RICE UNIVERSITY

Quantum Algebraic Geometry Codes

Thesis by

Zhengyi Han

RICE

Thesis for the Degree of Master of Science
Department of Computer Science
Rice University (Houston, Texas) Dec, 2024

RICE UNIVERSITY

Quantum Algebraic Geometry Codes

by

Zhengyi Han

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Master of Science

Approved, Thesis Committee:

Ronald Goldman, Chair
Professor of Computer Science

Joe Warren
Professor of Computer Science

Chelsea Walton
Professor of Mathematics

Houston, Texas

Dec, 2024

To my family,

for their unconditional love

and support.

ABSTRACT

Quantum Algebraic Geometry Codes

by

Zhengyi Han

Quantum error correction is an essential aspect of quantum information theory, providing protection for quantum states against noise and decoherence. This thesis investigates the construction of quantum error correction codes derived from classical algebraic geometry (AG) codes. We present two distinct construction techniques, highlighting the flexibility and self-orthogonality of AG codes, and demonstrate their ability to produce asymptotically good quantum codes. Additionally, we explore strategies to fine-tune the parameters of classical AG codes, ensuring they possess the desired properties for quantum code construction. This work serves as a comprehensive guide to the fundamental concepts and common methodologies underlying quantum algebraic geometry codes.

Acknowledgments

I would like to express my deepest gratitude to my master's advisor, Professor Ronald Goldman, for his unwavering support in my thesis topic selection and my future research path. I am especially thankful for his encouragement of my mathematical interests, his meticulous guidance on my thesis writing, and his thoughtful care throughout my master's journey.

My heartfelt thanks also go to Professor Chelsea Walton for her invaluable advice and support regarding my future academic endeavors, and to Professor Joe Warren for his generous assistance in assembling my thesis committee.

In both Professor Goldman and Professor Walton, I have found inspiring examples of the rigorous and meticulous approach characteristic of traditional scholars. From them, I have not only learned the importance of treating research and writing with seriousness and care but also how a good advisor should treat their students with patience and encouragement.

Finally, I want to thank my parents for supporting my decision to redefine my life path and pursue this academic journey. I am also deeply grateful to my friends at Rice University for their companionship and support along the way.

Thank you all for being a part of this meaningful chapter in my life.

Contents

Chapter 1

Introduction

The field of error correction has undergone significant evolution since its inception in the mid-20th century, driven by the need to ensure the reliable transmission and storage of information in the presence of noise. Classical error correction codes, such as Hamming codes and Reed-Solomon codes, laid the foundation for modern coding theory. These codes exploit algebraic and combinatorial structures to detect and correct errors, ensuring robust communication across unreliable channels.

In the quantum realm, the challenge of error correction is magnified. Unlike classical information, which can be copied and measured without disruption, quantum information adheres to the principles of quantum mechanics, including no-cloning and the uncertainty principle. These constraints necessitate entirely new approaches to error correction. The pioneering work of Shor [1] and Steane [2] in the mid-1990s introduced the first quantum error correction codes (QECCs), demonstrating the possibility of protecting quantum information against decoherence and operational errors. Since then, QECCs have become an indispensable tool in the quest for scalable quantum computing and secure quantum communication. The *CSS construction*, introduced by Calderbank, Shor, and Steane, further bridged the gap between classical codes and quantum codes by providing a systematic way to convert classical linear codes into quantum codes. This construction not only expanded the class of known quantum codes but also provided a rich framework for constructing new quantum codes from well-understood classical codes.

Algebraic geometry codes (AG codes), introduced by Goppa [3] in the 1970s, represent one of the most powerful classes of error correction codes in classical coding theory. By leveraging the rich mathematical structure of algebraic curves over finite fields, AG codes achieve exceptional performance in terms of both error correction capability and efficiency. Notably, AG codes can be asymptotically better than the Gilbert-Varshamov (GV) bound. The strength of AG codes lies in their connection to the theory of algebraic geometry, including tools such as Riemann-Roch theorem, modular curves and so on. These mathematical foundations enable the construction of codes with precisely controlled parameters, such as length, dimension, and minimum distance. For instance, AG codes derived from high-genus curves or specific families like modular and Hermitian curves exhibit superior error correction properties while maintaining efficient encoding and decoding algorithms. Moreover, the systematic nature of AG code construction has led to a wide array of explicit examples and families of codes, making them not only theoretically robust but also practically relevant.

This thesis is devoted to the study and construction of quantum algebraic geometry codes. The primary goal is to develop explicit constructions of quantum error correction codes derived from classical AG codes. Our main approach is to search for self-orthogonal classical AG codes and obtain quantum codes through Steane's construction. Due to the rich structure of AG codes, we can explicitly construct a family of desired self-orthogonal codes for quantum code construction using certain mathematical theories.

The organization of this thesis is as follows:

- **Chapter 2** provides an introduction to quantum error correction codes. We mainly focus on the key concept: *stabilizer formalism* introduced by Gottesman [4]. Shortly after that, the nonbinary case was well studied by Rains [5] and Ashikhmin and Knill [6]. This chapter establishes the foundational principles required for constructing and analyzing quantum codes.
- **Chapter 3** explores the theory of algebraic geometry and classical AG codes. It begins with a discussion of algebraic curves, divisors, and Riemann-Roch theory, followed by an explanation of how these concepts are used to construct classical AG codes. Special emphasis is placed on the parameters of these codes, such as their length, dimension, and minimum distance, which play a crucial role in their

performance.

- **Chapter 4** focuses on summarizing existing results on the construction of quantum codes from algebraic geometry. This chapter reviews how the rich structure of algebraic geometry has been used to design asymptotically good quantum codes [7], highlighting key techniques and performance metrics. Furthermore, it discusses various approaches and results for constructing self-orthogonal classical codes, which serve as the foundation for generating quantum codes through methods such as Steane's construction. The aim of this chapter is to provide a clear and comprehensive overview of how algebraic geometry can be leveraged in the context of quantum code construction.

The organization of this thesis was inspired by the structure and content of [8], which provided a clear and concise overview of the field. This article allowed me to quickly grasp the key developments and ongoing research in this area, serving as a valuable guide during the preparation of this thesis.

Chapter 2

Quantum Stabilizer Codes

2.1 Basic Definitions of Classical Linear Codes

Classical linear codes are fundamental in information theory and coding theory, primarily utilized for error detection and correction in data transmission and storage. Their linear structure facilitates both theoretical analysis and practical implementation, making them widely applicable in communication systems, storage devices, and other domains requiring reliable data transmission. This section provides the necessary background on classical linear codes to facilitate our subsequent discussion of quantum stabilizer codes and classical algebraic geometry codes.

A *linear code* C over a finite field $\mathbb{F}_q$, where q is a prime power, is defined as a k-dimensional linear subspace of $\mathbb{F}_q^n$. This means that C consists of all linear combinations of its basis vectors and has a length n and dimension k, denoted as an (n, k) linear code:

$$C \subseteq \mathbb{F}_q^n, \quad \dim_{\mathbb{F}_q}(C) = k.$$

The elements of C are called *codewords*, every vector in C is a codeword. The parameter n represents the length of each codeword, i.e. the number of physical bits, while k represents the number of independent data symbols encoded in each codeword.

The minimum distance d of a linear code C is a critical parameter that determines its error-detecting and error-correcting capabilities. The minimum distance is defined as the smallest Hamming distance between any two distinct codewords in C. Due to the code's linearity, the minimum distance is also equivalent to the smallest weight of any non-zero codeword:

$$d = \min\{\mathrm{wt}(\mathbf{c}) \mid \mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}\},$$

where $\mathrm{wt}(\mathbf{c})$ denotes the Hamming weight of the codeword **c**, i.e., the number of non-zero coordinates. A larger minimum distance d implies a greater ability to detect and correct errors.

Theorem 2.1.1 (Error-Correcting Capability)**.** *A (n, k, d) linear code C can detect up to $d - 1$ errors and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.*

Proof. Consider a received vector $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in C$ is the transmitted codeword and $\mathbf{e}$ is the error vector with Hamming weight $\mathrm{wt}(\mathbf{e}) = t$.

- **Error Detection**: If $t \leq d - 1$, then the error vector **e** alters the received vector so that **r** differs from **c** by less than the minimum distance d. Since all distinct codewords are at least d apart, the receiver can detect that an error has occurred.
- **Error Correction**: If $t \leq \lfloor \frac{d-1}{2} \rfloor$, the error pattern **e** is unique within this weight range. Thus, the receiver can accurately identify and correct the error, recovering the original codeword **c**.

□

The *generator matrix* G is a pivotal tool for constructing linear codes. For an (n, k) linear code C, a generator matrix G is a $n \times k$ matrix whose columns form a basis for C. We can view G as the encoding map from the information space $\mathbf{F}_q^k$ to the codewords $C \subseteq \mathbf{F}_q^n$, i.e. $C = \mathrm{im}(G)$.

The parity-check matrix H serves as a counterpart to the generator matrix G, enabling error detection to ensure the reliability of the code. In short, we define H by $\ker(H) = C$. The dimension of the codomain is not very important, and we usually take it as $n - k$ by the Rank-Nullity Theorem. Hence, for an (n, k) linear code C, the parity-check matrix H is an $(n - k) \times n$ matrix defined so that:

$$C = \{\mathbf{c} \in \mathbb{F}_q^n \mid H\mathbf{c} = \mathbf{0}\},$$

i.e. each row of H is orthogonal to C. As a result, we get the following proposition.

Proposition 2.1.2 (Orthogonality). *For any generator matrix G and parity-check matrix H of a linear code C,*

$$HG = \mathbf{0}.$$

Proof. By definition, every codeword $\mathbf{c}$ satisfies $H\mathbf{c} = \mathbf{0}$. Since the columns of G generate all codewords, $HG = \mathbf{0}$. □

Dual codes offer deeper insights into the structure of linear codes by examining the relationship between a code and its orthogonal complement. Given an (n, k) linear code $C \subseteq \mathbb{F}_q^n$, its dual code $C^\perp$ is defined by:

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v} \cdot \mathbf{c} = 0 \ \forall \mathbf{c} \in C\},$$

where $\mathbf{v} \cdot \mathbf{c}$ denotes the standard inner product:

$$\mathbf{v} \cdot \mathbf{c} = \sum_{i=1}^{n} v_i c_i.$$

The dual code $C^\perp$ is an $(n, n-k)$ linear code, and the dual of the dual code returns the original code, i.e., $(C^\perp)^\perp = C$.

Furthermore, if G is a generator matrix for C, then H^T serves as a generator matrix for $C^\perp$, and G^T is the parity-check matrix for $C^\perp$. The proof follows directly from the properties of the columns and rows of H and G. Note that we can only get information about n and k, but there is no theoretical guarantee regarding the distance d. Because the distance encodes finer-grained information rather than purely algebraic properties of a linear space — which, as we know, are determined solely by its dimension. To control the distance of dual codes, we need more information about the structure of the linear map G. Some AG codes can help us do that. The distance of the dual MDS (Maximum Distance Separable) codes is fully determined by the parameters of the original code. We'll give more detailed information in Section 3.1.

2.2 Quantum Mechanics on Qubits

In quantum mechanics, the state of a system encodes all its physical information. Unlike classical states, quantum states are represented by vectors in a complex Hilbert space. For a single particle, this quantum state corresponds to a wavefunction $\psi(x)$, which describes the probability distribution of the particle's position. More generally, quantum states are vectors in a Hilbert space, satisfying the axioms of quantum mechanics.

A single qubit, the basic unit of quantum information, has a state space given by $\mathbb{C}^2$. Using Dirac notation, a general state of a qubit is written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Here, $|0\rangle$ and $|1\rangle$ are the computational basis states. While they are often associated with two distinct quantum states of a physical system, such as energy levels in a two-level atom, their specific meaning depends on the physical implementation. For instance:

- In two-level atoms, $|0\rangle$ and $|1\rangle$ typically represent the ground and excited states.
- In photon-based qubits, $|0\rangle$ and $|1\rangle$ might represent horizontal and vertical polarization states, or different modes of the photon.

The coefficients α and β are complex probability amplitudes, with $|\alpha|^2$ and $|\beta|^2$ representing the probabilities of measuring the qubit in states $|0\rangle$ and $|1\rangle$, respectively. These coefficients encode the quantum state's superposition, a defining feature that allows the qubit to exist simultaneously in a continuum of states between $|0\rangle$ and $|1\rangle$.

The evolution of a quantum state is governed by a unitary operator U, which preserves the probability.

Quantum measurement is a probabilistic process. Every observable in quantum mechanics corresponds to an essentially self-adjoint operator acting on the Hilbert space of the system. For a single qubit, examples of such observables are the *Pauli matrices*:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Observables for qubits are Hermitian matrices, meaning their eigenvalues are real numbers, and they can be diagonalized by unitary transformations. The eigenvalues of these operators correspond to possible outcomes of measurements, and the associated eigenvectors define the measurement basis.

- The **Pauli Z operator** corresponds to a measurement of the qubit in the computational basis $\{|0\rangle, |1\rangle\}$, where the eigenvalues +1 and -1 indicate the outcomes $|0\rangle$ and $|1\rangle$, respectively.
- The **Pauli X operator** corresponds to a measurement in the basis $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. These states represent superpositions of the computational basis states.

When a qubit in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is measured, the probabilities of obtaining specific outcomes are determined by the *Born rule*. For example:

- A measurement of Z yields +1 with probability $|\alpha|^2$ and -1 with probability $|\beta|^2$.
- A measurement of X requires the state to be projected onto the $|+\rangle$ or $|-\rangle$ basis, with probabilities depending on the overlap of $|\psi\rangle$ with these basis vectors.

In quantum mechanics, the Pauli X and Z operators represent different types of measurements on a qubit. However, these two operators do not commute:

$$[X, Z] = XZ - ZX = 2iY \neq 0, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

This non-commutativity implies that X and Z cannot be diagonalized simultaneously, meaning that it is impossible to measure both observables precisely at the same time.

This impossibility is closely related to the *uncertainty principle*, which states that certain pairs of observables cannot be known simultaneously with arbitrary precision. In the case of X and Z, preparing a state that has a definite value for one observable (e.g., an eigenstate of Z) leaves the outcome of the other observable (in this case, X) entirely uncertain.

Proposition 2.2.1 (Simultaneous Measurement)**.** *Two observables can be measured simultaneously if and only if they commute, i.e., if their commutator is zero:*

$$[A, B] = AB - BA = 0.$$

If two matrices commute then they share the same eigenspace. Hence commutative observables can be diagonalized simultaneously since they are Hermitian. In quantum error correction, this property is crucial, since we use commuting Pauli operators to detect and correct errors without disturbing the encoded information.

When multiple qubits are involved, states live in the tensor product of the individual qubit spaces. For example, the state of two qubits is represented as:

$$|\psi_1\rangle \otimes |\psi_2\rangle = \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle .$$

In general, for n qubits, the state space is $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$. The tensor product structure reflects the fact that the overall state captures the behavior of all individual qubits and their interactions, following the properties of multilinear maps. In Dirac notation, the tensor product is often abbreviated, so $|01\rangle$ denotes $|0\rangle \otimes |1\rangle$.

An important concept in multi-qubit systems is entanglement. A state is entangled if it cannot be written as a product of individual qubit states. A well-known example of an entangled state is the Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Entangled states exhibit correlations that have no classical analog, making them essential in quantum information processing. To see its non-classical nature, consider measuring the two qubits in the computational basis $\{|0\rangle, |1\rangle\}$. If the first qubit is measured to be $|0\rangle$, the state of the entire system collapses to: $|00\rangle$, meaning the second qubit is also guaranteed to be in the state $|0\rangle$. Similarly, if the first qubit is measured to be $|1\rangle$, the system collapses to: $|11\rangle$. This perfect correlation persists even if the two qubits are spatially separated, a phenomenon known as *quantum non-locality*.

Readers interested in the axiomatic formulation of quantum mechanics may refer to [9, Section 3.6].

2.3 Stabilizer Codes

Quantum error-correcting codes (QECCs) are designed to protect quantum information from errors caused by decoherence and other noise in quantum systems. These codes generalize the principles of classical error correction to the quantum domain, accounting not only for bit-flip errors but also for phase-flip errors, as well as superpositions of these errors. This extension is essential, as quantum information is inherently fragile and can be easily disturbed by interactions with the environment.

In classical coding theory, a code is a subset of $\mathbb{F}_q^n$, where the task is to encode k-bit messages into n-bit codewords. In the quantum case, however, the codewords are vectors in $(\mathbb{C}^2)^{\otimes n}$, the n-qubit Hilbert space. A quantum code Q is formally defined as a subspace of this Hilbert space. If Q encodes k logical qubits using n physical qubits, we call Q an $[n, k]$ quantum code, and each state in this subspace is referred to as an encoded quantum state or a codeword.

Quantum systems are susceptible to a variety of errors, such as bit-flips, phase-flips, or their superpositions. For example, consider a single qubit in the state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$:

- A *bit-flip error* transforms $|0\rangle \to |1\rangle$, represented by the Pauli X-operator.
- A *phase-flip error* leaves $|0\rangle$ unchanged but transforms $|1\rangle \to -|1\rangle$, represented by the Pauli Z-operator.

- A combined error, represented by the Pauli Y-operator, applies both bit-flip and phase-flip operations.

Quantum codes must be able to detect and correct these types of errors to ensure reliable quantum computation.

Similar to classical codes, quantum codes are characterized by a parameter called the *distance* d. A quantum code has distance d if it can detect any set of up to $d-1$ qubit errors and correct any set of up to $\lfloor (d-1)/2 \rfloor$ errors. Thus, an $[n, k, d]$ quantum code encodes k logical qubits into n physical qubits and has a minimum distance d, determining its error-correcting capability.

One of the key challenges in quantum error correction is detecting errors without directly measuring the encoded information since measurement can collapse the quantum state. An important mathematical tool for describing quantum codes is the *Pauli group* $\mathcal{P}_n$, which consists of all n-fold tensor products of the single-qubit Pauli matrices I, X, Y, and Z, with phase factors (coefficients) $\{\pm 1, \pm i\}$. The Pauli operators are defined by:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Each Pauli operator corresponds to a specific quantum operation on a single qubit:

- X is the bit-flip operator, exchanging $|0\rangle$ and $|1\rangle$.
- Z is the phase-flip operator, leaving $|0\rangle$ unchanged but mapping $|1\rangle \rightarrow -|1\rangle$.
- Y applies both a bit-flip and a phase-flip, corresponding to $Y = iXZ$.

