $l = 1, 2$, let

$$I_l := \{\delta_l - 1, \ldots, n_l - 1\}.$$

For each $i_l \in I_l$, let

$$Q^{(l)}_{i_l}(Y) = Y^{i_l} + \sum_{t=0}^{\delta_l - 2} v^{(l)}_{i_l,t} Y^t$$

be the corresponding Q-polynomial at level l. Let ω_l be a primitive n_lth root of unity. Define the linear operator

$$\mathcal{L}^{(l)}_{i_l}[p](X) := \omega_l^{-i_l} p(\omega_l^{i_l} X) + \sum_{t=0}^{\delta_l - 2} v^{(l)}_{i_l,t} \omega_l^{-t} p(\omega_l^{t} X).$$

On monomials, this operator acts diagonally:

$$\mathcal{L}^{(l)}_{i_l}[X^j] = Q^{(l)}_{i_l}(\omega_l^{j-1}) X^j.$$

Define the level-2 transforms $g^{(2)}_{i_2} := \mathcal{L}^{(2)}_{i_2}[f]$, $i_2 \in I_2$, and the level-1 transforms $g^{(1)}_{i_1,i_2} := \mathcal{L}^{(1)}_{i_1}[g^{(2)}_{i_2}]$, $i_1 \in I_1,\ i_2 \in I_2$. Finally define the aggregate polynomial

$$G(X) := \prod_{i_2 \in I_2} \prod_{i_1 \in I_1} g^{(1)}_{i_1,i_2}(X).$$

We first show that $G \neq 0$. The operator $\mathcal{L}^{(2)}_{i_2}$ ensures that coefficient of every monomial whose exponent lies in $S_{2,+}$ is zero, so

$$g^{(2)}_{i_2} = \mathcal{L}^{(2)}_{i_2}[g] + \mathcal{L}^{(2)}_{i_2}[P_1].$$

The two summands have disjoint supports. Since every exponent in the support of g does not lie in $S_{2,+}$, Corollary 4.9 at level 2 implies $\mathcal{L}^{(2)}_{i_2}[g] \neq 0$. Hence $g^{(2)}_{i_2} \neq 0$.

Next, $\mathcal{L}^{(2)}_{i_2}[P_1]$ is still supported on $S_{1,+}$ so applying the operator $\mathcal{L}^{(1)}_{i_1}$ ensures that it is zero. Therefore,

$$g^{(1)}_{i_1,i_2} = \mathcal{L}^{(1)}_{i_1} \mathcal{L}^{(2)}_{i_2}[g].$$

Every exponent in the support of g avoids both $S_{1,+}$ and $S_{2,+}$. Thus, Corollary 4.9 at levels 1 and 2 imply $g^{(1)}_{i_1,i_2} \neq 0$ so $G \neq 0$.

Moreover, each operator preserves degree, so

$$\deg g^{(1)}_{i_1,i_2} \leq \deg g \leq \ell - 1.$$

Since $|I_1| = r_1$ and $|I_2| = r_2$, we have

$$\deg G \leq r_1 r_2(\ell - 1).$$

We now lower bound the number of roots of G. Let A range over the cosets of Ω_{n_1} in $\mathbb{F}_q^*$, and let $B \subset A$ range over the cosets of Ω_{n_2} contained in A. Write $w_B := |\mathrm{ev}(f)|_B$. Fix a bottom coset B and let

$$N_B := \left|\left\{x \in B : f(x) = f(\omega_2 x) = \cdots = f(\omega_2^{\delta_2 - 2} x) = 0\right\}\right|.$$

Each nonzero value of f on B can block at most $\delta_2 - 1$ such starting points, so

$$N_B \geq (n_2 - (\delta_2 - 1)w_B)_+ .$$

For any such starting point x, the number of $i_2 \in I_2$ for which $f(\omega_2^{i_2} x) = 0$ is at least $(r_2 - w_B)_+$. For each such pair (x, i_2), the definition of $\mathcal{L}_{i_2}^{(2)}$ gives $g_{i_2}^{(2)}(x) = 0$. Therefore,

$$\sum_{i_2 \in I_2} |\{x \in B : g_{i_2}^{(2)}(x) = 0\}| \geq \psi_2(w_B).$$

Summing over all bottom cosets $B \subset A$, we obtain

$$\sum_{i_2 \in I_2} |\{x \in A : g_{i_2}^{(2)}(x) = 0\}| \geq \sum_{B \subset A} \psi_2(w_B).$$

Equivalently, if

$$w_{A,i_2}^{(2)} := |\mathrm{ev}(g_{i_2}^{(2)})|_A,$$

then

$$\sum_{i_2 \in I_2} w_{A,i_2}^{(2)} \leq r_2 n_1 - \sum_{B \subset A} \psi_2(w_B).$$

Thus,

$$\frac{1}{r_2} \sum_{i_2 \in I_2} w_{A,i_2}^{(2)} \leq n_1 - \frac{1}{r_2} \sum_{B \subset A} \psi_2(w_B). \tag{5.8}$$

Now fix A and i_2. Applying the same incidence count at level 1 to the family $\{g_{i_1,i_2}^{(1)}\}_{i_1 \in I_1}$ gives

$$\sum_{i_1 \in I_1} |\{x \in A : g_{i_1,i_2}^{(1)}(x) = 0\}| \geq \psi_1(w_{A,i_2}^{(2)}).$$

Therefore, the root multiplicity contributed by A to G is at least

$$\sum_{i_2 \in I_2} \psi_1(w_{A,i_2}^{(2)}).$$

By Lemma 4.11, ψ_1 is convex, so Jensen's inequality gives

$$\sum_{i_2 \in I_2} \psi_1(w_{A,i_2}^{(2)}) \geq r_2 \psi_1\left(\frac{1}{r_2} \sum_{i_2 \in I_2} w_{A,i_2}^{(2)}\right).$$

Since ψ_1 is nonincreasing, substituting (5.8) gives

$$\sum_{i_2\in I_2} \psi_1(w^{(2)}_{A,i_2}) \geq r_2\psi_1\left(n_1 - \frac{1}{r_2}\sum_{B\subset A}\psi_2(w_B)\right).$$

Now sum over all top cosets A. The function

$$S \longmapsto r_2\psi_1\left(n_1 - \frac{S}{r_2}\right)$$

is convex because we have composed ψ_1, a convex function, with an affine function which maps $S \mapsto n_1 - S/r_2$. It is also nondecreasing because as S increases, the argument $n_1 - S/r_2$ decreases and ψ_1 is nonincreasing. Hence Jensen's inequality gives

$$|\{\text{roots of } G\}| \geq \frac{q-1}{n_1} r_2\psi_1\left(n_1 - \frac{1}{r_2}\cdot\frac{n_1}{q-1}\sum_A\sum_{B\subset A}\psi_2(w_B)\right).$$

But,

$$\sum_A\sum_{B\subset A}\psi_2(w_B) = \sum_B \psi_2(w_B),$$

where B now ranges over all bottom cosets in $\mathbb{F}_q^*$. By Jensen's inequality and the convexity of ψ_2,

$$\sum_B \psi_2(w_B) \geq \frac{q-1}{n_2}\psi_2\left(\frac{n_2}{q-1}|\mathrm{ev}(f)|\right).$$

Using that ψ_1 is nonincreasing, we obtain

$$|\{\text{roots of } G\}| \geq \frac{q-1}{n_1} r_2\psi_1\left(n_1 - \frac{n_1}{r_2 n_2}\psi_2\left(\frac{n_2}{q-1}|\mathrm{ev}(f)|\right)\right).$$

Since $G \neq 0$, its number of roots in $\mathbb{F}_q^*$, counted with multiplicity, is at most its degree. Therefore

$$r_1 r_2(\ell-1) \geq \frac{q-1}{n_1} r_2\psi_1\left(n_1 - \frac{n_1}{r_2 n_2}\psi_2\left(\frac{n_2}{q-1}|\mathrm{ev}(f)|\right)\right).$$

This proves the displayed inequality.

Finally, $\Theta_2(t)$ is nonincreasing in t. Hence the inequality

$$r_1 r_2(\ell-1) \geq \Theta_2\left(\frac{n_2}{q-1}|\mathrm{ev}(f)|\right)$$

implies

$$|\mathrm{ev}(f)| \geq \frac{q-1}{n_2}\tau_2.$$

Taking the minimum over all $\mathrm{ev}(f) \in C \setminus C^\perp$ proves the distance bound. ■

5.1.2 h-level bound

We will extend the distance bound to the general h-level hierarchical QTB code by iterating the same argument as in Theorem 5.7. We first present a lemma that will aid in the recursive argument.

Lemma 5.8. *For $l = 1, \dots, h$, set $\psi_l(t) := (r_l - t)_+ \left(n_l - (\delta_l - 1)t\right)_+$. Define $\Psi_h(t) := \psi_h(t)$, and for $l = h-1, h-2, \dots, 1$, define*

$$\Psi_l(t) := \psi_l\left(n_l - \frac{n_l}{r_{l+1}n_{l+1}}\Psi_{l+1}(t)\right).$$

Then each Ψ_l is convex and nonincreasing on $[0, n_h]$. Consequently,

$$\Theta_h(t) := \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1(t)$$

is also convex and nonincreasing on $[0, n_h]$.

Moreover, for each level-l coset B_l, let $w_{B_l} := |\mathrm{ev}(f)|_{B_l}$. Let $I_l = \{\delta_l - 1, \dots, n_l - 1\}$ and let $\mathcal{R}_l(B_l)$ denote the total number of zero incidences contributed inside B_l as follows: for each choice of lower-level indices

$$(i_{l+1}, \dots, i_h) \in I_{l+1} \times \cdots \times I_h,$$

apply the level-l incidence count to the family $\{g^{(l)}_{i_l,\dots,i_h}\}_{i_l \in I_l}$ and sum over all choices of $(i_{l+1}, \dots, i_h)$. Then

$$\mathcal{R}_l(B_l) \geq \left(\prod_{u=l+1}^{h} r_u\right)\Psi_l\left(\frac{n_h}{n_l}w_{B_l}\right),$$

where the empty product is interpreted as 1.

Proof. We first prove the analytic claim. By Lemma 4.11, for each l, the function $\psi_l(t)$ is convex and nonincreasing on $[0, \infty)$. We show by downward induction that each Ψ_l is convex and nonincreasing. The base case $\Psi_h = \psi_h$ is immediate from Lemma 4.11.

Assume Ψ_{l+1} is convex and nonincreasing. Define

$$A_l(t) := n_l - \frac{n_l}{r_{l+1}n_{l+1}}\Psi_{l+1}(t).$$

Since Ψ_{l+1} is convex and nonincreasing, the function A_l is concave and nondecreasing. Moreover, $0 \leq \Psi_{l+1}(t) \leq r_{l+1}n_{l+1}$ so $0 \leq A_l(t) \leq n_l$. Hence, all inputs to ψ_l lie in the interval where Lemma 4.11 applies. Because ψ_l is convex and nonincreasing, the composition rule for convex functions implies that $\Psi_l(t) = \psi_l(A_l(t))$ is convex. Also, since A_l is nondecreasing and ψ_l is nonincreasing, Ψ_l is nonincreasing. Indeed, if $t_1 \leq t_2$ then $A_l(t_1) \leq A_l(t_2)$. Applying ψ_l reverses the inequality:

$$\Psi_l(t_1) = \psi_l(A_l(t_1)) \geq \psi_l(A_l(t_2)) = \Psi_l(t_2).$$

This proves the induction. The same properties for Θ_h follow because Θ_h is a positive scalar multiple of Ψ_1.

We now prove the incidence bound by downward induction on l. For $l = h$, fix a bottom-level coset B_h. The one-level incidence count at level h gives

$$\mathcal{R}_h(B_h) \geq \psi_h(w_{B_h}) = \Psi_h(w_{B_h}),$$

which is the desired statement because $n_h/n_h = 1$ and the product $\prod_{u=h+1}^{h} r_u$ is empty.

Assume now that the claim holds at level $l+1$, and fix a level-l coset B_l. Decompose B_l into its level-$(l+1)$ child cosets:

$$B_l = \bigsqcup_{a=1}^{n_l/n_{l+1}} B_{l+1,a}.$$

Set $w_a := |\mathrm{ev}(f)|_{B_{l+1,a}}$. Let $\Lambda_{l+1} := I_{l+1} \times I_{l+2} \times \cdots \times I_h$ so

$$|\Lambda_{l+1}| = \prod_{u=l+1}^{h} r_u.$$

For $\boldsymbol{i} = (i_{l+1}, \ldots, i_h) \in \Lambda_{l+1}$ and a child coset $B_{l+1,a}$, define

$$w^g_{\boldsymbol{i},a} := |\mathrm{ev}(g^{(l+1)}_{i_{l+1},\ldots,i_h})|_{B_{l+1,a}},$$

the number of nonzero positions of the transformed polynomial $g^{(l+1)}_{i_{l+1},\ldots,i_h}$ on $B_{l+1,a}$.

By the induction hypothesis applied to the child coset $B_{l+1,a}$, the total number of zero incidences in $B_{l+1,a}$, summed over all lower-level operator choices $\boldsymbol{i} \in \Lambda_{l+1}$, is at least

$$\left(\prod_{u=l+2}^{h} r_u\right) \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a\right).$$

Equivalently,

$$\sum_{\boldsymbol{i}\in\Lambda_{l+1}} \left(n_{l+1} - w^g_{\boldsymbol{i},a}\right) \geq \left(\prod_{u=l+2}^{h} r_u\right) \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a\right).$$

Dividing by $|\Lambda_{l+1}|$, we get

$$\frac{1}{|\Lambda_{l+1}|} \sum_{\boldsymbol{i}\in\Lambda_{l+1}} w^g_{\boldsymbol{i},a} \leq n_{l+1} - \frac{1}{r_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a\right).$$

Now define the total effective weight of $g^{(l+1)}_{i_{l+1},\ldots,i_h}$ inside B_l by

$$w^g_{\boldsymbol{i}} := |\mathrm{ev}(g^{(l+1)}_{i_{l+1},\ldots,i_h})|_{B_l} = \sum_{a=1}^{n_l/n_{l+1}} w^g_{\boldsymbol{i},a}.$$

Averaging over $\boldsymbol{i} \in \Lambda_{l+1}$, we obtain

$$\begin{aligned}
\frac{1}{|\Lambda_{l+1}|} \sum_{\boldsymbol{i} \in \Lambda_{l+1}} w_{\boldsymbol{i}}^{g} &= \sum_{a=1}^{n_l/n_{l+1}} \frac{1}{|\Lambda_{l+1}|} \sum_{\boldsymbol{i} \in \Lambda_{l+1}} w_{\boldsymbol{i},a}^{g} \\
&\leq \sum_{a=1}^{n_l/n_{l+1}} \left(n_{l+1} - \frac{1}{r_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a \right) \right) \\
&= n_l - \frac{1}{r_{l+1}} \sum_{a=1}^{n_l/n_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a \right) \\
&= n_l - \frac{n_l}{r_{l+1} n_{l+1}} \cdot \frac{1}{n_l/n_{l+1}} \sum_{a=1}^{n_l/n_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a \right). \qquad (5.9)
\end{aligned}$$

For each fixed lower-level choice $\boldsymbol{i}$, the level-l incidence count gives at least $\psi_l(w_{\boldsymbol{i}}^{g})$ zero incidences inside B_l, summed over the r_l choices of the level-l operator. Therefore,

$$\mathcal{R}_l(B_l) \geq \sum_{\boldsymbol{i} \in \Lambda_{l+1}} \psi_l(w_{\boldsymbol{i}}^{g}).$$

Since ψ_l is convex, Jensen's inequality gives

$$\sum_{\boldsymbol{i} \in \Lambda_{l+1}} \psi_l(w_{\boldsymbol{i}}^{g}) \geq |\Lambda_{l+1}| \psi_l \left(\frac{1}{|\Lambda_{l+1}|} \sum_{\boldsymbol{i} \in \Lambda_{l+1}} w_{\boldsymbol{i}}^{g} \right).$$

And since ψ_l is nonincreasing, substituting the upper bound (5.9) gives:

$$\mathcal{R}_l(B_l) \geq \left(\prod_{u=l+1}^{h} r_u \right) \psi_l \left(n_l - \frac{n_l}{r_{l+1} n_{l+1}} \cdot \frac{1}{n_l/n_{l+1}} \sum_{a=1}^{n_l/n_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a \right) \right).$$

