STABILIZER CODES OVER FROBENIUS RINGS

A Thesis

by

SUSHMA NADELLA

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

May 2012

Major Subject: Computer Science

STABILIZER CODES OVER FROBENIUS RINGS

A Thesis

by

SUSHMA NADELLA

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Chair of Committee,	Andreas Klappenecker
Committee Members,	James Caverlee
	M. Suhail Zubairy
Head of Department,	Hank Walker

May 2012

Major Subject: Computer Science

ABSTRACT

Stabilizer Codes over Frobenius Rings. (May 2012)

Sushma Nadella, B.Tech., International Institute of Information Technology;

M.S., Texas A&M University

Chair of Advisory Committee: Dr. Andreas Klappenecker

In quantum information processing, the information is stored in the state of quantum mechanical systems. Since the interaction with the environment is unavoidable, there is a need for quantum error correction to protect the stored information. Until now, the methods for quantum error correction were mainly based on quantum codes that rely on the arithmetic in finite fields. In contrast, this thesis aims to develop a basic framework for quantum error correcting codes over a class of rings known as the Frobenius rings. This thesis focuses on developing the theory of stabilizer codes over the Frobenius rings and provides a systematic construction of codes over these rings. A special class of Frobenius rings called finite chain rings will be the emphasis of this thesis. The theory needed for comparing the minimum distance of stabilizer codes over the finite chain rings to that over the fields is studied in detail. This thesis finally derives that the minimum distance of stabilizer codes over finite chain rings cannot exceed the minimum distance over the fields.

To my family who are my greatest assets.

ACKNOWLEDGMENTS

This thesis would not have been possible without the support of many people. First and foremost I would like to express my deepest gratitude to my advisor Dr.Andreas Klappenecker whose guidance, support and assistance from the initial to the final phase has enabled me to successfully develop this thesis. I would like to thank my committee members, Dr.James Caverlee and Dr.M.Suhail Zubairy who have offered their assistance throughout this period. A special thanks to the NSF for their financial support for this project. Finally I would like to thank my family , who were there with me throughout my studies and motivated me to pursue masters degree. Last but not the least I would like to thank a special friend of mine, Ram for his love and persistent confidence in me. Thank you god for giving me all the strength that I needed.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURE Page

CHAPTER I

INTRODUCTION AND LITERATURE OVERVIEW

A. Introduction to Quantum Computing

This section deals with the basics that are needed to understand the quantum computing. Efforts are made to depict the differences between the classical computation and quantum computation. For detailed information, see [3].

1. Quantum Bits

A quantum bit is the basic information carrying structure in the quantum computer. A quantum bit has two clearly distinguishable states, $|0\rangle$ and $|1\rangle$ which correspond to the bits 0 and 1 in classical case. However, in addition to these states, a quantum bit can be present in an intermediate state that has no corresponding representation in the classical case. In general the state of the quantum bit is represented as $\alpha|0\rangle+\beta|1\rangle$ where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. In other words a quantum bit can be represented as a unit vector in a 2-dimensional complex vector space which has the basis $\{|0\rangle,\ |1\rangle\}$. It is customary to represent the quantum bits $|0\rangle, |1\rangle$ by the column vectors.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Generalizing to an n quantum bit quantum system, the basis of a n quantum bit system is generally denoted as $|000...00\rangle, |000...01\rangle, ...|111, ...11\rangle$. The state of a quantum

---

The journal model is *IEEE Transactions on Automatic Control.*

bit in an n quantum bit system is of the form,

$$\sum_{i \in {F_2}^n} a_i |i\rangle$$

where $F_2 = \{0, 1\}$, a_i is a complex number for all i $\in {F_2}^n$ and $\sum_{i \in {F_2}^n} |a_i|^2 = 1$.

2. Measurement

An important feature of a quantum bit is that we cannot determine the exact state of the quantum bit, i.e., the exact values of α and β cannot be examined. Measurement collapses the quantum bit into one of the basis states, thus destroying the state of the quantum bit. Suppose the state of quantum bit is $\alpha|0\rangle + \beta|1\rangle$, when this quantum bit is measured it collapses to state $|0\rangle$ with probability $|\alpha|^2$, or to state $|1\rangle$ with probability $|\beta|^2$.

3. Hilbert Space and Linear Operators

In addition to measurements that can be done on the quantum bit, there are operators which transform the state of the quantum bit, i.e., a operator acting on a quantum bit takes it from one normalized state to another normalized state [13]. In general, these operators need to be linear. Suppose x and y are two elements in $\mathbb{C}^m$ one can define a hermitian inner product on $\mathbb{C}^m$ as $\langle x|y\rangle = \overline{x_0}y_0 + \overline{x_1}y_1 + ... + \overline{x_{m-1}}y_{m-1}$. The norm $\| x \|$ of a vector $x \in \mathbb{C}^m$ is defined as $\| x \| = \sqrt{\langle x|x\rangle}$.

Suppose there is a linear operator U acting on the quantum bit as follows: $U|0\rangle = |\phi\rangle$ and $U|1\rangle = |\psi\rangle$, then the action of the linear operator on the quantum bit $\alpha|0\rangle + \beta|1\rangle$ is $\alpha|\phi\rangle + \beta|\psi\rangle$. Therefore U can be described as the 2x2 matrix that acts on a column vector which represents the quantum bit. A linear mapping that takes a unit vector in $\mathbb{C}^m$ to another unit vector in $\mathbb{C}^m$ is said to be a unitary mapping. The

necessary conditions for a linear map to be unitary is that, the operator U needs to be unitary, i.e., the matrix needs to satisfy the condition $UU^\dagger = I$. Such a unitary matrix satisfies, $\langle Ux|Uy\rangle = \langle x|y\rangle$ for all $x, y \in \mathbb{C}^m$. An operator that is frequently used in quantum systems is the projection operator. An operator P that maps an Hilbert space to another Hilbert space is called the projection operator if it satisfies the following conditions.

$$P = P^\dagger$$

$$P^2 = P$$

B. Error Correcting Codes

Error detection and correction are the important aspects of information and coding theory, which are universal in telecommunication applications. When data is transmitted over the network, it is often subject to bit errors. Therefore, we need techniques that identify these errors and correct them, removing the need to retransmit the whole data. Error detection helps to identify the correctness of the data transmitted by detecting such errors, whereas error correction helps in reconstructing the original data, thus saving time and money needed for retransmission. Thus designing efficient error correcting codes is very crucial for efficient transmission of data. The remainder of this section focuses on the basic concepts of the coding theory in the classical computation domain. Subsequently we discuss about quantum error correction and detail how it differs from the classical error correction. For more details refer to the book [1].

1. Classical Error Correction

Classical error correction deals with the design of the codes which detect and correct errors. For an easier understanding of error-correcting codes, it is convenient to impose an algebraic structure on them. Usually a finite field with q elements as the alphabet is considered and error-correcting codes have the structure of a vector space over the finite field. The elements of the vector space are called the vectors, and the operation on the code words is equivalent to the operations on the vectors in the vector space.

Typically a communication channel consists of the following stages, (see fig 1):

- Data to be transmitted is encoded using an encoding algorithm.
- The encoded data is sent through the transmission channel which is usually a noisy channel.
- Data is received at the receiver's side, which may be corrupted because of the bit errors.
- Data received is checked for any errors. (Error detection).
- Suitable error correction techniques are applied on the corrupted data and original data is restored.
- Data is decoded to give the original message that was initially sent by the sender.

By imposing an algebraic structure on the codes, each of the above 6 steps become fairly simple.

We will be using the following terminology (Refer to the book [2] for details.)

Vector Space : A vector space is a set that is closed under finite vector addition

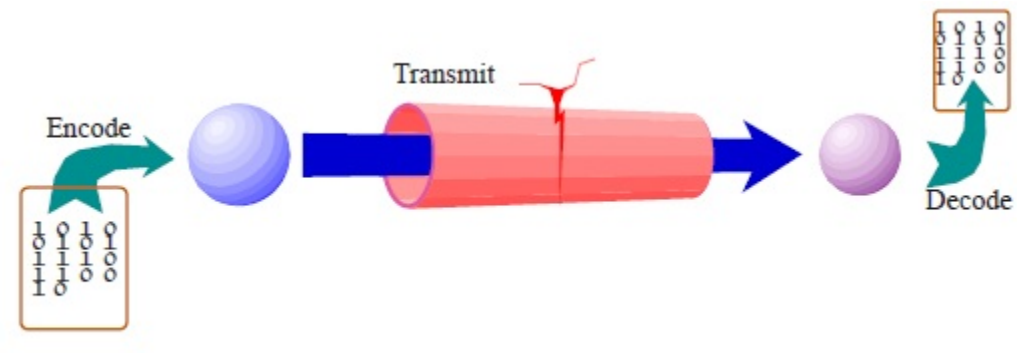

Fig. 1. Communication channel

and scalar multiplication. For a general vector space, the scalars are members of a field, in which case it is called a vector space over F.