The Pauli operators either commute or anti-commute with each other. Their commutation relations are given by:

$$[X, Y] = XY - YX = 2iZ, \quad [Y, Z] = YZ - ZY = 2iX, \quad [Z, X] = ZX - XZ = 2iY.$$

The Pauli group $\mathcal{P}_n$ for n-qubits consists of all tensor products of the form:

$$\mathcal{P}_n = \left\{ \alpha \, P_1 \otimes P_2 \otimes \cdots \otimes P_n \mid \alpha \in \{\pm 1, \pm i\}, \; P_j \in \{I, X, Y, Z\} \right\}.$$

The Pauli group plays a central role in stabilizer codes, since the generators of a stabilizer group are chosen from $\mathcal{P}_n$.

A key property of the Pauli group is that every pair of Pauli operators either commutes or anti-commutes:

$$P_i P_j = (-1)^{\omega(P_i, P_j)} P_j P_i,$$

where $\omega(P_i, P_j)$ is 0 if they commute and 1 if they anti-commute.

Another important property of the Pauli operators is that all their eigenvalues have an absolute value of 1 (they are unitary). Specifically:

$$\text{Eigenvalues of } X, Y, Z \in \{\pm 1, \pm i\}.$$

These operators represent the types of errors that can occur in a quantum system and serve as the building blocks for many quantum codes, including stabilizer codes.

Let me start with a statement: Stabilizer codes are the quantum counterparts of classical linear codes and represent one of the most widely accepted frameworks for quantum error correction.

A *stabilizer code* is defined by a stabilizer group S, which is a subgroup of the n-qubit Pauli group $\mathcal{P}_n$. The stabilizer group S defines a subspace of the n-qubit Hilbert space $(\mathbb{C}^2)^{\otimes n}$, called the *code space*, consisting of all quantum states that are invariant under the action of every element in the stabilizer group:

$$Q = \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,\middle|\, g\,|\psi\rangle = |\psi\rangle \,, \, \forall g \in S \right\}.$$

This definition means that each valid codeword $|\psi\rangle$ remains unchanged under the action of all stabilizer elements $g \in S$.

The stabilizer group S is generated by a set of independent Pauli operators, called *stabilizer generators*. If the group has $n - k$ independent generators, the code space will have dimension 2^k, meaning the code encodes k logical qubits into n physical qubits. This type of code is denoted as an $[n, k]$ stabilizer code.

Proposition 2.3.1. *The stabilizer group S is an abelian group.*

Proof. Since both g and h leave every codeword $|\psi\rangle$ in the code space invariant, we have:

$$g|\psi\rangle = |\psi\rangle, \quad h|\psi\rangle = |\psi\rangle .$$

Applying both operators in sequence gives:

$$gh|\psi\rangle = g(h|\psi\rangle) = g|\psi\rangle = |\psi\rangle ,$$

and similarly:

$$hg|\psi\rangle = h(g|\psi\rangle) = h|\psi\rangle = |\psi\rangle .$$

Thus, $gh|\psi\rangle = hg|\psi\rangle$ for all $|\psi\rangle \in Q$, implying that $gh = hg$. This ensures that the stabilizer group is abelian. □

Consider a set of k independent Pauli operators $\{g_1, g_2, \ldots, g_k\}$ that generate the stabilizer group S. These generators are independent if removing any element would reduce the size of the generated group.

Proposition 2.3.2. *If the stabilizer group has k independent generators, the dimension of the code space Q is given by:*

$$\dim(Q) = 2^{n-k}.$$

Proof. Since the stabilizer group S is abelian, all of its generators can be diagonalized simultaneously. Therefore we can find a common basis in which all the stabilizer generators are represented by diagonal matrices.

Each stabilizer generator has eigenvalues ±1, and each generator partitions the Hilbert space into two eigenspaces corresponding to these eigenvalues. Since each generator is independent and commutes with the others, the simultaneous eigenspace corresponding to the +1 eigenvalue for all generators defines the code space Q. Each independent stabilizer generator halves the dimension of the subspace it stabilizes.

Starting from the full Hilbert space of n qubits, which has dimension 2^n, the presence of k independent stabilizers reduces the dimension by a factor of 2^k, resulting in a code space of dimension 2^{n-k}.

□

In other words, the stabilizer group S defines $n - k$ logical qubits that can be used to encode quantum information. Thus, an $[n, k]$ stabilizer code encodes k logical qubits into n physical qubits, with the code space being the simultaneous +1 eigenspace of all elements in the stabilizer group.

We already know the number of logical qubits, now we move on to the distance. The distance of a stabilizer code is defined by:

$$d = \min \{\mathrm{wt}(E) \mid E \in N(S) \setminus S,\ E \neq I\},$$

where the *weight* of an operator is defined as the number of qubits on which it acts non-trivially (i.e., with X, Y, Z rather than the identity I). $N(S)$ is the normalizer of the stabilizer group in the Pauli group:

$$N(S) = \{E \in \mathcal{P}_n \mid Eg = gE,\ \forall g \in S\}.$$

To provide some intuition:

- The stabilizer group S defines the set of operators that leave the code space invariant, representing logical qubit states. Any operator in S acts trivially on the code space and does not introduce errors.

- The normalizer $N(S)$ includes operators that preserve the stabilizer structure but may act non-trivially on the code space, potentially inducing logical errors.
- The distance measures the smallest weight of such an operator in $N(S) \setminus S$ that could cause a logical error. The weight corresponds to the number of qubits affected by the operator, directly linking the distance to the error resilience of the code: the higher the distance, the greater the number of errors the code can detect and correct.

This definition ensures that a code with distance d can detect up to $d - 1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors. Thus, the distance provides a clear quantitative measure of the robustness of a quantum code against noise and errors.

The distance of the code determines the number of errors that can be detected and corrected:

- A code with distance d can detect up to $d - 1$ errors.
- And can correct up to $\lfloor (d-1)/2 \rfloor$ errors.

2.4 CSS Codes

CSS codes, named after their inventors Calderbank, Shor, and Steane, are a special type of stabilizer code. The CSS construction provides an efficient way to construct quantum error-correcting codes from classical linear codes. In the previous sections, we discussed stabilizer groups and their role in defining quantum codes. In this section, we will see that by representing stabilizers in a matrix or vector form, we can make stabilizer codes resemble classical linear codes. We will also explore the relationship between CSS codes, chain complexes, and homology groups, which highlights some of the interesting mathematical structures underlying quantum error correction. This connection will be explained at the end of this section.

2.4.1 Binary Representation of Stabilizers

In quantum error correction, stabilizers can be represented using binary vectors, which allows us to draw a connection between quantum codes and classical linear codes. Specifically, an n-qubit Pauli operator can be represented as a pair of binary vectors $(\mathbf{v}_X, \mathbf{v}_Z)$ of length n, where $\mathbf{v}_X$ indicates the positions of the X operators and $\mathbf{v}_Z$ indicates the positions of the Z operators. More precisely:

- For each qubit, if there is an X operator, the corresponding position in $\mathbf{v}_X$ is set to 1.
- For each qubit, if there is a Z operator, the corresponding position in $\mathbf{v}_Z$ is set to 1.
- If both X and Z are present (i.e., Y operator), both entries are set to 1.

This representation allows us to express a Pauli operator P as a binary vector $(\mathbf{v}_X, \mathbf{v}_Z) \in \mathbb{F}_2^{2n}$. Given a set of stabilizer generators, we can construct a matrix whose rows are the binary vectors representing these generators.

To understand the structure of these codes, it is useful to describe the Pauli group in terms of *symplectic space.* For an n-qubit system, consider the $2n$-dimensional vector space $V = \mathbb{Z}_2^{2n}$. Each Pauli operator can be associated with a vector $(a, b) \in \mathbb{Z}_2^{2n}$, where the vector components indicate the positions where the X- and Z-operators act:

$$P(a, b) = i^{\gamma} X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n},$$

where γ is an integer phase factor.

We define a symplectic form ω on the space $V = \mathbb{Z}_2^{2n}$ by:

$$\omega\left((a, b), (a', b')\right) = a \cdot b' - a' \cdot b \pmod 2.$$

This symplectic form encodes the commutation relations between Pauli operators. Specifically:

- If $\omega((a, b), (a', b')) = 0$, the corresponding Pauli operators commute.

- If $\omega((a,b),(a',b')) = 1$, the operators anti-commute.

The symplectic space provides a crucial perspective for analyzing the Pauli group, and we leave a detailed introduction to the relevant concepts for the Appendix. Now, we return to stabilizer codes (or CSS codes).

To determine if a set of Pauli operators forms a valid stabilizer group (i.e., an abelian group), we need to ensure that all the operators commute. In the binary representation, this condition can be expressed in terms of the symplectic inner product. Thus, for a matrix representing a set of stabilizer generators, the symplectic inner product between any two rows must be zero to guarantee that the stabilizer group is abelian. For a set of Pauli operators, we get the binary representation S, which is a matrix with $2n$ columns. The group generated by the operators is abelian if and only if $SS^T = \mathbf{0}$.

Once we have a matrix that correctly represents a stabilizer group, we can determine the dimension of the code space by analyzing the linear independence of the row vectors in the matrix. Let H be the matrix whose rows are the binary vectors representing the stabilizer generators. The rank of H, denoted by r, is the number of independent generators of the stabilizer group. This statement leads to the following lemma. It is quite intuitive, and the proof is not difficult, so we omit it here.

Lemma 2.4.1. Pauli operators are independent if and only if their binary representations are linearly independent.

Thus, according to Proposition 2.3.2, the dimension of the stabilizer code, which corresponds to the number of logical qubits k, is given by:

$$k = n - r,$$

where n is the number of physical qubits.

If a stabilizer group is generated by operators that have only X-components and only Z-components, then the binary representation of this set of generators forms a block-diagonal matrix composed of H_X and H_Z:

$$H = \begin{bmatrix} H_X & 0 \\ 0 & H_Z \end{bmatrix},$$

where $H_X,\ H_Z$ are matrics with n columns. If these operators commute with each other, we need $HH^T = \mathbf{0}$. In this special case, substituting the matrix representation into the equation $HH^T = \mathbf{0}$ yields:

$$H_X H_Z^T = 0.$$

Since the composition of two linear maps $H_Z^T,\ H_X$ is equal to $\mathbf{0}$, it's natural to consider the related chain complex. We will show the further relationship later. First, we begin to state the *CSS construction* explicitly.

2.4.2 CSS Construction

The CSS (Calderbank-Shor-Steane) construction starts with two classical linear codes C_1 and C_2, with $C_2^\perp \subseteq C_1$. The stabilizer generators for the CSS code are derived from the parity check matrices of these classical codes. Specifically:

- The X-type stabilizer generators are derived from the parity check matrix H_1 of code C_1.
- The Z-type stabilizer generators are derived from the parity check matrix H_2 of code C_2.

Since $C_1 = \ker(H_X),\ C_2^\perp = \operatorname{im}(H_Z^T)$, the condition $C_2^\perp \subseteq C_1$ equals to $H_X H_Z^T = 0$. The equation ensures that the corresponding stabilizer generators commute, resulting in a valid stabilizer group.

2.4.3 Chain Complex and Homology

The CSS construction naturally leads to a chain complex structure. Consider the following sequence of vector spaces and linear maps:

$$A_2 \xrightarrow{H_Z^T} A_1 \xrightarrow{H_X} A_0,$$

where A_0, A_1, A_2 are $\mathbb{F}_2$-vector space. You can view A_i as chain groups. H_Z^T is the transpose of the parity check matrix of C_Z, and H_X is the parity check matrix of C_X. The condition $C_Z^\perp \subseteq C_X$ ensures that the composition of these two maps is zero, i.e., $H_X H_Z^T = 0$. This condition gives rise to a chain complex, and the corresponding homology describes the structure of the CSS code. H_Z^T, H_X are boundary maps between chain groups.

The number of logical qubits k is given by the dimension of the first homology group, which can be computed as:

$$k = \dim(C_1) - \dim(C_2).$$

This formula corresponds to the number of degrees of freedom that are not constrained by the stabilizers, i.e., the number of logical qubits that can be used to encode information.

The distance d of the CSS code is determined by the minimum weight of a codeword in $C_Z \setminus C_X^\perp$ for X errors and the minimum weight of a codeword in $C_X \setminus C_Z^\perp$ for Z errors. Specifically:

- The distance for X errors is given by the minimum weight of a codeword in $C_Z \setminus C_X^\perp$.
- The distance for Z errors is given by the minimum weight of a codeword in $C_X \setminus C_Z^\perp$.

Thus, the CSS construction provides a powerful method for constructing quantum error-correcting codes with well-defined parameters for the number of logical qubits and the code distance.

2.4.4 Further on CSS codes

CSS codes indeed have a homological interpretation, but not all CSS codes are constructed from a specific chain complex. The quantum AG codes, which are the main focus of this paper, are all CSS codes. However, most existing quantum AG codes are constructed from certain self-orthogonal classical AG codes. In the following, we will provide a brief discussion on the homological interpretation of CSS codes, serving as an introduction to quantum error correction for the readers.

CSS codes, which are constructed using homological structures such as simplicial complexes or surfaces, provide a natural connection to topological order. The key idea lies in how these codes encode quantum information in a way that is robust against local perturbations, a hallmark of topological order.

Topological order refers to a phase of matter characterized by ground-state degeneracy and long-range entanglement, which are stable under local perturbations. Thus, CSS codes are not just an application of homology but also a bridge to understanding and simulating topological phases of matter. They provide a practical and mathematical framework to explore topological order through quantum error correction.

This article [10] introduces the first topological code and establishes the connection between QECC, topological order, and Hopf algebras. In addition, the author has another seminal paper [11] in this field, which we highly recommend to interested readers. We will not delve into further details here.

2.5 Quantum Codes on Qudits

Since this paper discusses how to construct quantum AG codes from classical AG codes, and classical AG codes are based on algebraic curves over finite fields, it is necessary to present the basic properties of quantum codes over finite fields. In this section, we extend stabilizer codes from binary codes to codes over q-dimensional qudits, where each qudit is associated with a finite field $\mathbb{F}_q$ (with $q = p^m$, a power of a prime). These codes maintain much of the structure from the binary case but introduce additional algebraic richness due to the finite field.

For qudits over $\mathbb{F}_q$, the state space for a single qudit is:

$$\mathcal{H} = \mathbb{C}^q,$$

with computational basis states $\{|k\rangle \mid k \in \mathbb{F}_q\}$. For an n-qudit system, the total Hilbert space is:

$$\mathcal{H}_n = \mathcal{H}^{\otimes n} = \mathbb{C}^{q^n}.$$

Each element in this space corresponds to a tensor product of basis states, such as $|k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle$ for $k_i \in \mathbb{F}_q$.

2.5.1 Pauli Operators for $\mathbb{F}_q$ Qudits

The generalized Pauli operators for a single qudit are defined as:

$$X(a)\,|k\rangle = |k+a\rangle\,, \quad Z(b)\,|k\rangle = \omega^{\mathrm{tr}(bk)}\,|k\rangle\,,$$

where $\omega = e^{2\pi i/p}$ is a primitive p-th root of unity, $a, b \in \mathbb{F}_q$, and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map:

$$\mathrm{tr}(x) = \sum_{i=0}^{m-1} x^{p^i}.$$

These operators satisfy the commutation relation:

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

The generalized Pauli group $\mathcal{P}(q)_n$ for n-qudits is generated by the tensor products of these operators:

$$\mathcal{P}(q)_n = \{\omega^c X(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n) \mid c \in \mathbb{Z}/p\mathbb{Z},\ a_i, b_i \in \mathbb{F}_q\}.$$

The error operators $X(a)Z(b)$ can be represented as vectors $(a, b) \in \mathbb{F}_q^{2n}$. The symplectic form for two such vectors $(a, b), (a', b') \in \mathbb{F}_q^{2n}$ is defined as:

$$\langle (a,b), (a',b') \rangle = \operatorname{tr}\left(\sum_{i=1}^{n} \left(a_i b_i' - b_i a_i' \right) \right).$$

Two operators $X(a)Z(b)$ and $X(a')Z(b')$ commute if and only if:

$$\langle (a,b), (a',b') \rangle = 0.$$

The stabilizer code Q over $\mathbb{F}_q$ is defined by a stabilizer group $\mathcal{S}$, which is an abelian subgroup of the generalized Pauli group $\mathcal{P}(q)_n$. such that all elements in $\mathcal{S}$ commute. The code space is the +1 eigenspace of all the stabilizer.

Since we have the symplectic representation, CSS codes can be constructed over $\mathbb{F}_q$ using two linear codes C_1 and C_2 such that:

$$C_2^{\perp} \subseteq C_1,$$

where the dual code $C^{\perp}$ is defined as:

$$C^{\perp} = \{ y \in \mathbb{F}_q^n \mid \langle x, y \rangle = \operatorname{tr}(x \cdot y) = 0 \text{ for all } x \in C \}.$$

The CSS code encodes logical qudits in the space:

$$|\overline{\psi}\rangle = \sum_{x \in C_2} |x + \psi\rangle,$$

where $\psi \in C_1 / C_2^{\perp}$ represents the logical information. Errors are detected and corrected by projecting onto the relevant code subspaces defined by C_1 and $C_2^{\perp}$.

The minimum distance d of the code is:

$$d = \min\{\mathrm{wt}(e) \mid e \in C_1 \setminus C_2^{\perp}\},$$

where $\mathrm{wt}(e)$ is the Hamming weight of the error vector e. This distance determines the number of correctable errors.

The generalization of stabilizer codes to $\mathbb{F}_q$ enables more flexibility and algebraic richness in quantum error correction. These codes form the foundation for quantum algebraic geometry codes.