Using the convexity of Ψ_{l+1}, Jensen's inequality gives

$$\frac{1}{n_l/n_{l+1}} \sum_{a=1}^{n_l/n_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_{l+1}} w_a \right) \geq \Psi_{l+1}\left(\frac{1}{n_l/n_{l+1}} \sum_{a=1}^{n_l/n_{l+1}} \frac{n_h}{n_{l+1}} w_a \right) = \Psi_{l+1}\left(\frac{n_h}{n_l} w_{B_l} \right) \qquad (5.10)$$

since $\sum_a w_a = w_{B_l}$. Since ψ_l is nonincreasing, substituting (5.10) can only increase the argument of ψ_l, we obtain

$$\mathcal{R}_l(B_l) \geq \left(\prod_{u=l+1}^{h} r_u \right) \psi_l \left(n_l - \frac{n_l}{r_{l+1} n_{l+1}} \Psi_{l+1}\left(\frac{n_h}{n_l} w_{B_l} \right) \right).$$

By the recursive definition of Ψ_l, this is

$$\mathcal{R}_l(B_l) \geq \left(\prod_{u=l+1}^{h} r_u \right) \Psi_l \left(\frac{n_h}{n_l} w_{B_l} \right).$$

This completes the induction. ■

Theorem 5.9 (h-level hierarchical QTB distance bound)**.** *Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be an h-level hierarchical QTB code with parameters $(r_1, \delta_1), \ldots, (r_h, \delta_h)$, and set $n_l := r_l + \delta_l - 1$ for $l = 1, \ldots, h$. Assume $n_h \mid n_{h-1} \mid \cdots \mid n_1 \mid (q-1)$. Also, assume that Corollary 4.9 holds at every level; concretely, for every l, either $\delta_l \geq 3$ and $\mathrm{char}(\mathbb{F}_q) \nmid \mathcal{M}_{r_l,\delta_l}$, or $\delta_l = 2$ and $n_l = r_l + 1$ is prime.*

For $l = 1, \ldots, h$, define $\psi_l(t) := (r_l - t)_+ \left(n_l - (\delta_l - 1)t\right)_+$. Define functions $\Psi_l : [0, n_h] \to \mathbb{R}_{\geq 0}$ recursively by $\Psi_h(t) := \psi_h(t)$, and for $l = h-1, h-2, \ldots, 1$,

$$\Psi_l(t) := \psi_l\left(n_l - \frac{n_l}{r_{l+1}n_{l+1}}\Psi_{l+1}(t)\right).$$

Define

$$\Theta_h(t) := \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1(t).$$

Let

$$\tau_h := \inf\left\{t \in [0, n_h] : \Theta_h(t) \leq \left(\prod_{l=1}^{h} r_l\right)(\ell - 1)\right\}.$$

Then

$$d(\mathcal{Q}) \geq \frac{q-1}{n_h}\tau_h.$$

Equivalently, every nonzero codeword $\mathrm{ev}(f) \in C \setminus C^\perp$ of weight w satisfies

$$\left(\prod_{l=1}^{h} r_l\right)(\ell - 1) \geq \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1\left(\frac{n_h}{q-1}w\right).$$

Proof. The proof is an iteration of the two-level argument in Theorem 5.7. We give the details needed to track the notation. Write

$$f = g + P_1 + \cdots + P_h,$$

where g is supported outside $S_+ = \bigcup_{l=1}^{h} S_{l,+}$, and P_l is supported on

$$S_{l,+} \setminus \bigcup_{k=l+1}^{h} S_{k,+}$$

for $l < h$, while P_h is supported on $S_{h,+}$. Since $\mathrm{ev}(f) \notin C^\perp$, we have $g \neq 0$. For each level l, set

$$I_l := \{\delta_l - 1, \ldots, n_l - 1\}.$$

For $i_l \in I_l$, define the operator

$$\mathcal{L}_{i_l}^{(l)}[p](X) := \omega_l^{-i_l} p(\omega_l^{i_l} X) + \sum_{t=0}^{\delta_l - 2} v_{i_l,t}^{(l)} \omega_l^{-t} p(\omega_l^t X),$$

so that

$$\mathcal{L}^{(l)}_{i_l}[X^j] = Q^{(l)}_{i_l}(\omega_l^{j-1})X^j.$$

We recursively define transformed polynomials by ascending through the hierarchy. First, for $i_h \in I_h$, set

$$g^{(h)}_{i_h} := \mathcal{L}^{(h)}_{i_h}[f].$$

For $l = h-1, h-2, \dots, 1$, and for a tuple

$$(i_l, i_{l+1}, \dots, i_h) \in I_l \times I_{l+1} \times \cdots \times I_h,$$

define

$$g^{(l)}_{i_l,i_{l+1},\dots,i_h} := \mathcal{L}^{(l)}_{i_l}\left[g^{(l+1)}_{i_{l+1},\dots,i_h}\right].$$

Finally, define

$$G(X) := \prod_{i_h\in I_h}\prod_{i_{h-1}\in I_{h-1}}\cdots\prod_{i_1\in I_1} g^{(1)}_{i_1,\dots,i_h}(X).$$

We first show that $G \neq 0$. At each level l, the operator $\mathcal{L}^{(l)}_{i_l}$ annihilates the positive-residue part. Since the operators act diagonally on monomials, the support of g remains disjoint from all positive-residue supports throughout the iteration. After all levels have been applied, we have

$$g^{(1)}_{i_1,\dots,i_h} = \mathcal{L}^{(1)}_{i_1}\mathcal{L}^{(2)}_{i_2}\cdots\mathcal{L}^{(h)}_{i_h}[g].$$

For every exponent j in the support of g, and for every level l, we have $j \notin S_{l,+}$. Therefore, $Q^{(l)}_{i_l}(\omega_l^{j-1}) \neq 0$ by Corollary 4.9 at level l. Thus, every nonzero coefficient of g remains nonzero after applying the product of diagonal operators so $g^{(1)}_{i_1,\dots,i_h} \neq 0$ for every tuple $(i_1, \dots, i_h)$. This implies $G \neq 0$. Moreover, each operator preserves degree, so

$$\deg g^{(1)}_{u_1,\dots,u_h} \le \deg g \le \ell - 1.$$

Since $|I_l| = r_l$, we obtain

$$\deg G \le \left(\prod_{l=1}^{h} r_l\right)(\ell - 1).$$

We now count roots. By Lemma 5.8, applied to each level-1 coset B_1, we have

$$|\{\text{roots of } G\}| \ge \left(\prod_{l=2}^{h} r_l\right)\sum_{B_1}\Psi_1\left(\frac{n_h}{n_1}|\mathrm{ev}(f)|_{B_1}\right).$$

Since Ψ_1 is convex, Jensen's inequality gives

$$\sum_{B_1}\Psi_1\left(\frac{n_h}{n_1}|\mathrm{ev}(f)|_{B_1}\right) \ge \frac{q-1}{n_1}\Psi_1\left(\frac{1}{(q-1)/n_1}\sum_{B_1}\frac{n_h}{n_1}|\mathrm{ev}(f)|_{B_1}\right)$$

and
$$\frac{1}{(q-1)/n_1}\sum_{B_1}\frac{n_h}{n_1}|\mathrm{ev}(f)|_{B_1} = \frac{n_h}{q-1}|\mathrm{ev}(f)|.$$
Thus,
$$|\{\text{roots of } G\}| \geq \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1\left(\frac{n_h}{q-1}|\mathrm{ev}(f)|\right).$$

Since $G \neq 0$, the number of roots of G, counted with multiplicity, is at most its degree. Hence,
$$\left(\prod_{l=1}^{h} r_l\right)(\ell-1) \geq \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1\left(\frac{n_h}{q-1}|\mathrm{ev}(f)|\right).$$
By construction, the function
$$\Theta_h(t) := \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1(t)$$
is nonincreasing in t. Therefore the preceding inequality implies
$$|\mathrm{ev}(f)| \geq \frac{q-1}{n_h}\tau_h.$$
Taking the minimum over all $\mathrm{ev}(f) \in C \setminus C^{\perp}$ proves the theorem. ■

Theorem 5.7 and Theorem 5.9 give implicit distance bounds which we now turn explicit in the following corollary. The final expression will be similar to (4.19).

Corollary 5.10. *Assume the hypotheses of Theorem 5.9. For each $l = 1, \dots, h$, set $a_l := \delta_l - 1$. Define the clipped inverse function $\mathrm{Inv}_l : \mathbb{R} \to [0, n_l]$ by*
$$\mathrm{Inv}_l(\theta) := \begin{cases} 0, & \theta \geq r_l n_l, \\ T_l, & \theta \leq 0, \\ \dfrac{n_l + a_l r_l - \sqrt{(n_l + a_l r_l)^2 - 4a_l(r_l n_l - \theta)}}{2a_l}, & 0 < \theta < r_l n_l, \end{cases}$$
where
$$T_l := \min\left\{r_l, \frac{n_l}{a_l}\right\}.$$
Define $y_1, \dots, y_h$ recursively by
$$y_1 := \mathrm{Inv}_1\left(r_1 n_1 \frac{\ell-1}{q-1}\right),$$
and, for $l = 2, \dots, h$, by
$$y_l := \mathrm{Inv}_l\left(\frac{r_l n_l}{n_{l-1}}(n_{l-1} - y_{l-1})\right).$$

Then

$$d(\mathcal{Q}) \geq \frac{q-1}{n_h} y_h. \tag{5.11}$$

Proof. Recall that

$$\psi_l(t) = (r_l - t)_+ (n_l - a_l t)_+.$$

On the interval where $\psi_l(t) > 0$, we have

$$\psi_l(t) = (r_l - t)(n_l - a_l t) = r_l n_l - (n_l + a_l r_l)t + a_l t^2.$$

Solving $\psi_l(t) = \theta$ for t gives

$$t = \frac{n_l + a_l r_l - \sqrt{(n_l + a_l r_l)^2 - 4a_l(r_l n_l - \theta)}}{2a_l}.$$

This is the smaller root, and it is the relevant one because ψ_l is nonincreasing on $[0, n_l]$. With the clipping convention in the definition of Inv_j, we have

$$\psi_l(t) \leq \theta \qquad \Longrightarrow \qquad t \geq \mathrm{Inv}_j(\theta). \tag{5.12}$$

By Theorem 5.9, every nonzero codeword of weight w satisfies

$$\left(\prod_{l=1}^{h} r_l\right)(\ell - 1) \geq \frac{q-1}{n_1}\left(\prod_{l=2}^{h} r_l\right)\Psi_1\left(\frac{n_h}{q-1}w\right),$$

where

$$\Psi_h(t) = \psi_h(t),$$

and, for $l = h-1, \ldots, 1$,

$$\Psi_l(t) = \psi_l\left(n_l - \frac{n_l}{r_{l+1}n_{l+1}}\Psi_{l+1}(t)\right).$$

Canceling the common factor $\prod_{l=2}^{h} r_l$, we get

$$\Psi_1\left(\frac{n_h}{q-1}w\right) \leq r_1 n_1 \frac{\ell - 1}{q-1}.$$

Set

$$t_0 := \frac{n_h}{q-1}w.$$

Then

$$\psi_1\left(n_1 - \frac{n_1}{r_2 n_2}\Psi_2(t_0)\right) \leq r_1 n_1 \frac{\ell-1}{q-1}.$$

By (5.12), this implies

$$n_1 - \frac{n_1}{r_2 n_2}\Psi_2(t_0) \geq y_1.$$

Equivalently,

$$\Psi_2(t_0) \leq \frac{r_2 n_2}{n_1}(n_1 - y_1).$$

Applying the same argument at level 2, we obtain

$$n_2 - \frac{n_2}{r_3 n_3}\Psi_3(t_0) \geq y_2,$$

and hence

$$\Psi_3(t_0) \leq \frac{r_3 n_3}{n_2}(n_2 - y_2).$$

Continuing recursively, after level $h-1$ we get

$$\Psi_h(t_0) \leq \frac{r_h n_h}{n_{h-1}}(n_{h-1} - y_{h-1}).$$

Since $\Psi_h(t_0) = \psi_h(t_0)$, another application of (5.12) gives $t_0 \geq y_h$. Substituting back $t_0 = \frac{n_h}{q-1}w$, we obtain

$$w \geq \frac{q-1}{n_h}y_h.$$

Taking the minimum over all nonzero codewords gives

$$d(\mathcal{Q}) \geq \frac{q-1}{n_h}y_h,$$

as desired. ■

For $h = 2$, we can unravel the bound in (5.11) to see that

$$d(\mathcal{Q}) \geq \frac{q-1}{n_2} \cdot \frac{n_2 + (\delta_2 - 1)r_2 - \sqrt{(n_2 + (\delta_2 - 1)r_2)^2 - 4(\delta_2 - 1)r_2 n_2 \frac{y_1}{n_1}}}{2(\delta_2 - 1)} \tag{5.13}$$

where

$$y_1 = \frac{n_1 + (\delta_1 - 1)r_1 - \sqrt{(n_1 + (\delta_1 - 1)r_1)^2 - 4(\delta_1 - 1)r_1 n_1 \left(1 - \frac{\ell-1}{q-1}\right)}}{2(\delta_1 - 1)}$$

is the explicit bound for Theorem 5.7. Additionally, y_1 is exactly the one-level bound in Theorem 4.12.

Remark 5.11. In order to apply the distance bound Theorem 5.9, we need Corollary 4.9 to hold at each level (and potentially Remark 4.10 at the bottom level). In particular, we must first fix $(r_l, \delta_l)_{l=1,\ldots,h}$ such that

$$r_1 \geq r_2 \geq \cdots \geq r_h \geq \delta_1 \geq \delta_2 \geq \cdots \geq \delta_h \geq 2$$

and $n_h \mid n_{h-1} \mid \cdots \mid n_1$. Then we compute $\mathcal{M}_{r_l,\delta_l}$ for each $l = 1, \ldots, h$ and obtain the following set of characteristics to exclude:

$$\mathcal{P} = \bigcup_{l=1}^{h} \{p : p \mid \mathcal{M}_{r_l,\delta_l}\}.$$

Finally, we choose q, a prime power such that $n_1 \mid (q-1)$ and $\mathrm{char}(\mathbb{F}_q) \notin \mathcal{P}$.

The recursive bound in Theorem 5.9 is a direct multilevel analogue of the one-level root-counting proof. However, the hierarchy does not necessarily improve the distance when compared to the one-level (r_1, δ_1) QTB code. Indeed, the explicit form in Corollary 5.10 gives

$$d(\mathcal{Q}) \geq \frac{q-1}{n_h} y_h,$$

whereas the top-level bound is

$$d(\mathcal{Q}) \geq \frac{q-1}{n_1} y_1.$$

We now explain why the recursive estimate cannot be expected to beat the top-level estimate.

Corollary 5.12. *For $l = 1, \ldots, h$, set $a_l := \delta_l - 1$ and $n_l := r_l + a_l$. Recall that*

$$\psi_l(t) = (r_l - t)_+ (n_l - a_l t)_+.$$

The recursion defining y_l says that, for $l \geq 2$,

$$y_l = \mathrm{Inv}_l \left(\frac{r_l n_l}{n_{l-1}} (n_{l-1} - y_{l-1}) \right).$$

We claim that

$$\frac{y_h}{n_h} \leq \frac{y_{h-1}}{n_{h-1}} \leq \cdots \leq \frac{y_1}{n_1}.$$

Proof. Set $x = y_{l-1}/n_{l-1}$ so we have $y_l = \mathrm{Inv}_l \left(r_l n_l (1-x) \right)$. We claim that $y_l/n_l \leq x$. Since $\mathrm{Inv}_l(\theta)$ is the smallest threshold beyond which $\psi_l(t) \leq \theta$, it suffices to show

$$\psi_l(n_l x) \leq r_l n_l (1-x).$$

If one of the clipped factors in $\psi_l(n_l x)$ is zero, then this is immediate. Otherwise,

$$\psi_l(n_l x) = (r_l - n_l x)(n_l - a_l n_l x).$$

Dividing by n_l, it is enough to prove $(r_l - n_l x)(1 - a_l x) \leq r_l(1-x)$. Subtracting the left-hand side from the right-hand side gives

$$r_l(1-x) - (r_l - n_l x)(1 - a_l x) = x \left(r_l(a_l - 1) + n_l - a_l n_l x \right).$$

In the nonzero range of $\psi_l(n_l x)$, we have $1 - a_l x > 0$, and hence, $a_l n_l x < n_l$. Therefore,

$$r_l(a_l - 1) + n_l - a_l n_l x \geq 0.$$

Thus, $\psi_l(n_l x) \leq r_l n_l(1 - x)$, and consequently $y_l/n_l \leq y_{l-1}/n_{l-1}$. Iterating this inequality gives

$$\frac{y_h}{n_h} \leq \frac{y_{h-1}}{n_{h-1}} \leq \cdots \leq \frac{y_1}{n_1}.$$

■

The loss comes from two sources. First, at each level the proof averages zero incidences using Jensen's inequality, which discards information about how the zeros are distributed among lower-level repair groups. Second, the aggregate polynomial obtained by multiplying all transformed polynomials has degree

$$\left(\prod_{l=1}^{h} r_l\right)(\ell - 1),$$

so each additional level increases the degree bound by a factor of r_l. This degree growth can overwhelm the extra zero incidences forced by the hierarchy. It remains an interesting open problem to develop a multilevel distance proof which uses the reduced nondual support $[\ell] \setminus (S_+ \cup S_-)$ more efficiently.

