# QUANTUM MAXIMUM DISTANCE SEPERABLE CODES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

MUSTAFA KIRCALI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

FEBRUARY 2025

Approval of the thesis:

**QUANTUM MAXIMUM DISTANCE SEPERABLE CODES**

submitted by **MUSTAFA KIRCALI** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Cryptography Department, Middle East Technical University** by,

Prof. Dr. Ayşe Sevtap KESTEL _____
Dean, Graduate School of **Applied Mathematics**

Assoc. Prof. Dr. Oğuz Yayla _____
Head of Department, **Cryptography**

Assist. Prof. Dr. Buket Özkaya _____
Supervisor, **Cryptography, METU**

Prof. Dr. Ferruh Özbudak _____
Co-supervisor, **Mathematics, Sabancı University**

**Examining Committee Members:**

Prof. Dr. Burcu Gülmez Temuz
Mathematics, Atılım University _____

Assist. Prof. Dr. Buket Ozkaya
Cryptography, METU _____

Prof. Dr. Barış Bülent Kırlar
Mathematics, Suleyman Demirel University _____

Assoc. Prof. Dr. Oğuz Yayla
Cryptography, METU _____

Assoc. Prof. Dr. Ergün Yaraneri
Mathematics, Istanbul Technical University _____

**Date:** _____

**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

Name, Last Name: MUSTAFA KIRCALI

Signature :

# ABSTRACT

QUANTUM MAXIMUM DISTANCE SEPERABLE CODES

KIRCALI, Mustafa
Ph.D., Department of Cryptography
Supervisor : Assist. Prof. Dr. Buket Özkaya
Co-Supervisor : Prof. Dr. Ferruh Özbudak

February 2025, 47 pages

Quantum error-correcting codes (QECCs) are a cornerstone of fault-tolerant quantum computing, providing an essential means to protect delicate quantum information from the inevitable errors introduced by decoherence, noise, and operational faults. Unlike classical error correction, which addresses primarily bit-flip errors, QECCs must contend with the more intricate errors that affect both the amplitude and phase of qubits. Among the various types of QECCs, Quantum Maximum Distance Separable (QMDS) codes are particularly noteworthy due to their optimal error correction capabilities, achieving the maximum possible distance for given parameters. Constructing new QMDS codes is a critical challenge in the literature.

In this thesis, we study a class of infinitely many explicit polynomials and derive their requisite arithmetical properties, which imply the construction of an infinite family of new $q$-ary QMDS codes of length strictly larger than $q + 1$. Ball and Vilar [4] demonstrated that the problem of constructing QMDS codes can be reduced to finding specific polynomials over finite fields with well-defined arithmetical properties, yet they were unable to explicitly construct these polynomials.

Keywords: Quantum Error Correction Codes, Hermitian Self-Orthogonal Codes, Reed-Solomon Codes

# ÖZ

KUANTUM MAKSİMUM AYRILABİLİR MESAFE KODLARI

KIRCALI, Mustafa
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Dr. Öğr. Üyesi Buket Özkaya
Ortak Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Şubat 2025, 47 sayfa

Kuantum hata düzeltme kodları (QECC), hata toleranslı kuantum hesaplamanın temel taşlarından biridir ve dekoherans, gürültü ile operasyonel hatalardan kaynaklanan kaçınılmaz hatalara karşı hassas kuantum bilgilerini korumak için önemli bir araç sunar. Klasik hata düzeltmenin ağırlıklı olarak bit dönüşümü hatalarına odaklanmasının aksine, QECC'ler qubit'lerin hem genlik hem de fazını etkileyen daha karmaşık hatalarla başa çıkmak zorundadır. QECC'lerin çeşitli türleri arasında, Kuantum Maksimum Mesafe Ayrılabilir (QMDS) kodları, optimal hata düzeltme yetenekleri sayesinde özellikle dikkat çekicidir; verilen parametreler için mümkün olan en yüksek mesafeyi elde ederler. Yeni QMDS kodları oluşturmak literatürde kritik bir zorluktur.

Bu tezde, sonsuz sayıda açıkça tanımlanmış polinom sınıfını inceliyor ve gerekli aritmetik özelliklerini çıkarıyoruz; bu özellikler, $q+1$'den kesinlikle daha uzun yeni $q$-lü QMDS kodlarının sonsuz bir ailesinin oluşturulmasını ima etmektedir. Ball ve Vilar [4] gösterdiği üzere, QMDS kodları oluşturma problemi, iyi tanımlanmış aritmetik özelliklere sahip sonlu alanlar üzerinde belirli polinomların bulunmasına indirgenebilmektedir; ancak bu polinomlar açıkça inşa edilememiştir.

Anahtar Kelimeler: Kuantum Hata Düzeltme Kodları, Hermityan Öz-Ortogonal Kodlar, Reed-Solomon Kodları

# ACKNOWLEDGMENTS

I would like to express my very great appreciation to Prof. Dr. Ferruh Özbudak for his patient guidance, enthusiastic encouragement and valuable advices during the development and preparation of this thesis. His willingness to give his time and to share his experiences has brightened my path.

I am also sincerely grateful to Asst. Prof. Buket Özkaya for her insightful feedback, support, and valuable suggestions.

I am deeply grateful to my family for their unwavering support, endless patience, and unconditional love. Their belief in me has been a constant source of strength throughout this journey. Without their encouragement and sacrifices, this achievement would not have been possible.

A special thanks to my friends Hakan Bacaksız and Doğukan Uçak for their companionship,and motivation. Their support during challenging times has made this journey both meaningful and memorable.

I would also like to extend my heartfelt appreciation to FAME CRYPT, the professors, and my colleagues from there. Their collaboration, insights, and shared passion for cryptography have been inspiring and invaluable throughout my research.

I would like to thank The Scientific and Technological Research Council of Turkey (TÜBİTAK) for supporting my TÜBİTAK 2244 doctoral program for this research.

Finally, I express my gratitude to everyone who has contributed, directly or indirectly, to the completion of this thesis. Your support has been truly appreciated.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

Quantum computers with high scalability have not been built yet, but so many people are working on implementing it. Quantum computers can theoretically solve many problems that classical computers find challenging. Quantum algorithms like Shor's algorithm [34] potentially break widely used encryption schemes that rely on the security of the integer factorization problem and the discrete logarithm problem. Another remarkable quantum algorithm is Grover's algorithm [14], which efficiently locates a single item within an unsorted database of $N$ items in $O(\sqrt{N})$ time using a quantum computer. In contrast, a classical computer would need $O(N)$ time to perform this task through exhaustive search. It has also been proven that $O(\sqrt{N})$ is the best-known result in the literature for this specific task.

Developing a quantum computer presents considerable challenges, particularly in maintaining the stability of quantum information. Quantum error correction codes (QECC) are a set of techniques designed to protect quantum data from errors caused by decoherence, interference, and operational faults. By encoding logical qubits into entangled states of multiple physical qubits, QECC enables quantum computations to proceed even in the presence of noise, laying the groundwork for scalable and fault-tolerant quantum computers.

QECC differ fundamentally from classical error correction codes due to the unique nature of quantum information. Unlike classical codes, which operate on bits that exist in definite states of 0 or 1, QECCs must work with qubits that can exist in superpositions of states and are subject to quantum phenomena like entanglement and interference. Furthermore, quantum errors are more complex than classical errors;

they can affect both the amplitude and phase of a qubit, requiring QECCs to address both types of errors simultaneously. Another key distinction is the no-cloning theorem, which prohibits copying quantum information, meaning redundancy must be achieved through entangling multiple qubits rather than replicating data. These differences make designing and implementing QECCs significantly more challenging, but also uniquely tailored to the demands of preserving quantum information.

A significant milestone in quantum information processing was achieved with Shor's groundbreaking work on QECCs, addressing the challenge of error correction within the constraints of the no-cloning theorem. Inspired by classical 3-bit repetition codes, Shor introduced the first quantum code in his 1995 paper [35], known as the "Shor code," which encodes one logical qubit into nine physical qubits (coding rate of $1/9$) and can correct arbitrary single-qubit errors, including bit-flip, phase-flip, and bit-phase-flip errors. Building on this foundation, Calderbank-Shor-Steane (CSS) codes were subsequently developed [36] by Calderbank and Shor, as well as by Steane, enabling robust quantum error correction by adapting classical binary linear codes to address quantum-specific challenges.

Another powerful framework in quantum error correction is the *stabilizer formalism*, introduced and extensively developed by Daniel Gottesman [10]. Stabilizer codes are defined as the simultaneous eigenspaces of commuting operators, known as *stabilizers*, that act on a set of qubits. These stabilizer operators are typically chosen to detect and correct specific classes of quantum errors, ensuring that logical information is protected from noise. Our construction in this thesis is based on the stabilizer formalism, allowing us to construct new QECCs with new parameters.

Quantum maximum-distance-separable (MDS) codes are a class of quantum error correction codes that achieve the highest possible error correction capabilities for a given code length and code rate. Analogous to classical MDS codes, quantum MDS codes satisfy the quantum Singleton bound, which relates the code length $n$, the number of logical qubits $k$, and the code's distance $d$ as $n - k \geq 2d - 2$. These codes are optimal in the sense that they can detect and correct the maximum number of errors for their parameters. Quantum MDS codes are constructed using techniques that extend classical MDS code principles to the quantum domain, often employing a sta-

bilizer formalism approach. They play a crucial role in quantum communication and fault-tolerant quantum computing by providing efficient and robust error correction in scenarios where minimizing redundancy is critical.

In the literature, there are three primary methods for constructing quantum MDS codes with optimal parameters: using constacyclic codes, negacyclic codes, and Generalized Reed-Solomon (GRS) codes. Kai et al. ([23], [24]) constructed several classes of quantum MDS codes by employing constacyclic and negacyclic codes. Additionally, GRS codes are widely employed in the construction of quantum MDS codes because of their algebraic properties. Li et al. proposed a unified framework for the construction of quantum MDS codes using GRS codes in [28]. Later, Jin et al. ([21], [22]) extended the findings from [28] and created new classes of quantum MDS codes. Following this, researchers have developed a wide range of quantum MDS codes with distances greater than $q/2 + 1$ through the use of GRS codes (see [16], [40], [32], [37], [19], [7], [8], [9], [15], [3]). Ball [3], demonstrated that the minimum distance of a quantum MDS code derived from GRS is at most q + 1.

The problem of constructing quantum MDS codes with $n \leq q+1$ has been completely solved in [12], [30], [21]. Constructing quantum MDS codes with $q+1 < n \leq q^2+1$ is still an open problem. There are many results on this problem when $q + 1 < n \leq q^2 + 1$. For the sake of clarity and comparison, we provide a table of quantum MDS codes with the "best results" in Quantum MDS code constructions. The meaning of the phrase "best results" is the same as in [9], and we keep using it.

Simeon Ball and Ricard Vilar showed that the construction of certain quantum MDS codes can be closely linked to the arithmetic properties of particular polynomials defined over $\mathbb{F}_{q^2}$. In particular, Ball and Vilar [4] provided necessary and sufficient conditions for a truncated Reed-Solomon code to be linearly equivalent to a Hermitian self-orthogonal code.

Ball and Vilar [4] reduced the problem of constructing quantum MDS codes to finding specific polynomials over $\mathbb{F}_{q^2}$ with certain arithmetical properties, but they could not explicitly construct such polynomials. We address this open problem by introducing a new class of explicit polynomials with specific arithmetical properties over finite fields. By reducing the problem to counting the roots of these polynomials over $\mathbb{F}_{q^2}$,

we derived an infinite class of $q$-ary quantum MDS codes. In this work, we successfully found these polynomials and demonstrated that they yield new quantum MDS codes.