Chapter 3

Algebraic Geometry Codes

3.1 Reed-Solomon Codes

Reed-Solomon (RS) codes constitute a fundamental class of error-correcting codes within the framework of algebraic coding theory. Defined over finite fields, RS codes leverage the properties of polynomial interpolation and evaluation to encode and decode messages with high reliability. Specifically, RS codes are constructed by evaluating polynomials of bounded degree at distinct points in a finite field, thereby establishing a direct connection between algebraic structures and coding mechanisms. This algebraic foundation not only facilitates efficient encoding and decoding algorithms but also ensures that RS codes is optimal in terms of their length, dimension, and minimum distance. Due to these mathematical properties, RS codes are employed in applications such as QR codes and DVDs, where robust error correction is essential to maintain data integrity in the presence of noise and other perturbations.

Let $\mathbb{F}_q$ denote a finite field with $q = p^m$ elements, where p is a prime number and m is a positive integer.

Definition 3.1.1 (Reed-Solomon Code)**.** A Reed-Solomon code $\mathrm{RS}(n, k)$ over the field $\mathbb{F}_q$ is a linear code defined by evaluating polynomials of degree less than k at n distinct elements of $\mathbb{F}_q$. Formally, the RS code is given by the codewords

$$\mathrm{RS}(n, k) = \left\{ (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in \mathbb{F}_q[x], \deg(f) < k \right\},$$

where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are distinct elements in $\mathbb{F}_q$.

Proposition 3.1.2. *RS codes have the following properties.*

1. ***Linearity:*** *RS codes are linear since the encoding map is a linear transformation. Specifically, for any two codewords corresponding to polynomials $f(x)$ and $g(x)$, and any scalars $a, b \in \mathbb{F}_q$, the linear combination $af(x) + bg(x)$ maps to the linear combination of the corresponding codewords.*
2. ***Maximum Distance Separable:*** *RS codes achieve the Singleton bound.*

3.1.1 The Singleton Bound and MDS Codes

Theorem 3.1.3 (Singleton Bound)**.** *Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. Then*

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

Proof. Suppose that $d > n - k + 1$. Consider any $n - k + 1$ positions in a codeword. The number of distinct possible patterns in these positions is q^{n-k+1}. However, the total number of codewords is q^k, which exceeds q^{n-k+1} since $k > 0$. By the pigeonhole principle, there exist at least two distinct codewords that agree on these $n-k+1$ positions. This implies that these two codewords differ in at most $n - (n - k + 1) = k - 1$ positions, which contradicts the assumption that the minimum distance is $d > n-k+1$. Therefore, the Singleton bound holds. □

Codes are called *Maximum Distance Separable (MDS) codes*, if they attain the Singleton bound with equality, i.e., $d = n - k + 1$. The following proof demonstrates that RS codes are MDS codes.

Theorem 3.1.4 (RS Codes are MDS)**.** *For a Reed-Solomon code $RS(n, k)$ over $\mathbb{F}_q$, the minimum distance satisfies $d = n - k + 1$.*

Proof. Let $f(x), g(x) \in \mathbb{F}_q[x]$ be two distinct polynomials with $\deg(f) < k$ and $\deg(g) < k$. Define $h(x) = f(x) - g(x)$. Since $f(x) \neq g(x)$, $h(x)$ is a non-zero polynomial with $\deg(h) < k$.

A non-zero polynomial of degree less than k can have at most $k-1$ roots in $\mathbb{F}_q$. Therefore, the equation $h(\alpha_i) = 0$ has at most $k - 1$ solutions among the n distinct evaluation points

$\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Consequently, the number of positions where f and g differ is at least $n - (k - 1) = n - k + 1$. Hence, the minimum distance d satisfies

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

From the Singleton bound, we have

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

Combining these inequalities, it follows that

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

Thus, Reed-Solomon codes achieve the Singleton bound and are therefore MDS codes. □

Recall that the dual code of an $[n, k, d]$ code is an $[n, n - k]$ code, but there is no guarantee on the distance. A remarkable property of MDS codes is that their duals also have good distance. This property is also useful for quantum codes, since dual codes appear in the CSS construction.

Proposition 3.1.5. *The dual of an MDS code is also an MDS code. In particular, the dual of an $[n, k, n - k + 1]$ code is an $[n, n - k, k + 1]$ code.*

3.1.2 Connection Between Reed-Solomon Codes and Algebraic Geometry Codes

(Might modify later)

Reed-Solomon (RS) codes can be viewed as a special case of algebraic geometry (AG) codes, which generalize RS codes by utilizing more complex algebraic curves. While RS codes are constructed using the affine line, in the language of AG codes, we typically consider their compactification, the projective line. This discussion involves certain algebraic geometry terminology, which will be explained in subsequent sections. By presenting this connection upfront, readers may find it clearer during their later reading. The relationship between RS codes and AG codes can be elucidated through several key aspects:

1. **Underlying Algebraic Structures:**
   - **RS Codes:** Constructed using the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$, where the function space is the ring of polynomials $\mathbb{F}_q[x]$.
   - **AG Codes:** Utilize more general algebraic curves (possibly of higher genus) over $\mathbb{F}_q$, where the function space is comprised of rational functions on these curves.
2. **Evaluation Points:**
   - **RS Codes:** Evaluation is performed at n distinct points on the projective line.
   - **AG Codes:** Evaluation is performed at a set of n distinct rational points on a chosen algebraic curve, allowing for greater flexibility and potentially larger code lengths relative to the field size.
3. **Function Spaces and Divisors:**
   - **RS Codes:** The choice of function space is equivalent to selecting a divisor of the form $D = kP$, where P is the point at infinity on the projective line.
   - **AG Codes:** Function spaces are associated with more general divisors on algebraic curves, enabling the construction of codes with parameters that can surpass those achievable by RS codes for certain lengths and field sizes.
4. **Parameters and Performance:**
   - **RS Codes:** As MDS codes, they achieve optimal parameters for their length and dimension, but their length is restricted by the field size ($n \leq q - 1$).
   - **AG Codes:** By leveraging higher genus curves, AG codes can achieve larger lengths and better asymptotic parameters, especially when the field size is fixed and the code length exceeds $q - 1$.
5. **Theoretical Implications:**

- **RS Codes:** Serve as a foundational example demonstrating the power of algebraic methods in coding theory.
- **AG Codes:** Extend the algebraic framework to more sophisticated geometric settings, offering a richer theory and attaining codes with superior properties in certain regimes.

Reed-Solomon codes are essentially AG codes derived from the projective line (a genus zero curve). By extending the geometric framework to include curves of higher genus, AG codes generalize the construction of RS codes, allowing for greater flexibility in code parameters and enabling the attainment of better bounds in scenarios where RS codes are constrained by their inherent limitations. This connection underscores the profound interplay between algebraic geometry and coding theory, paving the way for advanced error-correcting codes with enhanced capabilities.

To better explain algebraic geometry (AG) codes, we first need to introduce some fundamental concepts in algebraic geometry.

3.2 Algebraic curves

Throughout this section, $\mathbb{F}$ denotes an algebraically closed field. For the purposes of this work, $\mathbb{F}$ will often be the algebraic closure of a finite field $\mathbb{F}_q$. The n-dimensional affine space, denoted by $\mathbb{A}^n$, is equipped with coordinates $x_1, x_2, \dots, x_n$. Similarly, the n-dimensional projective space $\mathbb{P}^n$ is described using homogeneous coordinates $x_0, x_1, \dots, x_n$.

We first introduce the case of affine spaces. Compared to affine varieties, projective spaces are more complicated.

An *algebraic set* in $\mathbb{A}^n$ is defined as the set of common zeros of a collection of polynomials forming an ideal $I \subseteq \mathbb{F}[X_1, X_2, \dots, X_n]$:

$$B = V(I) = \{(x_1, x_2, \dots, x_n) \in \mathbb{A}^n \mid F(x_1, x_2, \dots, x_n) = 0 \text{ for every } F \in I\}.$$

We assume that the ideal I is *radical*, which implies that if $f^n \in I$ for some positive integer

n, then f must also belong to I. This ensures that I consists precisely of all polynomials that vanish on the set B, as guaranteed by the Nullstellensatz theorem.

Theorem 3.2.1 (Hilbert's Nullstellensatz)**.** *Let I be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$ over an algebraically closed field $\mathbb{F}$.*

- *If a polynomial $F \in \mathbb{F}[x_1, \ldots, x_n]$ vanishes at all points of the algebraic set $V(I)$, then $F^m \in I$ for some positive integer m.*
- *If the ideal I is radical, meaning that $F^n \in I$ implies $F \in I$, then I consists precisely of all polynomials that vanish on $V(I)$.*

An algebraic set B is called *irreducible* if B cannot be written as the union of two proper algebraic subsets of B. An ideal I is called *prime* if $FG \in I$ implies that $F \in I$ or $G \in I$ for all F, G such that $FG \in I$. The set $V(I)$ is irreducible if and only if I is a prime ideal.

All the curves in affine or projective space discussed in this section are required to be irreducible.

Definition 3.2.2. Consider a prime ideal I in the ring $\mathbb{F}[X_1, X_2, \ldots, X_n]$. The set $\mathcal{X}$ of zeros of I is called an *affine variety.*

Example 3.2.3. In the affine plane $\mathbb{A}^2$, consider the ideal generated by the polynomial $X^2 - Y^2$. The associated algebraic set is the union of two distinct lines, given by the equations $Y = X$ and $Y = -X$. Each of these lines represents an irreducible algebraic set in $\mathbb{A}^2$.

Two polynomials that differ by an element of the ideal I will have identical values at every point in the variety $\mathcal{X}$. This leads us to introduce the following construction.

Definition 3.2.4. The ring $\mathbb{F}[X_1, X_2, \ldots, X_n]/I$ is called the *coordinate ring* $\mathbb{F}[\mathcal{X}]$ of the variety $\mathcal{X}$.

Throughout this section, we adopt the convention of using uppercase letters $X_1, \ldots, X_n$, Y, Z to represent variables. Polynomials will be denoted by F, G, and H, with their cosets modulo the ideal I denoted by lowercase letters f, g, and h.

Since I is an prime ideal, the coordinate ring $\mathbb{F}[\mathcal{X}]$ forms an *integral domain.* In other words, if $fg = 0$, then either $f = 0$ or $g = 0$ for any $f, g \in \mathbb{F}[\mathcal{X}]$. With this understanding, we are now ready to introduce the following definition.

Definition 3.2.5. The *function field* $\mathbb{F}(\mathcal{X})$ of the variety $\mathcal{X}$ is *fraction field* of the coordinate ring $\mathbb{F}[\mathcal{X}]$. Specifically, elements of $\mathbb{F}(\mathcal{X})$ are ratios of polynomials from $\mathbb{F}[\mathcal{X}]$, that is,

$$\mathbb{F}(\mathcal{X}) = \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}[\mathcal{X}],\ g \neq 0 \right\}.$$

Elements of $\mathbb{F}(\mathcal{X})$ are referred to as *rational functions.* The *dimension* of the variety $\mathcal{X}$ is defined as the transcendence degree of $\mathbb{F}(\mathcal{X})$ over the base field $\mathbb{F}$. If the dimension of $\mathcal{X}$ is 1, $\mathcal{X}$ is classified as an *algebraic curve.*

In projective space $\mathbb{P}^n$, the situation becomes slightly more complicated due to the need for homogeneous coordinates. A tuple $(x_0 : x_1 : \ldots : x_n)$ represents a point in $\mathbb{P}^n$. The point $(x_0 : x_1 : \ldots : x_n)$ corresponds to the equivalence class of the line through the origin and the point $(x_0, x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)$.

Two coordinate tuples $(x_0 : x_1 : \ldots : x_n)$ and $(y_0 : y_1 : \ldots : y_n)$ represent the same point in $\mathbb{P}^n$ if and only if there exists a nonzero scalar $\lambda \in \mathbb{F}^*$ such that:

$$(x_0, x_1, \ldots, x_n) = \lambda(y_0, y_1, \ldots, y_n).$$

This equivalence relation identifies all points along the same line, so each point in $\mathbb{P}^n$ corresponds to a unique line through the origin in $\mathbb{A}^{n+1}$.

Geometrically, projective space $\mathbb{P}^n$ can be viewed as the result of identifying antipodal points on S^n. This construction introduces additional points "at infinity" that are not present in affine space $\mathbb{A}^n$. These points at infinity allow us to compactify affine space, meaning that parallel lines in $\mathbb{A}^n$ intersect at a unique point at infinity in $\mathbb{P}^n$.

Because of the form of projective coordinates, it makes sense to consider the zero set in $\mathbb{P}^n$ of homogeneous polynomials. For rational functions to be well-defined, both the numerator and denominator must be homogeneous polynomials of the same degree.

A *projective variety* $\mathcal{X}$ is defined as the zero set of a homogeneous prime ideal I in the polynomial ring $\mathbb{F}[X_0, X_1, \ldots, X_n]$.

We define the subring $\mathcal{R}(\mathcal{X})$ as the set of fractions F/G, where F and G are homogeneous polynomials of the same degree, with $G \notin I$. The maximal ideal $\mathcal{M}(\mathcal{X})$ of $\mathcal{R}(\mathcal{X})$ consists of all F/G with $F \in I$. By definition, the function field $\mathbb{F}(\mathcal{X})$ is the residue field: $\mathbb{F}(\mathcal{X}) = \mathcal{R}(\mathcal{X})/\mathcal{M}(\mathcal{X})$.

Definition 3.2.6. Let $\mathcal{X}$ be an affine or a projective variety, and let P be a point on $\mathcal{X}$. A *rational function* ϕ is said to be *regular* at the point P if there exist two polynomials F and G, both homogeneous of the same degree, such that $G(P) \neq 0$ and ϕ is represented as the coset F/G. In short, P is not a pole of the rational function ϕ. The set of all functions that are regular on every point of an open set U on $\mathcal{X}$ forms a ring, denoted $\mathbb{F}[U]$.

If $\mathcal{X}$ is an affine variety, the coordinate ring $\mathbb{F}[\mathcal{X}]$ coincides with the ring of regular functions on $\mathcal{X}$. Thus, there is no ambiguity in the notation $\mathbb{F}[\mathcal{X}]$. On the other hand, if $\mathcal{X}$ is projective, the only globally regular functions are the constant functions.

Definition 3.2.7. The *local ring* O_P (or $O_P(\mathcal{X})$) at a point P on a variety $\mathcal{X}$ consists of all rational functions that are regular at P.

Readers familiar with commutative algebra may notice that the definition of a local ring here closely resembles its definition in commutative algebra. For an affine variety $\mathcal{X}$, the *local ring* O_P at a point P can be understood as the localization of the ring of regular functions $\mathbb{F}[\mathcal{X}]$. In commutative algebra, the *localization* of a ring R at a prime ideal $\mathfrak{p}$ is defined as:

$$R_{\mathfrak{p}} = \left\{ \frac{f}{g} \mid f, g \in R,\ g \notin \mathfrak{p} \right\}.$$

This construction ensures that all elements of R outside the prime ideal $\mathfrak{p}$ are treated as invertible. Intuitively, localization allows us to focus on the behavior of functions at the point P, ignoring what happens elsewhere.

In the case of an affine variety, the local ring O_P consists of fractions f/g where $f, g \in \mathbb{F}[\mathcal{X}]$ and $g(P) \neq 0$. Here, the prime ideal $\mathfrak{p}$ corresponds to the set of functions in

$\mathbb{F}[\mathcal{X}]$ that vanish at P. Localization captures the idea that, except for the functions that vanish at P, all other functions are considered invertible.

For a *projective variety*, the concept of a local ring is more complicated. Since the only global regular functions on a projective variety are constants, we cannot directly apply the same construction as in the affine case. Instead, we restrict our attention to an affine open subset of the projective variety containing the point P. On this open subset, we perform the same algebraic localization operation as in the affine case. We will not delve into the detailed construction here, but the underlying idea remains similar: we focus only on the behavior of functions near P.

The local ring has a unique maximal ideal, denoted by $\mathcal{M}_P$, consisting of all functions that vanish at P:

$$\mathcal{M}_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}.$$

From now on, to simplify the discussion we will primarily focus on plane curves.

Definition 3.2.8 (Partial Derivative)**.** Let $F = \sum a_{ij}X^iY^j \in \mathbb{F}[X,Y]$. Then the partial derivative of F with respect to X is defined as:

$$F_X = \sum ia_{ij}X^{i-1}Y^j.$$

Similarly, the partial derivative with respect to Y is:

$$F_Y = \sum ja_{ij}X^iY^{j-1}.$$

Definition 3.2.9 (Singular and Nonsingular Points)**.** Consider a curve $\mathcal{X}$ in $\mathbb{A}^2$ defined by the equation $F = 0$. Let P be a point on the curve. If at least one of the partial derivatives F_X or F_Y is nonzero at P, then P is called a *simple* or *nonsingular* point of the curve. A curve is said to be *nonsingular*, *regular*, or *smooth* if all its points are nonsingular.

Let $P = (a,b)$ be a nonsingular point on $\mathcal{X}$. The *tangent line* to $\mathcal{X}$ at P is defined by the equation $d_P F = 0$, where

$$d_P F = F_X(a,b)(X-a) + F_Y(a,b)(Y-b).$$

The definitions for plane curves in projective space are similar. For a plane curve defined by the homogeneous equation $F(X,Y,Z) = 0$, we say that a point P is nonsingular if at least one of the partial derivatives F_X, F_Y, or F_Z is nonzero at P. In such cases, the point P is called a *simple* or *nonsingular* point of the curve.

Let $P = (a : b : c)$ be a nonsingular point of the curve. Then the tangent line at P has the equation

$$F_X(a,b,c)X + F_Y(a,b,c)Y + F_Z(a,b,c)Z = 0.$$

Intuitively, a singular point on a curve is a point where the curve behaves irregularly. Some common types of singularities include:

- **Node**: A point where the curve intersects itself with distinct tangents. This is a type of self-intersection.
- **Cusp**: A point where the curve has a sharp corner and the tangents coincide.
- **Tacnode**: A point where two branches of the curve touch tangentially but do not cross.

These singularities are places where the curve fails to be "smooth," meaning the tangent line is not well-defined in the usual sense.

Example 3.2.10. The Fermat curve $\mathcal{F}_m$ is a projective plane curve with the defining equation

$$X^m + Y^m + Z^m = 0.$$

The partial derivatives of $X^m + Y^m + Z^m$ are mX^{m-1}, mY^{m-1}, and mZ^{m-1}. Thus, considered as a curve over the finite field $\mathbb{F}_q$, it is regular if m is relatively prime to q.