We end this chapter with an example of a two-level hierarchical QTB code and its computed dimension and distance.

Example 4. Consider the two-level QTB code with parameters $(r_1, \delta_1) = (9, 4)$ and $(r_2, \delta_2) = (4, 3)$. Then $n_1 = 12$ and $n_2 = 6$ so $n_2 \mid n_1$. The bad-characteristic products from Corollary 4.9 are

$$\mathcal{M}_{4,3} = 2^8 \quad \text{and} \quad \mathcal{M}_{9,4} = 2^{76}3^{44}13^{20}37^4.$$

Thus the excluded characteristics are $\{2, 3, 13, 37\}$. The smallest prime power q satisfying $12 \mid (q - 1)$ and whose characteristic is not excluded is $q = 25$.

We compare the two-level hierarchical QTB code with the one-level QTB code having top-level parameters $(r, \delta) = (9, 4)$, over the same field $\mathbb{F}_{25}$ and with the same value of ℓ. The exact CSS distance was computed using the shortened-support criterion

$$d = \min\left\{|U| : \dim(C \cap \mathbb{F}_q^U) > \dim(C^\perp \cap \mathbb{F}_q^U)\right\}.$$

The results for $\ell = 13, \ldots, 24$ are as follows:

ℓ	k_{1lev}	d_{1lev}	k_{hier}	d_{hier}	d_{bound}
13	2	9	2	7	4
14	2	9	2	7	3
15	2	9	2	7	3
16	2	9	2	7	3
17	4	8	2	7	2
18	6	7	2	7	2
19	8	6	4	4	2
20	10	5	4	4	2
21	12	4	4	4	1
22	12	4	4	4	1
23	12	4	4	4	1
24	12	4	4	4	1

In this example, the two-level hierarchical code does not improve the true global distance over a one-level code with the same top level parameters. It sometimes has the same distance, but it is often worse. In the table d_{bound} is the distance bound of the one-level (r_1, δ_1) QTB code as in (4.19). Corollary 5.12 shows the h-level distance bound (5.11) is at best equal to (4.19). However, the example codes do beat the proven bound so the bound is not tight. This illustrates that hierarchy should be viewed primarily as improving the repair structure, but not automatically improving the global minimum distance.

Chapter 6

Folding Quantum Tamo–Barg Codes

6.1 Folded (r, δ) Quantum Tamo–Barg Codes

We now present a variant of the quantum Tamo–Barg (QTB) codes in Definition 4.1 by using a *folding* operation. This code generalizes the folded quantum Tamo–Barg code which appears in [14].

Definition 6.1 (Folded (r, δ) Quantum Tamo–Barg code)**.** Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be the QTB code with parameters q, r, δ, ℓ. Given an additional folding parameter $s \mid (q-1)/(r+\delta-1)$, we define the **folded Quantum Tamo–Barg (fQTB) code** $\tilde{\mathcal{Q}}$ to be the quantum code with local dimension q^s and block length $(q-1)/s$ obtained as follows. Fix a generator $\omega_{q-1} \in \mathbb{F}_q^*$ and for every $i \in [(q-1)/s]$, we block together s components at positions $F_{\omega_{q-1}^{i \cdot s}} = \{\omega_{q-1}^{i \cdot s}, \ldots, \omega_{q-1}^{i \cdot s+s-1}\}$ in $\mathcal{Q}$ into a single component of $\tilde{\mathcal{Q}}$. Let $\tilde{C}$ denote the $\mathbb{F}_q$-linear codes obtained by folding C so that $\tilde{\mathcal{Q}} = \mathrm{CSS}(\tilde{C}, \tilde{C})$.

For a given $x = \omega_{q-1}^b \in \mathbb{F}_q^*$, let $F_x \in \tilde{\mathbb{F}}_q^*$ be the unique element of $\tilde{\mathbb{F}}_q^*$ that contains x. Formally,

$$F_x = \{\omega_{q-1}^{\lfloor b/s \rfloor \cdot s + j} : j \in [s]\}.$$

Folding a code by definition preserves the rate, so a fQTB has the same rate as the associated unfolded QTB. We computed this rate in Lemma 4.4. We will now show that fQTBs are also QLRCs. First, we need a small lemma.

Lemma 6.2. *Assume $s \mid (q-1)/(r+\delta-1)$. Let $\alpha\Omega_{r+\delta-1} \subseteq \mathbb{F}_q^*$ be a coset of $\Omega_{r+\delta-1}$ and let $F_{\omega_{q-1}^{i \cdot s}}$ be a block of positions as defined in Definition 6.1. Then $|\alpha\Omega_{r+\delta-1} \cap F_{\omega_{q-1}^{i \cdot s}}| \le 1$ for all i.*

Proof. Fix $i \in [(q-1)/s]$ and let $\alpha = \omega_{q-1}^b$ for some $b \in \mathbb{Z}$. Then

$$\alpha\Omega_{r+\delta-1} = \left\{\omega_{q-1}^{b + t \cdot \frac{q-1}{r+\delta-1}} : t \in [r+\delta-1]\right\}.$$

Suppose there exist $t_1 \neq t_2$ such that

$$\omega_{q-1}^{b+t_1\cdot\frac{q-1}{r+\delta-1}}, \omega_{q-1}^{b+t_2\cdot\frac{q-1}{r+\delta-1}} \in F_{\omega_{q-1}^{i\cdot s}}.$$

Then we must have

$$b + t_1 \cdot \frac{q-1}{r+\delta-1} \equiv i\cdot s + e_1 \mod (q-1) \quad \text{and} \quad b + t_2 \cdot \frac{q-1}{r+\delta-1} \equiv i\cdot s + e_2 \mod (q-1)$$

for some $e_1, e_2 \in [s]$. Subtracting, we obtain

$$(t_1 - t_2)\cdot\frac{q-1}{r+\delta-1} \equiv e_1 - e_2 \mod (q-1)$$

with $e_1 - e_2 \in \{-(s-1), \ldots, (s-1)\}$. Since $s \mid \frac{q-1}{r+\delta-1}$, we get $s \mid (e_1 - e_2)$ which is not possible unless $e_1 = e_2$. Thus

$$(t_1 - t_2)\cdot\frac{q-1}{r+\delta-1} \equiv 0 \mod (q-1) \implies t_1 - t_2 \equiv 0 \mod (r+\delta-1),$$

but we assumed $t_1 \neq t_2$ and $0 \leq t_1, t_2 < r + \delta - 1$. This is a contradiction. Hence, each element of $\alpha\Omega_{r+\delta-1}$ resides in a distinct folded block. ■

Corollary 6.3. *Assume $s \mid (q-1)/(r+\delta-1)$. Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be the QTB code from Definition 4.1, and let $\tilde{\mathcal{Q}} = \mathrm{CSS}(\tilde{C}, \tilde{C})$ be its folded version. Then $\tilde{\mathcal{Q}}$ is a QLRC with parameters (r, δ) i.e., every folded repair group has size $r + \delta - 1$ and can correct $\delta - 1$ erasures using only symbols inside the group.*

Proof. By Theorem 3.3, it suffices to prove that $\tilde{C}$ is a classical LRC with parameters (r, δ).

Fix a coset $\alpha\Omega_{r+\delta-1}$. Define the folded repair group

$$\tilde{R}_\alpha := \{F_x : x \in \alpha\Omega_{r+\delta-1}\}.$$

By Lemma 6.2, the map $x \mapsto F_x$ is injective on $\alpha\Omega_{r+\delta-1}$, so

$$|\tilde{R}_\alpha| = |\alpha\Omega_{r+\delta-1}| = r + \delta - 1.$$

Next, by Corollary 4.6 (applied to the unfolded code C), there exist $\delta-1$ linearly independent local parity checks in $C^\perp$ supported on $\alpha\Omega_{r+\delta-1}$. Each such check induces (by folding) a parity check on $\tilde{C}$ supported on $\tilde{R}_\alpha$. Because the folding map is injective on $\alpha\Omega_{r+\delta-1}$, these induced checks remain linearly independent, and therefore correct up to $\delta-1$ erasures within $\tilde{R}_\alpha$ using only symbols from $\tilde{R}_\alpha$. Thus $\tilde{C}$ is a classical LRC. Therefore $\tilde{\mathcal{Q}} = \mathrm{CSS}(\tilde{C}, \tilde{C})$ is a QLRC with the same locality parameters. ■

Lastly, we will prove a distance bound for the fQTB. A trivial bound follows from Theorem 4.12:if we denote the distance of the fQTB as $\tilde{d}$, then $\tilde{d} \geq d/s$, but we will shortly present a more involved proof for a stronger bound. Before we do so, we present a lemma that we require in the proof.

Lemma 6.4. *For every $v \in \mathbb{N}$, the determinant polynomial* $\det \in \mathbb{F}_q[(Y_{ij})_{i,j\in[v]}]$ *has a root of multiplicity $v-t$ at every matrix $(x_{ij})_{i,j\in[v]}$ of rank t.*

Now we present a more involved argument than the unfolded distance proof that gives a significant boost to the relative distance. This argument follows the structure of the proof of [14, Theorem 63], but this proof has to deal with more general parameters.

Theorem 6.5. *Let $\tilde{\mathcal{Q}}$ be the code from Definition 6.1 with parameters q, r, δ, ℓ, s such that $r+\delta-1$ is prime and the uncertainty principle in Corollary 2.31 holds for $r+\delta-1$ over $\mathbb{F}_q$. Then $\tilde{\mathcal{Q}}$ has distance at least*

$$d = \frac{q-1}{s}\left(1 - \frac{\ell-1}{q-1} - \epsilon\right)$$

for

$$\epsilon = \max_{1\le m_f\le r+\delta-1} \min\left\{\left(1-\frac{\ell-1}{q-1}\right)\frac{m_f-1}{r+\delta-1}, \max_{\max\{1,m_f-(\delta-1)\}\le m_g\le m_f} \frac{\delta-1}{m_g}+\frac{m_g-1}{s}\right\}.$$

Proof. Fix an arbitrary $f(x) = \sum_{j\in[q-1]} f_j X^j \in \mathbb{F}_q[X]$ such that $\mathrm{ev}(f(X)) \in C \setminus C^\perp$ with associated folded codeword $\tilde{\mathrm{ev}}(f(X)) \in \tilde{C} \setminus \tilde{C}^\perp$. Our goal is to show $|\tilde{\mathrm{ev}}(f)| \ge d$.

Since $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$ for

$$S = ([\ell] \setminus S_-) \cup ([q-1] \cap S_+)$$

we may write $f(X) = g(X) + h(X)$ where $g(X) = \sum_j g_j X^j \in \mathbb{F}_q[X]^{[\ell]\setminus(S_-\cup S_+)}$ and $h(X) = \sum_j h_j X^j \in \mathbb{F}_q[X]^{[q-1]\cap S_+}$.

Let $M_f = \{i \in [r+\delta-1] : \exists j \equiv i \mod r+\delta-1 \text{ with } f_j \ne 0\}$ and $m_f = |M_f|$. Similarly, define $M_g = \{i \in [r+\delta-1] : \exists j \equiv i \mod r+\delta-1 \text{ with } g_j \ne 0\}$ and $m_g = |M_g|$. Note that

$$\max\{1, m_f - (\delta-1)\} \le m_g \le m_f \le r+\delta-1.$$

We show two upper bounds on $|\tilde{\mathrm{ev}}(f)| \ge d$; the first is tighter when m_f is small and the second is tighter when m_g is large.

1. Using the uncertainty principle in Corollary 2.31, we will bound $|\mathrm{ev}(f)|$ and then apply the fact $|\tilde{\mathrm{ev}}(f)| \ge |\mathrm{ev}(f)|/s$. For every $\alpha \in \mathbb{F}_q^*$, on the restriction to inputs in the coset $\alpha\Omega_{r+\delta-1}$, f agrees with $f \pmod{X^{r+\delta-1} - \alpha^{r+\delta-1}}$. Clearly, $f \pmod{X^{r+\delta-1}-\alpha^{r+\delta-1}}$ is a polynomial of degree $< r+\delta-1$ whose coefficients are supported within M_f. Therefore, $|f \pmod{X^{r+\delta-1}-\alpha^{r+\delta-1}}| \le m_f$ and by Corollary 2.31, either $\mathrm{ev}(f)|_{\alpha\Omega_{r+\delta-1}} = 0$ or $|\mathrm{ev}(f)|_{\alpha\Omega_{r+\delta-1}} \ge r+\delta-1+1-m_f = r+\delta-m_f$.

   If $M_f \subseteq \{1,\dots,\delta-1\}$, then $\mathrm{ev}(f) \in C^\perp$ by Lemma 5.3. This contradicts the assumption on $\mathrm{ev}(f)$ so there is some $i \in M_f \setminus \{1,\dots,\delta-1\}$. Knowing this, $\mathrm{ev}(f)|_{\alpha\Omega_{r+\delta-1}} = 0$

if and only if $f \pmod{X^{r+\delta-1} - \alpha^{r+\delta-1}} = 0$ which is only possible if the ith coefficient of $f \pmod{X^{r+\delta-1} - \alpha^{r+\delta-1}}$:

$$\sum_{j \in [\frac{q-1}{r+\delta-1}]} f_{i+(r+\delta-1)j} (\alpha^{r+\delta-1})^j$$

is zero. The polynomial

$$\sum_{j \in [\frac{q-1}{r+\delta-1}]} f_{i+(r+\delta-1)j} Y^j$$

has degree $\leq (\ell-1)/(r+\delta-1)$ because $f_{i+(r+\delta-1)j} = 0$ if $i + (r+\delta-1)j \geq \ell$ by definition of C. Therefore, it has $\leq (\ell-1)/(r+\delta-1)$ roots which implies there are $\leq (\ell-1)/(r+\delta-1)$ cosets $\alpha\Omega_{r+\delta-1}$ for which $\mathrm{ev}(f)|_{\alpha\Omega_{r+\delta-1}} = 0$.

Hence,

$$\begin{aligned}
|\mathrm{ev}(f)| &= \sum_{\alpha\Omega_{r+\delta-1} \in \mathbb{F}_q^*/\Omega_{r+\delta-1}} |\mathrm{ev}(f)|_{\alpha\Omega_{r+\delta-1}} \\
&\geq \left(\frac{q-1}{r+\delta-1} - \frac{\ell-1}{r+\delta-1}\right)(r+\delta-1+1-m_f) \\
&= (q-1)\left(1 - \frac{\ell-1}{q-1}\right)\left(1 - \frac{m_f-1}{r+\delta-1}\right).
\end{aligned}$$

Now, by definition,

$$|\tilde{\mathrm{ev}}(f)| \geq \frac{|\mathrm{ev}(f)|}{s} \geq \frac{q-1}{s}\left(1 - \frac{\ell-1}{q-1}\right)\left(1 - \frac{m_f-1}{r+\delta-1}\right)$$

2. By Lemma 5.5, h is piecewise of degree at most $\delta-1$. Since $\mathrm{ev}(h) \in C^\perp$ and $\mathrm{ev}(f) \notin C^\perp$ we must have $g \neq 0$.