Sub Space : A non-empty subset C of a vector space is a subspace if and only if C is closed under vector addition and scalar multiplication.

Linear Code : A linear code of length n over the field F is a subspace of F^n. Thus the words of code space F^n are vectors and we often refer to codewords as code vectors.

Hamming weight : The Hamming weight of a code word is the number of symbols different from the zero-symbol of the alphabet used.

Hamming distance : The Hamming distance between two code words is equal to the number of positions at which the corresponding symbols are different. It gives a measure of the number of the symbols that need to be changed to convert one code word to another code word.

Minimum distance : Minimum distance of a error correcting code is defined as the smallest distance between any two distinct code words.

2. Linear Codes

Let F be a finite field with q elements. A linear code C is defined as the k-dimensional subspace of ${F_q}^n$. The code is said to be an [n,k,d]-code where d is the minimum distance of the code. For a linear code, the minimum distance of the code is equal to the smallest of the weights of the non-zero codewords.

Encoding and Generator matrix: Let C be an $[n, k]$ code over F_q whose generator matrix is G. C contains q^k codewords each of which are distinct messages that need to be transmitted. Each of these messages are identified as k-tuples of ${F_q}^k$. Each message m is encoded as a codeword of length n which is obtained by multiplying the message with the generator matrix on the right. If $r_1, r_2, r_3...r_k$ denote the rows of the generator matrix then the encoded message is obtained as:

$$mG = \sum_{i=0}^{k} r_i m_i$$

mG is a codeword of C as it is formed as a linear combination of the rows of the generator matrix of C. This mapping maps the message codewords to a k-dimensional subspace of the n-dimensional space ${F_q}^n$.

Parity check Matrix and Dual Codes : For any two vectors u and v in ${F_q}^n$ inner product is defined as, $u.v = u_1v_1 + u_2v_2 + ... + u_nv_n$ which is an element of F_q. If $u.v = 0$, then the two vectors are called the orthogonal vectors. Suppose C is an [n,k] code with generator matrix G. Then $C^\perp$ is defined as the set of the vectors in ${F_q}^n$, such that each vector is orthogonal to all the vectors in C. In other words a vector v belongs to $C^\perp$ if and only if v is orthogonal to every vector of the generator matrix of C, i.e., $vG^T = 0$ where G^T denotes the transpose of G. If C denotes a $[n, k]$ code then $C^\perp$ has the parameters $[n, n - k]$. The generator matrix of the dual code $C^\perp$ forms the parity check matrix for the code C. A code with minimum distance

d has a parity check matrix in which any arbitrary set of d-1 columns are linearly independent.

Syndrome Decoding : The parity check matrix can be used for error detection as the parity check matrix nullifies all the code words in C, i.e., Hc=0 for all the codewords c in code C. Consider a vector u that is transmitted through a communication channel, that is corrupted with an error e which makes the vector u become $u' = u \oplus e$. When such a corrupted vector is multiplied with the parity check matrix H, we get the error syndrome, $Hu' = H(u \oplus e) = He$. If the syndrome $Hu' = 0$ then u' is a valid codeword. When the syndrome is non zero, then the transmitted code word must be corrupted. An important feature of the error syndrome is that it is independent of the codeword. It only depends on the error that occurred which makes error correction mechanism very natural. We can pre calculate the values of He', for all the possible values of e'. By having such a table, we can look up in the table of syndromes, and then calculate the corresponding error depending on the syndrome. Once the error is recognized, the codeword can be corrected as $u' \oplus e = u \oplus e \oplus e = u$.

3. Quantum Error Correction

Quantum systems are very sensitive to the environment and hence are quite error prone. The constant interference of the external environment with the quantum bits suggest that quantum error correction is essential. Consider a state of the quantum bit $\alpha|0\rangle + \beta|1\rangle$. Some of the aspects that make quantum error correction different from the classical error correction are:

- The values of the amplitudes α and β cannot be extracted from the quantum bit.

- As the no cloning theorem says the quantum bit cannot be cloned, thus making copying/redundancy not a suitable tool for error correction.

- Measurement alters the state of the quantum bit, which implies that any measurement of the quantum bit would destroy the information that is encoded in the superposition of the quantum bit. So error detection has to be carried out without extracting any information about the encoded state.

Unfortunately all the above do not allow the techniques of classical error correction to be readily applied to the quantum domain without substantial modification. Therefore, different mechanisms need to be developed to handle the delicate quantum states.

4. Criteria for Quantum Error Detection and Correction

Recall that the state of a n-bit non binary quantum system can be represented by a q^n dimensional complex vector space and the code is a q^k dimensional subspace of the q^n dimensional space. Each of the code words in the code space is a vector in the q^n dimensional space. A valid codeword refers to the codeword within the subspace encoded by the quantum code.

For the purpose of error detection, let us consider two code words x and y and let the error that is affecting the codewords be denoted by E. In general there are three kinds of errors that occur on the codewords. The first kind of errors that do not affect the codeword, i.e., $Ex = x$. Second kind of errors are those when they act on codeword, produce a codeword that is not present in the code, in other words such errors when they act on the codewords produce invalid codeword. The last kind of errors are the one's that act on one codeword and produce a different codeword that is present in the code, i.e., $Ea = b$ where a and b are the codewords in the code. The

first two kinds of errors are detectable and hence are called detectable errors, while the third kind of errors cannot be detected as it takes one valid codeword to another valid codeword. Hence the condition for an error E to be detected can be stated as; for distinct codewords x and y in the code $Ex \neq y$. Extending this to the criteria for quantum error detection we have that after an error E acts on the quantum bit, we must be able to distinguish the new state from all the distinct codewords, let $|i\rangle$ and $|j\rangle$ denote two quantum bits and E be the error acting on the quantum bit then we have the following.

An error E_i is detectable if and only if E_i satisfies the condition, $\langle j|E_i|i\rangle = C_i\delta_{ij}$. This is the necessary and sufficient condition for an error E_i to be detectable.
The above condition ensures this distinction thus making it also a sufficient condition for an error E to be detectable. See papers [15]

Error detection deals with individual errors, while error correction deals with the set of errors that a error correcting code can correct unlike individual errors. A set of errors E is correctable if it satisfies the condition that, for any two errors E_i and E_j in E, we have $E_i x \neq E_j y$. In other words we must be able to distinguish an error E_i acting on a codeword from an error E_j acting on a different codeword. Extending this to the quantum error correction we can say that the set E is correctable if for any two errors E_i and E_j in E, $E_j^\dagger E_i$ is detectable.

A set of errors E is correctable if and only if $\forall\ E_i, E_j\ \in E$ satisfies the condition, $\langle j|E_j^\dagger E_i|i\rangle = C_{ij}\delta_{ij}$. This is the necessary and sufficient condition for an error E to be correctable. By doing a linear transformation on the set of errors E, we can always find a newer set or basis E' such that, $E_i'C$ are mutually orthogonal. In this case error correction becomes apparent, as the steps to decoding would involve a measurement to see in which orthogonal space the quantum bit state is in and then accordingly apply the suitable inverse error operator and restore the state. (See [12])

C. Quantum Codes

A non binary quantum code that encodes k quantum bits into n quantum bits, has q^k basis codewords. The linear combination of the basis of the codewords is also a code word thus making the quantum code a vector space in its own right. Thus the code forms a q^k dimensional subspace of the q^n dimensional Hilbert space. Some of the earliest quantum codes that were constructed were the Shor's 9 bit code and the CSS codes. Stabilizer codes are the class of quantum error correcting codes that have gained popularity in the recent years, and they have become the interesting class of the quantum codes, ever since the earliest codes were compactly described using the stabilizer's formalism. The following section serves as introductory material for the stabilizer formalism in the latter sections.

1. Error Basis

The most common types of errors that affect the quantum bits are the

- **Bit flip Errors :** Errors which change the state $|0\rangle$ to $|1\rangle$ and vice-versa.
- **Phase flip Errors :** Errors which change the state $|0\rangle + |1\rangle$ *to* $|0\rangle - |1\rangle$ and vice-versa.
- **Bit and phase flip Errors :** A combination of both bit and phase flip errors.