Example 3.2.11. Let $q = r^2$. The Hermitian curve $\mathcal{H}_r$ over $\mathbb{F}_q$ is defined by the affine equation

$$U^{r+1} + V^{r+1} + 1 = 0.$$

The corresponding homogeneous equation is

$$U^{r+1} + V^{r+1} + W^{r+1} = 0.$$

Hence, it has $r + 1$ points at infinity, and it is the Fermat curve $\mathcal{F}_m$ over $\mathbb{F}_q$ with $r = m - 1$. The conjugate of an element $a \in \mathbb{F}_q$ over $\mathbb{F}_r$ is given by $\bar{a} = a^r$. Thus, the equation can also be written as

$$U\bar{U} + V\bar{V} + W\bar{W} = 0.$$

This is analogous to setting a Hermitian form over the complex numbers to zero and interpreting the result geometrically.

We will see in Chapter 4 that for certain constructions of codes on curves, it is convenient to have exactly one point at infinity. We will give a transformation such that the new equation of the Hermitian curve has this property. Choose an element $b \in \mathbb{F}_q$ such that $b^{r+1} = -1$. There are exactly $r + 1$ such elements, since $q = r^2$. Let $P = (1 : b : 0)$. Then P is a point on the Hermitian curve. The tangent line at P has the equation $U + bV = 0$. Multiplying with b gives the equation $V = bU$. Substituting $V = bU$ into the defining equation of the curve yields $W^{r+1} = 0$. Thus, P is the only intersection point of the Hermitian curve and the tangent line at P. New homogeneous coordinates are chosen so that this tangent line becomes the line at infinity. Let $X_1 = W$, $Y_1 = U$, and $Z_1 = bU - V$. Then the curve has the following homogeneous equation:

$$X_1^{r+1} = b^r Y_1^r Z_1 + bY_1 Z_1^r - Z_1^{r+1}$$

in the coordinates X_1, Y_1, Z_1.

Choose an element $a \in \mathbb{F}_q$ such that $a^r + a = -1$. There are r such elements. Let $X = X_1$,

$Y = bY_1 + aZ_1$, and $Z = Z_1$. Then the curve has the following homogeneous equation:

$$X^{r+1} = Y^r Z + Y Z^r$$

with respect to X, Y, Z. Hence, the Hermitian curve has the affine equation:

$$X^{r+1} = Y^r + Y$$

with respect to X and Y. This last equation has $(0 : 1 : 0)$ as the only point at infinity.

3.3 Local Properties of Curves

We want to show that the maximal ideal $\mathcal{M}_P$ of a local ring $\mathcal{O}_P$ is a principal ideal, i.e., it can be generated by a single element. Let $\mathcal{X}$ be a smooth curve in $\mathbb{A}^2$ defined by the equation $F = 0$, and let $P = (a, b)$ be a point on $\mathcal{X}$. The maximal ideal $\mathcal{M}_P$ is generated by $(x - a)$ and $(y - b)$. Now:

$$F_X(P)(x - a) + F_Y(P)(y - b) \neq 0 \mod \mathcal{M}_P^2.$$

Hence, the $\mathbb{F}$-vector space $\mathcal{M}_P/\mathcal{M}_P^2$ has dimension 1, therefore $\mathcal{M}_P$ has a single generator. In commutative algebra, the dimension is called the *Krull dimension.* Let $g \in \mathbb{F}[\mathcal{X}]$ be the coset of a polynomial G. Then g is a generator of $\mathcal{M}_P$ if and only if $d_P G$ is not a constant multiple of $d_P F$, where we define $d_P F = F_X(a, b)(X - a) + F_Y(a, b)(Y - b)$. Similarly, we can prove the above result holds for planar projective curves.

Definition 3.3.1 (Local Parameter)**.** Let t be a generating element of $\mathcal{M}_P$. Then we can write every element $z \in \mathcal{O}_P$ uniquely as $z = ut^m$, where u is a unit and $m \in \mathbb{N}_0$. The function t is called a *local parameter* at P. If $m > 0$, then P is a zero of multiplicity m for z. We write $m = \text{ord}_P(z) = v_P(z)$, and use the convention $v_P(0) = \infty$.

If a local ring is principal, it's called the *discrete valuation ring (DVR)* in commutative algebra. Now we list some properties of the discrete valuation ring:

Theorem 3.3.2 (Discrete Valuation)**.** *The map $v_P : \mathcal{O}_P \longrightarrow \mathbb{N}_0 \cup \{\infty\}$ is a discrete valuation. The map v_P is surjective, and satisfies the following properties for all $f, g \in \mathcal{O}_P$:*

1. *$v_P(f) = \infty$ if and only if $f = 0$.*
2. *$v_P(\lambda f) = v_P(f)$ for all nonzero $\lambda \in \mathbb{F}$.*
3. *$v_P(f + g) \geq \min\{v_P(f), v_P(g)\}$ with equality if $v_P(f) \neq v_P(g)$.*
4. *$v_P(fg) = v_P(f) + v_P(g)$.*

Here, $\infty > n$ for all $n \in \mathbb{N}_0$.

We extend the valuation v_P to $\mathbb{F}(\mathcal{X})$ by defining $v_P(f/g) = v_P(f) - v_P(g)$. If $v_P(z) = -m < 0$, then we say that z has a pole of order m at P. If z is an element of $\mathbb{F}(\mathcal{X})$ with $v_P(z) = m$, then we can write $z = at^m + z'$, where $a \in \mathbb{F}, a \neq 0$, and $v_P(z') > m$. In this way, we can express z as a Laurent series:

$$z = \sum_{i \geq n} a_i t^i,$$

where $a_i \in \mathbb{F}$ for all i and $a_n \neq 0$.

Later we will discuss divisors and differential forms, where the concepts introduced here will appear and be utilized multiple times.

3.3.1 Bézout's Theorem

Before diving into divisors and differential forms, we follow the usual textbook structure by first introducing intersection multiplicity and Bézout's theorem. In the study of algebraic curves, concepts such as discrete valuation rings (DVRs) and divisors are foundational. The notion of intersection multiplicity and Bézout's theorem, which we will now introduce, serve as key applications of DVRs. Bézout's theorem, in particular, provides a global perspective on the intersection of curves, complementing the local analysis afforded by DVRs.

These results are closely tied to the study of rational functions on curves. Specifically, the divisor of a rational function, known as a principal divisor, plays a central role in divisor theory. While the formal definition and properties of principal divisors will be introduced in the fourth subsection, we note here that Bézout's theorem and the notion of intersection multiplicity provide the tools needed to analyze the zeros and poles of rational functions, forming the basis for the degree calculation of principal divisors.

A polynomial of degree m in one variable, with coefficients in a field, has at most m zeros. If the field is algebraically closed and if the zeros are counted with multiplicities, then the number of zeros is exactly m. We shall now state a theorem, known as *Bézout's theorem*, which generalizes this fact to polynomials in several variables. The theorem holds in projective spaces.

The *degree* of a projective curve is the maximal number of points in the intersection with a hyperplane not containing the curve. Thus, the degree of a projective plane curve is equal to the degree of the defining equation.

We only consider the intersection of an irreducible nonsingular projective curve $\mathcal{X}$ of degree l and a hypersurface $\mathcal{Y}$ defined by the equation $G = 0$ of degree m. We assume that $\mathcal{X}$ is not contained in $\mathcal{Y}$.

Definition 3.3.3. For an projective curve $\mathcal{X}$, let P be a point of $\mathcal{X}$. $\mathcal{Y}$ is a hypersurface defined by homogeneous polynomial H with degree m and $H(P) \neq 0$. Let h be the class of H modulo the ideal defining $\mathcal{X}$. Then the *intersection multiplicity* $I(P; \mathcal{X}, \mathcal{Y})$ of $\mathcal{X}$ and $\mathcal{Y}$ in P is defined by $v_P(g/h^m)$.

This definition does not depend on the choice of H, since h/h' is a unit in $\mathcal{O}_P$ for any other choice of a linear form H' that is nonzero in P.

Theorem 3.3.4 (Bézout's Theorem)**.** *Let $\mathcal{X}$ be an irreducible nonsingular projective curve of degree l and $\mathcal{Y}$ a hypersurface of degree m in $\mathbb{P}^n$ such that $\mathcal{X}$ is not contained in $\mathcal{Y}$. Then they intersect in exactly lm points (if counted with multiplicity).*

We do not prove this theorem. If $\mathbb{F}$ is not algebraically closed or the curves are affine, then the curves intersect in at most lm points.

We mention a consequence of this theorem.

Corollary 3.3.5. Two projective plane curves of positive degree have a point in common.

3.4 Divisors on Algebraic Curves

In this section, we discuss divisors on an irreducible smooth projective curve $\mathcal{X}$ over an algebraically closed field $\mathbb{F}$. Divisors are a fundamental concept in algebraic geometry since they encode important information about the zeros and poles of rational functions.

Definition 3.4.1. A *divisor* D on $\mathcal{X}$ is a formal sum

$$D = \sum_{P \in \mathcal{X}} n_P P,$$

where $n_P \in \mathbb{Z}$, and $n_P = 0$ for all but finitely many points P. The *support* of a divisor is the set of points where $n_P \neq 0$. A divisor D is called *effective* if all $n_P \geq 0$ (denoted by $D \geq 0$). The *degree* of a divisor is defined as:

$$\deg(D) = \sum n_P.$$

Definition 3.4.2. Let $\mathcal{X}$ and $\mathcal{Y}$ be two projective plane curves, defined by equations $F = 0$ and $G = 0$. The *intersection divisor* $\mathcal{X} \cdot \mathcal{Y}$ is defined by:

$$\mathcal{X} \cdot \mathcal{Y} = \sum I(P; \mathcal{X}, \mathcal{Y}) P,$$

where $I(P; \mathcal{X}, \mathcal{Y})$ is the intersection multiplicity at the point P.

Bézout's theorem guarantees that $\mathcal{X} \cdot \mathcal{Y}$ is indeed a divisor and that the degree of $\mathcal{X} \cdot \mathcal{Y}$ is lm, where l and m are the degrees of $\mathcal{X}$ and $\mathcal{Y}$, respectively. Let $v_P = \text{ord}_P$ be the discrete valuation defined for functions on $\mathcal{X}$.

Definition 3.4.3. If f is a nonzero rational function on $\mathcal{X}$, the divisor of f is defined by:

$$(f) = \sum_{P \in \mathcal{X}} v_P(f) P.$$

In essence, the divisor of a rational function records the zeros and poles of f, along with their respective multiplicities or orders.

Theorem 3.4.4. *The degree of a divisor of a rational function is always zero.*

Proof. Let $\mathcal{X}$ be a projective curve of degree l. Let f be a rational function on the curve $\mathcal{X}$. Then f is represented by a quotient A/B of two homogeneous polynomials of the same degree, say m. Let $\mathcal{Y}$ and $\mathcal{Z}$ be the hypersurfaces defined by the equations $A = 0$ and $B = 0$, respectively. Then

$$v_P(f) = I(P; \mathcal{X}, \mathcal{Y}) - I(P; \mathcal{X}, \mathcal{Z}),$$

since $f = a/b = (a/h^m)(b/h^m)^{-1}$, where H is a homogeneous linear form representing h such that $H(P) \neq 0$. Hence

$$(f) = \mathcal{X} \cdot \mathcal{Y} - \mathcal{X} \cdot \mathcal{Z}.$$

So (f) is indeed a divisor and its degree is zero, since it is the difference of two intersection divisors of the same degree lm. □

Definition 3.4.5. The divisor of a rational function is referred to as a *principal divisor*. Two divisors D and D' are said to be *linearly equivalent* if and only if $D - D'$ is a principal divisor. We denote linear equivalence relation as $D \equiv D'$.

This defines an equivalence relation on the set of divisors.

Definition 3.4.6. Let D be a divisor on a curve $\mathcal{X}$. We define the vector space $\mathcal{L}(D)$ over $\mathbb{F}$ as:

$$\mathcal{L}(D) = \{f \in \mathbb{F}(\mathcal{X})^* \mid (f) + D \geq 0\} \cup \{0\}.$$

The dimension of $\mathcal{L}(D)$ over $\mathbb{F}$ is denoted by $l(D)$.

If $D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$, where $n_i, m_j > 0$, then the space $\mathcal{L}(D)$ consists of the zero function and those functions in the function field with zeros of multiplicity at least

m_j at the points Q_j (for $1 \le j \le s$), and no poles except possibly at the points P_i, where the order of poles is at most n_i (for $1 \le i \le r$).

Note that if $D \equiv D'$ and g is a rational function such that $(g) = D - D'$, then the map $f \mapsto fg$ defines an isomorphism between $\mathcal{L}(D)$ and $\mathcal{L}(D')$. That is why we view two divisors are equivalent if they differ only by a principal divisor. The vector space $\mathcal{L}(D)$ has finite dimension. And we have a bound for the dimension according to the following theorem.

Theorem 3.4.7.

(i) $l(D) = 0$ *if* $\deg(D) < 0$,

(ii) $l(D) \le 1 + \deg(D)$.

3.5 Differential Forms on Curves

Let $\mathcal{X}$ be an irreducible smooth curve with function field $\mathbb{F}(\mathcal{X})$. Readers familiar with the basic concepts of differential manifolds may draw parallels between the definitions and theorems presented in this section.

Definition 3.5.1. Let $\mathcal{V}$ be a vector space over $\mathbb{F}(\mathcal{X})$. An $\mathbb{F}(\mathcal{X})$-linear map $D : \mathbb{F}(\mathcal{X}) \to \mathcal{V}$ is called a *derivation* if D satisfies the product rule:

$$D(fg) = fD(g) + gD(f),$$

where $f, g \in \mathbb{F}(\mathcal{X})$.

Example 3.5.2. Let $\mathcal{X}$ be the projective line with function field $\mathbb{F}(\mathcal{X})$. For a polynomial $F = \sum a_i X^i \in \mathbb{F}[X]$, we define

$$D(F) = \sum i a_i X^{i-1}.$$

This definition extends to rational functions, so for $\frac{F}{G} \in \mathbb{F}(\mathcal{X})$, the derivation is given by:

$$D\left(\frac{F}{G}\right) = \frac{GD(F) - FD(G)}{G^2}.$$

Thus, $D : \mathbb{F}(\mathcal{X}) \rightarrow \mathbb{F}(\mathcal{X})$ is a derivation.

Definition 3.5.3. The set of all derivations $D : \mathbb{F}(\mathcal{X}) \rightarrow \mathcal{V}$ is denoted by $\mathrm{Der}(\mathcal{X}, \mathcal{V})$. If $\mathcal{V} = \mathbb{F}(\mathcal{X})$, we denote $\mathrm{Der}(\mathcal{X}, \mathcal{V})$ simply as $\mathrm{Der}(\mathcal{X})$.

Given two derivations $D_1, D_2 \in \mathrm{Der}(\mathcal{X}, \mathcal{V})$, their sum is defined by:

$$(D_1 + D_2)(f) = D_1(f) + D_2(f).$$

Similarly, for a function $f \in \mathbb{F}(\mathcal{X})$, the product of f with a derivation D is given by:

$$(fD)(g) = fD(g),$$

for all $g \in \mathbb{F}(\mathcal{X})$. Thus, $\mathrm{Der}(\mathcal{X}, \mathcal{V})$ becomes a vector space over $\mathbb{F}(\mathcal{X})$.

Theorem 3.5.4. *Let t be a local parameter at a point P. Then there exists a unique derivation $D_t : \mathbb{F}(\mathcal{X}) \rightarrow \mathbb{F}(\mathcal{X})$ such that $D_t(t) = 1$. Moreover,* $\mathrm{Der}(\mathcal{X})$ *is a one-dimensional vector space over* $\mathbb{F}(\mathcal{X})$*, with D_t as a basis element for every local parameter t.*

It follows from Theorem 3.5.4 that the tangent space of the algebraic curve $\mathcal{X}$ at each local point P is one-dimensional, which aligns with our previous discussion that the maximal ideal $\mathcal{M}_P$ of the local ring $\mathcal{O}_P$ of an algebraic curve is generated by a single element.

Definition 3.5.5. A *rational differential form* or simply a *differential* on $\mathcal{X}$ is an $\mathbb{F}(\mathcal{X})$-linear map from $\mathrm{Der}(\mathcal{X})$ to $\mathbb{F}(\mathcal{X})$. The set of all such rational differential forms on $\mathcal{X}$ is denoted by $\Omega(\mathcal{X})$.

Again, $\Omega(\mathcal{X})$ becomes a vector space over $\mathbb{F}(\mathcal{X})$ in the natural way. Consider the map

$$d : \mathbb{F}(\mathcal{X}) \longrightarrow \Omega(\mathcal{X}),$$

where for $f \in \mathbb{F}(\mathcal{X})$, the differential $df : \mathrm{Der}(\mathcal{X}) \longrightarrow \mathbb{F}(\mathcal{X})$ is defined by

$$df(D) = D(f) \quad \text{for all } D \in \mathrm{Der}(\mathcal{X}).$$

Thus, d acts as a derivation.

Theorem 3.5.6. *The space $\Omega(\mathcal{X})$ has dimension 1 over $\mathbb{F}(\mathcal{X})$, and dt serves as a basis for each point P with a local parameter t.*

Theorem 3.5.6 implies that the cotangent space at each point P on the algebraic curve $\mathcal{X}$ is one-dimensional.

For every point P and local parameter t_P, a differential ω can be uniquely expressed as $\omega = f_P\, dt_P$, where f_P is a rational function. We want to determine whether ω has a pole or a zero at P and the corresponding order.

Definition 3.5.7. Let ω be a differential on $\mathcal{X}$. The *order* or *valuation* of ω at P is defined by:

$$\mathrm{ord}_P(\omega) = v_P(\omega) = v_P(f_P).$$

A differential form ω is called *regular* if ω has no poles. The set of all regular differentials on $\mathcal{X}$ forms an $\mathbb{F}[\mathcal{X}]$-module, denoted $\Omega[\mathcal{X}]$.

If $\mathcal{X}$ is an affine plane curve defined by the equation $F = 0$ with $F \in \mathbb{F}[X, Y]$, then $\Omega[\mathcal{X}]$ is generated by dx and dy as an $\mathbb{F}[\mathcal{X}]$-module, subject to the relation:

$$f_x\, dx + f_y\, dy = 0.$$

The divisor of a differential is defined in the same way as for functions.