   Let $\det \in \mathbb{F}_q[(Y_{i,j})_{i,j\in[v]}]$ denote the determinant polynomial which takes as input a $v \times v$ matrix of variables $(Y_{i,j})_{i,j\in[v]}$ over $\mathbb{F}_q$ and outputs the determinant of the matrix. Define the matrices

$$\begin{aligned}
A(X) &= (\omega_{r+\delta-1}^i \omega_{q-1}^j X)_{i,j\in[m_g]}, \\
A_g(X) &= (\omega_{r+\delta-1}^{-i} g(\omega_{r+\delta-1}^i \omega_{q-1}^j X))_{i,j\in[m_g]}, \\
A_h(X) &= (\omega_{r+\delta-1}^{-i} h(\omega_{r+\delta-1}^i \omega_{q-1}^j X))_{i,j\in[m_g]}, \\
\text{and } A_f(X) &= (\omega_{r+\delta-1}^{-i} f(\omega_{r+\delta-1}^i \omega_{q-1}^j X))_{i,j\in[m_g]}
\end{aligned}$$

   and the polynomial $G(X) = \det(A_g(X)) \in \mathbb{F}_q[X]$. It follows that $\deg G \leq m \cdot \deg g \leq m(\ell-1)$. Now we show that $G(X)$ is a nonzero polynomial. We know $g(X) = \sum_{\alpha\in[\ell]\setminus(S_-\cup S_+)} g_\alpha X^\alpha$ so

$$A_g(X) = (\omega_{r+\delta-1}^{-i} g(\omega_{r+\delta-1}^i \omega_{q-1}^j X))_{i,j\in[m_g]}$$

$$= \sum_{\alpha\in[\ell]\setminus(S_-\cup S_+)} g_\alpha X^\alpha (\omega_{r+\delta-1}^{(\alpha-1)\cdot i}\omega_{q-1}^{\alpha\cdot j})_{i,j\in[m_g]}$$

$$= \sum_{\alpha\in[\ell]\setminus(S_-\cup S_+)} g_\alpha X^\alpha \begin{bmatrix} \omega_{r+\delta-1}^{(\alpha-1)\cdot 0} \\ \omega_{r+\delta-1}^{(\alpha-1)\cdot 1} \\ \vdots \\ \omega_{r+\delta-1}^{(\alpha-1)\cdot(m_g-1)} \end{bmatrix} \cdot \begin{bmatrix} \omega_{q-1}^{\alpha\cdot 0} & \omega_{q-1}^{\alpha\cdot 1} & \cdots & \omega_{q-1}^{\alpha\cdot(m_g-1)} \end{bmatrix}$$

$$= \sum_{i\in M_g} \begin{bmatrix} \omega_{r+\delta-1}^{(i-1)\cdot 0} \\ \omega_{r+\delta-1}^{(i-1)\cdot 1} \\ \vdots \\ \omega_{r+\delta-1}^{(i-1)\cdot(m_g-1)} \end{bmatrix} \cdot \sum_{\substack{\alpha\in[\ell]\setminus(S_-\cup S_+) \\ \alpha\equiv i \bmod (r+\delta-1)}} g_\alpha X^\alpha \begin{bmatrix} \omega_{q-1}^{\alpha\cdot 0} & \omega_{q-1}^{\alpha\cdot 1} & \cdots & \omega_{q-1}^{\alpha\cdot(m-1)} \end{bmatrix}.$$

$A_g(X)$ is an $m_g \times m_g$ matrix and $G(X) = \det(A_g(X))$ so in order to show $G(X)$ is nonzero, it suffices to show that $A_g(X)$ has full rank. It is then sufficient to show that the set of vectors

$$\left\{ \begin{bmatrix} \omega_{r+\delta-1}^{(i-1)\cdot 0} \\ \omega_{r+\delta-1}^{(i-1)\cdot 1} \\ \vdots \\ \omega_{r+\delta-1}^{(i-1)\cdot(m_g-1)} \end{bmatrix} : i \in M_g \right\}$$

and

$$\left\{ \sum_{\substack{\alpha\in[\ell]\setminus(S_-\cup S_+) \\ \alpha\equiv i \bmod (r+\delta-1)}} g_\alpha X^\alpha \begin{bmatrix} \omega_{q-1}^{\alpha\cdot 0} & \omega_{q-1}^{\alpha\cdot 1} & \cdots & \omega_{q-1}^{\alpha\cdot(m_g-1)} \end{bmatrix} : i \in M_g \right\}$$

are linearly independent over $\mathbb{F}_q[X]$. The first set of vectors form the columns of an $m_g \times m_g$ Vandermonde matrix which has full rank. If there is a nontrivial $\mathbb{F}_q[X]$ linear dependency in the second set of the vectors then taking the highest-degree term of the associated polynomials over X gives a nontrivial dependency among the vectors $[\omega_{q-1}^{\alpha\cdot j}]_{j\in[m_g]}$ for m_g distinct values of α. This forms another $m_g \times m_g$ Vandermonde matrix. Therefore, both sets of vectors are linearly independent so $G(X)$ is indeed nonzero.

It remains to bound the number of roots of $G(X)$. For a given $x = \omega_{q-1}^b \in \mathbb{F}_q^*$, recall that F_x is the index of the folded component of $\tilde{C}$ that contains the component x of C.

If $b \pmod s \in \{0, \ldots, s - m_g\}$, then because $s \mid \frac{q-1}{r+\delta-1}$ it follows that for each $i \in [m_g]$,

$$\{\omega_{r+\delta-1}^i \omega_{q-1}^j x : j \in [m_g]\} = \{\omega_{q-1}^{b+j+i\cdot\frac{q-1}{r+\delta-1}} : j \in [m_g]\} \subseteq F_{\omega_{r+\delta-1}^i x}.$$

The ith row of $A_f(x)$ consists of m_g elements, all members of $F_{\omega_{r+\delta-1}^i x}$, so the ith row of $A_f(x)$ consists of m_g out of the s components of $\tilde{\mathrm{ev}}(f)_{F_{\omega_{r+\delta-1}^i x}}$.

Let $Z_x = \{i \in [m_g] : \tilde{\mathrm{ev}}(f)_{F_{\omega^i_{r+\delta-1}x}} = 0\}$. If $b \pmod{s} \in \{0,\dots,s-m_g\}$, then for every $i \in Z_x$, by definition,

$$\begin{aligned}(0)_{j\in[m_g]} &= (\omega^{-i}_{r+\delta-1} f(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{j\in[m_g]}\\ &= (\omega^{-i}_{r+\delta-1} g(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{j\in[m_g]} + (\omega^{-i}_{r+\delta-1} h(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{j\in[m_g]}\end{aligned}$$

so

$$(\omega^{-i}_{r+\delta-1} g(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{j\in[m_g]} = (-\omega^{-i}_{r+\delta-1} h(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{j\in[m_g]}.$$

Fix $j \in [m_g]$ and consider the following column vector whose rows are restricted to Z_x,

$$\mathbf{c}_j = (\omega^{-i}_{r+\delta-1} h(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{i\in Z_x} \in \mathbb{F}_q^{|Z_x|}.$$

The points $\omega^i_{r+\delta-1}\omega^j_{q-1}x$, $i \in Z_x$ lie in the coset $\omega^j_{q-1}x\Omega_{r+\delta-1}$ because $\omega^i_{r+\delta-1} \in \Omega_{r+\delta-1}$ for all i. By Lemma 4.5, on this coset, there exists a polynomial $P_{j,x}(Y) = \sum_{t=1}^{\delta-1} p_{j,x,t}Y^t$ such that $\deg P_{j,x} \le \delta-1$, $P_{j,x}(0) = 0$, and for every $\omega \in \Omega_{r+\delta-1}$, $h(\omega^j_{q-1}x\cdot\omega) = P_{j,x}(\omega)$. Therefore,

$$\mathbf{c}_j = (\omega^{-i}_{r+\delta-1} P_{j,x}(\omega^i_{r+\delta-1}))_{i\in Z_x} = \sum_{t=1}^{\delta-1} p_{j,x,t}\cdot(\omega^{(t-1)\cdot i}_{r+\delta-1})_{i\in Z_x}$$

so $\mathbf{c}_j$ lies in the span of the $\delta-1$ vectors $(\omega^{0\cdot i}_{r+\delta-1})_{i\in Z_x}, \dots, (\omega^{(\delta-2)\cdot i}_{r+\delta-1})_{i\in Z_x}$. Since j was arbitrary, this is true for every $\mathbf{c}_j$, $j \in [m_g]$. Thus, the rank of

$$(-\omega^{-i}_{r+\delta-1} h(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{i\in Z_x, j\in[m_g]} = (\omega^{-i}_{r+\delta-1} g(\omega^i_{r+\delta-1}\omega^j_{q-1}x))_{i\in Z_x, j\in[m_g]}$$

is at most $\delta - 1$. Since, $[m_g] = Z_x \cup ([m_g] \setminus Z_x)$, the span of rows in $A_g(x)$ indexed by $[m_g] \setminus Z_x$ has dimension at most $m_g - |Z_x|$ and the span of the rows in $A_g(x)$ indexed by Z_x, as we just showed, has dimension at most $\delta - 1$. Hence, $\mathrm{rank}(A_g(x)) \le m_g - |Z_x| + \delta - 1$. By Lemma 6.4, $G(X)$ has a root of multiplicity $\ge |Z_x| - \delta + 1$ at $X = x$.

Summing over all $x = \omega^b_{q-1} \in \mathbb{F}_q^*$, it follows that the number of roots (with multiplicity) of $G(X)$ is at least

$$\begin{aligned}&\sum_{\substack{b\in[q-1]\\ b \bmod s\in\{0,\dots,s-m_g\}}} (|Z_{\omega^b_{q-1}}| - \delta + 1)\\ &\ge \sum_{x\in\mathbb{F}_q^*}(|Z_x| - \delta + 1) - \frac{(q-1)}{s}\cdot m_g\cdot(m_g-1)\\ &= \sum_{x\in\mathbb{F}_q^*}|Z_x| - (q-1)\left(\frac{m_g(m_g-1)}{s} + \delta - 1\right)\\ &= (q-1-|\tilde{\mathrm{ev}}(f)|s)m_g - (q-1)\left(\frac{m_g(m_g-1)}{s} + \delta - 1\right)\end{aligned}$$

$$= (q-1)m_g \left(1 - \frac{|\tilde{\mathrm{ev}}(f)| \cdot s}{q-1} - \frac{m_g - 1}{s} - \frac{\delta - 1}{m_g}\right).$$

Since $\deg G(X) \le m_g(\ell-1)$, $G(X)$ has at most $m_g(\ell-1)$ roots so

$$(q-1)m_g \left(1 - \frac{|\tilde{\mathrm{ev}}(f)| \cdot s}{q-1} - \frac{m_g - 1}{s} - \frac{\delta - 1}{m_g}\right) \le m_g(\ell-1)$$

and rearranging gives

$$|\tilde{\mathrm{ev}}(f)| \ge \frac{q-1}{s}\left(1 - \frac{\ell-1}{q-1} - \frac{m_g-1}{s} - \frac{\delta-1}{m_g}\right).$$

Combining the two bounds we obtain

$$d = \frac{q-1}{s}\left(1 - \frac{\ell-1}{q-1} - \epsilon\right)$$

for

$$\epsilon = \max_{1 \le m_f \le r+\delta-1} \min\left\{\left(1 - \frac{\ell-1}{q-1}\right)\frac{m_f-1}{r+\delta-1}, \max_{\max\{1, m_f-(\delta-1)\} \le m_g \le m_f} \frac{\delta-1}{m_g} + \frac{m_g-1}{s}\right\},$$

as desired.

■

Remark 6.6. The second case in the proof is a generalization of [14, Claim 68]. However, for us arguing the rank drop was more involved because the rows of $A_g(X)$ corresponding to Z_x were not all equal unlike in the proof of [14, Claim 68]. Instead, we looked at the columns of $A_g(X)$ restricted to Z_x and showed that its column rank must be $\le \delta - 1$ from which we could claim the multiplicity of a root of $G(X)$.

Remark 6.7. Since we require the uncertainty principle to hold for $r+\delta-1$ over $\mathbb{F}_q$, we must first fix δ then r and let q be a prime power that lies outside the finite set of characteristics where the uncertainty principle for $r+\delta-1$ does not hold.

6.1.1 Asymptotic distance bound

In order to obtain an asymptotic formulation of the distance, we desire to remove the m_f and m_g dependency in the distance bound. To that end, we present a technical lemma that will allow us to bound the ϵ in Theorem 6.5.

Lemma 6.8. *Let*

$$\epsilon = \max_{1 \le m_f \le r+\delta-1} \min\left\{\left(1 - \frac{\ell-1}{q-1}\right)\frac{m_f-1}{r+\delta-1}, \max_{\max\{1, m_f-(\delta-1)\} \le m_g \le m_f} \left(\frac{\delta-1}{m_g} + \frac{m_g-1}{s}\right)\right\}.$$

Let $n = r+\delta-1$ *and* $\lambda = 1 - \frac{\ell-1}{q-1}$. *If* $s = cn^2$ *for* $c \ge 2$, *then*

$$\epsilon \le \lambda\frac{\delta-2}{n} + \left(1 + \frac{1}{c}\right)\sqrt{\frac{\lambda(\delta-1)}{n}}.$$

Proof. Let $n := r + \delta - 1$ and $\lambda := 1 - \frac{\ell-1}{q-1}$. Define

$$\phi(m) := \frac{\delta - 1}{m} + \frac{m-1}{s}.$$

Then

$$\epsilon = \max_{1 \le m_f \le n} \min\left\{\lambda \frac{m_f - 1}{n},\ \max_{\max\{1, m_f-(\delta-1)\} \le m_g \le m_f} \phi(m_g)\right\}.$$

We first show that ϕ is nonincreasing on $[1, n]$. Indeed,

$$\phi'(m) = -\frac{\delta-1}{m^2} + \frac{1}{s}.$$

Since $s = cn^2$ with $c \ge 2$, we have

$$s \ge n^2 \ge \frac{n^2}{\delta - 1}.$$

Thus

$$\frac{1}{s} \le \frac{\delta-1}{n^2} \le \frac{\delta-1}{m^2} \qquad (1 \le m \le n),$$

and hence $\phi'(m) \le 0$ on $[1, n]$. Therefore, for fixed m_f, the maximum of $\phi(m_g)$ is attained at the left endpoint:

$$\max_{\max\{1, m_f-(\delta-1)\} \le m_g \le m_f} \phi(m_g) = \phi(\max\{1, m_f - (\delta - 1)\}).$$

Hence

$$\epsilon = \max_{1 \le m_f \le n} \min\left\{\lambda \frac{m_f - 1}{n},\ \phi(\max\{1, m_f - (\delta-1)\})\right\}.$$

We now split the maximum over m_f into two ranges.

Small-support range: $1 \le m_f < \delta$. In this range, $m_f - 1 \le \delta - 2$. Therefore

$$\min\left\{\lambda \frac{m_f - 1}{n},\ \phi(\max\{1, m_f - (\delta-1)\})\right\} \le \lambda \frac{m_f - 1}{n} \le \lambda \frac{\delta - 2}{n}.$$

Thus the contribution of all $m_f < \delta$ is at most $\lambda \frac{\delta-2}{n}$.

Large-support range: $\delta \le m_f \le n$. In this range, $m_f - (\delta - 1) = m_f - \delta + 1 \ge 1$. Therefore, $\max\{1, m_f - (\delta - 1)\} = m_f - \delta + 1$. Thus the large-support contribution is

$$\max_{\delta \le m_f \le n} \min\left\{\lambda \frac{m_f - 1}{n},\ \frac{\delta - 1}{m_f - \delta + 1} + \frac{m_f - \delta}{s}\right\}.$$

Set $u := m_f - \delta + 1$. Then $1 \le u \le r$, and $m_f - 1 = u + \delta - 2$. Hence

$$\lambda \frac{m_f - 1}{n} = \lambda \frac{u + \delta - 2}{n} = \lambda \frac{\delta - 2}{n} + \lambda \frac{u}{n},$$

while

$$\frac{\delta-1}{m_f-\delta+1}+\frac{m_f-\delta}{s}=\frac{\delta-1}{u}+\frac{u-1}{s}.$$

Therefore the large-support contribution is at most

$$\max_{1\le u\le r}\min\left\{\lambda\frac{\delta-2}{n}+\lambda\frac{u}{n},\ \frac{\delta-1}{u}+\frac{u-1}{s}\right\}.$$

Using

$$\min\{A+B,C\}\le A+\min\{B,C\},$$

with

$$A=\lambda\frac{\delta-2}{n},\qquad B=\lambda\frac{u}{n},\qquad C=\frac{\delta-1}{u}+\frac{u-1}{s},$$

we get

$$\max_{1\le u\le r}\min\left\{\lambda\frac{\delta-2}{n}+\lambda\frac{u}{n},\ \frac{\delta-1}{u}+\frac{u-1}{s}\right\}\le\lambda\frac{\delta-2}{n}+\max_{1\le u\le r}\min\left\{\lambda\frac{u}{n},\ \frac{\delta-1}{u}+\frac{u-1}{s}\right\}.$$

Furthermore, $(u-1)/s<u/s$, and enlarging the range from $1\le u\le r$ to $1\le u\le n$ gives

$$\max_{1\le u\le r}\min\left\{\lambda\frac{u}{n},\ \frac{\delta-1}{u}+\frac{u-1}{s}\right\}\le\max_{1\le u\le n}\min\left\{\lambda\frac{u}{n},\ \frac{\delta-1}{u}+\frac{u}{s}\right\}.$$

Combining the small-support and large-support ranges, we obtain

$$\epsilon\le\lambda\frac{\delta-2}{n}+\max_{1\le u\le n}\min\left\{\lambda\frac{u}{n},\ \frac{\delta-1}{u}+\frac{u}{s}\right\}.$$

It remains to bound the final maximum. We split into two cases.