Any error E acting on a quantum bit can be represented as a linear combination of bit-flip, phase-flip and bit-phase-flip errors. If we can correct errors E_1 and E_2, then we can correct the errors $aE_1 + bE_2$ which is possible because of the linear property of the quantum mechanics. Therefore if we can correct the basis of errors, then since any error can be written as a linear combination of the error basis, we can correct all the errors that occur. Error acting on the quantum bit is nothing

but a linear operator that takes the quantum bit from one state to another. The set of linear operators acting on the Hilbert space V is also a vector space L_v. If the Hilbert space has dimension d, then the space L_v has dimension d^2. Thus there are d^2 linear independent operators that form the basis of the operator space. The most commonly used error basis on a single quantum bit which is a 2-dimensional Hilbert space consists of the following 4 matrices.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_z = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

These matrices are together called the Pauli matrices. Extending the concept of the error basis to higher dimension p^m, [6], [7], the linear span of the error basis should, cover the whole set of linear operators, which implies the error basis should have p^{2m} elements. Let us denote this basis as $E_1, E_2, ..., E_{p^{2m}}$. The state of the n bit quantum system can be affected by the error operator of the form

$$e_1 \otimes e_2 \otimes ... \otimes e_n \tag{1.1}$$

where $e_i \in \{E_1, E_2, ..., E_{p^{2m}}\}$. Any general operator on a n dimensional $p^m - ary$ quantum system can be formed as a linear operator acting on the n fold tensor product

of individual $p^m - ary$ quantum system. Thus any general operator can be written as a linear combination of the operators of the form (1.1), thus making (1.1) as the error basis for the n dimensional $p^m - ary$ quantum system. An error basis is called a nice error basis if it satisfies the following conditions:

- It contains the identity matrix.
- Product of any two elements should be a scalar multiple of some element of the error basis.
- For any two distinct elements A and B of E, $\mathrm{tr}(A^\dagger B) = 0$.

The error basis

$$E = \{e_1 \otimes e_2 \otimes ... \otimes e_n | e_i \ \in \ \{E_1, E_2, ..., E_{p^{2m}}\}\} \tag{1.2}$$

is a nice error basis on the complex vector space C^{q^n} where $q = p^m$.

2. Stabilizer Codes

Stabilizer codes form the important class of quantum error correcting codes. Their importance lies in the fact that they are easier to understand than the arbitrary quantum codes and also have a close relation to the classical codes. Thus they serve as handy tools in understanding many of the quantum error correcting codes. They were first formulated by Daniel Gottesman [12]. Understanding the stabilizer formalism aids in understanding the construction of stabilizer codes. Error basis and the error group form the fundamental concepts of the stabilizer formalism. A stabilizer code is defined as the q^k dimensional subspace of the q^n dimensional Hilbert space which has the property that all the codewords remain invariant under the action of certain pauli operators. In other words all the code words are stabilized by few of the error

operators and hence the name stabilizer codes. Stabilizer codes are characterized by the Pauli operators that stabilize them. Before proceeding further, here are some special properties of the error operators.

- All error operators either commute or anti commute with each other i.e. either AB = BA or AB = -BA.
- All the operators have eigen values of +1 or -1.
- All the operators square to Identity i.e. $E^2 = \pm I$.

To understand how the error group and stabilizer code are related, a peek into definition of the mathematical structure, group is needed. A group G is defined as a collection of elements with binary operation, '.', which satisfies the following properties.

- For any two elements a and b of the group G, a.b $\in$ G.
- There exists an identity element i in the group such that a.i = i.a = a.
- For every element a there exists an inverse a^{-1} such that $a.a^{-1} = a^{-1}.a = i$.

Let G_n be the group generated by the nice error basis E. By including all the scalar multiples of the elements of the error basis, closure property of the group will be satisfied making G_n, a complete error group. A physics free introduction to error groups and quantum error correction can be found here, [8].

$$G_n = \{Group\ generated\ by\ the\ nice\ error\ basis\}.$$

This group is called the error group, that is generated by the nice error basis. Let S be the set of operators that stabilize the code C by which we mean for any operator A in S we have Ac = c for all codewords c $\in$ C. Notice that all the operators

in S need to commute with each other. Consider two operators A and B in S. If they do not commute we have ϕ = AB$|\phi\rangle$ = -BA$|\phi\rangle$ = -ϕ, which implies $\phi = 0$. Hence, this enforces the condition that all the error operators in the set S need to commute with each other without which the code space would only contain the zero codeword [16]. Thus S needs to be an abelian subgroup of the error group G_n. Recognizing the subgroup of the error group that stabilizes the code defines the stabilizer code.

Stabilizer code is defined as follows:

$$Q = \bigcap_{A \in S} \{|\phi\rangle \mid A|\phi\rangle = |\phi\rangle\}. \tag{1.3}$$

for some subgroup S of G_n. Thus the stabilizer code (1.3), is defined as the +1 joint eigenspace of the elements of the subgroup S of the error group G_n. The stabilizer code should exhaust all the vectors of the +1 joint eigenspace of S. If it does not then code Q does not form a stabilizer code.

Consider the set of operators which commute with all the elements of the stabilizer group S which is called the centralizer of the stabilizer group. Centralizer C contains the stabilizer group, because of the way the stabilizer group was formed (Abelian subgroup). Any operator outside this centralizer would anti-commute with at least one element of the group S. As told earlier the criteria for the set of errors E to be correctable by the code is that $E_j^\dagger E_i$ needs to be detectable for all $E_i, E_j \in E$.

1. If E_i, E_j are from the set S we have
   $\langle j|E_j^\dagger E_i|i\rangle = \langle j||i\rangle = \delta_{ij}$, thus making $E_j^\dagger E_i$ detectable.

2. If E_i, E_j are from outside the centralizer C, we have at least one operator from S that anti commutes with these errors,
   $\langle j|E_j^\dagger E_i|i\rangle = \langle j|E_j^\dagger E_i E|i\rangle$ = - $\langle j|EE_j^\dagger E_i|i\rangle$ = -$\langle j|E_j^\dagger E_i|i\rangle$ which implies $\langle j|E_j^\dagger E_i|i\rangle =$ 0 proving $E_j^\dagger E_i$ detectable.

3. If E_i, E_j are from C\S then we may not be able to correct these errors.

Thus we have established a condition on the kind of errors that are correctable by the stabilizer code. Having established the conditions, we now move to the section where the relation between the stabilizer codes and the classical codes becomes apparent.

3. Relation to Classical Codes

This section helps in deriving the relation between the stabilizer codes and the binary classical codes. To understand the relation we need to understand a crucial concept of commutativity of operators of the error group. Let $X_a = X(a_1, a_2, ..., a_n)$ denote the error operator $X^{a_1} \otimes X^{a_2} \otimes ... \otimes X^{a_n}$ acting on a n-bit quantum state. For example X(001) denotes the error operator $X^0 \otimes X^0 \otimes X^1$, i.e., $I \otimes I \otimes X$ acting on the 3 quantum bits. Similarly let $Z_b = Z(b_1, b_2, ..., b_n)$ denote the error operator $Z^{b_1} \otimes Z^{b_2} \otimes ... \otimes Z^{b_n}$. Any error operator can be represented as $X_a Z_b = X^{a_1} Z^{b_1} \otimes X^{a_2} Z^{b_2} \otimes ... X^{a_n} Z^{b_n}$.

Now consider two error operators $E_1 = X_a Z_b$ and $E_2 = X_{a'} Z_{b'}$. These two operators commute when $E_1 E_2 = E_2 E_1$. Now we have,

$$E_1 E_2 = (X_a Z_b)(X_{a'} Z_{b'}) = (-1)^{b.a'} X_{a+a'} Z_{b+b'} \tag{1.4}$$

$$E_2 E_1 = (X_{a'} Z_{b'})(X_a Z_b) = (-1)^{b'.a} X_{a+a'} Z_{b+b'} \tag{1.5}$$

Recall that XZ = -ZX which is the reason we get (-1) factor in equations (1.4) and (1.5). Hence if the two operators need to commute we need to have the condition $b.a' + b'.a = 0 \ mod \ 2$. However this commutativity condition slightly varies for the non-binary stabilizer codes. A complete theory of non-binary stabilizer codes has been formulated and studied in detail which can be found at [5]. For the purpose of understanding the theory let us stick to the binary case. The relation between stabilizer codes and classical codes stems from the fact that errors in the error group

can be characterized by the classical codes. Let us represent $X_a Z_b$ by a vector $(a|b)$. Notice that the multiplication of the operators in the error group transforms to the addition of the vectors $(a|b)$ and $(a'|b')$. Thus the stabilizer group S can now be represented as,

$$C = \{(a|b)|X_a Z_b \in S\}$$

Accordingly the centralizer which is the set of operators that commute with every element of S has an equivalent representation which is given by,

$$C' = \{(a'|b')|b.a' + b'.a = 0 \ mod \ 2 \ \forall \ (a|b) \in C\}$$

Thus C needs to have the property that any two vectors in it are closed under vector addition, which makes C the additive code and accordingly C' to be the dual of C with respect to the new inner product defined as $\langle (a|b), (a'|b') \rangle = b.a' + b'.a \ mod \ 2$. Since stabilizer is contained in the centralizer, C' should be a code which contains its dual C. Thus a additive code C' which is self orthogonal with respect to the above inner product precisely describes the stabilizer S of the quantum code Q. The generator matrix of the code C' describes the generators of the stabilizer thus establishing the relation between the classical codes and the binary stabilizer codes.