Definition 3.5.8. The divisor (ω) of a differential ω is defined by:

$$(\omega) = \sum_{P \in \mathcal{X}} v_P(\omega) P,$$

where only finitely many of the coefficients $v_P(\omega)$ are nonzero.

Let ω be a differential and $W = (\omega)$ its associated divisor. This divisor W is called a *canonical divisor.* If ω' is another nonzero differential, then $\omega' = f\omega$ for some rational function f. In this case, $(\omega') = W' \equiv W$, thus the canonical divisors form one equivalence class, denoted again by W.

We can also consider the space $\mathcal{L}(W)$, where rational functions map onto an isomorphic space of differentials via $f \mapsto f\omega$. By the definition of $\mathcal{L}(W)$, the image of f under this mapping is a regular differential, implying that $\mathcal{L}(W)$ is isomorphic to $\Omega[\mathcal{X}]$.

Definition 3.5.9. Let $\mathcal{X}$ be a smooth projective curve over $\mathbb{F}$. The *genus* g of $\mathcal{X}$ is defined by:

$$g = l(W),$$

where W is a canonical divisor on $\mathcal{X}$.

The genus of a curve plays a significant role in AG codes. Determining the genus of an algebraic curve involves more advanced theory, and here we present a powerful theorem.

Theorem 3.5.10 (Plücker Formula). *If $\mathcal{X}$ is a nonsingular projective curve of degree m in $\mathbb{P}^2$, then the genus g is given by:*

$$g = \frac{1}{2}(m-1)(m-2).$$

Example 3.5.11. By Theorem 3.5.10 the genus of both a line and a nonsingular conic are zero. In fact, any curve with genus zero is isomorphic to the projective line.

For the construction of codes over algebraic curves that generalize Goppa codes (codes defined by differential form), the concept of the residue of a differential at a point P is essential. This concept aligns with our treatment of the local behavior of a differential ω.

Definition 3.5.12. Let P be a point on $\mathcal{X}$, and let t be a local parameter at P. Suppose the differential ω is expressed as $\omega = f\,dt$, where f can be written as a Laurent series:

$$f = \sum_i a_i t^i.$$

The *residue* of ω at the point P is defined by:

$$\mathrm{Res}_P(\omega) = a_{-1}.$$

This definition is independent of the choice of the local parameter t.

One of the fundamental results in the theory of algebraic curves is the *residue theorem*, which we state without proof. Readers can refer to [12, Corollary 4.3.3]

Theorem 3.5.13 (Residue Theorem)**.** *If ω is a differential on a smooth projective curve $\mathcal{X}$, then:*

$$\sum_{P \in \mathcal{X}} \mathrm{Res}_P(\omega) = 0.$$

3.6 The Riemann-Roch Theorem

After the long preparation, we have finally arrived at the *Riemann-Roch theorem.* The theorem is not only a central result in algebraic geometry with numerous applications in other areas but also serves as a key tool for new developments in coding theory.

Theorem 3.6.1 (Riemann-Roch)**.** *Let D be a divisor on a smooth projective curve of genus g. Then, for any canonical divisor W, the following relation holds:*

$$l(D) - l(W - D) = \deg(D) - g + 1.$$

We omit the proof here. However, the theorem plays a crucial role in determining the degree of canonical divisors and offers deep insights into the structure of algebraic curves.

Corollary 3.6.2. For a canonical divisor W, the degree is given by:

$$\deg(W) = 2g - 2.$$

Proof. Everywhere regular functions on a projective curve are constant, that is to say,

$\mathcal{L}(0) = \mathbb{F}$, so $l(0) = 1$. Substituting $D = W$ in Theorem 3.6.1, the result follows from the definition of the genus. □

At first glance, Theorem 3.6.1 may not seem very useful. However, Corollary 3.6.2 gives us a way to apply it effectively.

Corollary 3.6.3. Let D be a divisor on a smooth projective curve of genus g, and let $\deg(D) > 2g - 2$. Then:

$$l(D) = \deg(D) - g + 1.$$

Proof. By Corollary 3.6.2, $\deg(W - D) < 0$, so by Theorem 3.4.7, $l(W - D) = 0$. □

In Riemann-Roch Theorem, the term $l(W - D)$ can be interpreted in the context of differentials. We introduce a generalization of $\mathcal{L}(D)$ to incorporate differentials.

Definition 3.6.4. Let D be a divisor on a curve $\mathcal{X}$. We define the space:

$$\Omega(D) = \{\omega \in \Omega(\mathcal{X}) \mid (\omega) - D \geq 0\},$$

and denote the dimension of $\Omega(D)$ over $\mathbb{F}$ by $\delta(D)$. This dimension is referred to as the *index of speciality* of the divisor D.

The connection between these differentials and functions is captured by the following theorem.

Theorem 3.6.5.

$$\delta(D) = l(W - D).$$

Proof. Let $W = (\omega)$ be a canonical divisor. We define a linear map

$$\phi : \mathcal{L}(W - D) \to \Omega(D), \quad \phi(f) = f\omega.$$

This map is clearly an isomorphism, establishing the equivalence between the two spaces. □

Finally, we introduce another significant concept in the context of AG codes: the *Weierstrass gap*. In the context of algebraic geometry codes, the concept of *Weierstrass gap* is a crucial tool that aids in selecting appropriate divisors and constructing generating functions effectively. I will introduces the definition and basic properties of Weierstrass gaps and non-gap numbers, along with their significance in code construction and analysis. For example, the gap appear on the parameters of Hermitian codes in Chapter4.

Let $\mathcal{X}$ be a smooth projective algebraic curve of genus g, and let P be a point on $\mathcal{X}$. For each positive integer m, consider the dimension $l(mP)$, which represents the space of rational functions on $\mathcal{X}$ with poles of order at most m at P. A positive integer m is called a *gap* of P if:

$$l(mP) = l((m-1)P),$$

indicating that no new rational function exists with a pole of order m at P beyond those that already have poles of order $m - 1$. Conversely, m is a *non-gap* if:

$$l(mP) > l((m-1)P),$$

which means there exists a rational function f such that $\mathrm{ord}_P(f) = -m$ and f has no other poles elsewhere on $\mathcal{X}$. Intuitively, gap numbers indicate impossible pole orders at P, while non-gap numbers correspond to realizable pole orders.

For a curve of genus g, the set of gap numbers at any point P always has exactly g elements. This result can be shown by Corrolary 3.6.3 and the following inequality:

$$1 = l(0) \leq l(P) \leq \cdots \leq l((2g-1)P) = g.$$

This property ensures that the complement of the gap set, i.e., the non-gap set, forms a semigroup under addition, as the sum of two non-gap numbers is also a non-gap number. The closeness under addition is followed by the multiplication of functions. The smallest non-gap number is always 0, corresponding to the constant function. The semigroup is called the *Weierstrass semigroup*.

Weierstrass gaps play a fundamental role in constructing divisors and generating functions for algebraic geometry codes. By identifying the gap set, we can ensure that divisors G avoid impossible pole orders, allowing the function space $L(G)$ to be effectively utilized. Furthermore, non-gap numbers guide the construction of generating functions, ensuring their existence and linear independence. While the theoretical importance of Weierstrass gaps is significant, this paper does not delve into their detailed application. Readers interested in exploring this topic further are encouraged to consult [12].

3.7 Codes from Algebraic Curves

We now turn our attention to the application of algebraic curves in coding theory. In this context, the alphabet for our codes is $\mathbb{F}_q$, with $\mathbb{F}$ representing the algebraic closure of $\mathbb{F}_q$. The theorems and results established in the previous sections will now be utilized, with some necessary adjustments. For instance, when working with functions from the coordinate ring, we restrict ourselves to those functions whose coefficients lie in $\mathbb{F}_q$.

Consider an affine curve $\mathcal{X}$ over $\mathbb{F}_q$, defined by a prime ideal I in the polynomial ring $\mathbb{F}_q[X_1, \ldots, X_n]$. The coordinate ring of $\mathcal{X}$, denoted by $\mathbb{F}_q[\mathcal{X}]$, is defined as the quotient $\mathbb{F}_q[X_1, \ldots, X_n]/I$. Furthermore, the function field of the curve, written as $\mathbb{F}_q(\mathcal{X})$, is the quotient field of the coordinate ring $\mathbb{F}_q[\mathcal{X}]$.

It is always assumed that the curve is *absolutely irreducible*, meaning that the defining ideal is also prime in $\mathbb{F}[X_1, \ldots, X_n]$. Similar modifications apply to projective curves. Notice that if $F(x_1, \ldots, x_n)^q = F(x_1^q, \ldots, x_n^q)$ for all $F \in \mathbb{F}_q[X_1, \ldots, X_n]$, then any zero $(x_1, \ldots, x_n)$ of F will also be a zero of the polynomial evaluated at its Frobenius image $(x_1^q, \ldots, x_n^q)$. Let $\mathrm{Fr} : \mathbb{F} \longrightarrow \mathbb{F}$ denote the Frobenius automorphism defined by $\mathrm{Fr}(x) = x^q$. This map naturally extends to coordinatewise operations in both affine and projective space.

If the curve $\mathcal{X}$ is defined over $\mathbb{F}_q$ and P is a point on $\mathcal{X}$, then $\mathrm{Fr}(P)$ is also a point of $\mathcal{X}$. A divisor D on $\mathcal{X}$ is called *rational* if the coefficients of both P and $\mathrm{Fr}(P)$ in D are the same for every point P on $\mathcal{X}$, i.e., the divisor is fixed under the action of the Galois group. The space $\mathcal{L}(D)$ will be considered only for rational divisors, as previously defined, but with the additional restriction that rational functions have coefficients in $\mathbb{F}_q(\mathcal{X})$. Under these adjustments, the previous theorems, including the Riemann-Roch theorem, remain valid over $\mathbb{F}_q$.

Let $\mathcal{X}$ be an absolutely irreducible, nonsingular projective curve defined over $\mathbb{F}_q$. We will now define two types of algebraic geometry codes derived from $\mathcal{X}$. The first type generalizes Reed-Solomon codes, while the second type generalizes Goppa codes.

Consider a set of rational points $P_1, P_2, \ldots, P_n$ on $\mathcal{X}$, and let D denote their formal sum:

$$D = P_1 + P_2 + \cdots + P_n.$$

Additionally, let G be another divisor whose support is disjoint from D. While it is not always necessary to impose restrictions on G, for the purposes of our construction, we assume:

$$2g - 2 < \deg(G) < n.$$

Definition 3.7.1. The *linear code* $C(D,G)$ of length n over $\mathbb{F}_q$ is the image of the linear map:

$$\begin{aligned} \alpha : \quad & L(G) \longrightarrow \mathbb{F}_q^n, \\ & f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)). \end{aligned}$$

Codes of this kind are called *geometric Reed-Solomon codes.*

Theorem 3.7.2. *The code $C(D,G)$ has dimension $k = \deg(G) - g + 1$, and the minimum distance d of $C(D,G)$ satisfies:*

$$d \geq n - \deg(G).$$

Proof. (i) If f belongs to the kernel of α, then $f \in \mathcal{L}(G-D)$. By Theorem 3.4.7(i), this implies $f = 0$. The result follows from the assumption $2g - 2 < \deg(G) < n$ and Corollary 3.6.3.

(ii) If $\alpha(f)$ has weight d, there are exactly $n - d$ points, say $P_{i_1}, P_{i_2}, \ldots, P_{i_{n-d}}$, where $f(P_{i_j}) = 0$. Therefore, $f \in \mathcal{L}(G - E)$ and $l(G - D) > 0$, where $E = P_{i_1} + \cdots + P_{i_{n-d}}$. Hence, $\deg(G - E) = \deg(G) - (n - d) \geq 0$ by Theorem 3.4.7. Thus, $d \geq n - \deg(G)$. □

We now introduce the second class of algebraic geometry codes, known as *geometric Goppa codes.*

Definition 3.7.3. The linear code $C^*(D, G)$ of length n over $\mathbb{F}_q$ is defined as the image of the linear map:

$$\begin{aligned} \alpha^* : \quad & \Omega(G - D) \longrightarrow \mathbb{F}_q^n, \\ & \qquad\qquad \eta \longmapsto (\mathrm{Res}_{P_1}(\eta), \mathrm{Res}_{P_2}(\eta), \ldots, \mathrm{Res}_{P_n}(\eta)). \end{aligned}$$

where $\mathrm{Res}_{P_i}(\eta)$ denotes the residue of the differential η at the point P_i on the curve.

The parameters of these codes are determined by the following theorem.

Theorem 3.7.4. *The code $C^*(D, G)$ has dimension*

$$k^* = n - \deg(G) + g - 1$$

and minimum distance

$$d^* \geq \deg(G) - 2g + 2.$$

Proof. These results follow directly from the Riemann-Roch theorem. According to $l(W - G) = \delta(G)$ and the degree of a canonical divisor is $2g - 2$, we just need to substitute those parameters in the Riemann-Roch theorem. □

Theorem 3.7.5. *The codes $C(D, G)$ and $C^*(D, G)$ are dual codes.*

Proof. From Theorem 3.7.2 and Theorem 3.7.4, we know that $k + k^* = n$. To prove the duality, it suffices to show that the inner product of a word from each code is zero.

Let $f \in \mathcal{L}(G)$ and $\eta \in \Omega(G - D)$. By definition, the differential $f\eta$ has no poles except possibly simple poles at the points $P_1, P_2, \ldots, P_n$. The residue of $f\eta$ at a point P_i is given by $f(P_i)\,\mathrm{Res}_{P_i}(\eta)$.

By Theorem 3.5.13, the sum of the residues over all poles is zero:

$$\sum_{i=1}^{n} f(P_i)\,\mathrm{Res}_{P_i}(\eta) = 0.$$

Thus, we have:

$$0 = \langle \alpha(f), \alpha^*(\eta) \rangle ,$$

which completes the proof. □

The use of polynomials instead of differentials does not result in any loss of generality, as stated in the following theorem. In fact, polynomials and differantials can be converted into each other.

Theorem 3.7.6. *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$. Let $P_1, \ldots, P_n$ be n rational points on $\mathcal{X}$, and define the divisor $D = P_1 + \cdots + P_n$. Then there exists a differential form ω with simple poles at the points P_i such that $\mathrm{Res}_{P_i}(\omega) = 1$ for all i. Furthermore:*

$$C^*(D, G) = C(D, W + D - G)$$

for all divisors G with support disjoint from that of D, where W is the divisor of ω.

Nevertheless, having both types of codes can be advantageous when dealing with decoding methods, since these methods often involve parity checks, requiring a generator matrix for the dual code.

We will provide several examples of algebraic geometry codes later. It becomes evident that we can find codes with desirable properties. For example, from Theorem 3.7.2, we observe that codes over a curve of genus 0 (i.e., projective lines) are MDS codes. Generally, if g is small, the codes approach the Singleton bound.

Chapter 4

Quantum Codes Constructed from Algebraic Geometry

4.1 Toolkits for Quantum Codes Construction

Usually, quantum algebraic geometry codes are obtained by CSS construction. However, unlike the chain complex structure we discussed earlier in the context of CSS codes, the approach for constructing quantum codes from Algebraic Geometry (AG) codes typically involves selecting a self-orthogonal AG code, i.e., one that satisfies $C^{\perp} \subseteq C$. The relationship also meets the CSS's requirement. We then choose both H_X and H_Z to be the parity-check matrix H of C:

$$\begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}.$$

This naturally satisfies the requirement for the corresponding stabilizer group to be abelian.

To provide clarity for the reader in the following sections, we present several theorems here in advance, which outline some methods for constructing quantum codes from classical codes.

Theorem 4.1.1 (q-ary CSS construction [13]). *Suppose that C_1 and C_2 are linear codes over $\mathbb{F}_q$ of length n and dimensions k_1 and k_2 respectively with $C_1 \subseteq C_2$. Then there exists a*

$$\left[n, k_2 - k_1, \min\{d(C_2 \setminus C_1), d(C_1^{\perp} \setminus C_2)\}\right]_q$$

code.

Next, we see how another inner product on $\mathbb{F}_{q^2}^n$ may be utilized to construct quantum codes over $\mathbb{F}_q$. We define that the Hermitian inner product on $\mathbb{F}_{q^2}^n$ is given by

$$u *_h v := \sum_{i=1}^{n} u_i v_i^q.$$

And we have the symplectic inner product *. Given $(a|b), (a'|b') \in \mathbb{F}_q^{2n}$, set

$$(a|b) * (a'|b') = \mathrm{Tr}(a \cdot b' - a' \cdot b)$$

where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace map.

In [13, Theorem 4], it is shown that a code that is self-orthogonal with respect to the Hermitian inner product $*_h$ is also self-orthogonal with respect to $*$. This idea can be used to construct q-ary quantum codes.

Theorem 4.1.2 (Hermitian construction [13]). *Suppose that D is a $[n, k, d]_{q^2}$ code which is self-orthogonal with respect to the Hermitian inner product. Let $D^{\perp h}$ denote the Hermitian dual of D. Then there exists a*

$$\left[n, n-2k, \min\{\mathrm{wt}(D^{\perp h} \setminus D)\}\right]_q$$

code.

An $[n, k, d]_q$ code is pure if its dual contains no nonzero vectors of weight less than d. For example, a self-dual code is pure. Suppose a quantum code Q is constructed from a classical code C in the CSS construction (taking $C_1 = C_2 = C$ in Corollary 1.1). Then Q is pure if and only if C is pure.

Besides the above construction method, sometimes we need to construct quantum codes over $\mathbb{F}_p$ from classical codes over $\mathbb{F}_q$, where $q = p^m$. On the one hand, quantum codes over $\mathbb{F}_p$ are easier to construct in practice, as we can use p-level systems as qudits, while implementing systems with excessively high levels poses practical difficulties. On the other hand, there are theoretical reasons as well. For certain types of codes, such as Reed-Solomon codes, over a fixed finite field $\mathbb{F}_q$, there is often only one code with sufficiently good properties. However, we hope to find a method to construct a family of quantum codes. This method involves expanding codes over $\mathbb{F}_q$ into codes over $\mathbb{F}_p$ element-wise. In this way, for $q = p^m$, we can obtain a family of quantum codes by simply choosing different values of m.