Case 1: $\lambda\le\frac{1}{n}$. By definition,

$$\epsilon\le\max_{1\le m_f\le n}\lambda\frac{m_f-1}{n}\le\lambda.$$

Since $\delta\ge2$, we have

$$\lambda\le\frac{1}{n}\implies\lambda\le\sqrt{\frac{\lambda}{n}}\le\sqrt{\frac{\lambda(\delta-1)}{n}}.$$

Therefore

$$\lambda\le\lambda\frac{\delta-2}{n}+\left(1+\frac{1}{c}\right)\sqrt{\frac{\lambda(\delta-1)}{n}},$$

and the claim follows in this case.

Case 2: $\lambda>\frac{1}{n}$. Set

$$B(u):=\lambda\frac{u}{n},\qquad B(u):=\frac{\delta-1}{u}+\frac{u}{s}.$$

Then $B(u)$ is increasing. Also,

$$C'(u) = -\frac{\delta - 1}{u^2} + \frac{1}{s} \leq 0 \qquad (1 \leq u \leq n),$$

because $s \geq n^2/(\delta - 1)$. Hence $C(u)$ is nonincreasing on $[1, n]$.

The two curves $B(u)$ and $C(u)$ meet at the positive real number

$$u^* = \sqrt{\frac{\delta - 1}{\frac{\lambda}{n} - \frac{1}{s}}},$$

because the equation $B(u) = C(u)$ is

$$\lambda\frac{u}{n} = \frac{\delta - 1}{u} + \frac{u}{s} \iff \left(\frac{\lambda}{n} - \frac{1}{s}\right) u^2 = \delta - 1.$$

Since B is increasing and C is nonincreasing, we have $\max_{1 \leq u \leq n} \min\{B(u), C(u)\} \leq B(u^*)$. Thus,

$$\max_{1 \leq u \leq n} \min\left\{\lambda\frac{u}{n},\ \frac{\delta - 1}{u} + \frac{u}{s}\right\} \leq \lambda\frac{u^*}{n}.$$

Substituting the value of u^*, we obtain

$$\lambda\frac{u^*}{n} = \frac{\lambda}{n}\sqrt{\frac{\delta - 1}{\frac{\lambda}{n} - \frac{1}{s}}} = \sqrt{\frac{\lambda(\delta - 1)}{n}} \cdot \frac{1}{\sqrt{1 - \frac{n}{\lambda s}}}.$$

Since $\lambda > 1/n$, we have

$$\frac{n}{\lambda s} < \frac{n^2}{s} = \frac{1}{c}.$$

Therefore

$$\lambda\frac{u^*}{n} \leq \sqrt{\frac{\lambda(\delta - 1)}{n}} \cdot \frac{1}{\sqrt{1 - \frac{1}{c}}}.$$

For $c \geq 2$, we have $1/c \leq 1/2$, and

$$\frac{1}{\sqrt{1 - x}} \leq 1 + x \qquad (0 \leq x \leq 1/2).$$

Applying this with $x = 1/c$, we get

$$\frac{1}{\sqrt{1 - \frac{1}{c}}} \leq 1 + \frac{1}{c}.$$

Hence

$$\max_{1 \leq u \leq n} \min\left\{\lambda\frac{u}{n},\ \frac{\delta - 1}{u} + \frac{u}{s}\right\} \leq \left(1 + \frac{1}{c}\right)\sqrt{\frac{\lambda(\delta - 1)}{n}}.$$

Combining this with the previous reduction, we obtain

$$\epsilon \leq \lambda \frac{\delta - 2}{n} + \left(1 + \frac{1}{c}\right) \sqrt{\frac{\lambda(\delta - 1)}{n}},$$

as desired. ■

Now we get the following corollary for the asymptotic bound using Lemma 6.8.

Corollary 6.9. *Let $\tilde{\mathcal{Q}}$ be the folded QTB code from Theorem 6.5. If*

$$s \geq 2(r + \delta - 1)^2,$$

then $\tilde{\mathcal{Q}}$ has distance at least

$$d \geq \frac{q-1}{s} \left(\left(1 - \frac{\ell - 1}{q - 1}\right) \frac{r+1}{r+\delta-1} - \left(1 + \frac{(r+\delta-1)^2}{s}\right) \sqrt{\frac{\delta - 1}{r + \delta - 1} \left(1 - \frac{\ell - 1}{q - 1}\right)} \right).$$

Moreover, for every $0 < R < (r - \delta + 1)/(r + \delta - 1)$, there exists an explicit family of QLRCs of locality (r, δ), rate $\geq R$, and relative distance at least

$$\left(\frac{1}{2} - \frac{R}{2} \cdot \frac{r+\delta-1}{r-\delta+1}\right) \frac{r+1}{r+\delta-1} - \frac{3}{2} \sqrt{\frac{\delta-1}{r+\delta-1} \left(\frac{1}{2} - \frac{R}{2} \cdot \frac{r+\delta-1}{r-\delta+1}\right)}.$$

Proof. The first claim follows immediately from Lemma 6.8, since if $s = c(r + \delta - 1)^2$, then

$$1 + \frac{1}{c} = 1 + \frac{(r+\delta-1)^2}{s}.$$

For the second claim, recall from (4.21) that

$$\frac{\ell - 1}{q - 1} = \frac{1}{2} - \frac{1}{2(q-1)} \left(1 + (1+\epsilon)\frac{r+\delta-1}{r-\delta+1}\right) + \frac{R}{2} \cdot \frac{r+\delta-1}{r-\delta+1}.$$

Taking $q \to \infty$, we obtain

$$1 - \frac{\ell - 1}{q - 1} = \frac{1}{2} - \frac{R}{2} \cdot \frac{r+\delta-1}{r-\delta+1}.$$

Therefore the asymptotic relative distance is at least

$$\begin{aligned}
&\left(1 - \frac{\ell - 1}{q - 1}\right) \frac{r+1}{r+\delta-1} - \left(1 + \frac{(r+\delta-1)^2}{s}\right) \sqrt{\frac{\delta - 1}{r + \delta - 1} \left(1 - \frac{\ell - 1}{q - 1}\right)} \\
&= \left(\frac{1}{2} - \frac{R}{2} \cdot \frac{r+\delta-1}{r-\delta+1}\right) \frac{r+1}{r+\delta-1} - \left(1 + \frac{(r+\delta-1)^2}{s}\right) \sqrt{\frac{\delta-1}{r+\delta-1} \left(\frac{1}{2} - \frac{R}{2} \cdot \frac{r+\delta-1}{r-\delta+1}\right)}.
\end{aligned}$$

Since $s \geq 2(r + \delta - 1)^2$, we have

$$1 + \frac{(r+\delta-1)^2}{s} \leq \frac{3}{2},$$

which yields the claimed bound. ■

6.1.2 Composite-order distance relaxation

Using Corollary 2.30, we can relax the primality requirement on $r+\delta-1$ at the cost of a slightly weaker bound. This will be particularly useful when we generalize the fQTB code to its hierarchical analogue.

Corollary 6.10. *Let $\tilde{\mathcal{Q}}$ be the folded QTB code from Definition 6.1 with parameters q, r, δ, ℓ, s and set $n := r+\delta-1$. Assume that $n \mid (q-1)$ and $s \mid (q-1)/n$. Also assume that the finite-field composite-order uncertainty principle from Corollary 2.30 holds for order n over $\mathbb{F}_q$.*

For $1 \le m \le n$, define

$$u_n(m) := \frac{n}{d_1 d_2}(d_1 + d_2 - m),$$

where $d_1 < d_2$ are consecutive divisors of n satisfying $d_1 \le m \le d_2$. Equivalently, $u_n(m)$ is Meshulam's composite-order uncertainty lower bound for a polynomial with coefficient support size at most m.

Let $\lambda := 1-(\ell-1)/(q-1)$. Then $\tilde{\mathcal{Q}}$ has distance at least

$$d(\tilde{\mathcal{Q}}) \ge \frac{q-1}{s}\left(\lambda - \epsilon_{\text{comp}}\right),$$

where

$$\epsilon_{\text{comp}} = \max_{1 \le m_f \le n} \min\left\{\lambda\left(1 - \frac{u_n(m_f)}{n}\right), \max_{\max\{1, m_f-(\delta-1)\} \le m_g \le m_f}\left(\frac{\delta-1}{m_g} + \frac{m_g-1}{s}\right)\right\}.$$

Proof. The proof is the same two-case argument as in Theorem 6.5, except that the prime-order uncertainty principle, Corollary 2.31, is replaced by the composite-order uncertainty principle, Corollary 2.30.

Fix $\mathrm{ev}(f) \in C \setminus C^{\perp}$ and write $f = g + h$ where

$$g \in \mathbb{F}_q[X]^{[\ell]\setminus(S_- \cup S_+)}, \qquad h \in \mathbb{F}_q[X]^{[q-1]\cap S_+}.$$

Let $M_f = \{i \in [r+\delta-1] : \exists j \equiv i \mod r+\delta-1 \text{ with } f_j \neq 0\}$ and $m_f = |M_f|$ and similarly define M_g and m_g for g.

We first modify Case 1 of Theorem 6.5. For a coset $\alpha\Omega_n \subseteq \mathbb{F}_q^*$, the restriction of f to $\alpha\Omega_n$ is represented by

$$f \pmod{X^n - \alpha^n},$$

a polynomial of degree $< n$ whose coefficient support has size at most m_f. Hence, by the composite-order uncertainty principle, either $\mathrm{ev}(f)|_{\alpha\Omega_n} = 0$, or $|\mathrm{ev}(f)|_{\alpha\Omega_n} \ge u_n(m_f)$. As in the proof of Theorem 6.5, since $\mathrm{ev}(f) \notin C^{\perp}$, there is at least one residue class $i \in M_f \setminus \{1, \dots, \delta-1\}$. For this residue class, the coefficient of X^i in $f \pmod{X^n - \alpha^n}$ is a polynomial in α^n of degree at most $(\ell-1)/n$. Therefore this coefficient vanishes for at most $(\ell-1)/n$ cosets $\alpha\Omega_n$. Thus the number of cosets on which f does not vanish identically is at least

$$\frac{q-1}{n} - \frac{\ell-1}{n} = \frac{q-1}{n}\left(1 - \frac{\ell-1}{q-1}\right) = \frac{q-1}{n}\lambda.$$

Consequently,

$$|\mathrm{ev}(f)| \geq \frac{q-1}{n}\lambda \cdot u_n(m_f).$$

Since folding can reduce Hamming weight by at most a factor of s, we get

$$|\widetilde{\mathrm{ev}}(f)| \geq \frac{q-1}{s}\lambda\frac{u_n(m_f)}{n}.$$

Equivalently, Case 1 gives

$$|\widetilde{\mathrm{ev}}(f)| \geq \frac{q-1}{s}\left[\lambda - \lambda\left(1 - \frac{u_n(m_f)}{n}\right)\right].$$

Case 2, the determinant-polynomial argument in Theorem 6.5, is unchanged. It gives

$$|\widetilde{\mathrm{ev}}(f)| \geq \frac{q-1}{s}\left(\lambda - \frac{\delta-1}{m_g} - \frac{m_g-1}{s}\right).$$

Thus for fixed m_f, every codeword has folded weight at least

$$\frac{q-1}{s}\left(\lambda - \min\left\{\lambda\left(1-\frac{u_n(m_f)}{n}\right), \max_{\max\{1, m_f-(\delta-1)\}\leq m_g \leq m_f}\left(\frac{\delta-1}{m_g} + \frac{m_g-1}{s}\right)\right\}\right).$$

Taking the worst case over $1 \leq m_f \leq n$ gives the claimed expression for ϵ_{comp}. ■

6.2 Folded Hierarchical Quantum Tamo–Barg Codes

We now fold the hierarchical quantum Tamo–Barg codes from Section 6.1. Let $n_l := r_l+\delta_l-1$ for $l = 1, \ldots, h$ and assume $n_h \mid n_{h-1} \mid \cdots \mid n_1 \mid (q-1)$. Let $\omega_{q-1} \in \mathbb{F}_q^*$ be a generator. We choose a folding parameter $s \mid (q-1)/n_1$. Since $n_l \mid n_1$ for every l, this also implies $s \mid (q-1)/n_l$.

For $i = 0, \ldots, (q-1)/s - 1$, define the folded block

$$F_{\omega_{q-1}^{is}} := \{\omega_{q-1}^{is}, \omega_{q-1}^{is+1}, \ldots, \omega_{q-1}^{is+s-1}\}.$$

Equivalently, for $x = \omega_{q-1}^{b} \in \mathbb{F}_q^*$, let

$$F_x = \{\omega_{q-1}^{\lfloor b/s \rfloor s+j} : 0 \leq j \leq s-1\}.$$

Definition 6.11 (Folded Hierarchical Quantum Tamo–Barg code)**.** Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be the h-level quantum Tamo–Barg code from Definition 5.1. The **folded Hierarchical Quantum Tamo–Barg (fHQTB) code** is the CSS code $\widetilde{\mathcal{Q}} := \mathrm{CSS}(\widetilde{C}, \widetilde{C})$, where $\widetilde{C} \subseteq (\mathbb{F}_q^s)^{(q-1)/s}$ is obtained from C by grouping the coordinates indexed by each folded block $F_{\omega_{q-1}^{is}}$ into a single coordinate over the alphabet $\mathbb{F}_q^s$.

Folding preserves the rate, which we computed it in Lemma 5.4. We next check that the folded code retains the hierarchical locality structure.

Lemma 6.12. *Fix $l \in \{1, \dots, h\}$. Let $\alpha\Omega_{n_l}$ be a coset of Ω_{n_l} in $\mathbb{F}_q^*$. Then every folded block $F_{\omega_{q-1}^{is}}$ intersects $\alpha\Omega_{n_l}$ in at most one point.*

Proof. Write

$$\alpha = \omega_{q-1}^{b}, \qquad \Omega_{n_l} = \langle \omega_{q-1}^{(q-1)/n_l} \rangle.$$

Thus

$$\alpha\Omega_{n_l} = \left\{ \omega_{q-1}^{b+t\frac{q-1}{n_l}} : 0 \le t \le n_l - 1 \right\}.$$

Suppose two distinct elements of this coset lie in the same folded block. Then for some $t_1 \neq t_2$ and some $e_1, e_2 \in \{0, \dots, s-1\}$,

$$b + t_1 \frac{q-1}{n_l} \equiv is + e_1 \pmod{q-1},$$

and

$$b + t_2 \frac{q-1}{n_l} \equiv is + e_2 \pmod{q-1}.$$

Subtracting gives

$$(t_1 - t_2)\frac{q-1}{n_l} \equiv e_1 - e_2 \pmod{q-1}.$$

Since $s \mid (q-1)/n_l$, the left-hand side is divisible by s. Hence $e_1 - e_2$ is divisible by s. But

$$-(s-1) \le e_1 - e_2 \le s - 1,$$

so $e_1 = e_2$. Therefore

$$(t_1 - t_2)\frac{q-1}{n_l} \equiv 0 \pmod{q-1},$$

which implies

$$t_1 \equiv t_2 \pmod{n_l}.$$

Since $0 \le t_1, t_2 \le n_l - 1$, this forces $t_1 = t_2$, a contradiction. Thus the intersection has size at most one. ∎

Corollary 6.13. *The folded h-level quantum Tamo–Barg code $\widetilde{\mathcal{Q}}$ from Definition 6.11 is an h-level $((r_1, \delta_1), \dots, (r_h, \delta_h))$-QHLRC.*

Proof. Let $l \in \{1, \dots, h\}$. For a coset $\alpha\Omega_{n_l}$, define the folded level-l repair group

$$\widetilde{R}_{\alpha,l} := \{F_x : x \in \alpha\Omega_{n_l}\}.$$

By Lemma 6.12, the map $x \mapsto F_x$ is injective on $\alpha\Omega_{n_l}$. Therefore

$$|\widetilde{R}_{\alpha,l}| = |\alpha\Omega_{n_l}| = n_l = r_l + \delta_l - 1.$$

We now show that $\widetilde{R}_{\alpha,l}$ can correct $\delta_l - 1$ erasures. Let the elements of $\alpha\Omega_{n_l}$ be written as

$$\omega_{q-1}^{b+t(q-1)/n_l}, \qquad t = 0, \dots, n_l - 1.$$

Because $s \mid (q-1)/n_l$, all these elements occur in folded blocks with the same internal offset $b \bmod s$. More generally, for each internal offset $e \in \{0, \dots, s-1\}$, the e-th scalar components of the folded blocks in $\widetilde{R}_{\alpha,l}$ form a coset of Ω_{n_l}.

By the unfolded hierarchical locality proved in Corollary 5.6, on each such coset there are $\delta_l - 1$ independent local parity checks coming from $C^\perp$, and any $\delta_l - 1$ erased scalar positions in that coset can be recovered. Applying this scalar recovery independently to each of the s internal offsets recovers all s components of any $\delta_l - 1$ erased folded symbols in $\widetilde{R}_{\alpha,l}$.