CHAPTER II

CODES OVER FROBENIUS RINGS

A. Introduction

In classical coding theory, there has been an upsurge of interest in codes over rings, since nonlinear binary codes have been realized as the gray images of linear Z_4 codes about a decade ago. The most natural class of rings that is suitable for coding theory is given by finite Frobenius rings, since they allow one to formulate the concept of dual codes as in the case of codes over finite fields. Codes over Frobenius rings form the largest class of codes over the rings. Arithmetic over the rings is much simpler when compared to the arithmetic over the fields. Hence if we can generalize most of the properties of codes over fields to rings, it would be great asset for further construction of codes over rings as it might involve a simpler arithmetic than the one's over field. Earlier works have concentrated on the classical codes over finite chain rings [9], where results were established comparing the minimum distance of the codes over rings to that of the minimum distance of the codes over the fields. Considering this as the main source of relating codes over rings to those over fields, we have tried to make similar comparisons of the quantum codes over rings to those over fields. This section provides a basic introduction to linear codes over rings.

Let R denote a finite ring with identity. A code C over the ring R is a subset of R^n module of rank n. Any additive subgroup C of R^n is called as the additive code. A code is called linear if it is a R-submodule of the R^n free module. For any two vectors u and v in the code space C, inner product is defined as:

$$(u, v) = \sum_i u_i v_i$$

The Dual $C^{\perp}$ of the code C, is defined as $C^{\perp} = \{w|(u,w) = 0 \ \forall \ u \in C\}$. The rank of code C has similar notion to that of dimension of code C over the finite fields. The rank of a code C is defined as the minimum number of generators of the code C. The free rank of the code C is defined as the maximum rank of the free sub-modules of the code C. A code is called a free R-submodule when its rank is equal to its free rank. In other words a free code is isomorphic to the R-module R^k for some k. For rest of the work in this chapter code refers to a linear code over the ring and when a code is free, it is referred to as the free code over the ring.

B. Frobenius Rings

Let R be a finite ring with identity. The character group of the additive group of R is denoted by $\hat{R} := \mathrm{Hom}_z(R, C^{\times})$. This group has the structure of an R-R bimodule by defining $\chi^r(x) := \chi(rx)$ and ${}^r\chi(x) := \chi(xr)$ for all $r, x \ \epsilon R$, and for all $\chi \in \hat{R}$. A finite ring R is called a Frobenius ring if ${}_R\hat{R} \cong_R R$. A character χ is called a generating character if for every $\phi \ \in \ \hat{R}$, there exists a $r \ \in R$, such that $\phi =^r \chi(x)$. A finite ring is Frobenius if and only if it admits a right or left generating character, Cf. [14].

Here are some of the examples of Frobenius rings:

i) A finite field F is a Frobenius rings with generating character being defined as, $\chi(a) = \exp^{2\pi i \, \mathrm{tr}(a)/p}$, where tr denotes the map from $F \ \rightarrow \ F_p$ and F_p denotes the prime subfield.

ii) The ring of integers mod m, denoted as R = Z/(m), belongs to this class of rings, with generating character defined as follows. Let $\xi = \exp(2\pi i/m)$. Then $\chi(x) = \xi^x, \ x \in Z/(m)$, is a generating character.

iii) The direct sum of Frobenius rings is also a Frobenius ring. If $R_1, R_2, R_3, ..., R_n$

each have generating characters $\chi_1, \chi_2, ..., \chi_n$ then ring R has the generating character $\chi = \prod \chi_i$.

iv) A Galois ring which is a Frobenius ring is a Galois extension of $\mathbb{Z}/(p^n)$, and is given by GR(p^n,r) = $\mathbb{Z}/(p^n)$ [X]/(f) where $f \in \mathbb{Z}/(p^n)$ is a monic irreducible polynomial of degree r. Because f is monic any element can be represented by a polynomial $\sum_{i=1}^{r} a_i X^{r-i}$ where $a_i \in \mathbb{Z}/(p^n)$. Let $\xi = \exp(2\pi i/p^n)$. Then $\chi(a) = \xi^{a1}$ is a generating character.

The following sections focus on developing the theory of stabilizer codes over the Frobenius rings. The concept of an error basis is first studied in detail which is the foundation, for the rest of the theory. Following this, the conditions for error detection are proved, which involves a special type of inner product, whose structure and properties are detailed in the following sections. The connection of stabilizer codes to classical codes are established in a theorem which lays out the conditions for the existence of the stabilizer code over the ring. The CSS construction of stabilizer codes which describes the construction of stabilizer codes from the classical codes is stated. Subsequently we restrict our attention to the finite chain rings to get good estimates for the minimum distance of stabilizer codes over such rings. For details about non-binary stabilizer codes over finite fields refer to [5].

C. Discretization

Let R be a finite ring with q elements. Let B denote an orthonormal basis of $\mathbf{C}^q$ with respect to the usual hermitian inner product. We use the Dirac ket notation and label the elements of the basis B by ring elements so that

$$B = \{|x\rangle \,|\, x \in R\}.$$

The addition and multiplication in the ring R will be used to define unitary shift and multiplication operators on $\mathbf{C}^q$. Indeed, for each a in R, we define a shift operator $X(a)\colon \mathbf{C}^q \to \mathbf{C}^q$ by

$$X(a)|x\rangle = |x + a\rangle$$

for all x in R. Let χ be an irreducible character of the additive abelian group $(R, +)$. For each b in R, we define a multiplication operator $Z(b)\colon \mathbf{C}^q \to \mathbf{C}^q$ by

$$Z(b)|x\rangle = \chi(bx)|x\rangle,$$

for all x in R.

Let us consider the normalized Hilbert-Schmidt inner product on the set of linear operators of $\mathbf{C}^q$,

$$\langle A \mid B\rangle = \frac{1}{q}\operatorname{tr}(A^\dagger B),$$

where tr denotes the trace of a matrix, and $A^\dagger$ is the adjoint of the operator A. Our goal is to determine when the set

$$\mathcal{E} = \{X(a)Z(b) \mid a, b \in R\}$$

forms an orthonormal basis of the set of linear operators on $\mathbf{C}^q$.

Given a character χ of the additive group $(R, +)$ and a ring element b in R, we observe that

$$\chi_b(x) := \chi(bx)$$

is again a character of $(R, +)$.

Proposition 1. *The operators $\mathcal{E} = \{X(a)Z(b) \,|\, a, b \in R\}$ form an orthonormal basis with respect to the normalized Hilbert-Schmidt inner product if and only if $\mathcal{C} = \{\chi_b \,|\, b \in R\}$ is the set of all irreducible characters of the additive group $(R, +)$.*

Proof. For a, b, a', b' in R, we have

$$\mathrm{tr}((X(a')Z(b'))^\dagger X(a)Z(b)) = \begin{cases} 0 & \text{if } a \neq a' \\ \sum_{x \in R} \overline{\chi(b'x)}\chi(bx) = \langle \chi_{b'} \,|\, \chi_b \rangle & \text{if } a = a' \ . \end{cases}$$

It follows that if $\mathcal{E}$ is an orthonormal basis, then the characters in $\mathcal{C}$ are pairwise orthogonal irreducible characters of $(R, +)$.