## 1.1 Outline of the Thesis

In this thesis, we study a class of infinitely many explicit polynomials and obtain their required arithmetical properties which imply the construction of an infinite class of new $q$-ary quantum MDS codes of length strictly larger than $q + 1$.

Firstly, we provide an overview of quantum computation and address the challenges associated with constructing quantum error correction codes.

Secondly, we discuss the earliest quantum error correction codes and describe methods for deriving quantum error correction codes from classical codes. We then define quantum MDS codes and review efforts to construct them.

Subsequently, we demonstrate that the problem of finding quantum MDS codes can be reduced to counting the roots of a polynomial over a finite field.

Finally, we will give new constructions of the $q$-ary quantum MDS codes of length strictly larger than $q + 1$.

# CHAPTER 2

# QUANTUM COMPUTING

## 2.1 Quantum Computing

Quantum computation is the study of information processing tasks that can be achieved using quantum mechanical systems. Qubits are essential for quantum computing because they serve as the basic units of quantum information. Unlike classical bits, which can only be in a state of 0 or 1, qubits can exist in a superposition of states, enabling quantum computers to perform many calculations simultaneously. Measurement is a crucial aspect of quantum computing. In quantum mechanics, measurement collapses a qubit's superposition state into one of the basis states. This process is probabilistic, with outcomes depending on the quantum state's amplitude prior to measurement. In addition to qubits, entanglement is a key quantum phenomenon that allows qubits to be interconnected in ways that classical bits cannot, leading to highly correlated states that are crucial for many quantum algorithms and protocols. The Pauli group plays a vital role in quantum error correction and other fundamental quantum operations, providing the mathematical tools needed to manage and manipulate qubits. Finally, quantum channels describe how quantum information is transmitted and processed, ensuring that the information encoded in qubits can be accurately communicated and preserved.

### 2.1.1 Qubit

A *qubit* is the fundamental unit of quantum information. In the complex plane (more precisely, a two-dimensional complex vector space), we can represent the computa-

tional basis states as

$$|0\rangle = \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ \\ 1 \end{bmatrix}.$$

A qubit state $|\psi\rangle$ can thus be written as a linear combination of these basis states:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where $\alpha$ and $\beta$ are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$.

A **qudit** generalizes the idea of a qubit to a $d$-dimensional complex vector space. We define $d$ orthonormal basis states:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad |d-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

A general qudit state $|\phi\rangle$ is then a linear combination of these $d$ basis states:

$$|\phi\rangle = \sum_{j=0}^{d-1} \gamma_j\,|j\rangle\,,$$

where $\sum_{j=0}^{d-1} |\gamma_j|^2 = 1$.

### Quantum Registers

A generalization of a qubit in the multi-qubit context is known as a **quantum register** or **quantum state**. A quantum register is a composite quantum system composed of multiple qubits that can collectively represent a more complex quantum state. While a qubit is the fundamental unit of quantum information, a quantum register can represent multi-qubit states, enabling the manipulation of larger and more intricate quantum information.

Mathematically, a quantum register comprising $n$ qubits can be represented as:

$$|\Psi\rangle = \alpha_0\,|00\ldots0\rangle + \alpha_1\,|00\ldots01\rangle + \alpha_2\,|00\ldots10\rangle + \ldots + \alpha_{2^n-1}\,|11\ldots1\rangle\,,$$

where $\alpha_i$ are complex amplitudes, and each term in the superposition corresponds to a different binary combination of the $n$ qubits in the register. Quantum registers are essential for performing complex quantum computations and algorithms, as they allow for the representation and manipulation of a wide range of quantum states and information.

### 2.1.2 Measurement

In quantum computation, *measurement* is the process of extracting information from a quantum system, collapsing it to one of its basis states, and obtaining a classical outcome. When a qubit is measured, it will collapse to either the $|0\rangle$ or $|1\rangle$ state with probabilities determined by the coefficients $\alpha$ and $\beta$ in its superposition. The outcome of a measurement is probabilistic, and subsequent measurements may yield different results.

The probability of measuring a qubit state $|\psi\rangle$ in the $|0\rangle$ state is given by $|\alpha|^2$, and the probability of measuring it in the $|1\rangle$ state is given by $|\beta|^2$. These probabilities are calculated as follows:

$$\text{Probability of } |0\rangle \text{ outcome:} \quad P(0) = |\alpha|^2, \tag{2.1}$$

$$\text{Probability of } |1\rangle \text{ outcome:} \quad P(1) = |\beta|^2. \tag{2.2}$$

### 2.1.3 Entanglement

Quantum entanglement is a fundamental concept in quantum mechanics where particles become interconnected in such a way that the quantum state of one particle cannot be described independently of the state of the other particle.

Let's assume two arbitrary quantum systems $A$ and $B$, with respective Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The Hilbert space of the composite system is the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. If the first system is in state $|\psi\rangle_A$ and the second in state $|\phi\rangle_B$, the state of the composite system is $|\psi\rangle_A \otimes |\phi\rangle_B$. States of the composite system that can be represented in this form are called separable states, or product states.

Not all states are separable states. Fix a basis $\{|i\rangle_A\}$ for $\mathcal{H}_A$ and a basis $\{|j\rangle_B\}$ for $\mathcal{H}_B$. The most general state in $\mathcal{H}_A \otimes \mathcal{H}_B$ is of the form

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij}|i\rangle_A \otimes |j\rangle_B.$$

This state is separable if there exist vectors $[c_i^A]$, $[c_j^B]$ so that $c_{ij} = c_i^A c_j^B$, yielding

$$|\psi\rangle_A = \sum_i c_i^A |i\rangle_A$$

and

$$|\phi\rangle_B = \sum_j c_j^B |j\rangle_B.$$

It is inseparable if for any vectors $[c_i^A]$, $[c_j^B]$ at least for one pair of coordinates $c_i^A, c_j^B$ we have $c_{ij} \neq c_i^A c_j^B$. If a state is inseparable, it is called an entangled state.

For example, given two basis vectors $\{|0\rangle_A, |1\rangle_A\}$ of $\mathcal{H}_A$ and two basis vectors $\{|0\rangle_B, |1\rangle_B\}$ of $\mathcal{H}_B$, the following is an entangled state:

$$\frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right).$$

If the composite system is in this state, it is impossible to attribute to either system $A$ or system $B$ a definite pure state.

### 2.1.4 Unitary Operators

A matrix $U$ is said to be unitary if $U^\dagger U = I$. In the same way, an operator $U$ is unitary if $U^\dagger U = I$. An operator is unitary if and only if each of its matrix representations is unitary. A unitary operator also satisfies $UU^\dagger = I$, and therefore $U$ is normal and has a spectral decomposition. Geometrically, unitary operators are important because they preserve inner products between vectors.

### 2.1.5 The Pauli Group

The Pauli group is a set of matrices that includes the identity matrix and the three Pauli matrices. These matrices are used to describe spin operators and are fundamental in

the study of quantum mechanics. Moreover, **Pauli matrices play a crucial role in describing quantum error operators** in quantum error-correcting codes.

The Pauli group for a single qubit, denoted as $\mathcal{P}_1$, consists of the following matrices:

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The Pauli group $\mathcal{P}_1$ includes these matrices, as well as their products with the imaginary unit $i$ and negative signs. Specifically, the elements of $\mathcal{P}_1$ are:

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}.$$

Each element of the Pauli group can be written as:

$$P = e^{i\theta}\,\sigma_j,$$

where $\theta \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ and $\sigma_j \in \{I, \sigma_x, \sigma_y, \sigma_z\}$.

The Pauli matrices have the following properties:

- $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$,
- $\sigma_x\sigma_y = i\sigma_z, \quad \sigma_y\sigma_z = i\sigma_x, \quad \sigma_z\sigma_x = i\sigma_y$,
- $\sigma_y\sigma_x = -i\sigma_z, \quad \sigma_z\sigma_y = -i\sigma_x, \quad \sigma_x\sigma_z = -i\sigma_y$.

The Pauli group is important in quantum computing because it forms the basis for error-correcting codes and is used to describe quantum gates. The generalization of

the Pauli group to $n$ qubits, $\mathcal{P}_n$, is given by the tensor products of the Pauli matrices for each qubit.

### 2.1.6 No-Cloning Theorem

In quantum mechanics, the No-Cloning Theorem states that it is impossible to create an exact copy of an arbitrary unknown quantum state. Formally, for any quantum state $|\psi\rangle$ in a Hilbert space, there does not exist a quantum operation $\hat{C}$ that can perfectly clone this state, such that:

$$\hat{C}\,|\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle\,, \tag{2.3}$$

where $|0\rangle$ represents a blank state, and $\otimes$ denotes the tensor product of quantum states.

The No-Cloning Theorem has profound implications for quantum information processing, as it prevents the straightforward copying of arbitrary quantum states, in contrast to classical information where copying is generally possible.

### 2.1.7 Quantum Channel

In quantum information theory, a quantum channel is a communication channel which can transmit quantum information, as well as classical information. A quantum channel, also known as a quantum operation or quantum map, is a completely positive trace-preserving (CPTP) map that describes the evolution of quantum states in an open quantum system.

Consider a quantum system with an associated Hilbert space $\mathcal{H}$. A quantum channel $\mathcal{E}$ is a linear map that takes a density matrix $\rho$ (representing the quantum state of the system) to another density matrix $\mathcal{E}(\rho)$. The map $\mathcal{E}$ must satisfy two properties:

- **Complete Positivity**: $\mathcal{E}$ is completely positive if, for any auxiliary Hilbert space $\mathcal{K}$ and any density matrix $\rho_{AK}$ on the joint system $\mathcal{H} \otimes \mathcal{K}$, the map $\mathcal{E} \otimes I_{\mathcal{K}}$ is positive. This means that $(\mathcal{E} \otimes I_{\mathcal{K}})(\rho_{AK})$ is a positive semidefinite matrix.

- **Trace Preservation**: $\mathcal{E}$ is trace-preserving if $\text{Tr}(\mathcal{E}(\rho)) = \text{Tr}(\rho)$ for all density matrices $\rho$.

A quantum channel $\mathcal{E}$ can be represented in terms of Kraus operators. If $\{K_i\}$ is a set of Kraus operators for the channel $\mathcal{E}$, then the action of the channel on a density matrix $\rho$ is given by

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger,$$

where the Kraus operators satisfy the completeness relation

$$\sum_i K_i^\dagger K_i = I.$$

**Examples:**

- **Depolarizing Channel**: The depolarizing channel $\mathcal{E}_p$ with depolarizing probability $p$ is defined as

  $$\mathcal{E}_p(\rho) = (1-p)\rho + p\frac{I}{d},$$

  where $d$ is the dimension of the Hilbert space $\mathcal{H}$, and $I$ is the identity matrix.

- **Amplitude Damping Channel**: The amplitude damping channel $\mathcal{E}_\gamma$ with damping probability $\gamma$ is described by the Kraus operators

  $$K_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad K_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}.$$

  The action of the channel on a density matrix $\rho$ is then

  $$\mathcal{E}_\gamma(\rho) = K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger.$$

## 2.2 Quantum Error Correcting Codes

Let $\mathbb{C}^q$ denote the $q$-dimensional Hilbert space over $\mathbb{C}$. A $q$-ary quantum code $Q$ of length $n$ is a $K$-dimensional subspace of the Hilbert space $\mathbb{C}^{q^n}$ of $n$ qudits. The parameters of $Q$ are written as $[[n, k, d]]_q$ if its minimum distance is $d$ and $K = q^k$.