The nesting of the folded repair groups follows from the nesting $\Omega_{n_h} \subseteq \cdots \subseteq \Omega_{n_1}$ and the injectivity of the folding map on every level-l coset. Hence $\widetilde{\mathcal{Q}}$ is an $((r_1, \delta_1), \dots, (r_h, \delta_h))$ QHLRC. ■

We now prove a distance bound for folded hierarchical QTB codes. The proof is the hierarchical analogue of the two-case argument for folded QTB codes. The first case uses the composite-order uncertainty principle on top-level cosets, while the second case applies the determinant-polynomial argument independently at each level of the hierarchy and retains the strongest resulting bound.

For $l = 1, \dots, h$, set $n_l := r_l + \delta_l - 1$, and assume $n_h \mid n_{h-1} \mid \cdots \mid n_1 \mid (q-1)$. Let

$$S_+ = \bigcup_{l=1}^{h} S_{l,+}, \qquad S_- = \bigcup_{l=1}^{h} S_{l,-}.$$

For each level l, define the level-l positive residue set

$$H_l := \{a \in [n_l] : \exists e \in S_+ \text{ such that } e \equiv a \pmod{n_l}\}.$$

Equivalently,

$$H_l = \bigcup_{u=1}^{h} \{a \in [n_l] : a \equiv j_u \pmod{\gcd(n_l, n_u)} \text{ for some } 1 \le j_u \le \delta_u - 1\}.$$

Since the n_l's form a divisibility chain, this set is easy to compute by reducing the hierarchical positive-residue set S_+ modulo n_l. Set $\kappa_l := |H_l|$.

For $1 \le m \le n_1$, define

$$u_{n_1}(m) := \frac{n_1}{d_1 d_2}(d_1 + d_2 - m),$$

where $d_1 < d_2$ are consecutive divisors of n_1 satisfying $d_1 \le m \le d_2$. This is the composite-order uncertainty lower bound.

Theorem 6.14 (Folded hierarchical QTB distance bound)**.** *Let $\widetilde{\mathcal{Q}} = \mathrm{CSS}(\widetilde{C}, \widetilde{C})$ be the folded h-level QTB code from Definition 6.11. Assume that the finite-field composite-order uncertainty principle from Corollary 2.30 holds for order n_1 over $\mathbb{F}_q$. Let*

$$\lambda := 1 - \frac{\ell - 1}{q - 1}.$$

For a nonzero codeword represented by $f = g + P$, define

$$M_{f,1} := \{a \in [n_1] : \exists e \equiv a \pmod{n_1} \text{ with } f_e \neq 0\},$$

and for each level l,

$$M_{g,l} := \{a \in [n_l] : \exists e \equiv a \pmod{n_l} \text{ with } g_e \neq 0\}.$$

Write

$$m_{f,1} := |M_{f,1}|, \qquad m_{g,l} := |M_{g,l}|.$$

Then every nonzero folded codeword satisfies

$$|\widetilde{\mathrm{ev}}(f)| \geq \frac{q-1}{s}\left(\lambda - \min\left\{\lambda\left(1 - \frac{u_{n_1}(m_{f,1})}{n_1}\right), \min_{1\leq l\leq h}\left(\frac{\kappa_l}{m_{g,l}} + \frac{m_{g,l}-1}{s}\right)\right\}\right).$$

Consequently,

$$d(\widetilde{\mathcal{Q}}) \geq \frac{q-1}{s}\left(\lambda - \epsilon_{\mathrm{hier}}\right),$$

where

$$\epsilon_{\mathrm{hier}} := \max_{\text{feasible profiles}} \min\left\{\lambda\left(1 - \frac{u_{n_1}(m_{f,1})}{n_1}\right), \min_{1\leq l\leq h}\left(\frac{\kappa_l}{m_{g,l}} + \frac{m_{g,l}-1}{s}\right)\right\}.$$

Here "feasible profiles" means all tuples

$$(m_{f,1}, m_{g,1}, \ldots, m_{g,h})$$

arising from some nonzero $f = g + P$ with $\mathrm{ev}(f) \in C \setminus C^\perp$ and

$$g \in \mathbb{F}_q[X]^{[\ell]\setminus(S_-\cup S_+)}, \qquad P \in \mathbb{F}_q[X]^{[q-1]\cap S_+}.$$

Proof. Fix $\widetilde{\mathrm{ev}}(f) \in \widetilde{C} \setminus \widetilde{C}^\perp$, and let $\mathrm{ev}(f) \in C \setminus C^\perp$ be the corresponding unfolded codeword. Decompose

$$f(X) = g(X) + P(X),$$

where

$$g \in \mathbb{F}_q[X]^{[\ell]\setminus(S_-\cup S_+)}, \qquad P \in \mathbb{F}_q[X]^{[q-1]\cap S_+}.$$

Since $\mathrm{ev}(P) \in C^\perp$ and $\mathrm{ev}(f) \notin C^\perp$, we have $g \neq 0$. We prove two lower bounds for $|\widetilde{\mathrm{ev}}(f)|$.

Case 1: the composite-order uncertainty bound. Consider a top-level coset $\alpha\Omega_{n_1} \subseteq \mathbb{F}_q^*$. The restriction of f to this coset is represented by $f \pmod{X^{n_1} - \alpha^{n_1}}$, a polynomial of degree $< n_1$ with coefficient support size at most $m_{f,1}$. By Corollary 2.30, either $\mathrm{ev}(f)|_{\alpha\Omega_{n_1}} = 0$, or

$$|\mathrm{ev}(f)|_{\alpha\Omega_{n_1}} \geq u_{n_1}(m_{f,1}).$$

Next, we bound the number of top-level cosets on which f vanishes identically. Let

$$H_1 = \{a \in [n_1] : \exists e \in S_+ \text{ with } e \equiv a \pmod{n_1}\}.$$

If $M_{f,1} \subseteq H_1$, then every exponent occurring in f lies in S_+, because membership in H_1 means that the entire congruence class modulo n_1 is contained in S_+. Hence $\mathrm{ev}(f) \in C^\perp$, contradicting our assumption. Therefore there exists $i \in M_{f,1} \setminus H_1$. For this residue class, the coefficient of X^i in $f \pmod{X^{n_1} - \alpha^{n_1}}$ is

$$\sum_j f_{i+n_1 j}(\alpha^{n_1})^j.$$

Because $i \notin H_1$, no exponent congruent to $i \pmod{n_1}$ lies in S_+. Thus these coefficients come only from the $[\ell]$-part of the code, and the above polynomial in α^{n_1} has degree at most$(\ell - 1)/n_1$. Consequently, it vanishes for at most $(\ell - 1)/n_1$ top-level cosets. Hence f is nonzero on at least

$$\frac{q-1}{n_1} - \frac{\ell - 1}{n_1} = \frac{q-1}{n_1}\lambda$$

top-level cosets. Therefore,

$$|\mathrm{ev}(f)| \geq \frac{q-1}{n_1}\lambda\, u_{n_1}(m_{f,1}).$$

Since folding decreases Hamming weight by at most a factor of s,

$$|\widetilde{\mathrm{ev}}(f)| \geq \frac{q-1}{s}\lambda\frac{u_{n_1}(m_{f,1})}{n_1}.$$

Equivalently,

$$|\widetilde{\mathrm{ev}}(f)| \geq \frac{q-1}{s}\left[\lambda - \lambda\left(1 - \frac{u_{n_1}(m_{f,1})}{n_1}\right)\right].$$

Case 2: determinant-polynomial bounds. We show that the determinant-polynomial argument can be applied at every level l. Fix $l \in \{1, \ldots, h\}$. Let ω_l be a primitive n_l-th root of unity and let ω_{q-1} be a generator of $\mathbb{F}_q^*$. Set $m_l := m_{g,l}$. Define

$$A_{g,l}(X) = \left(\omega_l^{-i} g(\omega_l^i \omega_{q-1}^j X)\right)_{0 \leq i,j \leq m_l - 1},$$

and define $A_{f,l}(X)$ and $A_{P,l}$ similarly. Let $G_l(X) := \det(A_{g,l}(X))$.

We first show that $G_l(X) \neq 0$. Decompose g by residue classes modulo n_l:

$$g(X) = \sum_{a \in M_{g,l}} X^a g_a(X^{n_l}).$$

Then

$$A_{g,l}(X) = \sum_{a\in M_{g,l}} \left(\omega_l^{(a-1)i}\right)_{0\le i\le m_l-1} \cdot \left(\sum_{e\equiv a \pmod{n_l}} g_e X^e (\omega_{q-1}^{ej})_{0\le j\le m_l-1} \right).$$

The column vectors

$$\left(\omega_l^{(a-1)i}\right)_{0\le i\le m_l-1}, \qquad a\in M_{g,l},$$

form a Vandermonde matrix and are linearly independent. The corresponding row vectors are also linearly independent over $\mathbb{F}_q[X]$: a nontrivial relation would give, by taking the highest-degree term in X, a nontrivial Vandermonde relation among

$$(\omega_{q-1}^{ej})_{0\le j\le m_l-1}$$

for distinct exponents e. Thus $A_{g,l}(X)$ has full rank over $\mathbb{F}_q(X)$, and hence $G_l(X) \neq 0$. Moreover, $\deg G_l \le m_l(\ell-1)$.

We now bound the number of roots of G_l. Fix $x = \omega_{q-1}^b \in \mathbb{F}_q^*$. If $b \bmod s \in \{0,\dots,s-m_l\}$, then for each $0\le i\le m_l-1$, the points

$$\omega_l^i\omega_{q-1}^j x, \qquad j=0,\dots,m_l-1,$$

lie in the folded block $F_{\omega_l^i x}$. Define

$$Z_{x,l} := \{0\le i\le m_l-1 : \widetilde{\mathrm{ev}}(f)_{F_{\omega_l^i x}} = 0\}.$$

For $i\in Z_{x,l}$, the i-th row of

$$A_{f,l}(x) := A_{g,l}(x) + A_{P,l}(x)$$

is zero, where

$$A_{P,l}(X) = \left(\omega_l^{-i} P(\omega_l^i\omega_{q-1}^j X)\right)_{0\le i,j\le m_l-1}.$$

Therefore, on the rows indexed by $Z_{x,l}$,

$$A_{g,l}(x) = -A_{P,l}(x).$$

We bound the rank of $A_{P,l}(x)$ restricted to the rows $Z_{x,l}$. Fix a column j. The points

$$\omega_l^i\omega_{q-1}^j x, \qquad i\in Z_{x,l},$$

lie in the level-l coset $\omega_{q-1}^j x\Omega_{n_l}$. Since the exponents of P lie in S_+, their residues modulo n_l lie in H_l. Thus, on this coset, P is a linear combination of monomials ω^a for $a\in H_l$ where $\omega\in\Omega_{n_l}$. After the row scaling by ω_l^{-i}, each column of the restricted matrix lies in the span of the κ_l vectors

$$(\omega_l^{(a-1)i})_{i\in Z_{x,l}}, \qquad a\in H_l.$$

Hence

$$\operatorname{rank}\left(A_{P,l}(x)|_{Z_{x,l},\,[m_l]}\right) \le \kappa_l.$$

It follows that

$$\operatorname{rank} A_{g,l}(x) \le m_l - |Z_{x,l}| + \kappa_l.$$

By Lemma 6.4, $G_l(X)$ has a root at $X = x$ of multiplicity at least $|Z_{x,l}| - \kappa_l$.

Summing over all $x = \omega_{q-1}^b \in \mathbb{F}_q^*$, and using the same folding-window count as in the one-level folded proof, the total number of roots of G_l, counted with multiplicity, is at least

$$(q-1)m_l\left(1 - \frac{|\widetilde{\mathrm{ev}}(f)|\, s}{q-1} - \frac{m_l - 1}{s} - \frac{\kappa_l}{m_l}\right).$$

Since $G_l \neq 0$ and $\deg G_l \le m_l(\ell - 1)$, we obtain

$$(q-1)m_l\left(1 - \frac{|\widetilde{\mathrm{ev}}(f)|\, s}{q-1} - \frac{m_l - 1}{s} - \frac{\kappa_l}{m_l}\right) \le m_l(\ell - 1).$$

Rearranging gives the level-l determinant bound

$$|\widetilde{\mathrm{ev}}(f)| \ge \frac{q-1}{s}\left(\lambda - \frac{\kappa_l}{m_{g,l}} - \frac{m_{g,l} - 1}{s}\right).$$

Since this holds for every level $l = 1, \ldots, h$, we may keep the strongest of these determinant bounds:

$$|\widetilde{\mathrm{ev}}(f)| \ge \frac{q-1}{s}\left(\lambda - \min_{1 \le l \le h}\left[\frac{\kappa_l}{m_{g,l}} + \frac{m_{g,l} - 1}{s}\right]\right).$$

Combining this with the uncertainty-case bound, we obtain

$$|\widetilde{\mathrm{ev}}(f)| \ge \frac{q-1}{s}\left(\lambda - \min\left\{\lambda\left(1 - \frac{u_{n_1}(m_{f,1})}{n_1}\right),\ \min_{1 \le l \le h}\left(\frac{\kappa_l}{m_{g,l}} + \frac{m_{g,l} - 1}{s}\right)\right\}\right).$$

Finally, taking the worst case over all feasible profiles gives the stated lower bound. ■

Remark 6.15. When $h = 1$, we have $H_1 = \{1, \ldots, \delta_1 - 1\}$, so $\kappa_1 = \delta_1 - 1$, and the theorem recovers the composite-order folded QTB distance bound presented in Corollary 6.10. For $h > 1$, each level l gives a valid determinant estimate, and the theorem keeps the best one. This is a genuine multilevel generalization of the determinant case. Nevertheless, the uncertainty case remains top-level because it is applied to restrictions of f on cosets of Ω_{n_1}.

Chapter 7

Decoding Quantum Tamo–Barg Codes

In this chapter, we present a classical decoding algorithm Dec_C to decode a (r,δ) Quantum Tamo–Barg code $\mathcal{Q} = \mathrm{CSS}(C,C)$ with parameters q,ℓ,r,δ as defined in Definition 4.1. Our decoding algorithm Dec_C can efficiently correct up to e errors. The algorithm $\mathrm{ListDec}_{\mathrm{RS}(q,\ell)}$ used in Algorithm 1 decodes a Reed-Solomon code as stated in Theorem 2.19. Recall that

$$S_{\pm} = \bigcup_{j=1}^{\delta-1} (\pm j + (r+\delta-1)\mathbb{Z})$$

and $B^{\perp} = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1]\cap S_+})$ is the space of piecewise polynomials of degree at most $\delta-1$ and no constant term, as shown in Lemma 4.5. Let $n := r+\delta-1$. Define the sets $\Gamma_i = \{0,\ldots,\delta-2,i\}$ for $i \in \{\delta-1,\ldots,n-1\}$. Also recall the polynomial Q_i as used in the proof of Theorem 4.12. The algorithm takes a corrupted codeword a as input and outputs a closest codeword $c' \in C$ such that $\mathrm{dis}(c'-a, C^{\perp})$ is less than e. The performance of Algorithm 1 is summarized in Theorem 7.1.

Theorem 7.1. *Let $\mathcal{Q}$ be the (r,δ) QTB code from Definition 4.1. If $\delta \geq 3$, assume $\mathrm{char}(\mathbb{F}_q) \nmid \mathcal{M}_{r,\delta}$ or if $\delta = 2$, assume $r+1$ is prime. Then $\mathcal{Q}$ can be decoded from errors of weight $< e$ for*

$$e = \frac{q-1}{4}\left(\frac{1}{\delta-1} + \frac{r}{r+\delta-1} - \sqrt{\left(\frac{r}{r+\delta-1} - \frac{1}{\delta-1}\right)^2 + \frac{4r}{(\delta-1)(r+\delta-1)}\cdot\frac{\ell}{q-1}}\right) \tag{7.1}$$

in $(q^{O(\delta)}\,\mathrm{poly}(r,q))$ time.

Remark 7.2. The error bound e in Theorem 7.1 is slightly less than half the distance bound in Theorem 4.12; one can see this by replacing ℓ with $\ell-1$ in the expression for e.

The following lemma helps prove that Algorithm 1 runs in polynomial-time. We show that computing $\mathrm{dis}(\mathrm{ev}(g)-a, B^{\perp})$ can be done efficiently. Let

$$\langle Y,\ldots,Y^{\delta-1}\rangle = \left\{ P(Y) \mid P(Y) = \sum_{j=1}^{\delta-1} y_j Y^j, \quad y_j \in \mathbb{F}_q \right\}.$$

Algorithm 1: Classical decoding algorithm for a (r,δ) Quantum Tamo–Barg code $\mathcal{Q} = \mathrm{CSS}(C, C)$ with parameters q, ℓ, r, δ.