Conversely, suppose that $\mathcal{C}$ is the set of all irreducible characters of $(R, +)$. This implies that the characters χ_b and $\chi_{b'}$ are orthogonal when $b \neq b'$. It follows that $\mathcal{E}$ is an orthonormal basis. □

Let R be a finite ring. We denote by $\mathrm{Irr}(R) = \mathrm{Hom}((R, +), \mathbf{C}^\times)$ the set of irreducible characters of the additive group $(R, +)$. We say that an irreducible character χ of $(R, +)$ is generating if and only if $\mathrm{Irr}(R) = \{\chi_b \,|\, b \in R\}$, where $\chi_b(x) = \chi(bx)$ for all x in R. A finite ring R does not necessarily have a generating character. We call a ring nice if and only if it has a generating character. From the definition of Frobenius rings which says a ring is Frobenius if and only if it admits a left or a right generating character it implies that a Frobenius ring is a nice ring. Thus for a Frobenius ring, the operators $X(a)Z(b)$ form an orthonormal basis.

Lemma 2. *The set* $E = \{X(a)Z(b) | a, b \in R\}$ *is a nice error basis on* $\mathbb{C}^q$

Proof. The operator X(0)Z(0) is the identity operator which belongs to E. The product of any two operators $X(a)Z(b)$, $X(a')Z(b')$ is a scalar multiple of some operator in E. $X(a)Z(b)X(a')Z(b') = \chi(ba')X(a + a')Z(b + b')$, which proves the second property of the nice error basis. (Refer to the definition of nice error basis in chapter-1 1). The above proposition proves the third property that $Tr(A^\dagger B) = 0$ for distinct $A = X(a)Z(b)$ and $B = X(a')Z(b')$. Hence the above set is a nice error basis. □

D. Bilinear Forms

Let $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in R^n. By slight abuse of notation, we define shift and multiplication operators on n quantum system with state space $\mathbf{C}^q \otimes \cdots \otimes \mathbf{C}^q \cong \mathbf{C}^{q^n}$ by

$$\begin{aligned} X(a) &= X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n), \\ Z(b) &= Z(b_1) \otimes Z(b_2) \otimes \cdots \otimes Z(b_n). \end{aligned}$$

Having defined the operators on the space $\mathbb{C}^{q^n}$, and the proof for nice error basis above we state the following corollary.

Corollary 3. *The set* $E = \{X(a)Z(b)|a, b \in R^n\}$ *is a nice error basis on* $\mathbb{C}^{q^n}$.

Now let us consider the error group generated by the the nice error basis above. By including all the scalar multiples of the operators of the error basis, we get the error group generated by it which is as follows

$$G_n = \{\chi(c)X(a)Z(b)|a, b \in R^n, c \in R\}$$

As stated earlier, all the elements of error group either commute or anti-commute with, each other. If we can establish the condition for two error operators to commute with each other, it will help in characterization of the errors in terms of the classical codes thus establishing the relation between the stabilizer codes and classical codes.

Proposition 4. *Let* R *be a nice ring with generating character* χ. *Let* a, b *and* a', b' *be elements of* R^n. *Then the operators* $X(a)Z(b)$ *and* $X(a')Z(b')$ *of the error group commute if and only if*

$$\chi(b \cdot a' - b' \cdot a) = 1.$$

Proof. For any $x \in R^n$, we have $X(a)Z(b)|x\rangle = X(a)\chi(b \cdot x)|x\rangle = \chi(b \cdot x)|x + a\rangle$, and $Z(b)X(a)|x\rangle = Z(b)|x + a\rangle = \chi(b \cdot x)\chi(b \cdot a)|x + a\rangle$, hence

$$\chi(b \cdot a)X(a)Z(b) = Z(b)X(a).$$

It follows that

$$X(a)Z(b)X(a')Z(b') = \chi(b \cdot a')X(a + a')Z(b + b')$$

and

$$X(a')Z(b')X(a)Z(b) = \chi(b' \cdot a)X(a + a')Z(b + b').$$

Therefore, we can conclude that $X(a)Z(b)$ and $X(a')Z(b')$ commute if and only if $\chi(b \cdot a' - b' \cdot a) = 1$, as claimed. □

Consider the additive group of the ring R. For each character χ in $\mathrm{Hom}(R, \mathbf{C}^\times)$ there exists a unique function ψ in $\mathrm{Hom}(R, \mathbf{Q}/\mathbf{Z})$ such that

$$\chi(x) = \exp(2\pi i \psi(x)).$$

We can define a form $\langle \cdot \,|\, \cdot \rangle_\chi \colon R^{2n} \times R^{2n} \to \mathbf{Q}/\mathbf{Z}$ such that

$$\langle (a|b) \,|\, (a'|b') \rangle_\chi = \psi(b \cdot a' - b' \cdot a)$$

for all $(a|b)$ and $(a'|b')$ in R^{2n}.

The properties (1), (2), and (3) of the next lemma show that $\langle \cdot \,|\, \cdot \rangle_\chi$ is a $\mathbf{Z}$-bilinear form, and the properties (4) and (5) show that the form is left- and right nondegenerate.

Lemma 5. *Let R be a nice ring with generating character χ. Then*

(1) $\langle u_1 + u_2 \,|\, v \rangle_\chi = \langle u_1 \,|\, v \rangle_\chi + \langle u_2 \,|\, v \rangle_\chi$

(2) $\langle u \,|\, v_1 + v_2 \rangle_\chi = \langle u \,|\, v_1 \rangle_\chi + \langle u \,|\, v_2 \rangle_\chi$

(3) $\langle nu \,|\, v \rangle_\chi = \langle u \,|\, nv \rangle_\chi = n \langle u \,|\, v \rangle_\chi$

holds for all u_1, u_2, v and u, v_1, v_2 in R^{2n}, and all n in $\mathbf{Z}$. Furthermore,

(4) if $\langle u \,|\, v \rangle_\chi = 0$ holds for all v in R^{2n}, then $u = 0$.

(5) if $\langle u \,|\, v \rangle_\chi = 0$ holds for all u in R^{2n}, then $v = 0$.

Proof. The properties (1), (2), and (3) follow from the biadditivity of the dot product, the distributive law, and the fact that ψ is a homomorphism.

To prove property (4), consider an element $u = (u_0, \ldots, u_{n-1}|u_n, \ldots, u_{2n-1})$ in R^{2n}. Seeking a contradiction, suppose that $u \neq 0$ but $\langle u \,|\, v \rangle_\chi = 0$ holds for all v in R^{2n}. Let i be the smallest index such that $u_i \neq 0$. Let d_i denote the element in R^{2n} that takes the value 1 at coordinate $i + n \pmod{2n}$ and is 0 everywhere else. Then $\langle u \,|\, d_i r \rangle_\chi = 0$ for all r in R shows that (i) the left ideal Ru_i must be contained in the kernel of χ if i is in the range $0 \leq i \leq n-1$; (ii) the right ideal $u_i R$ must be contained in the kernel of χ if i is in the range $n \leq i \leq 2n-1$. Since χ is a generating character, any right or left ideal contained in the kernel of χ must be $\{0\}$, so u_i must be 0, contradicting our assumption that $u \neq 0$.

The property (5) can be proved in a similar way. □

We call u and v in R^{2n} orthogonal if and only if $\langle u \,|\, v \rangle_\chi = 0$. We denote by $u \perp v$ that u and v are orthogonal. Let S be subset of R^{2n}. We denote by $S^\perp$ the set

$$S^\perp = \{u \in R^{2n} \,|\, \langle s \,|\, u \rangle_\chi = 0 \text{ for all } s \in S\}$$

and by ${}^\perp S$ the set

$${}^\perp S = \{u \in R^{2n} \,|\, \langle u \,|\, s \rangle_\chi = 0 \text{ for all } s \in S\}.$$

In addition to $\langle \cdot \,|\, \cdot \rangle_\chi$, it will be convenient to define a form $\langle \cdot \,|\, \cdot \rangle_s \colon R^{2n} \times R^{2n} \to R$ by

$$\langle (a|b) \,|\, (a'|b') \rangle_s = b \cdot a' - b' \cdot a.$$

The forms are related as follows:

$$\chi(\langle u \,|\, v \rangle_s) = \chi(b \cdot a' - b' \cdot a) = \exp(2\pi i \langle u \,|\, v \rangle_\chi).$$

These bilinear forms have defined the new inner product between the two vectors u and v given by $\langle u \,|\, v \rangle_\chi$, which we call as the symplectic inner product. We now derive the properties of the cardinality of the dual code of C, i.e., $C^\perp$ which consists of all the codewords that are orthogonal to every codeword in C with respect to the symplectic inner product. The following lemma establishes the relationship between the cardinality of code C and its dual $C^\perp$.