### 2.2.1 Quantum Singleton Bound

Similar to the classical codes, an $[[n, k, d]]_q$ quantum stabilizer code has to satisfy the quantum Singleton bound (see Theorem 1, below).

**Theorem 1.** *(Quantum Singleton Bound) Let $C = [[n, k, d]]_q$ be a quantum error-correction code. Then $k + 2d \leq n + 2$.*

Corresponding to this bound, one can define quantum Maximum Distance Seperable (MDS) code.

**Quantum MDS Code:** A quantum code for which equality holds in Theorem 1 i.e., $C = [[n, n - 2d + 2, d]]_q$, is called a quantum MDS code.

Ketkar et al. [25], stated quantum MDS conjecture as follows.
**QMDS Conjecture:** If the classical MDS conjecture holds, then there are no non-trivial MDS stabilizer codes of lengths exceeding $q^2 + 1$, except when $q$ is even and $d = 4$ or $d = q^2$ or in which case $n \leq q^2 + 2$.

## 2.3 Known Quantum MDS Codes

In the literature, there are three primary methods for constructing quantum MDS codes with optimal parameters: using constacyclic codes, negacyclic codes, and Generalized Reed-Solomon (GRS) codes. Kai et al. ([23], [24]) constructed several classes of quantum MDS codes by employing constacyclic and negacyclic codes. Following this, researchers have created many quantum MDS codes using constacyclic codes. Additionally, GRS codes are widely employed in constructing quantum MDS codes due to their algebraic properties. Li et al. proposed a unified framework for constructing quantum MDS codes using GRS codes in [28]. Later, Jin et al. ([21], [22]) extended the findings from [28] and created new classes of quantum MDS codes.Following this, researchers have developed a wide range of quantum MDS codes with distances greater than $q/2 + 1$ through the use of GRS codes (see [16], [40], [32], [37], [19], [7], [8], [9], [15], [3]). Ball [3], demonstrated that the minimum distance of a quantum MDS code derived from GRS is at most q + 1.

The problem of constructing quantum MDS codes with $n \leq q+1$ has been completely solved in [12], [30], [21]. Constructing quantum MDS codes with $q+1 < n \leq q^2+1$ is still an open problem. There are many results on this problem when $q+1 < n \leq q^2+1$. For the sake of clarity and comparison, we provide a table of quantum MDS codes with the "best results" in Quantum MDS code constructions. The meaning of the phrase "best results" is the same as in [9], and we keep using it. Namely, a table of constructions of $q$-ary quantum MDS codes with the length n in the range, $q+1 < n \leq q^2+1$ and satisfying the condition $(q-1) \mid (n-1)$, such that all the known results on quantum MDS codes in this range are consequences of this table.

Table 2.1: Some Known Results on $[n, n-2d+2, d]_q$-Quantum MDS Codes.

| **Type** | **Forms of $n$** | Class | **Length $n$** | **Minimum Distance d** | **References** |
|---|---|---|---|---|---|
| **0** | $n \leq q+1$ | **0.1** | $n \leq q+1$ | $2 \leq d \leq n/2+1$, | [12], [30], [21] |
| **1** | $(q+1) \mid (n-2)$ | **1.1** | $n = q^2+1$ | $2 \leq d \leq q+1, \quad d \neq q$ | [28] , [26], [**?**], [23], [22], [13], [7] |
| | | **1.2** | $n = t(q+1)+2$ $(p,t,d) \neq (2, q-1, q)$ | $2 \leq d \leq t+2$, | [7] |
| **2** | $(q+1) \mid (n-1)$ | **2.1** | $n = 1 + r\frac{q^2-1}{s}$ $s \mid (q-1), 1 \leq r \leq s$ | $2 \leq d \leq r\frac{q-1}{s}+1$ | [8] |
| **3** | $(q+1) \mid n$ | **3.1** | $n = r\frac{q^2-1}{s}$ $s \mid (q-1), 1 \leq r \leq s$ | $2 \leq d \leq r\frac{q-1}{s}$ | [8] , [32] |
| | | **3.2** | $n = r\frac{q^2-1}{2s}$ $2s \mid (q-1), 1 \leq r \leq 2s$ | $2 \leq d \leq (s+1)\frac{q-1}{2s}$ | [40] , [24] |
| | | **3.2** | $n = \frac{q^2-1}{2}$ | $2 \leq d \leq q$ | [24] |
| **4** | $q \mid n$ | **4.1** | $n = q^2$ | $2 \leq d \leq q+1$ | [28] |
| | | **4.2** | $n = tq, 1 \leq t \leq q$ | $2 \leq d \leq \left\lfloor \frac{tq+q-1}{q+1} \right\rfloor + 1$ | [28], [38], [7] |
| **5** | $(q-1) \mid (n-1)$ | **5.1** | $n = 1 + r\frac{q^2-1}{2s+1}$, $(2s+1) \mid (q+1), 1 \leq r \leq 2s+1$ | $2 \leq d \leq (s+1)\frac{q-1}{2s+1}$ | [22], [19], [8] |
| | | **5.2** | $n = 1 + (2t+1)\frac{q^2-1}{2s+1}$, $(2s+1) \mid (q+1), 1 \leq t \leq s-1$ | $2 \leq d \leq (s+t+1)\frac{q-1}{2s+1}$ | [8] |
| | | **5.3** | $n = 1 + r\frac{q^2-1}{2s}$, $2s \mid (q+1), 1 \leq r \leq 2s$ | $2 \leq d \leq (s+1)\frac{q-1}{2s}$ | [8] |
| | | **5.4** | $n = 1 + (2t+2)\frac{q^2-1}{2s}$, $2s \mid (q+1), 1 \leq t \leq s-1$ | $2 \leq d \leq (s+t+1)\frac{q-1}{2s}$ | [8] |
| **6** | $(q-1) \mid n$ | **6.1** | $n = (2t+1)\frac{q^2-1}{2s+1}$, $(2s+1) \mid (q+1), 1 \leq t \leq s$ | $d \leq (s+t+1)\frac{q-1}{2s+1}$ | [8], [19] |
| | | **6.2** | $n = 2t\frac{q^2-1}{2s+1}$, $(2s+1) \mid (q+1), 1 \leq t \leq s-1$ | $d \leq (s+t+1)\frac{q-1}{2s+1} - 1$ | [19] , [33] |
| | | **6.3** | $n = (2t+1)\frac{q^2-1}{2s}$, $2s \mid (q+1), 1 \leq r \leq 2s$ | $d \leq (s+t)\frac{q-1}{2s} - 1$ | [8] |
| | | **6.4** | $n = 2t\frac{q^2-1}{2s}$, $2s \mid (q+1), 1 \leq t \leq s$ | $2 \leq d \leq (s+t)\frac{q-1}{2s} - 1$ | [33], [40] |
| | | **6.5** | $n = t(q-1)$, $1 \leq t \leq q-1$ | $2 \leq d \leq \left\lfloor \frac{tq-1}{q+1} \right\rfloor + 1$ | [15] |
| **7** | $n \mid (q^2+1)$ | **7.1** | $n = \frac{q^2+1}{2}$ | $2 \leq d \leq q$, $d$ odd | [23] |
| | | **7.2** | $n = \frac{q^2+1}{5}$, $q \equiv \pm 3 (\text{mod } 10)$ | $2 \leq d \leq \frac{3q+1}{5}$, $d$ even | [39], [24], [17] |
| | | **7.3** | $n = \frac{q^2+1}{5}$, $q \equiv \pm 3 (\text{mod } 10)$ | $2 \leq d \leq \frac{3q+1}{5}$, $d$ even | [27] |

# CHAPTER 3

# QUANTUM CODES FROM CLASSICAL CODES

## 3.1 Classical Codes

Claude Shannon is known as father of modern digital communications and information theory, made groundbreaking contributions that form the cornerstone of coding theory. His seminal 1948 paper [31], "A Mathematical Theory of Communication" laid the theoretical foundation for digital circuits and telecommunications. Shannon introduced key concepts such as information entropy, the capacity of a communication channel, and the fundamental limits on compressing and reliably transmitting data, which are important to understanding and advancing coding theory. His work not only sparked the development of efficient coding techniques to maximize data transmission but also provided a theoretical framework for error detection and correction, vital for reliable communication over noisy channels.

In Shannon's information theory, the communication process encompasses several critical components: the *source of information*, which generates the message; *encoding*, where the message is prepared for transmission, often involving compression and error-correcting codes; *noise*, representing unwanted interference during transmission, a key element in determining channel capacity; and *decoding*, the final step where the received message is processed to reconstruct the original, correcting transmission errors. These components are fundamental in designing efficient and reliable communication systems.

In coding theory, a *general code* refers to a scheme used for transforming information from one format to another, primarily for compression and error correction. The

core aim of coding is to facilitate the reliable transmission of data across potentially noisy channels. This involves developing efficient data representation methods and error detection and correction mechanisms. For instance, consider an alphabet $\{A, B, C, \ldots, Z\}$ as a basic set of symbols. In coding, this set can be used to create various codewords, where each symbol or combination of symbols represents specific data or instructions, thereby enabling the transmission of complex information in a structured and interpretable manner.

Linear codes hold a special place in coding theory due to their algebraic structure and arithmetic properties. This linear structure enables the use of matrix operations for encoding and decoding, simplifying the implementation of error-correction algorithms. The algebraic framework of linear codes provides a systematic approach for designing codes with specific properties, such as minimum distance and error-correcting capability, making them crucial for efficient and reliable data transmission in various applications.

Let $q$ be a prime power and $\mathbb{F}_q^n$ denote the vector space all $n\text{-}tuples$ over the finite field $\mathbb{F}_q$. An $(n, M)$ $code$ $C$ over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size M. We write the vectors $(a_1, a_2, ..., a_n)$ in $\mathbb{F}_q^n$. We call the vectors in $C$ $codewords$. If $C$ is $k\text{-}dimensional$ subspace of $\mathbb{F}_q^n$, then $C$ will be called $[n, k]$ $linear$ $code$ over $\mathbb{F}_q$. A $generator$ $matrix$ for an $[n, k]$ code $C$ is any $k \times n$ matrix $G$ whose rows form a basis for $C$. There is an $(n-k) \times n$ matrix $H$, called a $parity$ $check$ $matrix$ for the $[n, k]$ code $C$, defined by

$$C = \{x \in \mathbb{F}_q^n \colon Hx^T = 0\}.$$

Let $q$ be an odd prime power. Let $\mathbb{F}_q$ be the finite field with $q$ elements and $\mathbb{F}_q^*$ be the multiplicative group of nonzero elements of $\mathbb{F}_q$. A $q$-ary $[n, k, d]$-linear code is just a vector subspace of $\mathbb{F}_q^n$ with dimension $k$ and minimum Hamming distance $d$, and $n$ is called the length of the code. We refer [18], on further information.

A canonical Hermitian form on $\mathbb{F}_{q^2}^n$ is given by

$$(a,b)_h = \sum_{i=1}^{n} a_i b_i^q.$$

If $C$ is a linear code over $\mathbb{F}_{q^2}$, then its Hermitian dual is defined as

$$C^{\perp_h} = \{b \in \mathbb{F}_{q^2}^n \mid (a,b)_h = 0, \text{ for all } u \in C\}.$$

The code $C$ is called Hermitian self-orthogonal if $C \subseteq C^{\perp_H}$.

The $distance$ $d(a,b)$ between two vectors $a, b \in \mathbb{F}_q^n$ is defined to be a number of coordinates in which $a$ and $b$ differ. The $distance$ of a code $C$ is the smallest distance between distinct codewords and is important in determining the error-correcting capability of $C$. The $weight$ $wt(\mathbf{a})$ of a vector $\mathbf{a} \in \mathbb{F}_q^n$ is the number of nonzero coordinates in $\mathbf{a}$.