Input : Corrupted codeword $a : \mathbb{F}_q^* \to \mathbb{F}_q$ with $\mathrm{dis}(a, C) < e$
Output: $c' \in C$ such that $\mathrm{dis}(c' - a, C^\perp) < e$
Function $\mathrm{Dec}_C(a)$**:**
  $\mathcal{L} \leftarrow \emptyset$
  for $i \in \{\delta - 1, \dots, r + \delta - 2\}$ **do**
    Fix $\omega \in \Omega_{r+\delta-1}$ and construct the Vandermonde matrix $V_i = [\omega^{(j-1)\gamma}]_{1 \le j \le \delta - 1, \gamma \in \Gamma_i}$ and let $v_i = (v_{i,0}, \dots, v_{i,\delta-2}, 1)$ be a nontrivial vector such that $V_i v_i = 0$.
    Define $a_i : \mathbb{F}_q^* \to \mathbb{F}_q$ by $a_i(X) = \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t} a(\omega^t X) + \omega^{-i} a(\omega^i X)$
    $\mathcal{L}_i \leftarrow \mathrm{ListDec}_{\mathrm{RS}(q,\ell)}(a_i)$
    for $g_i(X) = \sum_{j \in [\ell]} g_{i,j} X^j \in \mathcal{L}_i$ **do**
      if $g_{i,j} = 0$ *for every* $j \in S_- \cup S_+$ **then**
        Add $\mathrm{ev}\left(g(X) := \sum_{j \in [\ell] \setminus (S_- \cup S_+)} Q_i(\omega^{j-1})^{-1} g_{i,j} X^j\right)$ to $\mathcal{L}$
  return $\mathrm{argmin}_{\mathrm{ev}(g) \in \mathcal{L}} \mathrm{dis}(\mathrm{ev}(g) - a, B^\perp)$

Lemma 7.3. *Let* $B^\perp = \mathrm{ev}(\mathbb{F}_q[X]^{[q-1] \cap S_+})$ *be as in Lemma 4.3. Given a function* $b : \mathbb{F}_q^* \to \mathbb{F}_q$*, the quantity* $\mathrm{dis}(b, B^\perp)$ *can be computed by solving independent nearest-neighbor problems on the cosets of* Ω_n*, where* $n = r + \delta - 1$*. More precisely,*

$$\mathrm{dis}(b, B^\perp) = \sum_{\alpha\Omega_n} \left(n - \max_{P \in \langle Y, \dots, Y^{\delta-1} \rangle} |\{\omega \in \Omega_n : b(\alpha\omega) = P(\omega)\}| \right).$$

In particular, by exhaustive search over the $q^{\delta-1}$ *polynomials in* $\langle Y, \dots, Y^{\delta-1} \rangle$*, this can be computed in time* $O\left((q-1)q^{\delta-1}\delta\right)$*. Thus for fixed* δ*, the computation is polynomial in* q*.*

Proof. By Lemma 4.5, a function lies in $B^\perp$ if and only if, on every coset $\alpha\Omega_n$, it is represented by a polynomial

$$P_\alpha(Y) \in \langle Y, \dots, Y^{\delta-1} \rangle.$$

Moreover, the choices of the polynomials P_α on distinct cosets are independent. Therefore minimizing the Hamming distance to $B^\perp$ separates over cosets:

$$\mathrm{dis}(b, B^\perp) = \sum_{\alpha\Omega_n} \min_{P \in \langle Y, \dots, Y^{\delta-1} \rangle} |\{\omega \in \Omega_n : b(\alpha\omega) \neq P(\omega)\}|.$$

For a fixed coset, this is equal to

$$n - \max_{P \in \langle Y, \dots, Y^{\delta-1} \rangle} |\{\omega \in \Omega_n : b(\alpha\omega) = P(\omega)\}|.$$

This proves the formula.

For the runtime claim, the local space $\langle Y, \dots, Y^{\delta-1}\rangle$ has dimension $\delta - 1$ over $\mathbb{F}_q$, so it contains $q^{\delta-1}$ polynomials. For each such polynomial, we can evaluate it on the n points of Ω_n and count agreements in time $O(n\delta)$. Since there are $(q-1)/n$ cosets, this gives the stated runtime. ∎

Proof of Theorem 7.1. Let $\mathcal{Q} = \mathrm{CSS}(C, C)$ be the (r, δ) Quantum Tamo–Barg code with parameters q, ℓ, r, δ. To show Algorithm 1 efficiently decodes $\mathcal{Q}$, it is sufficient to show that any input corrupted word a can be written as $a = c+b$ where $c \in C$ and $b : \mathbb{F}_q^* \to \mathbb{F}_q$ is some corruption of Hamming weight $|b| < e$, and outputs $c' \in C$ such that $c' - c \in C^\perp$.

Assume $c = \mathrm{ev}(f)$ is a codeword in C. Let $n := r + \delta - 1$. Fix a coset $\alpha\Omega_n \in \mathbb{F}_q^*/\Omega_n$. Let $\Gamma_i = \{0, \dots, \delta - 2, i\}$ for $i \in \{\delta - 1, \dots, r + \delta - 2\}$. Construct the Vandermonde matrix $V_i = [\omega^{(j-1)\gamma}]_{1\le j\le\delta-1,\gamma\in\Gamma_i}$ which has rank $\delta-1$ and let $v_i = (v_{i,0}, \dots, v_{i,\delta-2}, 1)$ be a nontrivial vector such that $V_i v_i = 0$.

For a given $i \in \{\delta - 1, \dots, r + \delta - 2\}$, we have

$$a_i(x) = \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}a(\omega^t x) + \omega^{-i}a(\omega^i x)$$

equal to

$$c_i(x) = f_i(x) = \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}f(\omega^t x) + \omega^{-i}f(\omega^i x)$$

at every point x for which $\omega^\gamma x \notin \mathrm{supp}(b)$ for all $\gamma \in \Gamma_i$. Within a given coset $A := \alpha\Omega_n \in \mathbb{F}_q^*/\Omega_n$, the number of such points which are not in the support of b is $\psi(|b|_A)$ where

$$\psi(t) := (r - t)_+(n - (\delta - 1)t)_+$$

as in Lemma 4.11. Indeed, let

$$N_A := |\{x \in A : x, \omega x, \dots, \omega^{\delta-2}x \notin \mathrm{supp}(b)\}|.$$

Each error position in A can lie in at most $\delta-1$ of the consecutive blocks $\{x, \omega x, \dots, \omega^{\delta-2}x\}$, so

$$N_A \ge (n - (\delta - 1)|b|_A)_+.$$

For each such x, all $|b|_A$ errors lie among the remaining r possible positions indexed by $i \in \{\delta - 1, \dots, n - 1\}$. Hence at least $(r - |b|_A)_+$ choices of i remain valid. Therefore the contribution of the coset A is at least

$$(r - |b|_A)_+(n - (\delta - 1)|b|_A)_+ = \psi(|b|_A).$$

The function ψ is convex on $[0, \infty)$. Hence Jensen's inequality gives

$$\sum_{A\in\mathbb{F}_q^*/\Omega_n} \psi(|b|_A) \ge \frac{q-1}{n}\psi\left(\frac{n|b|}{q-1}\right).$$

Since $|b| < e$, it follows that
$$\psi\left(\frac{n|b|}{q-1}\right) \geq \psi\left(\frac{ne}{q-1}\right).$$
Therefore,
$$\sum_{A \in \mathbb{F}_q^*/\Omega_n} \psi(|b|_A) \geq \frac{q-1}{n}\psi\left(\frac{ne}{q-1}\right).$$
We now justify that the argument of ψ remains in the nonzero decreasing range for the value of e in (7.1). Set
$$\eta := \frac{1}{\delta-1}, \qquad \xi := \frac{r}{n}, \qquad \mu := \frac{\ell}{q-1},$$
and
$$H(Y) := \eta + \xi - \sqrt{(\xi-\eta)^2 + 4\eta\xi Y}.$$
Then (7.1) says
$$e = \frac{q-1}{4}H(\mu).$$
Since H is decreasing in Y and $0 \leq Y < 1$, we have
$$H(\mu) \leq H(0) = \eta + \xi - |\xi - \eta| = 2\min\{\eta, \xi\}.$$
Thus
$$e \leq \frac{q-1}{2}\min\left\{\frac{1}{\delta-1}, \frac{r}{n}\right\}.$$
Multiplying by $n/(q-1)$, we obtain
$$\frac{ne}{q-1} \leq \frac{1}{2}\min\left\{\frac{n}{a}, r\right\}.$$
Therefore
$$\frac{ne}{q-1} < \min\left\{\frac{n}{a}, r\right\},$$
so $\frac{ne}{q-1}$ lies in the nonzero range of ψ. Therefore,
$$\frac{q-1}{n}\psi\left(\frac{ne}{q-1}\right) = \frac{(\delta-1)n}{q-1}\left(\frac{r(q-1)}{n} - e\right)^2 - ((r-1)(\delta-1)-r)\left(\frac{r(q-1)}{n} - e\right).$$
Averaging over all $i \in \{\delta-1, \ldots, r+\delta-2\}$, there must be some i such that
$$\begin{aligned} &|\{x \in \mathbb{F}_q^* : a_i(x) = f_i(x)\}| \\ &\geq \frac{(\delta-1)n}{r(q-1)}\left(\frac{r(q-1)}{n} - e\right)^2 - \frac{((r-1)(\delta-1)-r)}{r}\left(\frac{r(q-1)}{n} - e\right). \end{aligned} \tag{7.2}$$

Recall that by Lemma 4.3, since $C = \mathrm{ev}(\mathbb{F}_q[X]^S)$ for
$$S = ([\ell] \setminus S_-) \cup ([q-1] \cap S_+)$$

we may write $f(X) = g(X) + h(X)$ where $g(X) \in \mathbb{F}_q[X]^{[\ell]\setminus(S_- \cup S_+)}$ and $h(X) \in \mathbb{F}_q[X]^{[q-1]\cap S_+}$. Define g_i, h_i analogously to f_i so $f_i = g_i + h_i$. Consider the polynomial

$$Q_i(Y) = \sum_{t=0}^{\delta-2} v_{i,t} Y^t + Y^i.$$

By construction, $Q_i(\omega^\gamma) = 0$ for $\gamma = 0, \dots, \delta - 2$. For a coset element $x \in \alpha\Omega_n$,

$$\sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t}(\omega^t x)^j + \omega^{-i}(\omega^i x)^j = x^j \left(\sum_{t=0}^{\delta-2} v_{i,t}\omega^{(j-1)t} + \omega^{(j-1)i} \right) = x^j Q_i(\omega^{j-1}) = 0$$

for $j = 1, \dots, \delta - 1$. It follows that

$$h_i(x) = \sum_{t=0}^{\delta-2} v_{i,t}\omega^{-t} h(\omega^t x) + \omega^{-i} h(\omega^i x) = 0$$

for all $x \in \mathbb{F}_q^*$ so $f_i = g_i$. Therefore, (7.2) is equivalent to

$$\begin{aligned} &|\{x \in \mathbb{F}_q^* : a_i(x) = g_i(x)\}| \\ &\geq \frac{(\delta-1)n}{r(q-1)} \left(\frac{r(q-1)}{n} - e \right)^2 - \frac{((r-1)(\delta-1)-r)}{r} \left(\frac{r(q-1)}{n} - e \right). \end{aligned} \tag{7.3}$$

The coefficients of g_i are given by

$$g_{i,j} = Q_i(\omega^{j-1}) g_j$$

so g and g_i have coefficients of the same support by Corollary 4.9. In particular, $\deg g_i = \deg g < \ell$ so $\mathrm{ev}(g_i) \in \mathrm{RS}(q, \ell)$ is a Reed-Solomon codeword. Therefore, (7.3) says $a_i = \mathrm{ev}(g_i) + b_i$ is a corrupted Reed-Solomon codeword with

$$\begin{aligned} |b_i| &= q - 1 - |\{x \in \mathbb{F}_q^* : a_i(x) = g_i(x)\}| \\ &\leq q - 1 - \frac{(\delta-1)n}{r(q-1)} \left(\frac{r(q-1)}{n} - e \right)^2 - \frac{((r-1)(\delta-1)-r)}{r} \left(\frac{r(q-1)}{n} - e \right) \\ &= (q-1) \left(1 - \frac{(\delta-1)n}{r} \left(\frac{r}{n} - \frac{e}{q-1} \right)^2 + \frac{((r-1)(\delta-1)-r)}{r} \left(\frac{r}{n} - \frac{e}{q-1} \right) \right) \end{aligned}$$

By Theorem 2.19, the output of running $\mathrm{ListDec}_{\mathrm{RS}(q,\ell)}(a_i)$ is a list containing $\mathrm{ev}(g_i)$ as long as

$$1 - \frac{(\delta-1)n}{r} \left(\frac{r}{n} - \frac{e}{q-1} \right)^2 + \frac{((r-1)(\delta-1)-r)}{r} \left(\frac{r}{n} - \frac{e}{q-1} \right) < 1 - \sqrt{\frac{\ell}{q-1}}$$

which simplifies to needing

$$e < \frac{q-1}{2}\left(\frac{1}{\delta-1}+\frac{r}{n}-\sqrt{\left(\frac{r}{n}-\frac{1}{\delta-1}\right)^2+\frac{4r}{(\delta-1)n}\cdot\sqrt{\frac{\ell}{q-1}}}\right). \tag{7.4}$$

Let

$$\eta = \frac{1}{\delta-1}, \quad \xi = \frac{r}{n}, \quad \mu = \frac{\ell}{q-1},$$

and

$$H(Y) = \eta + \xi - \sqrt{(\xi-\eta)^2 + 4\eta\xi Y}.$$

Substituting the variables, by the assumption of (7.1) on e, (7.4) holds if we can show that $H(\mu) < 2H(\sqrt{\mu})$. Since $0 \le \mu < 1$, letting $F(Y) = 2H(Y) - H(Y^2)$, it suffices to show $F(Y) > 0$ for $0 \le Y < 1$. Differentiating,

$$F'(Y) = -\frac{4\eta\xi}{\sqrt{(\xi-\eta)^2+4\eta\xi Y}} + \frac{4\eta\xi Y}{\sqrt{(\xi-\eta)^2+4\eta\xi Y^2}}$$

and $F'(Y) < 0$ is equivalent to

$$\frac{Y}{\sqrt{(\xi-\eta)^2+4\eta\xi Y^2}} < \frac{1}{\sqrt{(\xi-\eta)^2+4\eta\xi Y}} \iff (1-Y^2)(\xi-\eta)^2 + 4\eta\xi Y^2(1-Y) > 0$$

which is true for $0 \le Y < 1$. Hence, F is decreasing on $[0,1)$ and $F(1) = 0$ so $F > 0$ on $[0,1)$.

Therefore, $\mathcal{L}_i$ in Algorithm 1 will contain g_i and after iteration i, $\mathcal{L}$ will contain $\mathrm{ev}(g)$. If Algorithm 1 outputs $\mathrm{ev}(g') \in \mathcal{L}$, then $g' \in \mathbb{F}_q[X]^{[\ell]\setminus(S_-\cup S_+)}$ and

$$\mathrm{dis}(\mathrm{ev}(g') - a, B^\perp) \le \mathrm{dis}(\mathrm{ev}(g) - a, B^\perp) \le |\mathrm{ev}(g+h) - a| = |\mathrm{ev}(f) - a| = |b| < e.$$

Since $B^\perp \subseteq C^\perp$, we have $\mathrm{dis}(\mathrm{ev}(g) - a, C^\perp) < e$ and $\mathrm{dis}(\mathrm{ev}(g') - a, C^\perp) < e$ so $\mathrm{dis}(\mathrm{ev}(g) - \mathrm{ev}(g'), C^\perp) < 2e$. By definition of e and Theorem 4.12, $\mathcal{Q}$ has distance $\min_{c\in C\setminus C^\perp} |c| \ge 2e$ so $\mathrm{ev}(g) - \mathrm{ev}(g') \in C^\perp$. Thus, $\mathrm{Dec}_C(a)$ outputs some $\mathrm{ev}(g') \in \mathrm{ev}(g) + C^\perp$, as desired.

The calls to $\mathrm{ListDec}_{\mathrm{RS}(q,\ell)}$ run in $q^{O(1)}$ time. Lemma 7.3 implies the last line of Algorithm 1 runs in $O(|\mathcal{L}| \cdot (q-1)q^{\delta-1}\delta) = (q^{O(\delta)}\,\mathrm{poly}(r,q))$ time. The rest of Algorithm 1 also runs in $(q^{O(\delta)}\,\mathrm{poly}(r,q))$ time so the entire decoding procedure takes $(q^{O(\delta)}\,\mathrm{poly}(r,q))$ time. ■

Remark 7.4. The decoding algorithm in Algorithm 1 efficiently decodes (r,δ) Quantum Tamo–Barg (QTB) codes. Moreover, extending Algorithm 1 similarly to [14, Algorithm 2], we can obtain a decoding algorithm for the folded quantum Tamo–Barg codes presented in Section 6.1.