Lemma 6. *Let R be a nice ring with generating character χ. Let C be a subgroup of $(R^{2n}, +)$. Then*

$$|C|\,|C^\perp| = |R^{2n}| \quad \textit{and} \quad |C|\,|{}^\perp C| = |R^{2n}|$$

Proof. For each v in R^{2n}, the map $\Phi_v \colon R^{2n} \to \mathbf{C}$ given by

$$\Phi_v(x) = \chi(\langle x \,|\, v \rangle_s) = \exp(2\pi i \langle x \,|\, v \rangle_\chi)$$

is an irreducible character of $(R^{2n}, +)$. The set $\{\Phi_v \mid v \in R^{2n}\}$ actually contains all irreducible characters of $(R^{2n}, +)$, since it follows from Lemma 5 (5) that $\Phi_v = \Phi_{v'}$ if and only if $v = v'$.

The set of characters of $(R^{2n}, +)$ that are equal to 1 when restricted to C is given by

$$\{\Phi_v \mid v \in C^\perp\},$$

hence there are precisely $|C^\perp|$ such characters. On the other hand, the characters of $(R^{2n}, +)$ that are equal to 1 when restricted to C correspond to the inflations of characters of the quotient group R^{2n}/C, hence there are $[R^{2n} \colon C]$ such characters. Therefore, we have $|C||C^\perp| = |C|[R^{2n} : C] = |R^{2n}|$, as claimed.

One can show that $|C|\,|{}^\perp C| = |R^{2n}|$ in a similar way. □

The above proofs take into account that C and $C^\perp$ are not necessarily linear codes, they can be any additive subgroup of R^{2n}. Often, linear codes are of interest to

us and many results in the literature have been established, taking into consideration the linear codes. So we also restrict ourselves to linear codes often and make use of the theory of the well established linear codes over fields. This would not destroy any of the previous theory we have stated since every linear code is an additive code. Likewise if we impose C to be linear, which is when C is a submodule of the R^{2n} module, we have an additional result that relates the the codes $C^{\perp}$ and $C^{\perp_s}$. The following lemma establishes this result.

Lemma 7. *Let R be a finite (commutative) chain ring with generating character χ. Let C and D be R-submodules of R^{2n}. Then*

$$C \perp D \quad \text{if and only if} \quad C \perp_s D.$$

Proof. It follows from the definitions that $C \perp_s D$ implies $C \perp D$.

Conversely, suppose that $C \perp D$. Let x in C and y in D be arbitrary elements. Since C is a module, rx in C for all r in R. Since $\langle \cdot \,|\, \cdot \rangle_s$ is a bilinear R-form when R is a commutative ring, we have $1 = \chi(\langle rx \,|\, y\rangle_s) = \chi(r\langle x \,|\, y\rangle_s) = \chi_r(\langle x \,|\, y\rangle_s$ for all r in R. As χ is a generating character, this means that $\langle x \,|\, y\rangle_s$ is in the kernel of all irreducible characters of $(R, +)$, and therefore $\langle x \,|\, y\rangle_s = 0$. This proves that $C \perp D$ implies that $C \perp_s D$. □

E. Stabilizer Codes

Let R be a nice ring and n a positive integer. Suppose that the group

$$\langle X(a)Z(b) \,|\, a, b \in R^n \rangle$$

has exponent m. Let ω denote a primitive mth root of unity, $\omega = \exp(2\pi i/m)$. We define the error group G_n generated by the operators $X(a)Z(b)$, $a, b \in R^n$, as

$$G_n = \langle \omega^c X(a)Z(b) \,|\, a, b \in R^n, c \in \mathbf{Z} \rangle.$$

The center $Z(G_n)$ of the group G_n is given by $Z(G_n) = \{\omega^c 1 \,|\, c \in \mathbf{Z}\}$, a group of order m.

We define the weight $\mathrm{wt}(g)$ of an element g in G_n to be the number of non-scalar tensor components of g. For $(a|b)$ in R^{2n}, we define its symplectic weight $\mathrm{swt}((a|b))$ to be the number of indices i such that $a_i \neq 0$ or $b_i \neq 0$. It follows from these definitions that

$$\mathrm{wt}(\omega^c X(a)Z(b)) = \mathrm{swt}((a|b)).$$

Let R be a ring with q elements. Let S be a subgroup of G_n. The stabilizer code $\mathrm{Fix}(S)$ associated with S is given by

$$\mathrm{Fix}(S) = \{v \in \mathbf{C}^{q^n} \,|\, Ev = v \text{ for all } E \in S\}.$$

In general, a quantum code Q is a subspace of $\mathbf{C}^{q^n}$. We call Q a stabilizer code if and only if there exists a subgroup S of G_n such that $\mathrm{Fix}(S) = Q$.

Theorem 8. *An $((n, K, d))_R$ stabilizer code exists if and only if there exists an additive code $C \leq R^{2n}$ of size $|C| = |R|^n/K$ such that $C \leq C^\perp$ and $\mathrm{swt}(C^\perp \setminus C) = d$ if $K > 1$, and $\mathrm{swt}(\mathbf{C}^\perp - \{0\}) = d$ if $K = 1$.*

Proof. Suppose that an $((n, K, d))_R$ stabilizer code Q exists. This implies that there exists a subgroup S of G_n of order $|R|^n/K$ such that $\mathrm{Fix}(S) = Q$. Let C be the subgroup of R^{2n} given by $C \cong SZ(G_n)/Z(G_n)$. Then $|C| = |S| = |R|^n/K$. We have $C^\perp \cong C_{G_n}(S)/Z(G_n)$. Since S is an abelian group, we have $SZ(G_n) \leq C_{G_n}(S)$, and hence $C \leq C^\perp$. The weight of an element $\omega^c X(a)Z(b)$ is equal to the $\mathrm{swt}(a|b)$. If

$K = 1$ then Q is a pure quantum code, thus $\mathrm{wt}(C_{G_n}(S) \backslash Z(G_n)) = \mathrm{swt}(C^{\perp} - \{0\}) = d$. If $K > 1$, then the elements of $C_{G_n}(S) \setminus SZ(G_n)$ have at least weight d so that $\mathrm{swt}(C^{\perp} \setminus C) = d$.

Conversely, suppose that C is an additive code of R^{2n} such that $|C| = |R|^n/K$, $C \leq C^{\perp}$, and $\mathrm{swt}(C^{\perp} \backslash C) = d$ if $K > 1$, and $\mathrm{swt}(C^{\perp} - \{0\}) = d$ if K=1. Let $N = \{\omega^c X(a) Z(b) | c \in \mathbf{Z} \text{ and } (a|b) \in C\}$. This is an abelian normal subgroup of the group G_n; indeed, it is normal because it is the pre-image of $C = N/Z(G_n)$, and abelian since C is self-orthogonal.

Choose a character ϕ of N such that $\phi(\omega^c 1) = \omega^c$ for $c \in \mathbf{Z}$. Then

$$P_N = \frac{1}{N} \sum_{E \in N} \phi(E^{-1}) E$$

is an orthogonal projector onto a vector space Q, because P_N is idempotent in the group ring $\mathbf{C}[G_n]$. We have

$$\dim Q = \mathrm{Tr}\, P_N = |Z(G_n)||R^n|/|N| = |R^n|/|C| = K.$$

Each coset of N modulo $Z(G_n)$ contains exactly one matrix E such that $Ev = v$ for all v in Q. Let $S = \{E \in N | Ev = v \text{ for all } \in Q\}$. Then S is an abelian subgroup of G_n and its order is given by $|S| = |C| = |R|^n/K$. The vector space Q is clearly a subspace of $\mathrm{Fix}(S)$ and $\dim Q = |R|^n/|S|$, hence $Q = \mathrm{Fix}(S)$.

If $K > 1$, then an element $\omega^c X(a) Z(b)$ in $C_{G_n} \backslash SZ(G_n)$ cannot have weight less than d, because this would imply that $(a|b) \in C$ which is not possible. If $K = 1$, then the same follows for $K = 1$. Hence Q is an $((n, K, d))_R$ stabilizer code. □

We now proceed to the construction of a stabilizer code, from an existing classical code over the ring R. The CSS construction allows for this construction, which involves the self orthogonal codes over the rings. The following section gives the lemmas for

these constructions. There exists a simple class of CSS codes, in which a CSS code is specified by a classical code, say C satisfying certain conditions on orthogonality. The construction of the quantum CSS code over the Frobenius ring is mentioned in the below lemma.