**Theorem 2.** *If $a, b \in \mathbb{F}_q^n$, then $d(a,b) = wt(a-b)$. If $C$ is a linear code, the minimum distance $d$ is the same as the minimum weight of the nonzero codewords of $C$.*

*Proof.* The proof can be found in ([18]. □

Due to this theorem, in the context of linear codes, the minimum distance is often referred to as the minimum weight of the code. If the minimum weight $d$ of an $[n,k]$ code is known, then we refer to the code as an $[n,k,d]$ code.

Let $N_i$, also denoted $N_i(C)$, be the number of codewords of weight $i$ in $C$. The list $N_i$ for $0 \leq i \leq n$ is called the weight distribution or weight spectrum of $C$.

**Theorem 3.** *Let $C$ be an $[n,k,d]$ code over $\mathbb{F}_q$. Then:*
*(i)* $N_0(C) + N_1(C) + \ldots + N_n(C) = q^k$.
*(ii)* $N_0(C) = 1$ *and* $N_1(C) = N_2(C) = \ldots = N_{d-1}(C) = 0$.

*Proof.* The proof can be found in [18].

**Encoding**

Let $C$ be an $[n, k]$ linear code over the field $\mathbb{F}_q$ with a generator matrix $G$. This code contains $q^k$ codewords, each corresponding uniquely to one of the $q^k$ possible messages. These messages can be viewed as $k$-tuples $a$ in $\mathbb{F}_q^k$. The standard method of encoding a message $a$ is by producing the codeword $c = aG$. If $G$ is in standard form, the first $k$ coordinates of the codeword $c$ represent the information symbols $a$, while the remaining $n - k$ coordinates are the parity check symbols—redundancy added to help recover $a$ in case of errors.

The method just described explains how to encode a message $a$ using the generator matrix of the code $C$. There is also an alternative encoding method using the parity check matrix $H$. This is simplest when $G$ is in standard form $[I_k \mid A]$. Suppose $a = a_1 \dots a_k$ is to be encoded as the codeword $c = c_1 \dots c_n$. Since $G$ is in standard form, $c_1 \dots c_k = a_1 \dots a_k$. The task is then to determine the $n - k$ parity check symbols $c_{k+1} \dots c_n$. Using $0 = Hc^T = [-A^T \mid I_{n-k}]c^T$, it follows that $A^T a^T = [c_{k+1} \dots c_n]^T$.

**Decoding**

The process of decoding, which involves identifying the codeword (and thus the message $a$) that was sent upon receiving a vector $b$. The search for efficient and fast decoding algorithms is a major focus of research in coding theory because of their critical applications. Mostly, while encoding is relatively simple, decoding becomes significantly more difficult as the size of the code increases.

When the codeword $c \in \mathbb{F}_2^n$ is transmitted through a channel, the received vector is $b \in \mathbb{F}_2^n$ and is decoded as $\hat{c} \in \mathbb{F}_2^n$. Let $e = b - c$, so that $b = c + e$. The effect of noise in the communication channel is to introduce an error vector $e$ to the codeword $c$, and the objective of decoding is to identify $e$. Nearest neighbor decoding involves finding an error vector $e$ with the smallest weight such that $b - e$ belongs to the code. This error vector may not be unique.

To analyze vectors that are closest to a given codeword, the concept of spheres around codewords is quite useful. The sphere of radius $r$ centered at a vector $a$ in $\mathbb{F}_q^n$ is defined as the set

$$S_r(a) = \{b \in \mathbb{F}_q^n \mid d(a, b) \leq r\}$$

which includes all vectors whose distance from $a$ is less than or equal to $r$. The number of vectors in $S_r(a)$ is given by

$$\sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

These spheres remain disjoint as long as their radius is sufficiently small.

### 3.1.1 Punctured Codes

Let $C$ be an $[n, k, d]$ code over $\mathbb{F}_q$. Puncturing $C$ involves deleting the same coordinate $i$ from each codeword. If $G$ is a generator matrix for $C$, then a generator matrix for puncture code $C^*$ can be obtained by removing column $i$ from $G$ . In summary, we can state the following lemma from [11].

**Lemma 4** (Punctured Code)**.** *Let $\mathcal{C} = [n, k, d]_q$ where $n = 2k$ is an arbitrary linear code over $\mathbb{F}_q$ with generator matrix $G \in \mathbb{F}_q^{k\times n}$. Define the punctured code $P(\mathcal{C}) = \langle G_i \circ G_j : i, j \in \{1, \ldots, k\}\rangle^{\perp}$, where*

$$G_i \circ G_j = (G_{i,1}G_{j,1}, \ldots, G_{i,n}G_{j,n}),$$

*and $G_{i,l}$ denotes the entry in row $i$ and column $l$ of $G$. If $P(\mathcal{C})$ contains a vector $v$ of weight $n' \leq n$ such that all entries $v_i$ are squares, then there exists a code $\mathcal{C}' = [n', k, d' \geq d - (n - n')]$ that is contained in its dual.*

### 3.1.2 Bound of Linear codes

In classical error-correcting codes, understanding the limits on the parameters of linear codes is essential for designing efficient coding schemes. One fundamental concept is the Singleton bound, which provides a simple yet powerful upper limit on the minimum distance of a linear code given its length and dimension. Codes that achieve this bound with equality are known as Maximum Distance Separable (MDS) codes and play a crucial role in the theory of coding due to their optimal error-correcting capability.

In addition to the Singleton bound, asymptotic bounds offer valuable insights into the behavior of codes as their length increases indefinitely. These bounds are essential

for understanding the trade-offs between code rate and error-correcting capability in large-scale applications. Notably, the Gilbert-Varshamov bound provides a lower bound on the achievable rate of a code given its minimum distance, indicating the existence of codes that meet these parameters with high probability.

We will explore singleton bound, MDS codes, asymptotic bound, and Gilbert-Varshamov bound.

**Singleton Bound and MDS codes**

The Singleton bound for a linear code is

$$d \leq n - k + 1.$$

An $[n, k, d]$ linear code is called an MDS (Maximum Distance Separable) code if its minimum distance $d$ satisfies:

$$d = n - k + 1.$$

**Gilbert-Varshamov Bound**

Let $R = \frac{k}{n}$ be the rate of the code and $\delta = \frac{d}{n}$ be the relative minimum distance. The asymptotic Gilbert-Varshamov bound states that for sufficiently large $n$, there exist codes such that:

$$R \geq 1 - H(\delta)$$

where $H(\delta)$ is the binary entropy function defined as:

$$H(\delta) = -\delta \log_2(\delta) - (1 - \delta) \log_2(1 - \delta)$$

.

### 3.2 CSS Codes (Calderbank-Shor-Steane Codes)

Calderbank-Shor-Steane (CSS) codes enable the construction of quantum error correction codes using pairs of classical error-correcting codes.

An $[n, k_1 - k_2]$ CSS code, which is capable of correcting $t$ bit errors as well as phase errors, can be constructed from classical linear block codes $C_1(n, k_1)$ and $C_2(n, k_2)$,

if $C_2 \subseteq C_1$ and both $C_1$ as well as the dual of $C_2$, i.e., $C_2^{\perp}$, can correct $t$ errors. Here, $C_1$ is used for correcting bit errors, while $C_2^{\perp}$ is used for phase-error correction.

## 3.3 Stabilizer Codes

Stabilizer codes generalize the idea of CSS codes. They are constructed using a group of operators (stabilizers) that leave the quantum state of a system invariant. These operators are typically represented by Pauli matrices. Stabilizer codes form a large class of QECCs and include many of the most commonly used codes in quantum computing. It is well-established, see, e.g., [2], [5], [25], that quantum stabilizer codes can be modelled by classical linear codes with relevant orthogonality properties. We can construct quantum codes as long as we can construct classical linear codes with symplectic, Euclidean or Hermitian self-orthogonality [1], [6], [27],, [36].

### 3.3.1 Constacyclic Codes

A linear code $C$ of length $n$ over $\mathbb{F}_{q^2}$ is an $\mathbb{F}_{q^2}$-subspace of $\mathbb{F}_{q^2}^n$. For $\lambda \in \mathbb{F}_{q^2}^*$, a linear code $C$ of length $n$ over $\mathbb{F}_{q^2}$ is said to be $\lambda$-constacyclic if $(\lambda a_{n-1}, a_0, \cdots, a_{n-2}) \in C$ for every $(a_0, a_1, \cdots, a_{n-1}) \in C$. When $\lambda = 1$, $\lambda$-constacyclic codes are cyclic codes,

Each codeword $\mathbf{a} = a_0, a_1, \cdots, a_{n-1}) \in C$ is identified with its polynomial representation $a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$. In this way, every $\lambda$-constacyclic code $C$ is identified with exactly one ideal of the quotient algebra $\mathbb{F}_{q^2}[X]/\langle X^n - \lambda \rangle$. We say that $C$ is generated uniquely by a monic divisor $g(X)$ of $X^n - \lambda$; so, $g(X)$ is the generator polynomial of $C$ and we say that $C = \langle g(X) \rangle$. The irreducible factorization of $X^n - \lambda$ in $\mathbb{F}_{q^2}[X]$ determines all $\lambda$-constacyclic codes of length $n$ over $\mathbb{F}_{q^2}$.

Let $\lambda \in \mathbb{F}_{q^2}^*$ be a primitive $r$th root of unity. Then there exists a primitive $rn$th root of unity (in some extension field of $\mathbb{F}_{q^2}$), say $\eta$, such that $\eta^n = \lambda$. The roots of $X^n - \lambda$ are precisely the elements $\eta^{1+ri}$ for $0 \leq i \leq n-1$. Set $\theta_{r,n} = \{1 + ri \mid 0 \leq i \leq n-1\}$. The defining set of a constacyclic code $C = \langle g(X) \rangle$ of length $n$ is the set $Z = \{j \in \theta_{r,n} \mid \eta^j \text{ is a root of } g(X)\}$. It is obvioust to see that the defining set $Z$ is a

union of some $q^2$-cyclotomic cosets modulo $rn$ and $\dim_{\mathbb{F}_{q^2}}(C) = n - |Z|$.

The Hermitian construction employs constacyclic and negacyclic codes to construct QMDS codes [2].

**Theorem 5.** *[Hermitian Construction [2]] Let $C = [n, k, d_H]$ be a $q^2$-ary linear code satisfying $C^{\perp_H} \subseteq C$. Then there exists a $q$-ary quantum code with parameters $[[n, 2k - n, \geq d_H]]_q$.*

One example of QMDS codes derived from constacyclic codes in the literature is provided by Hu et al. [17], where they use the given lemma.

**Lemma 6.** *Assume that $q$ is an odd prime power with $q \equiv 3 \pmod{10}$ and $\frac{q+1}{r}$ is odd. Let $s = \frac{q^2+1}{2}$ and $n = \frac{q^2+1}{5}$. If $C$ is an $\eta$-constacyclic code over $\mathbb{F}_{q^2}$ of length $n$ with defining set $Z = \bigcup_{j=0}^{\delta} C_{s-jr}$, where $0 \leq \delta \leq \frac{3(q-3)}{10}$ and $C_{s-jr}$ is the $q^2$-cyclotomic coset containing $s - jr \mod rn$, then $C$ is a Hermitian dual-containing code.*

Using Theorem 5 and lemma 6, this theorem follows.