Regarding this element-wise expansion, we need to establish a theoretical framework to show that certain original properties of the codes (e.g., orthogonality) can still be preserved after expansion. This enables us to more conveniently construct codes over $\mathbb{F}_p$ from codes over $\mathbb{F}_q$.

The *trace*, $\mathrm{tr} : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p$, is a linear mapping from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$:

$$\mathrm{tr}(\alpha) = \alpha^{p^0} + \alpha^{p^1} + \cdots + \alpha^{p^{k-1}}.$$

The elements, $\alpha_1, \alpha_2, \ldots, \alpha_k$, form a basis of $\mathbb{F}_{p^k}$, over $\mathbb{F}_p$), if and only if

$$\det\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \alpha_1^p & \alpha_2^p & \cdots & \alpha_k^p \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{p^{k-1}} & \alpha_2^{p^{k-1}} & \cdots & \alpha_k^{p^{k-1}} \end{pmatrix} \neq 0.$$

The set, $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, is a *trace orthogonal basis* if

$$\mathrm{tr}(\alpha_i \alpha_j) = 0, \quad 1 \leq i, j \leq k, \quad i \neq j.$$

If, in addition, $\mathrm{tr}(\alpha_i^2) = 1$, then $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ is a *self-dual basis.*

The finite field $\mathbb{F}_{p^k}$ is a k-dimensional vector space over $\mathbb{F}_p$; once we choose a basis, $\mathcal{B}$, there is a homomorphism, $\mathcal{B} : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p^k$:

$$v \mapsto \mathcal{B}(v), \quad \forall v \in \mathbb{F}_{p^k}.$$

This homomorphism allows us to express any vector, $v \in \mathbb{F}_{p^k}$, as a linear combination of basis $\mathcal{B}$. Any linear transformation, $A \in GL(n, \mathbb{F}_{p^k})$, described by the $n \times n$ matrix, $A = [a_{ij}], 1 \leq i, j \leq n$, can be expressed by substituting a_{ij} with $\mathcal{B}(a_{ij})$. The relationship is easy to understand via the following commutative diagram:

$$\begin{tikzcd}
(\mathbb{F}_q)^n \arrow[r, "A"] \arrow[d, "\mathcal{B}"'] & \mathbb{F}_q)^n \arrow[d, "\mathcal{B}"] \\
(\mathbb{F}_p)^{kn} \arrow[r, "\mathcal{B}(A)"] & (\mathbb{F}_p)^{kn}.
\end{tikzcd}$$

Let $\mathcal{B}^\perp = (b'_1, b'_2, \ldots, b'_k)$ be the dual of the basis $\mathcal{B} = (b_1, b_2, \ldots, b_k)$, i.e.

$$\mathrm{tr}(b_i b'_j) = \delta_{ij}, \quad 1 \leq i, j \leq k.$$

Proposition 4.1.3. *Let $C^\perp$ be the dual of the $[N, K]$ linear code, C, over the finite field, $\mathbb{F}_{p^k}$. Let $\mathcal{B}(C)$ be the p-expansion of the code, C, with respect to basis, $\mathcal{B}$, and let $\mathcal{B}^\perp(C^\perp)$ be the p-expansion of the dual of C, with respect to the dual basis, $\mathcal{B}^\perp$; then*

$$\mathcal{B}^\perp(C^\perp) = [\mathcal{B}(C)]^\perp.$$

Proof. The proof can be found in [14]. □

This proposition allows us to conclude that the following diagram is commutative:

$$\begin{tikzcd}
C \arrow[r] \arrow[d, "\text{basis } \mathcal{B}"'] & C^\perp \arrow[d, "\text{dual basis } \mathcal{B}^\perp"] \\
\mathcal{B}(C) \arrow[r] & \mathcal{B}^\perp(C^\perp) = \mathcal{B}(C)^\perp.
\end{tikzcd}$$

4.2 Quantum Codes from One-point AG Codes

For codes $C_\mathcal{L}(D, G)$ and $C_\Omega(D, G)$, these codes are sometimes called m-point codes if the divisor G has m distinct $\mathbb{F}_q$-rational points in its support. Typically, an m-point code is constructed by taking the divisor D to be the sum of all $\mathbb{F}_q$-rational points not in the support of G, and we will keep this convention. We will use the term multipoint code to mean an m-point code with $m \geq 2$.

4.2.1 Quantum Reed-Solomon Codes

Actually, Reed-Solomon codes are one-point AG codes on the projective line. More specifically, RS codes are $C_{\mathcal{L}}(D, G)$, where $D = P_1 + \cdots + P_n$ and $G = kP_\infty$. $P_1, \ldots, P_n$ are the evaluation points and k is the maximal degree of polynomials.

Quantum Reed-Solomon codes can be obtained from classical self-orthogonal RS codes. The qRS codes achieve the quantum Singleton bound: $n - k \geq 2(d - 1)$ because RS codes meet the classical Singleton bound. Now we move to RS codes over $\mathbb{F}_{2^m}$. If $2k < n$, we can construct an $(n, k, d)_{2^m}$ RS code C, such that C is weakly self-dual, i.e. $C \subseteq C^\perp$. To present a construction method for self-orthogonal Reed-Solomon codes, we introduce an alternative definition of Reed-Solomon codes. In the previous definition, the codewords of an RS code were the evaluations of polynomials of degree less than k at n points. In the following definition, however, the codewords correspond to the coefficients of polynomials of degree less than n. These two definitions are equivalent, but the equivalence is not immediately obvious. It is established through the Fourier transform, which connects the value domain and frequency domain of functions over a finite field.

Here we want our RS codes to be *cyclic codes*, i.e., for a codeword $c = (c_0c_1 \ldots c_{n-2}c_{n-1}) \in V_n$, $c' = (c_{n-1}c_0c_1 \ldots c_{n-2})$, a cyclic shift of c is also a codeword.

Consider a codeword $c = (c_0, c_1, \ldots, c_{n-1})$, which corresponds to the polynomial

$$c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}.$$

A cyclic shift of c, resulting in $c' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, can be described algebraically as

$$c'(x) = (x \cdot c(x)) \mod (x^n - 1).$$

This operation demonstrates the cyclic property, as multiplying the polynomial $c(x)$ by x

in $\mathbb{F}_q[x]/(x^n - 1)$ is equivalent to the shift of c.

Because of the linearity and cyclic property of the codes, we can view the codes as a principal ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$, and the generator of the principal ideal is called the *generator polynomial.* More precisely, a cyclic code C is defined as:

$$C = \{c(x) = m(x)g(x) \mid m(x) \in \mathbb{F}_q[x], \deg(m) \leq n - \deg(g(x))\}.$$

Here:

- $g(x)$ is the generator polynomial.
- $m(x)$ is the message polynomial, which determines the codeword $c(x)$.

It's not hard to see that, because $0 \in C$, $g(x)$ should be a divisor of $x^n - 1$.

With the statement above, we can construct a self-orthogonal RS code from the view of the generator polynomial.

A classical, $[n, k, d]$, Reed-Solomon code, over $\mathbb{F}_{2^k}$, with length $n = 2^m - 1$, distance d, and dimension $k = n - d + 1$, is a cyclic code with the generator polynomial

$$g(x) = (x - \beta^j)(x - \beta^{j+1}) \cdots (x - \beta^{j+d-2}),$$

with β, a primitive root of $\mathbb{F}_{2^k}$.

Proposition 4.2.1. *The $[n, k, d]$ Reed-Solomon code, C, is self-orthogonal when $j = 0$ and $d > n/2 + 1$.*

Proof. If

$$g(x) = (x - \beta^0)(x - \beta^1) \cdots (x - \beta^{d-2})$$

is the generator polynomial of C, then the generator polynomial of the dual code, $C^\perp$, is the reciprocal polynomial of $(x^N - 1)/g(x)$:

$$g^\perp(x) = (x - \beta^{-(d-1)})(x - \beta^{-d}) \cdots (x - \beta^{-(N-1)}).$$

Given $N = 2^k - 1$ and β is a primitive element of $GF(2^k)$, it follows that $\beta^N = 1$, and we can write:

$$g^{\perp}(x) = (x - \beta^{N-(d-1)})(x - \beta^{N-d}) \cdots (x - \beta^{N-(N-1)}).$$

The highest power of β in the expression of $g^{\perp}(x)$ satisfies the inequality, $N - d + 1 \leq d - 1$; indeed, $d > N/2 + 1 \implies N \leq 2d - 2$ or $N - d + 1 \leq 2d - 2 - d + 1$. It follows that $g^{\perp}(x)$ is a divisor of $g(x)$; thus, $C \subseteq C^{\perp}$.

□

Theorem 4.2.2. *[14] Given $\delta > \frac{2^m-1}{2} + 1$, there is a quantum Reed-Solomon code with parameters*

$$[[m(2^m - 1), m(2\delta - 2^m - 1), \geq 2^m - \delta + 1]]_2.$$

The result is just obtained by taking a self-orthogonal RS code C over $\mathbb{F}_{2^m}$, expanding it into a binary code $\mathcal{B}(C)$ and choosing $C_1 = C_2 = \mathcal{B}(C)$ in the CSS construction.

In [15], there is a generalization to any other finite fields with odd characteristics. We can also apply the generalized Steane's construction for a new quantum code based on RS code [16].

4.2.2 Quantum Hermitian Codes

Hermitian codes are the most widely studied AG codes after Reed-Solomon codes. Quantum Hermitian codes are based on classical Hermitian codes. And the construction can be obtained from Theorem 4.1.1 with respect to the symplectic inner product $*$ and Theorem 4.1.2 with respect to the Hermitian inner product $*_h$.

Let $q = r^2$. The Hermitian curve $\mathcal{H}_r$ over $\mathbb{F}_q$ is defined by the projective equation

$$X^{r+1} = Y^r Z + Y Z^r,$$

with only one point at infinity.

Proposition 4.2.3. *The genus of the Hermitian curve H is $r(r-1)/2$. And H has $1+r^3$ points in $\mathbb{P}^2(\mathbb{F}_q)$.*

Hermitian codes are the most widely studied AG codes after Reed-Solomon codes. The exact parameters of one-point Hermitian codes are known due to [17]. Usually, Hermitian codes are $C_{\mathcal{L}}(P_1+\cdots+P_{r^3}, \alpha P_\infty)$. Since the analysis of parameters of Hermitian codes is quite complicated, we will skip it here. Parameters of the Hermitian codes $C_{\mathcal{L}}(P_1+\cdots+P_{r^3}, \alpha P_\infty)$ are given in the following table. Here $\alpha = \max\{a \in H(P_\infty) : a \leq \alpha\}$ is the largest element of the Weierstrass semigroup at the point P_∞ that is no bigger than α. We will not cover the topics of the Weierstrass semigroup and Weierstrass gaps here. In brief, they are among the main tools used to determine the exact value of the distance in AG codes. For more details, you may refer to this article [18] and the lecture notes [19].

α	$k(\alpha)$	$d(\alpha)$
$0 \leq \alpha \leq q^2-q-s$ $\alpha = sq+t$ $0 \leq b \leq q-1$	$\frac{a(a+1)}{2}+b+1$	$q^3-\alpha$
$q^2-q-s < \alpha < q^3-q^2+q$	$\alpha+1-\frac{q(q-1)}{2}$	$n-\alpha$
$q^3-q^2+q \leq \alpha < q^3$ $\alpha = q^3-q^2+aq+b$ $0 \leq a, b \leq q-1$	$\alpha+1-\frac{q(q-1)}{2}$	$q^3-\alpha$ if $a<b$ $q^3-\alpha+b$ if $a \geq b$
$q^3 \leq \alpha \leq q^3+q^2-q-2$	$a+2$ if $b=a$ $a+1$ if $b<a$	

If $\alpha_1 < \alpha_2$, then

$$C_L(D, \alpha_1 P_\infty) \subseteq C_L(D, \alpha_2 P_\infty).$$

Applying Theorem 4.1.1 with $C_1 = C_L(D, \alpha_1 P_\infty)$ and $C_2 = C_L(D, \alpha_2 P_\infty)$ and the normal symplectic inner product $*$ yields the following fact.

Theorem 4.2.4 ([20, Theorem 3]). *For $0 \leq \alpha_1 < \alpha_2 \leq q^3+q^2-q-2$, there exists a*

$$\left[q^3, k(\alpha_2)-k(\alpha_1), \geq \min\{d(\alpha_2), d(q^3+q^2-q-2-\alpha_1)\}\right]_{q^2}$$

code where $k(\alpha)$ and $d(\alpha)$ are given in the table above

Quantum Hermitian codes can also be constructed using Hermitian codes which are self-orthogonal with respect to the Hermitian inner product. According to [21], the dual of the one-point Hermitian code $C_L(D, \alpha P_\infty)$ over $\mathbb{F}_{q^2}$ is given by

$$C_L(D, \alpha P_\infty)^\perp = C_L\left(D, \left(q^3 + q^2 - q - 2 - \alpha\right) P_\infty\right)$$

. It follows that $C_L(D, \alpha P_\infty)$ is self-orthogonal if $2\alpha \leq q^3 + q^2 - q - 2 - \alpha$. Using this, one can prove that $C_L(D, \alpha P_\infty)$ is self-orthogonal with respect to the Hermitian inner product for $0 \leq \alpha \leq q^2 - 2$ (see [20, Lemma 7] for details). Now Theorem 4.1.2 gives another family of quantum Hermitian codes.

Theorem 4.2.5 ([13, Theorem 8]). *If $0 < \alpha \leq q^2 - 2$, then there exists a*

$$\left[q^3, q^3 - 2k(\alpha), \geq d(q^3 + q^2 - q - 2 - \alpha)\right]_q$$

code where $k(\alpha)$ and $d(\alpha)$ are given in the table above.

4.3 General Construction

The quantum Reed-Solomon and quantum Hermitian codes defined earlier are special cases of a more general construction for quantum codes from AG codes detailed in this section.

Let X be a smooth, projective, absolutely irreducible curve of genus g over a finite field $\mathbb{F}_q$. Suppose that A and B are divisors on X such that $A \leq B$, and let $D = P_1 + \cdots + P_n$ be another divisor on X whose support consists of n distinct $\mathbb{F}_q$-rational points none of which are in the support of A or B. Then

$$\mathcal{L}(A) \subseteq \mathcal{L}(B)$$

and so

$$C_L(D, A) \subseteq C_L(D, B).$$

Applying Theorem 4.1.1, we can construct a large family of quantum codes from AG codes.

Theorem 4.3.1. *Let A, B, and $D = P_1 + \cdots + P_n$ be divisors on a smooth, projective, absolutely irreducible curve X of genus g over $\mathbb{F}_q$. Assume that $A \leq B$ and $(\operatorname{supp} A \cup \operatorname{supp} B) \cap \operatorname{supp} D = \emptyset$ and $\deg B < n$. Then there exists a $[n, l(B) - l(A), d]_q$ code where*

$$d \geq \min\{d(C_L(D, B) \setminus C_L(D, A)), d(C_\Omega(D, A) \setminus C_\Omega(D, B))\}$$

$$\geq \min\{n - \deg B, \deg A - (2g - 2)\}.$$

Proof. This follows immediately from Theorem 4.1.1. We just need to take $C_1 = C_L(D, A)$ and $C_2 = C_L(D, B)$). The fact that $\deg A \leq \deg B < n$ implies $\dim C_L(D, B) = \ell(B)$ and $\dim C_L(D, A) = \ell(A)$. □

In the next example, we see how one may apply Theorem 1.12 to a multipoint code.

Example 4.3.2. Let X be a smooth, projective, absolutely irreducible curve of genus g over $\mathbb{F}_q$. Consider the m-point code $C_L(D, \sum_{i=1}^m a_i Q_i)$ on X over $\mathbb{F}_q$. Since $\mathbb{F}_q$ is finite, the *class number* of the function field of X over $\mathbb{F}_q$ is finite. Hence, there exists a rational function f with the divisor

$$(f) = \sum_{i=2}^m b_i Q_i - b_1 Q_1$$

where $b_i \geq a_i$ for all i, $2 \leq i \leq m$, and $b_1 := \sum_{i=2}^m b_i$. Multiplication by f gives rise to a vector space isomorphism

$$\phi : \mathcal{L}\left(\sum_{i=1}^m a_i Q_i\right) \to \mathcal{L}\left((a_1 + b_1)Q_1 - \sum_{i=2}^m (b_i - a_i) Q_i\right)$$

$$h \mapsto fh$$

which in turn induces an isometry ϕ^* of codes

$$C_L\left(D, \sum_{i=1}^{m} a_i Q_i\right) \cong C_L\left(D, (a_1+b_1)Q_1 - \sum_{i=2}^{m}(b_i - a_i)Q_i\right).$$

Since $(a_1+b_1)Q_1 - \sum_{i=2}^{m}(b_i - a_i)Q_i \le (a_1+b_1)Q_1$, we get

$$C_L\left(D, (a_1+b_1)Q_1 - \sum_{i=2}^{m}(b_i - a_i)Q_i\right) \subseteq C_L(D, (a_1+b_1)Q_1).$$

Therefore, if $a_1 + b_1 < |\operatorname{supp} D|$ then Theorem 1.12 yields a quantum code over $\mathbb{F}_q$ of length $|\operatorname{supp} D|$ and dimension

$$\ell\left((a_1+b_1)Q_1\right) - \ell\left((a_1+b_1)Q_1 - \sum_{i=2}^{m}(b_i - a_i)Q_i\right).$$

A bound on the minimum distance is given by the theorem also.

$$d \ge \min\left\{n - (a_1+b_1), (a_1+b+1) - \sum_{i=2}^{m}(b_i - a_i) - (2g-2)\right\}.$$

Due to the complexity of multipoint codes, the distance is challenging to analyze precisely. As a result, determining the minimum distance of the quantum code may be challenging. A notable exception to this is the family of two-point Hermitian codes whose exact minimum distance has been determined in the works of Homma and Kim [22], [23], [24], [25].

Of course, one may also apply Theorem 4.3.1 to construct quantum codes from classical AG multipoint codes. While this construction provides a great deal of flexibility, it produces codes whose minimum distances may be hard to completely determine. For this reason, we will not give a more detailed introduction.

Next, we consider how Theorem 4.1.2 may be applied to AG codes. The idea is a generalization of our construction from Hermitian codes with respect to the Hermitian inner product.