Bibliography

[1] Sean Ballentine, Alexander Barg, and Serge Vlăduţ. "Codes With Hierarchical Locality From Covering Maps of Curves". In: *IEEE Transactions on Information Theory* 65.10 (2019), pp. 6056–6071. DOI: 10.1109/TIT.2019.2919830.

[2] Kaifeng Bu, Weichen Gu, and Xiang Li. *Quantum locally recoverable code with intersecting recovery sets*. 2025. arXiv: 2501.10354 [quant-ph]. URL: https://arxiv.org/abs/2501.10354.

[3] A. R. Calderbank and Peter W. Shor. "Good quantum error-correcting codes exist". In: *Physical Review A* 54.2 (Aug. 1996), pp. 1098–1105. ISSN: 1094-1622. DOI: 10.1103/physreva.54.1098. URL: http://dx.doi.org/10.1103/PhysRevA.54.1098.

[4] Augustin-Louis Cauchy. "Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment". In: *Journal de l'École polytechnique* 10.17 (1815). OEuvres complètes, ser. 2, vol. 1, pp. 91–169, pp. 29–112.

[5] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, July 2006. ISBN: 0471241954.

[6] David A Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. 2nd. Vol. 185. Graduate Texts in Mathematics. New York: Springer Science & Business Media, 2005. ISBN: 978-0-387-20706-3.

[7] P. G. Lejeune Dirichlet. "Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält". In: *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin* 48 (1837), pp. 45–71.

[8] Carlos Galindo, Fernando Hernando, and Ryutaroh Matsumoto. *Quantum (r, δ)-Locally Recoverable BCH and Homothetic-BCH Codes*. 2026. arXiv: 2601.22567 [cs.IT]. URL: https://arxiv.org/abs/2601.22567.

[9] Carlos Galindo et al. *Optimal quantum locally recoverable codes from matrix-product construction*. 2025. arXiv: 2310.15703 [cs.IT]. URL: https://arxiv.org/abs/2310.15703.

[10] Carlos Galindo et al. *Quantum (r, δ)-locally recoverable codes*. 2024. arXiv: 2412.16590 [cs.IT]. URL: https://arxiv.org/abs/2412.16590.

[11] Robert B. Gardner and N. K. Govil. "Eneström–Kakeya Theorem and Some of Its Generalizations". In: *Current Topics in Pure and Computational Complex Analysis*. Ed. by Santosh Joshi, Michael Dorff, and Indrajit Lahiri. New Delhi: Springer India, 2014, pp. 171–199. ISBN: 978-81-322-2113-5. DOI: 10.1007/978-81-322-2113-5_8. URL: https://doi.org/10.1007/978-81-322-2113-5_8.

[12] Izrail Moiseevich Gelfand, Mikhail M Kapranov, and Andrei V Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Boston: Birkhäuser, 1994. ISBN: 978-0-8176-3660-9.

[13] Daniel Goldstein, Robert M. Guralnick, and I. M. Isaacs. "Inequalities for finite group permutation modules". In: *Transactions of the American Mathematical Society* 357.10 (May 2005), pp. 4017–4042. DOI: 10.1090/s0002-9947-05-03927-9.

[14] Louis Golowich and Venkatesan Guruswami. "Quantum locally recoverable codes". In: *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM. 2025, pp. 5512–5522.

[15] Parikshit Gopalan et al. "On the locality of codeword symbols". In: *IEEE Trans. on Inf. Theory* 58.11 (2012), pp. 6925–6934.

[16] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. 1997. arXiv: quant-ph/9705052 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/9705052.

[17] M. Grassl, Th. Beth, and T. Pellizzari. "Codes for the quantum erasure channel". In: *Physical Review A* 56.1 (July 1997), pp. 33–38. ISSN: 1094-1622. DOI: 10.1103/physreva.56.33. URL: http://dx.doi.org/10.1103/PhysRevA.56.33.

[18] Markus Grassl. "Algebraic quantum codes: linking quantum mechanics and discrete mathematics". In: *International Journal of Computer Mathematics: Computer Systems Theory* 6.4 (2021), pp. 243–259. DOI: 10.1080/23799927.2020.1850530. eprint: https://doi.org/10.1080/23799927.2020.1850530. URL: https://doi.org/10.1080/23799927.2020.1850530.

[19] Jaron Skovsted Gundersen et al. "Puncturing Quantum Stabilizer Codes". In: *IEEE Journal on Selected Areas in Information Theory* 6 (2025), pp. 74–84. ISSN: 2641-8770. DOI: 10.1109/jsait.2025.3562287. URL: http://dx.doi.org/10.1109/JSAIT.2025.3562287.

[20] V. Guruswami and M. Sudan. "Improved decoding of Reed-Solomon and algebraic-geometric codes". In: *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*. 1998, pp. 28–37. DOI: 10.1109/SFCS.1998.743426.

[21] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[22] C.G.J. Jacobi. "De functionibus alternantibus earumque divisione per productum e differentiis elementorum conflatum." lat. In: *Journal für die reine und angewandte Mathematik* 22 (1841), pp. 360–371. URL: http://eudml.org/doc/147139.

[23] Govinda M. Kamath et al. “Codes with local regeneration”. In: *2013 Information Theory and Applications Workshop (ITA)*. 2013, pp. 1–5. DOI: 10.1109/ITA.2013.6502947.

[24] Govinda M. Kamath et al. “Codes With Local Regeneration and Erasure Correction”. In: *IEEE Trans. on Inf. Theory* 60.8 (2014), pp. 4637–4660. DOI: 10.1109/TIT.2014.2329872.

[25] Yang Li et al. *Improved bounds and optimal constructions of pure quantum locally recoverable codes*. 2025. arXiv: 2512.07256 [cs.IT]. URL: https://arxiv.org/abs/2512.07256.

[26] Yang Li et al. *On optimal quantum LRCs from the Hermitian construction and t-designs*. 2025. arXiv: 2508.13553 [cs.IT]. URL: https://arxiv.org/abs/2508.13553.

[27] Gaojun Luo et al. *Bounds and Constructions of Quantum Locally Recoverable Codes from Quantum CSS Codes*. 2023. arXiv: 2312.11115 [cs.IT]. URL: https://arxiv.org/abs/2312.11115.

[28] Roy Meshulam. “An uncertainty inequality for finite abelian groups”. In: *European Journal of Combinatorics* 27.1 (2006), pp. 63–67. ISSN: 0195-6698. DOI: https://doi.org/10.1016/j.ejc.2004.07.009. URL: https://www.sciencedirect.com/science/article/pii/S0195669804001453.

[29] Jürgen Neukirch. *Algebraic Number Theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften. Berlin, Heidelberg: Springer-Verlag, 1999. ISBN: 978-3-540-65399-8. DOI: 10.1007/978-3-662-03983-0.

[30] Birenjith Sasidharan, Gaurav Kumar Agarwal, and P. Vijay Kumar. “Codes with hierarchical locality”. In: *2015 IEEE International Symposium on Information Theory (ISIT)*. 2015, pp. 1257–1261. DOI: 10.1109/ISIT.2015.7282657.

[31] Sandeep Sharma, Vinayak Ramkumar, and Itzhak Tamo. *Quantum Locally Recoverable Codes via Good Polynomials*. 2024. arXiv: 2411.01504 [cs.IT]. URL: https://arxiv.org/abs/2411.01504.

[32] Andrew Steane. “Multiple-particle interference and quantum error correction”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 452.1954 (Nov. 1996), pp. 2551–2577. ISSN: 1471-2946. DOI: 10.1098/rspa.1996.0136. URL: http://dx.doi.org/10.1098/rspa.1996.0136.

[33] Itzhak Tamo and Alexander Barg. “A Family of Optimal Locally Recoverable Codes”. In: *IEEE Transactions on Information Theory* 60.8 (2014), pp. 4661–4676. DOI: 10.1109/TIT.2014.2321280.

[34] Terence Tao. “An uncertainty principle for cyclic groups of prime order”. In: *arXiv Mathematics e-prints*, math/0308286 (Aug. 2003), math/0308286. DOI: 10.48550/arXiv.math/0308286. arXiv: math/0308286 [math.CA].

[35] James D. Teoh et al. “Dual-rail encoding with superconducting cavities”. In: *Proceedings of the National Academy of Sciences* 120.41 (Oct. 2023). ISSN: 1091-6490. DOI: 10.1073/pnas.2221736120. URL: http://dx.doi.org/10.1073/pnas.2221736120.

[36] N. Trudi. *Teoria de' determinanti e loro applicazioni*. Libreria scientifica e industriale di B. Pellerano, 1862. URL: https://books.google.com/books?id=sIVZc_PczqsC.

[37] Yue Wu et al. “Erasure conversion for fault-tolerant quantum computing in alkaline earth Rydberg atom arrays”. In: *Nature Communications* 13.1 (Aug. 2022). ISSN: 2041-1723. DOI: 10.1038/s41467-022-32094-6. URL: http://dx.doi.org/10.1038/s41467-022-32094-6.

[38] Kun Zhou and Meng Cao. *Optimal Quantum* (r, δ)*-Locally Repairable Codes via Classical Ones*. 2025. arXiv: 2507.18175 [quant-ph]. URL: https://arxiv.org/abs/2507.18175.

Appendix A

Code Files

Below is the SageMath code used for the computations in Example 4. The first script is to compute the resultant product and the second script is to compute the dimension and distance.

```
# SageMath code for computing M_{r,delta}
# M_{r,delta} = product_{m=0}^{r-1} product_{s=delta-1}^{n-1}
# Res(A_{m,s}(X), Phi_n(X)),
# where A_{m,s}(X) = h_m(1, X, X^2, ..., X^{delta-2}, X^s).

def complete_homogeneous_specialization(m, exponents):
 """
 Return h_m(X^e for e in exponents) as a polynomial in ZZ[X].

 The generating function is
 sum_{m >= 0} h_m T^m = product_{e in exponents} 1/(1 - X^e T).

 We compute the coefficient of T^m by dynamic programming.
 """
 R.<X> = PolynomialRing(ZZ)

 # coeffs[j] will store the coefficient of T^j
 coeffs = [R(0)] * (m + 1)
 coeffs[0] = R(1)

 for e in exponents:
 new_coeffs = [R(0)] * (m + 1)

 # multiply by 1 + X^e T + X^{2e} T^2 + ... + X^{me} T^m
 for old_deg in range(m + 1):
 if coeffs[old_deg] == 0:
 continue
 for add_deg in range(m - old_deg + 1):
```

```
 new_coeffs[old_deg + add_deg] += coeffs[old_deg] * X^(e * add_deg)

 coeffs = new_coeffs

 return coeffs[m]


def A_m_s_poly(r, delta, m, s):
 """
 Construct A_{m,s}(X) = h_m(1, X, ..., X^{delta-2}, X^s).
 """
 exponents = list(range(delta - 1)) + [s]
 return complete_homogeneous_specialization(m, exponents)


def M_r_delta(r, delta, verbose=False):
 """
 Compute M_{r,delta} and return:
 M_abs: absolute value of the product of resultants
 factors: prime factorization of M_abs
 data: list of ((m,s), resultant, factorization)
 """
 R.<X> = PolynomialRing(ZZ)

 n = r + delta - 1
 Phi = cyclotomic_polynomial(n, var=X)

 M = ZZ(1)
 data = []

 for m in range(r):
 for s in range(delta - 1, n):
 A = A_m_s_poly(r, delta, m, s)
 Res = A.resultant(Phi)
 Res_abs = abs(ZZ(Res))

 M *= Res_abs
 data.append(((m, s), Res, factor(Res_abs)))

 if verbose and Res_abs != 1:
 print(f"(m,s)=({m},{s}), Res={Res}, factor={factor(Res_abs)}")

 M_abs = abs(ZZ(M))
 return M_abs, factor(M_abs), data

```

```

# Compute the two examples:
M43, fac43, data43 = M_r_delta(4, 3, verbose=True)
print("M_{4,3} =", M43)
print("factor(M_{4,3}) =", fac43)
print("bad characteristics for (r,delta)=(4,3):", sorted([p for p, e in fac43]))

print()

M94, fac94, data94 = M_r_delta(9, 4, verbose=True)
print("M_{9,4} =", M94)
print("factor(M_{9,4}) =", fac94)
print("bad characteristics for (r,delta)=(9,4):", sorted([p for p, e in fac94]))
```

Listing A.1: SageMath code for the resultant product computation

```
# SageMath code for Example~\ref{ex:two_level_qtb_vs_one_level_true_distance}

q = 25
F.<a> = GF(q)
gamma = F.multiplicative_generator()
N = q - 1

# We use exponents in {0,...,q-2}.
# The coordinate ordering is gamma^0, gamma^1, ..., gamma^{q-2}.

def plus_set(n, delta):
 return {
 e for e in range(N)
 if any(e % n == j % n for j in range(1, delta))
 }

def minus_set(n, delta):
 return {
 e for e in range(N)
 if any(e % n == (-j) % n for j in range(1, delta))
 }

def support_one_level(ell):
 """
 One-level QTB support sets with (r,delta)=(9,4), so n=12.
 """
 n1, delta1 = 12, 4
```

```
    Splus = plus_set(n1, delta1)
    Sminus = minus_set(n1, delta1)

    S = (set(range(ell)) - Sminus) | Splus
    T = ((set(range(q - ell)) - {0}) - Sminus) | Splus

    return sorted(S), sorted(T)

def support_two_level(ell):
    """
    Two-level hierarchical QTB support sets with
    (r_1,delta_1)=(9,4), n_1=12,
    (r_2,delta_2)=(4,3), n_2=6.
    """
    n1, delta1 = 12, 4
    n2, delta2 = 6, 3

    Splus = plus_set(n1, delta1) | plus_set(n2, delta2)
    Sminus = minus_set(n1, delta1) | minus_set(n2, delta2)

    S = (set(range(ell)) - Sminus) | Splus
    T = ((set(range(q - ell)) - {0}) - Sminus) | Splus

    return sorted(S), sorted(T)

def eval_matrix(exponents):
    """
    Generator matrix for ev(F_q[X]^exponents) evaluated on F_q^*.
    Rows are exponent evaluation vectors.
    """
    return Matrix(F, [
        [(gamma^k)^e for k in range(N)]
        for e in exponents
    ])

def css_distance(S, T, assume_cyclic=True):
    """
    Computes the exact CSS distance for CSS(C,C), where
    C = ev(F_q[X]^S) and C^perp = ev(F_q[X]^T).

    We use the shortened-support criterion:
    d = min |U| such that
    dim(C cap F_q^U) > dim(C^perp cap F_q^U).

    Since C = (C^perp)^perp, a generator matrix for C^perp
```

```
 is a parity-check matrix for C. Thus
 dim(C cap F_q^U) = |U| - rank(H_U),
 where H is a generator matrix for C^perp.

 Also
 dim(C^perp cap F_q^U)
 = dim(C^perp) - rank(G_{C^perp,U^c}).

 The code is cyclic, so when assume_cyclic=True we only search
 supports U containing coordinate 0.
 """
 H = eval_matrix(T)
 dim_D = H.rank()
 coords = list(range(N))

 for wt in range(1, N + 1):
  if assume_cyclic:
   iterator = Subsets(coords[1:], wt - 1)
  else:
   iterator = Subsets(coords, wt)

 for tail in iterator:
  if assume_cyclic:
   U = set([0]) | set(tail)
  else:
   U = set(tail)

 U = sorted(U)
 Uc = [i for i in coords if i not in U]

 H_U = H.matrix_from_columns(U)
 H_Uc = H.matrix_from_columns(Uc)

 dim_C_shortened = wt - H_U.rank()
 dim_D_shortened = dim_D - H_Uc.rank()

 if dim_C_shortened > dim_D_shortened:
  return wt, U

 return None, None

print("ell | k_one | d_one | k_hier | d_hier")
print("--------------------------------------")

for ell in range(13, 25):
```

```
S1, T1 = support_one_level(ell)
Sh, Th = support_two_level(ell)

k_one = len(S1) - len(T1)
k_hier = len(Sh) - len(Th)

d_one, U_one = css_distance(S1, T1)
d_hier, U_hier = css_distance(Sh, Th)

print(f"{ell:2d} | {k_one:5d} | {d_one:5d} | {k_hier:6d} |
    {d_hier:6d}")
```

Listing A.2: SageMath code for the exact-distance computation