**Theorem 7.** *Let $q$ be an odd prime power with $q \equiv 3 \pmod{10}$. Then, there exist quantum MDS codes with parameters*

$$\left[\left\lceil \frac{q^2+1}{5} \right\rceil, \left\lceil \frac{q^2+1}{5} \right\rceil - 2d + 2, d\right]_q$$

*over $\mathbb{F}_q$, where $2 \leq d \leq \left\lfloor \frac{3q+1}{5} \right\rfloor$, and $d$ is even.*

### 3.3.2 Negacyclic Codes

#### Negacyclic Codes

Negacyclic codes are a subclass of linear cyclic codes characterized by a negacyclic shift operation. These codes have a rich algebraic structure, making them valuable for constructing quantum error-correcting codes, particularly Quantum Maximum Distance Separable (QMDS) codes.

A negacyclic code of length $n$ over the finite field $\mathbb{F}_q$ satisfies the property:

$$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (-a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C.$$

This property corresponds to invariance under a negacyclic shift, distinguishing negacyclic codes from traditional cyclic codes. Algebraically, a negacyclic code is an ideal in the ring $\mathbb{F}_q[x]/\langle x^n + 1\rangle$, where $x^n + 1$ must factorize into irreducible polynomials over $\mathbb{F}_q$.

Negacyclic codes are particularly useful in quantum error correction due to their compatibility with the Hermitian construction. This method employs negacyclic codes to ensure Hermitian self-orthogonality, a key requirement for constructing stabilizer codes. This property ensures that the corresponding quantum code can correct both bit-flip and phase-flip errors.

Researchers like Kai and Zhu [23] have demonstrated the utility of negacyclic codes in constructing QMDS codes with flexible parameters. Their work involves leveraging the algebraic properties of negacyclic codes, such as their polynomial representation and defining sets, to derive quantum codes with large minimum distances. Moreover, negacyclic codes play a role in addressing the QMDS conjecture, particularly in constructing codes with lengths exceeding $q + 1$.

The ability to derive QMDS codes from negacyclic structures highlights the interplay between classical and quantum coding theory. Negacyclic codes not only provide a theoretical foundation for QMDS code construction but also inspire new approaches to quantum error correction through their algebraic richness.

### 3.3.3 Generalized Reed-Solomon Codes

Let $n$ be an integer such that $1 \leq n \leq q$. Define $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ as an $n$-tuple consisting of distinct elements from $\mathbb{F}_q$, and let $u = (u_0, \ldots, u_{n-1})$ be an $n$-tuple of non-zero (though not necessarily distinct) elements from $\mathbb{F}_q$. Suppose $k$ is an integer satisfying $1 \leq k \leq n$. Then the codes

$$\text{GRS}_k(\alpha, u) = \{(u_0 f(\alpha_0), u_1 f(\alpha_1), \ldots, u_{n-1} f(\alpha_{n-1})) \mid f \in P_k\}$$

are known as the generalized Reed–Solomon or GRS codes.

The Reed-Solomon code over $\mathbb{F}_{q^2}$ is given by

$$C = \left\{ (f(a_1), \ldots, f(a_{q^2}), f_{(k-1)}) \mid f \in \mathbb{F}_{q^2}[X], \deg(f) \leq k-1 \right\}.$$

### 3.4 QECC codes from Hermitian Self-Orthognal Codes

The problem of finding QECC codes is reduced to finding hermitian self-orthogonal codes by following theorem.

**Theorem 8.** *If there exists an $[n, k, n-k+1]_{q^2}$-Hermitian self-orthogonal MDS code $C$, i.e., $C \subseteq C^{\perp_H}$, then there exists an $[[n, n-2k, k+1]]_q$-quantum MDS code.*

In the literature, Jin [20] introduce Hermitian self-orthogonal codes and provide some sufficient conditions under which a GRS code is Hermitian self-orthogonal.

There is a classical construction of quantum stabilizer codes that relies on the following theorem from Calderbank et al. [[5] , Theorem 2].

**Theorem 9.** *If there is a $[n, k, d']_{q^2}$ linear code $C$ such that $C \subseteq C^{\perp_h}$, then there exists an $[[n, n-2k, d]]_q$ quantum code, where $d$ is the minimum weight of the elements of $C^{\perp_h} \setminus C$ if $k \neq \frac{1}{2}n$ and $d$ is the minimum weight of the non-zero elements of $C^{\perp_h} = C$ if $k = \frac{1}{2}n$.*

### 3.5 Hermitian Self-Orthogonal Reed-Solomon Codes

In this section, we will give recent result of Simeon Ball and Ricard Vilar [4]. Namely, in [4] the authors gave a useful connection for construction of certain quantum MDS codes with arithmetic properties of some polynomials over $\mathbb{F}_{q^2}$. This connection allowed them to solve some conxectures in literature. Moreover, it relates the problem of constructing certain quantum MDS codes to a problem of constructing some polynomials over $\mathbb{F}_{q^2}$ with certain prescribed arithmetical properties.

Ball and Vilar [[4],Theorem 5] provided necessary and sufficient conditions for a truncation of a Reed-Solomon code to be linearly equivalent to a Hermitian self-orthogonal code. We recall these results in the following theorem and corollary.

**Theorem 10.** *Suppose $k \leq q-1$ and $n \leq q^2$. There is a linear $[n, k, n-k+1]_{q^2}$ Hermitian self-orthogonal truncated generalized Reed-Solomon code if and only if there is a polynomial $g(X) \in \mathbb{F}_{q^2}[X]$ of degree at most $(q-k)q-1$, where*

$$g(X) + g(X)^q$$

*has $q^2 - n$ distinct zeros when evaluated at $x \in \mathbb{F}_{q^2}$.*

Using Theorem 8 and Theorem 10, one can conclude the following corollary. We present a simple proof for completeness.

**Corollary 1.** *If there exists a polynomial $g(X) \in \mathbb{F}_{q^2}[X]$ of degree at most $(q-k)q-1$, where $g(X)+g(X)^q$ has N distinct zeros when evaluated at $x \in \mathbb{F}_{q^2}$, where $k \leq q-1$ then there is a $[[q^2-N, q^2-N-2k, k+1]]_q$ quantum MDS code.*

**Proof:**

Let $C$ be an $[n, k, n-k+1]_{q^2}$ Hermitian self-orthogonal MDS code. Then, Hermitian dual of $C$ is $C^{\perp_h} = [n, n-k, k+1]_{q^2}$ since the dual of a linear MDS code is also MDS code. Note that

$$d(C^{\perp_h} \setminus C) \geq d(C^{\perp_h}) = k+1. \tag{3.1}$$

Using Theorem 9 and (1), we obtain a quantum code $Q$ with parameters $[[n, n-2k, k+1]]_q$ where,

$$d \geq k+1. \tag{3.2}$$

Using Theorem 1, we obtain that

$$d \leq \frac{n+2-(n-2k)}{2} = k+1. \tag{3.3}$$

Combining (2) and (3), we complete the proof. □

### 3.5.1 Equivalence Codes

A linear code $D$ is said to be *linearly equivalent* to a linear code $C$ over $\mathbb{F}_q$ if, after a suitable re-ordering of the coordinates, there exist nonzero scalars $\theta_1, \theta_2, \ldots, \theta_n \in \mathbb{F}_q$ such that

$$D = \{(\theta_1 u_1, \theta_2 u_2, \ldots, \theta_n u_n) \mid (u_1, u_2, \ldots, u_n) \in C\}.$$

A *truncation* of a code $C$ is a code obtained from $C$ by deletion of one or more coordinates.

For any linear code $C$ over $\mathbb{F}_{q^2}$ of length $n$, Rains [29] defined the *puncture code* $P(C)$ by

$$P(C) = \left\{ \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} \lambda_i u_i v_i^q = 0 \text{ for all } u, v \in C \right\}.$$

**Theorem 11** ([29], Theorem 2)**.** *Let $C$ be a linear code over $\mathbb{F}_{q^2}$ of length $n$. There exists a truncation of $C$ to a linear code over $\mathbb{F}_{q^2}$ of length $r \leq n$ which is linearly equivalent to a Hermitian self-orthogonal code if and only if there is an element of $P(C)$ of weight $r$.*

The automorphism of equivalence codes studied by Rains is instrumental in determining the punctured codes in this way. However, the analysis of the puncture code corresponding to other automorphism types remains a challenging problem.

# CHAPTER 4

# NEW QUANTUM MDS CODES

## 4.1 New Quantum MDS Codes

In this chapter, we will show that a class of infinitely many explicit polynomials and obtain their required arithmetical properties which imply construction of an infinite class of new $q$-ary quantum MDS codes of length strictly larger than $q+1$. We use Table 1 to compare our results.

In [2], Ashikhmin and Knill provided a method to construct $q$-ary quantum MDS codes from classical Hermitian self-orthogonal MDS codes over $\mathbb{F}_{q^2}$ as follows.

## 4.2 New $q$-ary quantum MDS codes of length strictly larger than $q+1$

In this section, we present new $q$-ary quantum MDS codes. Our results are based on Theorem 10 and Corollary 1.

First, we consider the case that $\mathbb{F}_q$ is a finite field of odd characteristic and $L \geq 2$ is an even integer.

**Theorem 12.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $L \geq 2$ be even integer. Define the polynomial*

$$g(x) = x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1 \in \mathbb{F}_q[x].$$

*We call that Condition (*) holds if the equation*

$$xL \equiv \frac{q+1}{2} \mod q+1$$

*is solvable.*

*Then the polynomial $g(x)+g(x)^q$ has exactly $N$ roots in $\mathbb{F}_{q^2}$ where*

$$N = N_1 + N_2$$

*and*

$$N_1 = \begin{cases} (q-1)\gcd(L, q+1) & \textit{if Condition (*) holds}\ , \\ \\ 0 & \textit{otherwise}, \end{cases}$$

*and*

$$N_2 = \begin{cases} (q-1)\gcd(L+1, q+1) & \textit{if } p \mid (L+1), \\ \\ (q-1)(\gcd(L+1, q+1)-1) & \textit{otherwise}. \end{cases}$$

**Proof:**

We will count the number of roots $x$ of $g(x)+g(x)^q$ with $x \in \mathbb{F}_{q^2}$ . We may assume that $x \in \mathbb{F}_{q^2}^*$ since $g(0)+g(0)^q \neq 0$ when $q$ is odd. As $x^{q^2-1}=1$,

$$\begin{aligned} g(x)+g(x)^q &= x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1 \\ &\quad + x^{qL(q-1)} + x^{q(L-1)(q-1)} + \cdots + x^{q(q-1)} + 1 \\ \\ &= x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1 \\ &\quad + \frac{1}{x^{L(q-1)}} + \frac{1}{x^{(L-1)(q-1)}} + \cdots + \frac{1}{x^{(q-1)}} + 1 \\ \\ &= \frac{\left(x^{L(q-1)}+1\right)\left(x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1\right)}{x^{L(q-1)}}. \end{aligned}$$

Let $N_1$, $N_2$ be the number of roots of $x^{L(q-1)}+1$ and $x^{L(q-1)}+x^{(L-1)(q-1)}+\cdots x^{(q-1)}+1$ over $\mathbb{F}_{q^2}$, respectively. As $L$ is even, we have

$$\gcd(x^{L(q-1)}+1, x^{L(q-1)}+x^{(L-1)(q-1)}+\cdots+x^{(q-1)}+1)=1. \tag{4.1}$$

Indeed, let $f(x) \in \mathbb{F}_{q^2}[X]$ be the monic polynomial, which is the greatest common divisor of $x^{L(q-1)}+1$ and $x^{L(q-1)}+x^{(L-1)(q-1)}+\cdots+x^{(q-1)}+1$ in $\mathbb{F}_{q^2}[X]$.