Lemma 4.3.3. The algebraic geometry code $C_L(D,G)$ is self-orthogonal with respect to the Hermitian inner product if there exists a differential η such that $v_{P_i}(\eta) = -1$, $\eta_{P_i}(1) = 1$ for $1 \leq i \leq n$, and

$$D + (\eta) \geq (q+1)G.$$

Proof. Let $D = P_1 + \cdots + P_n$ and G be divisors on a smooth, projective, absolutely irreducible curve X over $\mathbb{F}_q$ where $P_1, \ldots, P_n$ are distinct $\mathbb{F}_q$-rational points not in the support of G. Recall that the dual of $C_L(D,G)$ may be expressed as

$$C_L(D,G)^{\perp} = C_L(D, D - G + (\eta))$$

where η is a differential on X such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for $1 \leq i \leq n$. Notice that for $h \in \mathcal{L}(G)$,

$$\begin{aligned} \mathrm{ev}(f) *_h \mathrm{ev}(h) = 0 &\iff \sum_{i=1}^{n} f(P_i)h(P_i) = 0 \quad \forall f \in L(G), \\ &\iff h^q \in L(D - G + (\eta)), \\ &\iff q(h) \geq G - D + (\eta). \end{aligned}$$

The last inequality holds if $D + (\eta) \geq (q+1)G$.

It follows that given $h \in \mathcal{L}(G)$, $\mathrm{ev}(f) *_h \mathrm{ev}(h) = 0$ for all $f \in \mathcal{L}(G)$ if

$$D + (\eta) \geq (q+1)G.$$

□

The next result is a consequence of the lemma above. Here, P_0 denotes the common zero of the functions x and y on the Hermitian curve over $\mathbb{F}_{q^2}$.

Proposition 4.3.4. *Suppose that* $0 \leq a+b < q^2-2$. *Then the two-point code* $C_L(D, aP_\infty + bP_0)$ *on the Hermitian curve defined by* $y^{q+1} + y = x^{q+1}$ *over* $\mathbb{F}_{q^2}$ *is self-orthogonal with respect to the Hermitian inner product.*

Proof. Take $\eta = \frac{y^{b+1}}{z}\,dz$. Then

$$(\eta) = \left(q^3 + q^2 - q - (b+1)(q+1)\right) P_\infty - \left((b+1)(q+1)+1\right) P_0 - D$$

and the conditions of Lemma 1.1 are satisfied. □

Proposition 4.3.5. *Let* $0 \le a+b < q^2-2$. *Then there exists a*

$$\left[q^3-1, q^3 - 2\ell(aP_\infty + bP_0) - \ell, d\right]_q$$

code where

$$d = \min\left\{\mathrm{wt}\left(C_L(D, aP_\infty + bP_0)^{\perp h} \setminus C_L(D, aP_\infty + bP_0)\right)\right\}.$$

4.4 Quantum Codes from Curves with Automorphisms

In this section, we will study algebraic curves with automorphism structures and construct quantum codes from them [26]. Additionally, we will use hyperelliptic curve codes as an example later in this section. On the one hand, we can more easily construct self-orthogonal classical AG codes [27], and subsequently quantum codes, from algebraic curves with automorphisms that include an involution. On the other hand, the automorphisms of the curve may provide insights into the automorphisms of the constructed codes. However, the latter will not be further discussed in this paper. Readers can refer to [26, 28].

Let $\mathcal{X}$ be a genus g curve defined over a finite field $\mathbb{F}_q$ and F is its function field. The following lemma is cited from [12, Prop. VII.1.2]. It allows us to construct differentials with special properties that help to construct a self-orthogonal code.

Lemma 4.4.1. Let x and y be elements of F such that $v_{P_i}(y) = 1$, $v_{P_i}(x) = 0$ and $x(P_i) = 1$ for $i = 1, \dots, n$. Then the differential $\eta := x\frac{dy}{y}$ satisfies $v_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_i}(\eta) = 1$ for $i = 1, \dots, n$.

First, let us explore how additional information from the existence of automorphisms on an algebraic curve can assist in constructing quantum codes.

Theorem 4.4.2. *Let $\mathcal{X}$ be a genus g irreducible algebraic curve defined over $\mathbb{F}_q$ and $P_1, \dots, P_n$ degree one rational points on $\mathcal{X}$. Let $\sigma \in \mathrm{Aut}(\mathcal{X})$ be an involution such that $\sigma P_i \neq P_j, \forall i, j = 1, \dots, n$. Further assume that we have a divisor G such that $\sigma G = G$, $v_{P_i}(G) = v_{P_{\sigma(i)}}(G) = 0$ for all i. Then, there exists a quantum code $Q_{\mathcal{X}} = [n, k, d]$ such that*

$$k = \dim G - \dim(G - P_1 - \cdots - P_n - \sigma(P_1) - \cdots - \sigma(P_n)) - n,$$

$$d \geq n - \left\lfloor \frac{\deg G}{2} \right\rfloor$$

Proof. Let $F = F_q(\mathcal{X})$ be the function field of $\mathcal{X}$. Let $P_1, \dots, P_n$ be pairwise distinct places of degree one such that $\sigma P_i \neq P_j, \forall i, j = 1, \dots, n$. Then, by the strong approximation theorem there is a differential η such that

$$\begin{cases} v_{P_i}(\eta) = -1, \\ \mathrm{Res}_{P_i}(\eta) = 1, \\ \mathrm{Res}_{\sigma P_i}(\eta) = -1. \end{cases}$$

Further assume that we have a divisor G such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$ for all i. Define

$$C(G) = \{(f(P_1), \dots, f(P_n), f(\sigma P_1), \dots, f(\sigma P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^{2n}\}.$$

Let

$$H = (P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n) - G + (\eta),$$

where η is the differential above. Then, we have $C(G)^\perp = C(H)$.

Let us assume that $H \leq G$. Then, $\mathcal{L}(H) \subseteq \mathcal{L}(G)$. Hence, $C(D, G)^\perp \subseteq C(D, G)$. We have $k = \dim C(D, G) - n$ which implies the result.

Let $f \in \mathcal{L}(G)$ such that $\mathrm{wt}(f(P_1), \dots, f(\sigma P_n)) = \delta \neq 0$. Hence, there exists a set of coordinates $f(P_1), \dots, f(P_{i-\delta})$ which are all zero. Thus, we have $f \in \mathcal{L}\left(G - \sum_{j=1}^{n-\delta}(P_{i,j} + \sigma P_{i,j})\right)$.

The dimension of this space is > 0, which implies the result. □

Since we already have the theorem above, we like to construct quantum codes starting from algebraic curves which have non-trivial automorphisms now. The most common class of curves is obviously the hyperelliptic curve. However, we start in a more general setting. Our first class of curves are curves which have a cyclic group embedded in the automorphism group of the curve. The hyperelliptic curves will be studied in more detail in the next subsection.

4.4.1 Codes on the Cyclic Covers of the Projective Line

In this subsection, the examples of our curves do not necessarily have an involution. In this specific example, we only use one of its automorphisms to construct self-orthogonal classical AG codes, which are then used to construct quantum codes. Let k be a field of characteristic $p > 0$ and $F_0 = k(x)$ a function field of the projective line $\mathbb{P}^1(k)$. We consider a degree r cyclic extension $F := k(x, y)$, where

$$y^r = f(x) = \prod_{i=1}^{s} (x - \alpha_i)^{d_i}, \quad 0 < d_i < m.$$

for some fixed $m \in \mathbb{Z}^+$. The only places of F_0 that ramify are the places which correspond to the points $x = \alpha_i$. We denote such places by $Q_1, \dots, Q_s$ and by $\mathbb{B} := \{Q_1, \dots, Q_s\}$ the set of these places. The ramification indexes are $e(Q_i) = \frac{r}{\gcd(r,d_i)}$.

Let $\mathcal{X}$ denote the algebraic curve with affine equation

$$y^r = f(x)$$

defined over k, and $G := \mathrm{Aut}(\mathcal{X})$ be the automorphism group. Then, there is a cyclic group $C_r = \mathrm{Gal}(F/F_0)$ of order r such that $C_r \hookrightarrow \mathrm{Aut}(\mathcal{X})$. Fix a generator $\sigma \in C_r$.

Lemma 4.4.3. Let $\tau \in \mathrm{Aut}(\mathcal{X})$ such that $\tau \notin C_r$, s be the number of ramified places of the extension F/F_0, and $d = \deg f(x)$. Then, the equation of the curve is given by

$$y^r = f(x^\delta)$$

for some $\delta \mid d$. Moreover, $f(x^\delta)$ is a monic polynomial with the constant coefficient 1.

Let $\mathcal{X}$ be an algebraic curve defined over a field $\mathbb{F}_q$ of characteristic $p > 0$ given by an equation

$$y^r = f(x^\delta)$$

where $d = \deg f(x)$. Let $C_r \hookrightarrow \mathrm{Aut}(\mathcal{X})$ such that $C_r = \langle \sigma \rangle$. The corresponding cover $\psi : \mathcal{X} \longrightarrow \mathcal{X}^\circ$ has d branch points. Let B be the branch set. For a given rational point $P \in \mathcal{X}$ we define $\mathrm{Orb}_\sigma(P) = \{\sigma(P) \in \mathcal{X} \mid |\, \mathrm{Orb}_\sigma(P)| = r\}$.

Let $P_1, \dots, P_n$ be rational points on $\mathcal{X}$ such that $\psi(P_i) \notin B$ for all $i = 1, \dots, n$. Define the divisor

$$D = \sum_{i=1}^{n} \left(P_i + \sigma(P_i) + \cdots + \sigma^{r-1}(P_i)\right) = \sum_{i=1}^{n} \mathrm{Orb}(P_i).$$

Then $\deg D = rn$. For some $P \in \mathcal{X}$ such that $\psi(P) \in B$ we define $G = mP$ for some integer m. Then $\sigma(G) = G$. We can take infinity to be one of the branch points in B. In that case the point P is the fiber is denoted by P_∞. It is common in coding theory to take G to be mP_∞.

We define an algebraic geometry code as previously $C_\mathcal{X} = \mathcal{L}(G, D)$. The proof of the following theorem is similar to that of Theorem 1.

Theorem 4.4.4. *Let $\mathcal{X}$ be an algebraic curve defined over a field $\mathbb{F}_q$ of characteristic $p > 0$ such that $C_r = \langle \sigma \rangle \hookrightarrow \mathrm{Aut}(\mathcal{X})$. Let $P_1, \dots, P_n$ rational points on $\mathcal{X}$ such that $|\, \mathrm{Orb}_\sigma(P_i)| = r$ and $\mathrm{Orb}_\sigma(P_i) \cap \mathrm{Orb}_\sigma(P_j) = \emptyset$ for all i, j. Further assume that we have a divisor G such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$ for all i. Then, there exists a quantum code $Q_\mathcal{X} = [nr, k, d]$ such that*

$$k = \dim G - \dim(G - D) - nr, \quad d \geq nr - \left\lfloor \frac{\deg G}{2} \right\rfloor.$$

4.4.2 Hyperelliptic Quantum Codes

According to Theorem 4.4.2, we want algebraic curves with at least one involution and many rational points. An obvious class of curves which assures the existence of an involution is, of course, the hyperelliptic curves. In this subsection, we want to construct quantum codes starting with AG-codes which come from hyperelliptic curves with respect to *weighted* symplectic inner product. So the idea of construction is different from the codes we discussed before. We focus on odd characteristics. Let $K := \mathbb{F}_{p^m}$ be a finite field of characteristic $p > 2$, and X_g a genus g hyperelliptic curve given by the equation $y^2 = f(x)$. Let $F := K(x, y)$ be the function field and σ denotes the involution of X_g. Then F has a set of rational places which are not fixed by the hyperelliptic involution. Choose a set of distinct points in F such that

$$SP = \{P_1, \dots, P_n, \sigma(P_1), \dots, \sigma(P_n)\},$$

such that $\pi(P_i) = \alpha_i$, where π is the hyperelliptic projection.

Let P_∞ denote the point at infinity and $D, G \in \mathrm{Div}(X_g)$ be as follows

$$D := \sum_{i=1}^{n} P_i + \sum_{i=1}^{n} \sigma(P_i) \quad \text{and} \quad G := (n + g - 1 - r)P_\infty,$$

where $0 \le r \le n - g$. Then D has degree $2n$. By Riemann-Roch theorem there exists $\eta \in F$ such that

$$\eta = \frac{1}{y \prod_{i=1}^{n} (x - \alpha_i)} dx$$

Hence, $(\eta) = (2n + 2g - 2)P_\infty - D$. We denote

$$W := (\eta) = (2n + 2g - 2)P_\infty - D, \quad \text{and} \quad H := D - G + W.$$

Then W is a canonical divisor, and the residues of η at the places $P_1, \dots, P_n, \sigma(P_1), \dots, \sigma(P_n)$

satisfy

$$a_i := \mathrm{Res}_{P_i}(\eta) = -\mathrm{Res}_{\sigma(P_i)}(\eta)$$

for $i = 1, \dots, n$.

Now we can construct a Goppa code $C(D,G)$ and $C(D,H)$. The weighted symplectic inner product is defined as below

$$\langle x, y \rangle_s^a = \sum_{i=0}^{C} 4na_i \left(x_i y_{n+i} - x_{n+i} y_i \right).$$

for all $x, y \in C$ and all $a_i \neq 0$.

Lemma 4.4.5. Let $C(D,G)$ and $C(D,H)$ be as above. Then

$$C(D,G)^{\perp_s} = C(D,H) \cdot \mathrm{diag}(a_1, \dots, a_n, 1, \dots, 1)$$

Moreover, $C(D,G) \subseteq C(D,G)^{\perp_s}$ with respect to the symplectic inner product $\langle, \rangle_s^a$.

Proof. Since $G = (n+g-1-r)P_\infty$ then we replace (η) to get $H = (n+g-1+r)P_\infty \geq G$. Hence, $\mathcal{L}(G) \subset \mathcal{L}(H)$ and $C(D,G) \subset C(D,H)$. From the above lemma we have that $C(D,G)\langle a, s \rangle_s = C(D,H)$. □

We transform $C(D,G)$ to a self-orthogonal code $C'(D,G)$ with respect to the standard symplectic inner product by multiplying each component x_i of every codeword by the corresponding a_i, for $1 \leq i \leq n$.

Then, we have the following:

Proposition 4.4.6. *$C'(D,G)$ is a stabilizer code with parameters $[n,k,d]$, where $k = g+r-1$ and $d \geq \frac{n-k}{2}$.*

Proof. We can construct a stabilizer code since $C'(D,G)$ is self-orthogonal; see Thm. 1. The new code has the same parameters with $C'(D,G)$. So it is left to compute k and d.

From the Riemann-Roth theorem we have that

$$k = \dim H - \dim(H - D) - n = (n + g - 1 + r) - n = g + r - 1,$$

since $\dim(H - D) = 0$. For d we have $d \geq n - \left\lfloor \frac{\deg H}{2} \right\rfloor \geq \frac{n-k}{2}$. □

We summarize in the following theorem.

Theorem 4.4.7. *Let $\mathcal{X}$ be a genus g irreducible hyperelliptic curve defined over $\mathbb{F}_q$ and $P_1, \ldots, P_n$ degree one rational points on $\mathcal{X}$. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ be an involution such that $\sigma P_i \neq P_j$, $\forall i, j = 1, \ldots, n$. Further assume that we have a divisor G such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma(P_i)}(G) = 0$ for all i. Then, there exists a quantum code $Q_{\mathcal{X}} = [n, k, d]$ such that*

$$k = \dim G - \dim\left(G - P_1 - \cdots - P_n - \sigma(P_1) - \cdots - \sigma(P_n)\right) - n, \quad d \geq n - \left\lfloor \frac{\deg G}{2} \right\rfloor.$$

4.5 Asymptotically Good Quantum Codes

By leveraging certain properties of AG codes, we can conclude that there exists a family of asymptotically good quantum codes. For a family of quantum codes with parameters (n, k, d), being asymptotically good means that as the code length $n \longrightarrow \infty$, the rate $R = \frac{k}{n}$ and the relative distance $\delta = \frac{d}{n}$ do not approach zero.

The content of this section is primarily based on the paper [7]. Moreover, the construction of quantum codes in this paper follows Steane's generalized CSS construction [29], with improved parameter estimates provided by [30]. Additionally, the codes we construct are based on fields with characteristic 2. The following theorem is given in [29].

Theorem 4.5.1. *Given a classical binary error-correcting code $C = [n, k, d]$ which contains its dual, $C^{\perp} \subseteq C$, and which can be enlarged to $C' = [n, k' > k + 1, d']$, a nondegenerate quantum code of parameters $[n, k + k' - n, \min\{d, \lceil \frac{3d'}{2} \rceil\}]$ can be constructed.*

The proof is quite constructive, we choose to omit here. But we need to mention that the result only holds for binary codes because the proof process makes use of the arithmetic property on $\mathbb{F}_2$. And there are generalization for nonbinary cases [31]. Their results show that for a self-orthogonal classical codes over $\mathbb{F}_q$, we can construct a $[n, k + k' - n, \min\{d, \lceil \frac{(q+1)d'}{q} \rceil\}]$ quantum code.

With the above theorem, we aim to find a triple $C^\perp \subseteq C \subseteq C'$ to construct quantum CSS codes over $\mathbb{F}_{2^m}$. First, we need to find an AG code that contains its dual. However, initially, instead of restricting ourselves to fields with characteristic 2, let us consider a more general finite field. Then, we will show why characteristic 2 is special in our construction.

Definition 4.5.2. Let $\theta \in (\mathbb{F}_q^*)^n$. For a code $C \subseteq \mathbb{F}_q^n$, we define

$$C_\theta^\perp = \left\{ x \in \mathbb{F}_{q^n} \,\middle|\, \sum_{i=1}^n \theta_i x_i y_i = 0, \ \forall y \in C \right\}.$$

Let $\mathcal{X}$ be a smooth projective geometrically irreducible algebraic curve of genus g defined over $\mathbb{F}_q$. G is an effective divisor of degree a, and $\mathcal{P}' := \{P_1, \dots, P_{n'}\} \subset X(\mathbb{F}_q)$ is a set of $\mathbb{F}_q$ points so that $\operatorname{supp} G \cap \mathcal{P}' = \emptyset$. we define a divisor $P' = P_1 + \cdots + P_{n'}$.