Lemma 9. *CSS Code Construction.Let C_1 and C_2 denote two classical linear codes with parameters $[n, k_1, d_1]_r$ and $[n, k_2, d_2]_r$ such that $C_2^{\perp} \leq C_1$. Then there exists a $[[n, k1+k2-n, d]]_r$ stabilizer code with minimum distance $d = min\{wt(c)|c \, \epsilon \, (C_1 \backslash C_2^{\perp}) \cup (C_2 \backslash C_1^{\perp})\}$ that is pure to $min\{d_1, d_2\}$.*

Proof. Let C=$C_1^{\perp} X C_2^{\perp} \leq R^{2n}$. If $(c_x|c_z)$ and $(c'_x|c'_z)$ are two codewords in C then $(c_z.c'_x - c'_z.c_x) = 0$ and since 0 which is trivial lies in the kernel of all the characters, we have $\chi_r(c_z.c'_x - c'_z.c_x) = 1$. Therefore $C \leq C^{\perp_s}$. Since the cartesian product C has $|R|^{2n-k1-k2}$ elements, from the above theorem, the stabilizer code has the dimension $|R|^{k1+k2-n}$. The proof for the minimum distance is obvious from the construction and the above theorem. □

Corollary 10. *If C is a self-orthogonal code with parameters$[n, k, d]_r$. Then there exists a $[[n, 2k - n, \geq d]_r$ stabilizer code that is pure to d.*

F. Finite Chain Rings

This section focuses on codes over finite chain rings and compares the minimum distance of codes over rings to those over fields. We have considered finite chain rings to be a good choice for this comparison because of their structure. Artinian rings are the rings that satisfy descending chain condition on ideals. In general Artinian rings generalize both finite rings and rings which are finite dimensional vector spaces over the fields. One of the simplest Artinian rings with a unique maximal ideal are the local rings. With a unique maximal ideal M, they can be easily related to

fields as $R/M \cong F_q$. Finite chain rings are local rings with the additional constraint that the ideals are ordered by inclusion. This special structure, helps in the easy characterization of the shape of any module over the finite chain ring because of which, many of the structure theorems for codes over fields hold naturally to the modules over the rings, in particular to codes over the rings. Linear codes over finite chain rings have been studied extensively in the past ([10], [11]) and also comparisons of classical codes over rings to those over fields, [9] in the past have been done taking these rings into consideration, which motivated us to follow the same lines for the quantum codes.

A ring R is called a finite chain ring if and only if the lattice of left ideals of R form a chain. A finite chain ring is a finite local principal ideal ring. Let J denote the Jacobson radical of a finite chain ring R, that is, J is the unique maximal ideal of R. The smallest positive integer ν such that $J^\nu = \{0\}$ is called the nilpotency index of J. The nilpotency index of J and the size of the finite field R/J are two crucial parameters of a finite chain ring R, as the following well-known lemma shows.

Lemma 11. *Let R be a finite chain ring with Jacobson radical J. If the finite field R/J has q elements, and J has nilpotency index ν, then*

$$|J^i| = q^{\nu-i} \quad \textit{and} \quad |R/J^i| = q^i$$

for $1 \leq i \leq \nu$. In particular, the number of elements of the ring R and of its Jacobson radical J are respectively given by $|R| = q^\nu$ and $|J| = q^{\nu-1}$.

Proof. Since J annihilates J^i/J^{i+1} for all i in the range $1 \leq i < \nu$, we can regard J^i/J^{i+1} as an R/J-module, so it is a vector space over the field $F = R/J$. Since R is a finite chain ring, there exists an element γ in R such that $J^i = R\gamma^i$, so J^i is a cyclic R-module. Therefore, $J^i/J^{i+1} = J^i/JJ^i$ is a one-dimensional vector space over

F; hence, it follows that $|J^i/J^{i+1}| = q$ for all $1 \leq i < \nu$. Therefore, we can conclude that $|J^i| = q^{\nu-i}$ holds for all i in the range $1 \leq i \leq \nu$, as claimed.

Since J^i is the annihilator of $J^{\nu-i}$, we have $R/J^i \cong J^{\nu-i}$ as left R-modules; hence, $|R/J^i| = |J^{\nu-i}| = q^i$ for all i in the range $1 \leq i < \nu$. Furthermore, $|R| = |R/J||J| = pp^{\nu-1} = p^\nu$. Therefore, $|R/J^i| = q^i$ holds for the full range $1 \leq i \leq \nu$, as claimed. □

Modules over the ring and its properties are very important from the perspective of the linear codes. The following lemmas establish certain properties regarding the structure of the modules over the finite chain ring. One important property of the modules that we will be considering is the shape of the module. The partition $\lambda \dashv log|M|_q$ such that ${}_RM \cong \oplus R/N^{\lambda_i}$ is called the shape of ${}_RM$ and denoted by $(\lambda_1, \lambda_2, ..., \lambda_n)$. The conjugate shape λ' is defined as follows $\lambda'_i = |\{j; \lambda_j \geq i\}|$. The largest part ${\lambda_1}'$ of the conjugate shape λ' is equal to the total number of parts of λ and is called the rank of the module.

Proposition 12. *Let R be a finite chain ring and ${}_RM$ a left R-module of finite cardinality $|{}_RM|$. Suppose that the Jacobson radical J of the ring R has nilpotency index ν. The there exists a unique partition $(\lambda_1, \ldots, \lambda_r)$ of $\log_q |M|$ with $\nu \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$ such that*

$$ {}_RM \cong R/J^{\lambda_1} \oplus R/J^{\lambda_2} \oplus \cdots \oplus R/J^{\lambda_r} \tag{2.1} $$

as a left R-module.

Proof. For any Artinian principal ideal ring R and left R-module ${}_RM$ there exists a unique family $(P_i, n_i)_{i \in I}$ such that

(i) the P_i are maximal ideals of R;

(ii) the n_i are positive integers such that n_i does not exceed the nilpotency index of the ideal P_i;

(iii) ${}_RM \cong \oplus_{i\in I} R/P_i^{n_i}$;

see [Theorem 6.9] in [4]. A finite chain ring has a unique maximal ideal J. The claimed decomposition (2.1) of ${}_RM$ follows from this result. By Lemma 11, we have $|{}_RM| = q^{\lambda_1+\lambda_2+\cdots+\lambda_r}$, which proves that $(\lambda_1, \ldots, \lambda_r)$ is a partition of $\log_q |{}_RM|$. □

The above lemma gives an unique characterization of the shape of the module M over a finite chain ring. The following lemma establishes the relation between the shape of the code and its dual, a result which will be used in the later sections to relate the dimensionality of the submodule quotient and its dual.

Lemma 13. *The homomorphism from R^{2n} to $C^{\#} = Hom(C, R)_R$ is surjective.*

Proof. Let $e_1, e_2, ..., e_{2n}$ denote the standard basis vectors of R^{2n}. To show that f is surjective, pick an f $\in C^{\#}$. Then for any $w = (c_1, c_2, ..., c_n, c_{n+1}, c_{n+2}, ..., c_{2n})$ it can be written as $w = \sum c_i e_i$ in R^{2n}.

$$\begin{aligned} f(w) &= f(\sum c_i e_i) \\ &= \sum c_i f(e_i) \\ &= \langle (c_1, ..., c_n | c_{n+1}, ..., c_{2n}) | (\overline{-f(e_{n+1})}, ..., \overline{-f(e_{2n})} | f(e_1), ..., f(e_n)) \rangle_s. \\ &= \phi_v(w) \end{aligned}$$

where v = $(\overline{-f(e_{n+1})}, ..., \overline{-f(e_{2n})} | f(e_1), ..., f(e_n))$.
so f = ϕ_v for this choice of w. Every linear map $Hom(C, R)_R$ can be extended to R^{2n}, thus making the homomorphism surjective. □

Theorem 14. *Let $C \leq R^{2n}$ be a linear code over R of shape λ . Then the dual of the code $C^{\perp}$ has the complementary shape $(\nu - \lambda_{2n}, \nu - \lambda_{2n-1}, ..., \nu - \lambda_1)$ and conjugate shape $(2n - \lambda'_\nu, 2n - \lambda'_{\nu-1}, ..., 2n - \lambda'_1)$.*