Put $t = x^{q-1} \in \mathbb{F}_{q^2}[X]$. We have

$$\begin{aligned} f(x) &= \gcd(t^L+1, t^L+t^{L-1}+\cdots+t+1) \\ &= \gcd(t^L+1, t^{L-1}+\cdots+t) \\ &= \gcd(t^L+1, t^{L-2}+\cdots+1). \end{aligned} \tag{4.2}$$

As $L \geq 2$ is an even integer, we have

$$\gcd(2L, L-1) = \gcd(L, L-1) = 1.$$

This implies that

$$\gcd(t^{2L}-1, t^{L-1}-1) = t-1. \tag{4.3}$$

Using (5), we obtain that

$$f(x) \mid \gcd(t^{2L}-1, t^{L-1}-1) \tag{4.4}$$

as $t^{2L}-1 = (t^L+1)(t^L-1)$ and $t^{L-1}-1 = (t-1)(t^{L-2}+\cdots+1)$.

Combining (6) and (7) we conclude that

$$f(x) \mid (t-1). \tag{4.5}$$

Note that

$$\gcd(t-1, t^L+1) = 1 \tag{4.6}$$

as the characteristic of $\mathbb{F}_{q^2}$ is odd. Combining (5), (8), and (9) we complete a proof of (4).

Therefore, we can say that $N_1$ and $N_2$ has no common roots. Hence,

$$N = N_1 + N_2.$$

It is clear that $N_1$ is either zero or $\gcd(L(q-1), q^2-1) = (q-1)\gcd(L, q+1)$. Let $\langle g \rangle = \mathbb{F}_{q^2}^*$ be a generator of the multiplicative group. $N_1$ is not zero if and only if there exists integer $i$ such that $g^{iL(q-1)} = g^{(q^2-1)/2} = -1$ or equivalently

$$iL(q-1) \equiv \frac{q^2-1}{2} \mod (q^2-1)$$

is solvable. The last condition is equivalent to Condition (*).

We will examine two cases in order to obtain $N_2$. Recall that $p$ is the characteristic of $\mathbb{F}_{q^2}$. First, we assume that $p \mid (L+1)$. It is clear that if $x \in \mathbb{F}_q^*$ is a root of $x^{L(q-1)} + \ldots + x^{q-1} + 1$ in this case.

If $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, then it is clear that

$$x^{L(q-1)} + \ldots + x^{q-1} + 1 = \frac{x^{(L+1)(q-1)} - 1}{x^{(q-1)} - 1}.$$

Hence the number of roots $x$ in the subset $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ of $x^{L(q-1)} + \ldots + x^{q-1} + 1$ is

$$\begin{aligned} &\gcd((L+1)(q-1), q^2-1) - (q-1) \\ &= (q-1)\gcd(L+1, q+1) - (q-1), \end{aligned}$$

as $(q-1) \mid (q^2-1)$ and we exclude $\mathbb{F}_q^*$ in the subset $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. These arguments imply that

$N_2 = (q-1) + (q-1)\gcd(L+1, q+1) - (q-1) = (q-1)\gcd(L+1, q+1)$ if $p \mid (L+1)$.

Secondly we assume that $p \nmid (L+1)$. If $x \in \mathbb{F}_q^*$, then $x$ is not root of $x^{L(q-1)} + \ldots + x^{q-1} + 1$ in this case. Therefore, using the same arguments as in the first case, we conclude that $N_2 = (q-1)(\gcd(L+1, q+1) - 1)$ if $p \nmid (L+1)$.

□

Using Corollary 1 and Theorem 12 we obtain the following corollary.

**Corollary 2.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic. Assume that $q \geq 5$. Let $L$ be even integer with $2 \leq L \leq q-2$. Let $g(x)$ be the polynomial defined in Theorem 12 depending on $L$. Let $N$ be the exact number of roots of $g(x) + g(x)^q$ in $\mathbb{F}_{q^2}$, which is determined in Theorem 12. Let $k$ be an integer with $2 \leq k \leq q$ and $L(q-1) \leq (q-k)q - 1$. Then there exists a quantum MDS code with parameters $[[q^2 - N, q^2 - N - 2k, k+1]]_q$.*

Secondly, we consider the case that $\mathbb{F}_q$ is a finite field of odd characteristic and $L \geq 1$ is an odd integer.

**Theorem 13.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic $p$ and $L \geq 1$ be an odd integer. Define the polynomial*

$$g(x) = x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1 \in \mathbb{F}_q[x].$$

*Then the polynomial $g(x) + g(x)^q$ has exactly $N$ roots in $\mathbb{F}_{q^2}$ where*

$$N = N_1 + N_2 - (q-1)$$

*and*

$$N_1 = (q-1)\gcd(L, q+1)$$

*and*

$$N_2 = \begin{cases} (q-1)\gcd(L+1, q+1) & \textit{if } p \mid (L+1), \\ (q-1)(\gcd(L+1, q+1)-1) & \textit{otherwise}. \end{cases}$$

**Proof:**

The proof is similar to the proof of Theorem 12. The difference is that

$$\gcd(x^{L(q-1)}+1, x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots x^{(q-1)} + 1) = x^{(q-1)},$$

since $L$ is odd. It is known that $x^{q-1}+1$ splits in $\mathbb{F}_{q^2}$, so we can say that

$$N = N_1 + N_2 - (q-1).$$

Any root of $x^{q-1}+1$ is also a root of $x^{L(q-1)}+1$ since L is odd. So it is clear that,

$$N_1 = (q-1)\gcd(L, q+1).$$

The proof of $N_2$ is the same as the proof of Theorem 12.

□

Using Corollary 1 and Theorem 13 we obtain the following corollary.

**Corollary 3.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic. Let $L$ be an odd integer with $1 \leq L \leq q-2$. Let $g(x)$ be the polynomial defined in Theorem 13 depending on $L$. Let $N$ be the exact number of roots of $g(x) + g(x)^q$ in $\mathbb{F}_{q^2}$, which is determined in Theorem 13. Let $k$ be an integer with $2 \leq k \leq q$ and $L(q-1) \leq (q-k)q - 1$. Then there exists a quantum MDS code with parameters $[[q^2 - N, q^2 - N - 2k, k+1]]_q$.*

In Examples 7, 8 and 9 of [4], the authors presented some explicit examples providing new quantum MDS codes. Nevertheless, it seems difficult to construct all such polynomials giving quantum MDS codes explicitly. Our results provide an infinite class of new quantum MDS codes with different parameters of the examples in [4]. We use different arithmetical methods than used in the examples of [4] in our results.

### 4.3 Comparison

In this section, we show that Corollary 2 and Corollary 3 imply infinitely many new quantum MDS codes. We observe that for each $L < \frac{q}{2}$, there exists an infinitely many new quantum MDS codes depending on the choice of suitable $q$. We provide some examples by selecting small values for L.

For example, we construct the following new class of codes by putting $L = 2$:

(i). $[[q^2 - 3(q-1), q^2 - 3(q-1) - 2k, k+1]]_q$, where $q \equiv 3 \pmod{12}$ and $\frac{q-1}{2} \leq k < q-2$.

For example, we construct the following new classes of codes by putting $L = 3$:

(ii). $[[q^2 - 3(q-1), q^2 - 3(q-1) - 2k, k+1]]_q$ where $q \equiv 5$ or $7 \pmod{12}$ and $\frac{q-1}{2} \leq k < q-3$.

(iii). $[[q^2 - 5(q-1), q^2 - 5(q-1) - 2k, k+1]]_q$ where $q \equiv 11 \pmod{12}$ and $\frac{q-1}{2} \leq k < q-3$ .

Note that Table 2.1 is a table of best results in the literature which are comparable to the parameters of the quantum MDS codes that we construct in this paper. Next, we show that we find infinitely many new quantum MDS codes among the quantum MDS codes that we construct in this paper. Let us compare our class (i), namely the

quantum MDS codes with parameters $[[q^2-3(q-1), q^2-3(q-1)-2k, k+1]]_q$, where $q \equiv 3 \mod 12$ and $\frac{q-1}{2} \leq k < q-2$, with other classes of Table 2.1 to demonstrate that our class is new. For an odd prime power $q > 3$, the length is $q^2-3(q-1) > q+1$. Thus, our quantum MDS codes that are not in type 0 of Table 2.1. Our length $n = q^2-3(q-1)$ fits precisely into type 5 of Table 1, since $(q-1) \mid (q^2-3(q-1)-1)$. Our length is not in other types of Table 2.1. There are 4 four classes of Table 2.1 which are in the form of $(q-1) \mid (n-1)$. We compare our class to these 4 classes of Table 2.1.

**Class 5.1 of Table 2.1:** The length $n$ is $1 + r\frac{q^2-1}{2s+1}$ , where $(2s+1) \mid (q+1)$,$1 \leq r \leq 2s+1$ with minimum distance $d$ satisfies $2 \leq d \leq (s+1)\frac{q-1}{2s+1}$. The condition $(2s+1) \mid (q+1)$ implies that q must be even. Therefore, our quantum MDS codes cannot be obtained by this class.

**Class 5.2 of Table 2.1:** The length $n$ is $1+(2t+1)\frac{q^2-1}{2s+1}$, where $(2s+1) \mid (q+1), 1 \leq t \leq s-1$ and the minimum distance $d$ satisfies $2 \leq d \leq (s+t+1)\frac{q-1}{2s+1}$. Similar to class 5.1, the condition $(2s+1) \mid (q+1)$ implies that q must be even. Therefore, our quantum MDS codes cannot be obtained by this class.

**Class 5.3 of Table 2.1:** The length $n$ is $1 + r\frac{q^2-1}{2s}$, where $2s \mid (q+1)$, $1 \leq r \leq 2s$ with minimum distance $d$ satisfies $2 \leq d \leq (s+1)\frac{q-1}{2s}$. For suitable choices of $(r, s)$, it is possible to construct our length by this class. However, in this class, minimum distance $d$ satisfies $d \leq \frac{q-1}{2}$. So, we have quantum MDS codes with the same length but with larger minimum distances.

**Class 5.4 of Table 2.1:** The length $n$ is $1+(2t+2)\frac{q^2-1}{2s}$, where $2s \mid (q+1), 1 \leq t \leq s-1$ and minimum distance $d$ satisfies $2 \leq d \leq (s+t+1)\frac{q-1}{2s}$. There is no suitable choice of $(t, s)$ to construct our lengths. Therefore, our quantum MDS codes cannot be obtained by this class.

Similarly, we show that our other classes yield infinitely many new quantum MDS codes by using the same arguments.

The problem of constructing quantum MDS codes with $n \leq q+1$ has been completely solved in [12], [30], [21]. Therefore, it is interesting to construct quantum MDS codes with $n > q+1$, which is the case we consider in this paper. Moreover, in [13], Grassl and Rötteler gave many examples quantum MDS codes when $q \leq 32$ using by exhaustive search. It would be difficult to obtain new quantum MDS codes with $n > q+1$ if $q \leq 32$. Nevertheless, constructing quantum MDS codes with $q+1 < n \leq q^2+1$ is a very active research area in particular for $q > 32$. There are many open problems for certain length in the range $q+1 < n \leq q^2+1$ and $q > 32$. We observe that for each $L < \frac{q}{2}$, there exists an infinitely many new quantum MDS codes depending on the choice of suitable $q$. Determining new quantum codes by generalizing $L$ is not easy problem but we found some known codes when $q \leq 32$ by Grassll and Rötteler . We will give some numerical examples that give us new quantum codes when $q > 32$ and $d \leq \frac{q}{2}$.