We want to find a divisor A with $\delta(-A) > 0$, then we can find a nonzero $\omega_0 \in \Omega(-A)$, which will be used in the following construction. By Theorem 3.6.5, $\delta(-A) = l(W + A)$ for a canonical divisor W. And according to Riemann-Roch Theorem,

$$l(W + A) \geq \deg(W + A) + 1 - g.$$

We expect $l(W + A)$ to be nonzero, so we can choose A so that $\deg(W + A) = g$, i.e. $deg(A) = 2 - g$. With this intuition, suppose that $a \leq (n' + g)/2 - 1$, then there exists an effective divisor E with degree $n' + g - 2 - 2a$. Let $A = P' - 2G - E$, $deg(A) = 2 - g$. Therefore we can find a nonzero $\omega_0 \in \Omega(-A)$.

We consider the "residue map":

$$\mathcal{R}: \ \Omega(-A) \to \mathbb{F}_q^{n'}$$

$$\omega \mapsto (\operatorname{Res}_{P_1}(\omega), \dots, \operatorname{Res}_{P_{n'}}(\omega)).$$

Acctually, $\mathrm{im}(\mathcal{R})$ is just the code $C_\Omega(P', P' - A)$. And $\ker(\mathcal{R})$ is $\Omega(2G + E)$.

We define a point set $\mathcal{P}_0 := \{P_i \in \mathcal{P}' : \operatorname{Res}_{P_i}(\omega_0) = 0\}$. Then

$$\omega_0 \in \Omega\left(2G + E - \left(P' - \sum_{P_i \in \mathcal{P}_0} P_i\right)\right) = \Omega\left(-A + \sum_{P_i \in \mathcal{P}_0} P_i\right).$$

Since ω_0 is nonzero, we have:

$$\deg\left(-A + \sum_{P_i \in \mathcal{P}_0} P_i\right) \leq 2g - 2,$$

by Riemann-Roch Theorem. The above equation implies that $|\mathcal{P}_0| \leq g$.

Let $\mathcal{P} = \mathcal{P}' \setminus \mathcal{P}_0$, without loss of generality, we can label elements in $\mathcal{P}$ by $\{P_1, \ldots, P_n\}$. Then $n \geq n' - g$. Now for the divisor $P = P_1 + \ldots + P_n$, we have $\omega_0 \in \Omega(2G + E - D)$. Let $\theta = (\operatorname{Res}_{P_1}(\omega_0), \ldots, \operatorname{Res}_{P_n}(\omega_0))$, we define the code

$$C = C_{\mathcal{L}}(P, G)^{\perp}_{\theta} = \left\{x \in GF_q^n \mid \sum_i \theta_i x_i y_i = 0,\ \forall y \in C_{\mathcal{L}}(P, G)\right\}.$$

We claim that $C_{\mathcal{L}}(P, G) \subseteq C$. Because $\forall f, g \in \mathcal{L}(G)$:

$$\sum_{i=1}^{n} f(P_i) g(P_i) \theta_i = \sum_{i=1}^{n} f(P_i) g(P_i) \operatorname{Res}_{P_i}(\omega_0) = \omega_0(fg) = 0.$$

The last equation holds because $\omega_0 \in \Omega(2G + E - P)$ and $f, g \in \mathcal{L}(G)$. Therefore, we prove the claim above. Also, for $f \in C^{\perp}_{\theta}$, f must lie in $C_{\mathcal{L}}(P, G)$. Since $C_{\mathcal{L}}(P, G) \subseteq C$ We conclude that $C^{\perp}_{\theta} \subseteq C$.

Note that, if $q = 2^m$, any element in $\mathbb{F}_q$ is a square. Let $\theta_i = \eta_i^2$. Consider the coordinate multiplication map:

$$m_\eta : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

$$x \mapsto (\eta_1 x_1, \ldots, \eta_1 x_1).$$

For codes $C' := m_\eta(C)$, $C'^{\perp}$ is contained in C'.

Up to now, we find a proper code containing its own dual by the AG construction. And now we need to analyse its parameters. Since the bilinear form

$$\langle \cdot, \cdot \rangle_\theta : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$

$$(x, y) \mapsto \sum_{i=1}^{n} x_i y_i \theta_i$$

is nondegenerate, $\dim(C_{\mathcal{L}}(P,G)_\theta^\perp) = n - \dim(C_{\mathcal{L}}(P,G))$. The dimension of $C_{\mathcal{L}}(P,G)$ is $deg(G) + 1 - g$ according to Theorem 3.7.2, and m_η is an isometry between vector space with Hamming weight. So the dimension k of C and C' is $n - a + g - 1$, the minimum distance d of C and C' is $\geq a - 2g + 2$ for $a \geq 2g - 1$. Recall that $a \leq (n' + g)/2 - 1$, so $2g - 1 \leq a \leq (n' + g)/2 - 1$ and we need $n' > 3g$ to make the inequality hold.

Summing up, we get the following theorem.

Theorem 4.5.3. *If there exists a curve over $\mathbb{F}_q$ of genus g with at least $n' \geq 3g$ $\mathbb{F}_q$ points, then for any $n \leq n' - g$ and any $a = 2g - 1, \ldots, n/2 + g - 1$ there is an $[n, k, d]_q$ code C with*

$$k = n - a + g - 1,$$

$$d \geq a - 2g + 2,$$

so that $C \subseteq C_\theta^\perp$ for some $\theta \in (\mathbb{F}_q^*)^n$.

Moreover, if q is a power of 2, there is such a code with $C \subseteq C^\perp$.

We want to show that the code constructed above can be asymptotically good, so we need to keep an eye on the following parameters:

$$\text{rate } R = k/n = 1 - \frac{a + 1 - g}{n}, \text{ and relative distance } \delta = d/n \geq \frac{a - 2g + 2}{n}.$$

From the equations, we see that R rises with the increase of n and with the decrease of a, while δ rises with the increase of a and with the decrease of n. Also, it's not hard to observe that $R + \delta \geq 1 - g/n$. Hence, for fixed δ, we should choose the maximum n available to maximize R. Therefore, we will always choose $n = n' - g$ from now on.

However, the above discussion just stands on a fixed algebraic curve. To analyze the asymptotic behavior, we need to ask: is there a family of algebraic curves for our construction? Fortunately, we have the following theorem [32].

Theorem 4.5.4. *There is a family of curves over $\mathbb{F}_q$, q being a square, such that*

$$\limsup_{g \to \infty} \frac{|\mathcal{X}(\mathbb{F}_q)|}{g(\mathcal{X})} \longrightarrow 0,$$

where $|\mathcal{X}(\mathbb{F}_q)|$ is the number of rational points on the curve $\mathcal{X}$ over $\mathbb{F}_q$ and $g(\mathcal{X})$ is the genus of the curve.

Combining the formula for R, δ, the range of a, and the theorem above, it's not hard to get the following corollary.

Corollary 4.5.5. Let q be an even power of a prime. Then for any

$$\alpha \in \left(\frac{2}{\sqrt{q} - 2}, \frac{1}{2} + \frac{1}{\sqrt{q} - 2} \right),$$

there exist families of codes with asymptotic parameters

$$R = 1 - \alpha + \frac{1}{\sqrt{q} - 2},$$

$$\delta \geq \alpha - \frac{2}{\sqrt{q} - 2},$$

with the property $C \supseteq C_\theta^\perp$ for some $\theta \in (GF_q^*)^n$.

If q is an even power of 2, there exist such codes with the property $C \supseteq C^\perp$.

As mentioned at the beginning of this section, we aim to construct quantum codes through a generalized CSS construction (over $\mathbb{F}_2$), so we need a triple $C^\perp \subseteq C \subset C'$. And now we already have $C^\perp \subseteq C$. To get codes C' so that $C \subset C'$, we can take a divisor $G' < G$.

Then $C_{\mathcal{L}}(P, G') \subseteq C_{\mathcal{L}}(P, G)$ and we have the opposite inclusion for their duals. If we take Supp$G' \cup P = \emptyset$, ω_0 can remain the same. Thus, we get the following corollary, which will help us construct asymptotically good quantum codes in the next steps.

Corollary 4.5.6. Let $q = 2^{2m}$. Then for any pair of real numbers (α, α') such that

$$\frac{2}{2^m - 2} \leq \alpha' < \alpha \leq \frac{1}{2} + \frac{1}{2^m - 2}$$

there exists families of triples of 2^{2m}-ary codes $C' \supset C \supset C^{\perp}$ with asymptotic parameters

$$R' = 1 - \alpha' + \frac{1}{2^m - 2}, \quad \delta' \geq \alpha' - \frac{2}{2^m - 2}$$

$$R = 1 - \alpha + \frac{1}{2^m - 2}, \quad \delta \geq \alpha - \frac{2}{2^m - 2}.$$

Finally, with all the preparation above, we can construct asymptotically good quantum codes using AG codes. Let us outline this process.

1. Start with a family of algebraic function fields over $\mathbb{F}_{2^m}$ with the property that

$$\lim_{g \to \infty} \frac{N(F)}{g(F)} = 2^m - 1.$$

Each algebraic function field will then give us a triple of classical linear codes $C' \supset C \supset C^{\perp}$ over $\mathbb{F}_{2^{2m}}$.

2. Let C' and C be an $[n', k', d']$ code and an $[n, k, d]$ code respectively. Binary expand C and $C^{\perp}$ with respect to a self-orthogonal basis to get a triple of binary codes $D' \supset D \supset D^{\perp}$ with parameters

$$n_{D'} = n_D = 2n, \quad k_{D'} = 2mk', \quad k_D = 2mk, \quad d_{D'} \geq d', \quad d_D = d.$$

3. By the generalized CSS construction, each triple gives us a quantum stabilizer code

$$[[2mn, 2m(k + k' - n), \geq \min\{d, d'\}]].$$

The corresponding asymptotic parameters are

$$R_Q = R + R' - 1$$

$$\delta_Q \geq \frac{1}{2m} \min\left\{\delta, \frac{3\delta'}{2}\right\}$$

where R, R', δ, δ' are the parameters of algebraic geometric $\mathbb{F}_{2^{2m}}$ codes.

Let us now try to find a dependence between R_Q and δ_Q. Letting $\gamma = \frac{1}{2^m-2}$. We know that for $q = 2^{2m}$ and for any pair of real numbers (α, α') such that $2\gamma \leq \alpha' < \alpha \leq \frac{1}{2} + \gamma$,

$$R_Q = 1 - (\alpha + \alpha') + 2\gamma$$

$$\delta_Q \geq \frac{1}{2m} \min\{\alpha - 2\gamma,\ \frac{3}{2}(\alpha' - 2\gamma)\}.$$

For any fixed δ_Q, in order to maximize R_Q, we want $\alpha - 2\gamma = \frac{3}{2}(\alpha' - 2\gamma)$, i.e., $\alpha' = \frac{2}{3}(\alpha + \gamma)$. Hence,

$$R_Q = 1 - \frac{5}{3}\alpha + \frac{4}{3}\gamma$$

$$\delta_Q \geq \frac{1}{2m}(\alpha - 2\gamma).$$

Therefore, for any $m \geq 3$ and $\delta \leq \frac{1}{2m}\left(\frac{1}{2} - \frac{1}{2^m-2}\right)$, we get

$$R_Q = 1 - \frac{2}{2^m - 2} - \frac{10}{3}m\delta.$$

Immediately, we see that the asymptotic parameters of QAG codes are separated from zero and so they are asymptotically good as claimed.

Chapter 5

Conclusions

In this thesis, we explored the application of algebraic geometry (AG) codes in the construction of quantum error correction codes (QECCs). By leveraging the established theory and structure of AG codes, we have summarized existing results and provided insights into how these codes can be utilized to address key challenges in quantum information processing.

The rich theoretical foundation of AG codes, which has been extensively studied in classical coding theory for over three decades, remains a fertile ground for further exploration. Unlike many randomized code constructions, AG codes offer explicit constructions with well-defined parameters, providing a significant advantage in terms of both theoretical clarity and practical implementation. Moreover, these codes often benefit from mature polynomial-based decoding algorithms, which make them more accessible and efficient compared to other classical codes.

In the context of quantum codes, algebraic geometry offers several unique benefits. For instance, it provides systematic methods to identify self-orthogonal classical codes, a key requirement for constructing QECCs through methods such as Steane's construction. Additionally, the structure of AG codes simplifies the construction of nested codes with inclusion properties, which can be achieved by selecting divisors that satisfy the partial ordering. These features underscore the versatility of AG codes in quantum error correction.

Looking beyond error correction, quantum AG codes show promise in facilitating advanced quantum operations. For example, their structure may provide advantages in manipulating logical qubits, such as in magic state distillation, where these codes could outperform other QECCs. Recent results [33–35]in this area indicate a growing interest and potential for further development.

Furthermore, there is room for innovation by extending quantum AG code theory to incorporate tools from algebraic geometry that go beyond traditional constructions. For instance, chain complexes derived from Čech cohomology or other cohomological frameworks might inspire new classes of quantum codes. There already are codes based on Khovanov homology in low-dimensional topology [36]. Maybe homology in algebraic geometry could help with results in quantum codes. This direction is particularly relevant due to the potential limitations of simplicial complexes in achieving optimal code parameters. I hypothesize that codes constructed using simplicial complexes may inherently face certain restrictions on their performance. In contrast, quantum codes derived from other types of complexes, such as "square complex", have demonstrated improved parameters [37]. These alternative approaches highlight the possibility of overcoming the limitations of simplicial complexes and achieving better error correction capabilities through the use of more general and flexible mathematical structures.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical review A*, vol. 52, no. 4, p. R2493, 1995.

[2] A. Steane, "Multiple-particle interference and quantum error correction," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[3] V. D. Goppa, "A new class of linear correcting codes," *Problemy Peredachi Informatsii*, vol. 6, no. 3, pp. 24–30, 1970.

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

[5] E. M. Rains, "Nonbinary quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.

[6] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[7] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, p. 032311, Feb 2001.

[8] J.-L. Kim and G. L. Matthews, "Quantum error-correcting codes from algebraic curves," in *Advances in algebraic geometry codes*, pp. 419–444, World Scientific, 2008.

[9] B. C. Hall, "Quantum theory for mathematicians," 2013.

[10] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of physics*, vol. 303, no. 1, pp. 2–30, 2003.

[11] A. Kitaev, "Anyons in an exactly solved model and beyond," *Annals of Physics*, vol. 321, no. 1, pp. 2–111, 2006.

[12] H. Stichtenoth, *Algebraic function fields and codes*, vol. 254. Springer Science & Business Media, 2009.

[13] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[14] M. Grassl, W. Geiselmann, and T. Beth, "Quantum reed—solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 13th International Symposium, AAECC-13 Honolulu, Hawaii, USA, November 15–19, 1999 Proceedings 13*, pp. 231–244, Springer, 1999.

[15] M. Grassl, T. Beth, and M. Roetteler, "On optimal quantum codes," *International Journal of Quantum Information*, vol. 2, no. 01, pp. 55–64, 2004.

[16] R. Li and X. Li, "Quantum codes constructed from binary cyclic codes," *International Journal of Quantum Information*, vol. 2, no. 02, pp. 265–272, 2004.

[17] K. Yang and P. V. Kumar, "On the true minimum distance of hermitian codes," in *Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17–21, 1991*, pp. 99–107, Springer, 1992.

[18] A. Garcia and R. Lax, "Goppa codes and weierstrass gaps," in *Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17–21, 1991*, pp. 33–42, Springer, 1992.

[19] J. H. v. L. Tom Høholdt and R. Pellikaan, "Algebraic geometry codes," 1998.

[20] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum codes from hermitian curves," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 16th International Symposium, AAECC-16, Las Vegas, NV, USA, February 20-24, 2006. Proceedings 16*, pp. 136–143, Springer, 2006.

[21] H. Stichtenoth, "Self-dual goppa codes," *Journal of Pure and Applied Algebra*, vol. 55, no. 1-2, pp. 199–211, 1988.

[22] M. Homma and S. J. Kim, "The complete determination of the minimum distance of two-point codes on a hermitian curve," *Designs, Codes and Cryptography*, vol. 40, no. 1, pp. 5–24, 2006.

[23] M. Homma and S. J. Kim, "Toward the determination of the minimum distance of two-point codes on a hermitian curve," *Designs, Codes and Cryptography*, vol. 37, no. 1, pp. 111–132, 2005.

[24] M. Homma and S. J. Kim, "The two-point codes on a hermitian curve with the designed minimum distance," *Designs, Codes and Cryptography*, vol. 38, pp. 55–81, 2006.

[25] M. Homma and S. J. Kim, "The two-point codes with the designed distance on a hermitian curve in even characteristic," *Designs, Codes and Cryptography*, vol. 39, pp. 375–386, 2006.

[26] S. Wesemeyer, "On the automorphism group of various goppa codes," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 630–643, 1998.

[27] S. Bouyuklieva, "A method for constructing self-dual codes with an automorphism of order 2," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 496–504, 2000.

[28] T. Shaska, "Quantum codes from algebraic curves with automorphisms," *Condensed Matter Physics*, vol. 11, p. 383, 2008.

[29] A. Steane, "Enlargement of calderbank-shor-steane quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.

[30] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," in *Proceedings of the 1999 IEEE Information Theory and Communications Workshop (Cat. No. 99EX253)*, pp. 127–, 1999.

[31] S. Ling, J. Luo, and C. Xing, "Generalization of steane's enlargement construction of quantum codes and applications," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 4080–4084, 2010.

[32] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of number theory*, vol. 61, no. 2, pp. 248–273, 1996.

[33] A. Wills, M.-H. Hsieh, and H. Yamasaki, "Constant-overhead magic state distillation," 2024.

[34] L. Golowich and V. Guruswami, "Asymptotically good quantum codes with transversal non-clifford gates," 2024.

[35] Q. T. Nguyen, "Good binary quantum codes with transversal ccz gate," 2024.

[36] M. Harned, P. V. Konda, F. S. Liu, N. Mudumbi, E. Y. Shao, and Z. Xiao, "Khovanov homology and quantum error-correcting codes," 2024.

[37] P. Panteleev and G. Kalachev, "Asymptotically good quantum and locally testable classical ldpc codes," in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 375–388, 2022.