### 4.4 Quantum MDS codes when q is even

For even values of $q$, we constructed quantum MDS codes, which have already been known in the literature.

**Theorem 14.** *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $L \geq 2$ be an even integer. Define the polynomial*

$$g(x) = x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1 \in \mathbb{F}_q[x].$$

*Then the polynomial $g(x) + g(x)^q$ has exactly $N$ roots in $\mathbb{F}_{q^2}$ where*

$$N = N_1 + N_2 + 1$$

*and*

$$N_1 = (q-1)\gcd(L, q+1)$$

**Quantum Codes over $q$ where $p^e = q$**

| $p$ | $e$ | $L$ | Quantum Codes |
|---|---|---|---|
| 3 | 2 | 2 | $[[73,69,3]]_q$, $[[73,67,4]]_q$, $[[73,65,5]]_q$, $[[73,63,6]]_q$, $[[73,61,7]]_q$, $[[73,59,8]]_q$ |
| 3 | 2 | 4 | $[[49,45,3]]_q$, $[[49,43,4]]_q$, $[[49,41,5]]_q$, $[[49,39,6]]_q$ |
| 3 | 2 | 6 | $[[81,77,3]]_q$, $[[81,75,4]]_q$ |
| 5 | 1 | 2 | $[[17,13,3]]_q$, $[[17,11,4]]_q$ |
| 5 | 2 | 2 | $[[625,621,3]]_q$, $[[625,619,4]]_q$, $[[625,617,5]]_q$, $[[625,615,6]]_q$, $[[625,613,7]]_q$, $\ldots$, $[[625,579,24]]_q$ |
| 7 | 1 | 2 | $[[37,33,3]]_q$, $[[37,31,4]]_q$, $[[37,29,5]]_q$, $[[37,27,6]]_q$ |
| 7 | 1 | 4 | $[[25,21,3]]_q$, $[[25,19,4]]_q$ |
| 7 | 2 | 2 | $[[2401,2397,3]]_q$, $[[2401,2395,4]]_q$, $\ldots$, $[[2401,2307,48]]_q$ |
| 7 | 2 | 4 | $[[2209,2205,3]]_q$, $[[2209,2203,4]]_q$, $\ldots$, $[[2209,2119,46]]_q$ |
| 7 | 2 | 6 | $[[2353,2349,3]]_q$, $[[2353,2347,4]]_q$, $\ldots$, $[[2353,2267,44]]_q$ |
| 7 | 2 | 8 | $[[2401,2397,3]]_q$, $[[2401,2395,4]]_q$, $\ldots$, $[[2401,2323,40]]_q$ |
| 9 | 1 | 2 | $[[81,77,3]]_q$, $[[81,75,4]]_q$, $[[81,73,5]]_q$, $[[81,71,6]]_q$, $[[81,69,7]]_q$, $[[81,67,8]]_q$ |
| 9 | 1 | 4 | $[[49,45,3]]_q$, $[[49,43,4]]_q$, $[[49,41,5]]_q$, $[[49,39,6]]_q$ |
| 9 | 1 | 6 | $[[81,77,3]]_q$, $[[81,75,4]]_q$ |
| 9 | 2 | 2 | $[[6561,6557,3]]_q$, $[[6561,6555,4]]_q$, $\ldots$, $[[6561,6403,80]]_q$ |
| 9 | 2 | 4 | $[[6561,6557,3]]_q$, $[[6561,6555,4]]_q$, $\ldots$, $[[6561,6407,78]]_q$ |
| 9 | 2 | 6 | $[[6561,6557,3]]_q$, $[[6561,6555,4]]_q$, $\ldots$, $[[6561,6411,76]]_q$ |
| 9 | 2 | 8 | $[[6481,6477,3]]_q$, $[[6481,6475,4]]_q$, $\ldots$, $[[6481,6337,74]]_q$ |

Figure 4.1: Some numerical examples for small q values when L is even and q is odd.

*and*

$$N_2 = (q-1)(\gcd(L+1, q+1) - 1).$$

**Proof:**

$x = 0 \in \mathbb{F}_{q^2}$ is a root of $g(x) + g(x)^q = 0$, when $q$ is even. Then the number of roots of $g(x) + g(x)^q$ in $\mathbb{F}_{q^2}$

$$N = 1 + N^*$$

where $N^*$ is the number of roots of $g(x) + g(x)^q$ in $\mathbb{F}_{q^2}^*$. If we assume that $x \in \mathbb{F}_{q^2}^*$ then, as in the proof of Theorem 12, we have

$$g(x) + g(x)^q = \frac{(x^{L(q-1)} + 1)(x^{L(q-1)} + \cdots + x^{(q-1)} + 1)}{x^{L(q-1)}}.$$

| $p$ | $e$ | $L$ | Quantum Codes |
|---|---|---|---|
| 3 | 2 | 1 | $[[73,69,3]]_q$, $[[73,67,4]]_q$, $[[73,65,5]]_q$, ..., $[[73,57,9]]_q$ |
| 3 | 2 | 3 | $[[73,69,3]]_q$, $[[73,67,4]]_q$, ..., $[[73,61,7]]_q$ |
| 3 | 2 | 5 | $[[33,29,3]]_q$, $[[33,27,4]]_q$, $[[33,25,5]]_q$ |
| 3 | 2 | 7 | $[[73,69,3]]_q$ |
| 5 | 1 | 1 | $[[21,17,3]]_q$, $[[21,15,4]]_q$, $[[21,13,5]]_q$ |
| 5 | 1 | 3 | $[[13,9,3]]_q$ |
| 5 | 2 | 1 | $[[601,597,3]]_q$, $[[601,595,4]]_q$, ..., $[[601,553,25]]_q$ |
| 5 | 2 | 3 | $[[601,597,3]]_q$, $[[601,595,4]]_q$, ..., $[[601,559,22]]_q$ |
| 7 | 1 | 1 | $[[43,39,3]]_q$, $[[43,37,4]]_q$, $[[43,35,5]]_q$, ..., $[[43,31,7]]_q$ |
| 7 | 1 | 3 | $[[31,27,3]]_q$, $[[31,25,4]]_q$, $[[31,23,5]]_q$ |
| 7 | 1 | 5 | $[[43,39,3]]_q$ |
| 7 | 2 | 1 | $[[2353,2349,3]]_q$, $[[2353,2347,4]]_q$, ..., $[[2353,2259,48]]_q$, $[[2353,2257,49]]_q$ |
| 7 | 2 | 3 | $[[2353,2349,3]]_q$, $[[2353,2347,4]]_q$, ..., $[[2353,2261,47]]_q$ |
| 7 | 2 | 5 | $[[2161,2157,3]]_q$, $[[2161,2155,4]]_q$, ..., $[[2161,2073,45]]_q$ |
| 7 | 2 | 7 | $[[2353,2349,3]]_q$, $[[2353,2347,4]]_q$, ..., $[[2353,2269,43]]_q$ |
| 9 | 1 | 1 | $[[73,69,3]]_q$, $[[73,67,4]]_q$, $[[73,65,5]]_q$, ..., $[[73,57,9]]_q$ |
| 9 | 1 | 3 | $[[73,69,3]]_q$, $[[73,67,4]]_q$, ..., $[[73,61,7]]_q$ |
| 9 | 1 | 5 | $[[41,37,3]]_q$, $[[41,35,4]]_q$, $[[41,33,5]]_q$ |
| 9 | 1 | 7 | $[[73,69,3]]_q$ |
| 9 | 2 | 1 | $[[6481,6477,3]]_q$, $[[6481,6475,4]]_q$, ..., $[[6481,6323,80]]_q$, $[[6481,6321,81]]_q$ |
| 9 | 2 | 3 | $[[6481,6477,3]]_q$, $[[6481,6475,4]]_q$, ..., $[[6481,6325,79]]_q$ |
| 9 | 2 | 5 | $[[6481,6477,3]]_q$, $[[6481,6475,4]]_q$, ..., $[[6481,6327,78]]_q$ |
| 9 | 2 | 7 | $[[6481,6477,3]]_q$, $[[6481,6475,4]]_q$, ..., $[[6481,6333,75]]_q$ |

Figure 4.2: Some numerical examples for small q values when L is odd and q is odd.

Let $N_1$, $N_2$ be the number of roots of $x^{L(q-1)}+1$ and $x^{L(q-1)}+x^{(L-1)(q-1)}+\cdots x^{(q-1)}+1$ over $\mathbb{F}_{q^2}$, respectively. If $L$ is even then we have

$$\gcd(x^{L(q-1)}+1, x^{L(q-1)}+\cdots+x^{(q-1)}+1)=1.$$

Indeed, it is enough to prove that

$$\gcd(t^L+1, t^L+\cdots+t+1)=1$$

over the ring $\mathbb{F}_q[t]$. It is clear that $(t^L+\cdots+t+1)(t+1) = t^{L+1}+1$ as the characteristic is 2. So it holds that

$$\gcd(t^L+1, t^{L+1}+1)=t+1.$$

We conclude that

$$\gcd(t^L+1, t^L+\cdots+t+1) \mid \gcd(t^{L+1}+1, t+1)=t+1.$$

We can say that

$$\gcd(t^L + 1, t^l + \cdots + t + 1) = 1,$$

if $(t+1) \nmid (t^L + \cdots + t + 1)$.

If $L$ is even then

$$Ev(t^L + 1, t^L + \cdots + t + 1) = (L+1)1 = 1 \neq 0.$$

So it is clear that

$$N_1 = (q-1)\gcd(L, q+1).$$

We can say that $2 \nmid (L+1)$, when $L$ is even. If $x \in \mathbb{F}_q^*$, then $x$ is not a root of $x^{L(q-1)} + \cdots + x^{(q-1)} + 1$.

We also have

$$x^{L(q-1)} + \cdots + x^{q-1} + 1 = \frac{x^{(L+1)(q-1)} - 1}{x^{q-1} - 1}.$$

Finally, we calculate

$$N_2 = (q-1)\left\{\gcd(L+1, q+1) - 1\right\}.$$

□

Using Corollary 1 and Theorem 14 we obtain the following corollary.

**Corollary 4.** *Let $\mathbb{F}_q$ be a finite field of characteristic 2. Assume that $q \geq 4$. Let $L$ be an even integer with $2 \leq L \leq q-2$. Let $g(x)$ be the polynomial defined in Theorem 14 depending on $L$. Let $N$ be the exact number of roots of $g(x) + g(x)^q$ in $\mathbb{F}_{q^2}$, which is determined in Theorem 14. Let $k$ be an integer with $2 \leq k \leq q$ and $L(q-1) \leq (q-k)q - 1$. Then there exists a quantum MDS code with parameters $[[q^2 - N, q^2 - N - 2k, k+1]]_q$.*

Finally, we consider the case that $\mathbb{F}_q$ is a finite field of even characteristic and $L \geq 1$ is an odd integer.

**Theorem 15.** *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $L \geq 1$ be an odd integer. Define the polynomial*

$$g(x) = x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots + x^{(q-1)} + 1 \in \mathbb{F}_q[x].$$

*Then the polynomial $g(x) + g(x)^q$ has exactly $N$ roots in $\mathbb{F}_{q^2}$ where*

$$N = 1 + N_1 + N_2 - (q-1)$$

*and*

$$N_1 = (q-1)\gcd(L, q+1)$$

*and*

$$N_2 = (q-1)\gcd(L+1, q+1).$$

**Proof:**

As in the proof of Theorem 14 , $x = 0 \in \mathbb{F}_{q^2}$ is a root of $g(x) + g(x)^q$. The proof is similar to the proof of Theorem 12. The first difference is that

$$\gcd\left(x^{L(q-1)} + 1, x^{L(q-1)} + \cdots + x^{(q-1)} + 1\right) = x^{(q-1)} + 1.$$

Indeed, it is enough to prove that

$$\gcd(t^L + 1, t^L + \cdots + t + 1) = t + 1,$$

over the ring $\mathbb{F}_q[t]$. We have $(t^L + \cdots + t + 1)(t+1) = t^{L+1} + 1$ as the characteristic is 2.

Moreover, we can say that

$$\gcd(t + 1, t^{L+1} + 1) = t + 1.$$

Hence,

$$\gcd(t^L + 1, t^L + \cdots + t + 1) \text{ is a divisor of } t + 1.$$

As $L$ is odd, $(t + 1)|(t^L + \cdots + t + 1)$.

Hence,

$$N = 1 + N_1 + N_2 - (q - 1),$$

where $N_1$, $N_2$ be the number of roots of $x^{L(q-1)} + 1$ and $x^{L(q-1)} + x^{(L-1)(q-1)} + \cdots x^{(q-1)} + 1$ over $\mathbb{F}_{q^2}$, respectively.

As in the proof of Theorem 14 , we have

$$N_1 = (q - 1)\gcd(L, q + 1).$$

As $L$ is odd, $2|(L+1)$. If $x \in \mathbb{F}_{q^2}^*$, then $x$ is a root of $x^{L(q-1)} + \cdots + x^{(q-1)} + 1$. Using similar arguments as in the proofs of Theorem 13 and 14 we obtain

$$N_2 = (q - 1)\gcd(L + 1, q + 1).$$

□

Using Corollary 1 and Theorem 15 we obtain the following corollary.

**Corollary 5.** *Let $\mathbb{F}_q$ be a finite field of characteristic 2. Assume that $q \geq 4$. Let $L$ be an odd integer with $1 \leq L \leq q - 2$. Let $g(x)$ be the polynomial defined in Theorem 15 depending on $L$. Let $N$ be the exact number of roots of $g(x) + g(x)^q$ in $\mathbb{F}_{q^2}$, which is determined in Theorem 15. Let $k$ be an integer with $2 \leq k \leq q$ and $L(q - 1) \leq (q - k)q - 1$. Then there exists a quantum MDS code with parameters $[[q^2 - N, q^2 - N - 2k, k + 1]]_q$.*

These quantum MDS codes yield the same parameter in Class 5.2 of Table 2.1. However, we do not know whether these codes are equivalent to each other; this remains an open problem.

# CHAPTER 5

# CONCLUSION

Scalable quantum computers have not yet been realized, although significant efforts are underway to develop them. In theory, these devices could solve problems that are currently intractable for classical computers. For instance, Shor's algorithm [34] has the potential to break encryption schemes based on the difficulty of integer factorization and discrete logarithms, while Grover's algorithm [14] can search an unsorted database of $N$ items in $O(\sqrt{N})$ time—a speedup that is optimal compared to the $O(N)$ time required by classical methods.

QECCs are a cornerstone of fault-tolerant quantum computing, providing a means to protect fragile quantum information from the inevitable errors caused by decoherence, noise, and operational faults. Unlike classical error correction, which deals with simple bit-flip errors, QECC must address the more complex quantum errors that affect both the amplitude and phase of qubits. This dual protection ensures the stability and reliability of quantum computations, laying the groundwork for scalable and robust quantum systems. Among these codes, QMDS codes stand out for their optimality, achieving the maximum error correction capabilities for given parameters. Constructing new QMDS codes, particularly those with novel lengths and parameters, is a critical challenge with far-reaching implications for both theoretical advancements and practical applications in quantum computing.

Ball and Vilar demonstrated that the problem of constructing QMDS codes can be reduced to finding specific polynomials over finite fields with well-defined arithmetical properties. However, they were unable to explicitly construct these polynomials. In this thesis, we successfully identified and constructed such polynomials. These

constructions enable the derivation of an infinite class of QMDS codes with new parameters.

In this thesis, we study a class of infinitely many explicit polynomials and obtain their required arithmetical properties, which imply the construction of an infinite class of new $q$-ary quantum maximum-distance-separable QMDS codes of length strictly larger than $q + 1$.

We develop a novel approach to constructing QMDS codes by explicitly building polynomials with well-defined arithmetic properties, demonstrating that our method yields new codes when $q$ is odd and successfully recovers the QMDS codes known in the literature for even values of $q$.

# REFERENCES


[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, On quantum and classical bch codes, IEEE Transactions on Information Theory, 53(3), pp. 1183–1188, 2007.

[2] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, IEEE Transactions on Information Theory, 47(7), pp. 3065–3072, 2001.

[3] S. Ball, Some constructions of quantum mds codes, Designs, Codes and Cryptography, 89, pp. 811 – 821, 2019.

[4] S. Ball and R. Vilar, Determining When a Truncated Generalised Reed-Solomon Code Is Hermitian Self-Orthogonal, IEEE Trans. Info. Theor., 68(6), pp. 3796–3805, 2022.

[5] A. Calderbank, E. Rains, P. Shor, and N. Sloane, Quantum error correction via codes over gf(4), IEEE Transactions on Information Theory, 44(4), pp. 1369–1387, 1998.

[6] B. Chen, S. Ling, and G. Zhang, Application of constacyclic codes to quantum mds codes, IEEE Transactions on Information Theory, 61(3), pp. 1474–1484, 2015.

[7] W. Fang and F.-W. Fu, Two new classes of quantum mds codes, Finite Fields and Their Applications, 53, pp. 85–98, 2018, ISSN 1071-5797.

[8] W. Fang and F.-W. Fu, Some new constructions of quantum mds codes, IEEE Trans. Inf. Theor., 65(12), p. 7840–7847, dec 2019, ISSN 0018-9448.

[9] W. Fang, J. Wen, and F.-W. Fu, Quantum mds codes with new length and large minimum distance, Discrete Mathematics, 347(1), p. 113662, 2024, ISSN 0012-365X.

[10] D. Gottesman, Stabilizer codes and quantum error correction, arXiv: Quantum Physics, 1997.

[11] M. Grass and T. A. Gulliver, On self-dual mds codes, pp. 1954–1957, 2008.

[12] M. Grassl, T. Beth, and M. Roetteler, On optimal quantum codes, International Journal of Quantum Information, 02, pp. 55–64, 2003.

[13] M. Grassl and M. Rötteler, Quantum mds codes over small fields, 2015 IEEE International Symposium on Information Theory (ISIT), pp. 1104–1108, 2015.

[14] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, p. 212–219, Association for Computing Machinery, New York, NY, USA, 1996, ISBN 0897917855.

[15] G. Guo, R. Li, and Y. Liu, Application of hermitian self-orthogonal grs codes to some quantum mds codes, Finite Fields and Their Applications, 76, p. 101901, 2021, ISSN 1071-5797.

[16] X. He, Constructing new $Q$-ary quantum MDS codes with distances bigger than $\frac{q}{2}$ from generator matrices, Quant. Inf. Comput., 18(3-4), pp. 0223–0230, 2018.

[17] L. Hu, Q. Yue, and X. Zhu, New quantum mds code from constacyclic codes, Chinese Annals of Mathematics, Series B, 37, pp. 891–898, 11 2016.

[18] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[19] L. Jin, H. Kan, and J. Wen, Quantum mds codes with relatively large minimum distance from hermitian self-orthogonal codes, Designs, Codes and Cryptography, 84, 09 2017.

[20] L. Jin, S. Ling, J. Luo, and C. Xing, Application of classical hermitian self-orthogonal mds codes to quantum mds codes, IEEE Transactions on Information Theory, 56(9), pp. 4735–4740, 2010.

[21] L. Jin and C. Xing, Euclidean and hermitian self-orthogonal algebraic geometry codes and their application to quantum codes, IEEE Transactions on Information Theory - TIT, 58, pp. 5484–5489, 08 2012.

[22] L. Jin and C. Xing, A construction of new quantum mds codes, IEEE Transactions on Information Theory, 60(5), pp. 2921–2925, 2014.

[23] X. Kai and S. Zhu, New quantum mds codes from negacyclic codes, Information Theory, IEEE Transactions on, 59, pp. 1193–1197, 02 2013.

[24] X. Kai, S. Zhu, and P. Li, Constacyclic codes and some new quantum mds codes, Information Theory, IEEE Transactions on, 60, pp. 2080–2086, 04 2014.

[25] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Transactions on Information Theory, 52(11), pp. 4892–4914, 2006.

[26] G. G. La Guardia, New quantum mds codes, IEEE Transactions on Information Theory, 57(8), pp. 5551–5554, 2011.

[27] S. Li, M. Xiong, and G. Ge, Pseudo-cyclic codes and the construction of quantum mds codes, IEEE Transactions on Information Theory, 62, pp. 1–1, 04 2016.

[28] Z. Li, L. Xing, and X. Wang, Quantum generalized reed-solomon codes: Unified framework for quantum mds codes, ArXiv, abs/0812.4514, 2008.

[29] E. Rains, Nonbinary quantum codes, IEEE Transactions on Information Theory, 45(6), pp. 1827–1832, 1999.

[30] M. Rötteler, M. Grassl, and T. Beth, On quantum mds codes, International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings., pp. 356–356, 2004.

[31] C. E. Shannon, A mathematical theory of communication, The Bell System Technical Journal, 27(3), pp. 379–423, 1948.

[32] X. Shi, Q. Yue, and X. Zhu, Construction of some new quantum mds codes, Finite Fields and Their Applications, 46, pp. 347–362, 2017, ISSN 1071-5797.

[33] X. Shi, Q. Yue, and X. Zhu, Construction of some new quantum mds codes, Finite Fields and Their Applications, 46, pp. 347–362, 2017, ISSN 1071-5797.

[34] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev., 41, pp. 303–332, 1995.

[35] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A, 52, pp. R2493–R2496, Oct 1995.

[36] A. Steane, Enlargement of calderbank-shor-steane quantum codes, IEEE Transactions on Information Theory, 45(7), pp. 2492–2495, 1999.

[37] F. Tian and S. Zhu, Some new quantum mds codes from generalized reed–solomon codes, Discrete Mathematics, 342(12), p. 111593, 2019, ISSN 0012-365X.

[38] L. Wang and S. Zhu, New quantum mds codes derived from constacyclic codes, Quantum Information Processing, 14, 05 2014.

[39] T. Zhang and G. Ge, Some new classes of quantum mds codes from constacyclic codes, IEEE Transactions on Information Theory, 61(9), pp. 5224–5228, 2015.

[40] T. Zhang and G. Ge, Quantum mds codes with large minimum distance, Des. Codes Cryptography, 83(3), p. 503–517, jun 2017, ISSN 0925-1022.

# CURRICULUM VITAE

## PERSONAL INFORMATION

**Surname, Name:** Kırcalı, Mustafa
**Nationality:**

## EDUCATION

| **Degree** | **Institution** | **Year of Graduation** |
|---|---|---|
| B.S. | B.S. Izmir University of Economics | 2018 |
| High School | Izmir Anatolian High School | 2014 |

## PROFESSIONAL EXPERIENCE

| **Year** | **Place** | **Enrollment** |
|---|---|---|
| 2019-2024 | FAME Crypt | Researcher |

## PUBLICATIONS

### International Conference Publications

Kırcalı, Mustafa and Ozbudak, Ferruh: New q-ary quantum MDS codes of length strictly larger than q + 1, Quantum Information Processing, 23, 12, 387, 2024