Proof. Each $v \in R^{2n}$ induces a linear map $\phi_r(v) : C_R \to R_R,\ u \to \langle u|v\rangle_s$. The mapping is linear since $\phi_{(v1+v2)} = \phi_{v1} + \phi_{v2}$ and $\phi_{(cv)} = c\phi_v$. In this way we obtain a surjective homomorphism (By Lemma 13) from R^{2n} to $C^{\#} = Hom(C, R)_R$ whose kernel is $C^{\perp_s}$. From lemma 5 we have that $C \perp D$ if and only if $C \perp_s D$. Hence the kernel of the homomorphism is $C^{\perp}$ and therefore $R^{2n}/C^{\perp} \cong C^{\#}$. Hence the shapes of $C^{\#}$ and $C^{\perp}$ are complimentary. A module C and its dual $C^{\#}$ have the same shape. Hence the shape of $C^{\perp}$ is complimentary to the shape of C. Conjugate shape follows from the definition above. □

G. Submodule Quotients

Let R be a ring and C be a submodule of the R-module (R^{2n}). Given a ring element r, we define the submodule quotient $(C : r)$ as

$$(C : r) = \{e \in (R^{2n}) \mid re \in C\}.$$

Let R be a finite chain ring whose Jacobson radical J is generated by R and ν is the nilpotency index of J, that is $J^{\nu} = 0$ and $J^{\nu-1} \neq 0$. Consider the submodule quotient $(C : \gamma)$. We can build a tower of submodule quotients which follow this inclusion principle. $C \subseteq (C : \gamma) \subseteq ... \subseteq (C : \gamma^{\nu-1})$. We denote by $\overline{C}$ the image of C under reduction modulo $J(R)$. Taking the image of the submodule quotients under reduction modulo $J(R)$, we get the tower of codes $\overline{C} \subseteq \overline{(C : \gamma)} \subseteq ... \subseteq \overline{(C : \gamma^{\nu-1})}$. This tower helps in studying the structure of the code C over the ring and a detailed study of the structure of these submodule quotients will help in drawing the comparisons between the codes over finite chain rings and fields. Thus some of the properties of these submodule quotients will be established in the following lemmas, which will be used later while comparing the minimum distance of the codes over the rings to that

of fields.

Lemma 15. *Let R be a finite commutative chain ring, γ an element of R generating the Jacobson radical J of R, and ν the smallest positive integer such that $J^\nu = \{0\}$. Let C be an R-submodule of R^{2n}. Then*

$$\overline{(C : \gamma^{\nu-i-1})}^{\perp} = \overline{(C^{\perp} : \gamma^i)}$$

holds for all i in the range $0 \leq i \leq \nu - 1$.

Proof. Let $u = (a|b)$ be an arbitrary element of $(C^{\perp} : \gamma^i)$. It follows from the definition of a submodule quotient that $r\gamma^i u = (r\gamma^i a | r\gamma^i b) \in C^{\perp}$ holds for all r in R. For any element $v = (c|d)$ in the submodule quotient $(C : \gamma^{\nu-i-1})$, we have $\gamma^{\nu-i-1}v \in C$. Therefore,

$$\langle u|v\rangle_s = r\gamma^{v-1}(a.d - b.c)$$

belongs to the kernel of χ. In other words, $\gamma^{\nu-1}(a.d - b.c)$ is in the kernel of all characters χ^r with $r \in R$. Since χ is a generating character, the element $\gamma^{\nu-1}(a.d-b.c)$ is in the kernel of all characters, hence it must be equal to 0. By [G. Norton, A. Salagean, On the structure of linear and cyclic codes over finite chain rings, Corollary 2.3], it follows that $a.d - b.c$ must be a multiple of γ, so it is in the Jacobson radical $J(R)$. Therefore, we can conclude

$$\overline{(C^{\perp} : \gamma^i)} \perp \overline{(C : \gamma^{\nu-i-1})}.$$

It remains to be shown that the dimensions of $\overline{(C^{\perp} : \gamma^i)}$ and $\overline{(C : \gamma^{\nu-i-1})}$ sum to $2n$. The following two lemmas prove the dimensionality of the submodule quotients. □

For a R-module M and $x \in M$, we say

- x has period γ^i, if $i \in \{0, 1, ..., \nu\}$ is the smallest integer satisfying $\gamma^i x = 0$.

- x has height i, if $i \in \{0, 1, ..., \nu\}$ is the largest integer satisfying $x = \gamma^i y$ for some y$\in$ M.

Furthermore, we define the following notations:

$$\gamma^i M = \{\gamma^i x;\ x\ \in M\}$$

$$M[\gamma^i] = \{x\ \in\ M;\ \gamma^i x = 0\}$$

If M is free, the $M[\gamma^i] = \gamma^{\nu-i} M$ for $0 \leq i \leq \nu$.(see [11])

Lemma 16. *Let C be an R-submodule of R^{2n}.Suppose C has shape λ (Arranged in decreasing order). Then the dimension of $\overline{(C : \gamma^i)}$ is given by $k_0 + k_1 + ... + k_i$ where k_l denotes the number of parts of λ equal to $\nu - l$.*

Proof. There exists a uniquely determined partition λ such that C has a basis $c_1, c_2, ...c_k$ with periods $\gamma^{\lambda_1}, \gamma^{\lambda_2}, ...$ respectively where k is the rank of the module C. For convenience let us assume that basis elements are arranged in the decreasing order of their periods (i.e., increasing order of their heights). Let e be an element in $(C : \gamma^i)$. Since e $\in (C : \gamma^i)$, we have $\gamma^i e \in C$, hence there exists $r_1, r_2, ...r_k\ \in R$ such that

$$\gamma^i e = r_1 c_1 + r_2 c_2 + ... + r_k c_k.$$

Since R^{2n} is a free module we have the property that $R^{2n}[\gamma^i] = \gamma^{\nu-i} R^{2n}$. Hence every basis element c_i can be written as $c_i = (\gamma^{\nu-\lambda_i} c_{i1}, \gamma^{\nu-\lambda_i} c_{i2}, ..., \gamma^{\nu-\lambda_i} c_{in})$. Therefore we can write $\gamma^i e$ in the form

$$\gamma^i e = r_1 c_1 + r_2 c_2 + ... + r_j c_j + \gamma^i(\gamma^{\nu-\lambda_{j+1}-i} r_{j+1} c_{j+1} + ... + \gamma^{\nu-\lambda_k-i} r_k c_k)$$

where the index j is chosen such that $\lambda_j \geq \nu - i$ and $\lambda_{j+1} < \nu - i$. Hence $r_1 c_1 + r_2 c_2 + ... + r_j c_j$ is also divisible by γ^i. Thus

$$e \equiv \sum_{i=1}^{j} r_i' c_i + \sum_{l=j+1}^{k} \gamma^{\nu-\lambda_l-i} r_l c_l \mod (\gamma^{v-i}).$$

Taking the projection of e modulo the Jacobson radical we have $\overline{e} = \sum_{i=1}^{j} \overline{r_i'}\overline{c_i}$, which makes $\{\overline{c_1}, \overline{c_2}, ...\overline{c_j}\}$ to be the generating set for $\overline{(C : \gamma^i)}$. Since this set is independent, dimension of the $\overline{(C : \gamma^i)}$ is given by $k_0 + k_1 + ... + k_i$.

□

Lemma 17. *The dimensions of* $\overline{(C^\perp : \gamma^i)}$ *and* $\overline{(C : \gamma^{\nu-i-1})}$ *sum to* $2n$.

Proof. The dimensionality of $\overline{(C^\perp : \gamma^i)}$ is given by $d = k_0 + k_1 + ... + k_i$ from the above lemma. Since every code over the field is a free code, we have $\overline{(C^\perp : \gamma^i)}$ is a free code, its shape is given by $\lambda_1 = \lambda_2 = ...\lambda_d = \nu$ and conjugate shape $\lambda_1{}' = \lambda_2{}' =, ..., \lambda_\nu{}' = d$. Hence the rank of $\overline{(C^\perp : \gamma^i)}$ = d. From Theorem 13, which discusses the relation between shape of C and its dual $C^\perp$, we have that the the shapes of C and $C^\perp$ are complimentary and $C^\perp$ has the conjugate shape $(2n-\lambda_\nu', 2n-\lambda_{\nu-1}', ..., 2n-\lambda_1')$, which implies rank of $\overline{(C : \gamma^{\nu-i-1})} = 2n - \lambda_\nu' = 2n - d$. Since for codes over fields rank is nothing but the dimension, we have $\dim(\overline{(C^\perp : \gamma^i)}) + \dim(\overline{(C : \gamma^{\nu-i-1})})$ = d + 2n - d = 2n. □

Having established the orthogonality of the submodule quotients, we are now ready to give a comparison of the minimum distances of the quantum codes over these rings to that over the finite fields. Recall that the weight of the error X(a)Z(b) is characterized by the symplectic weight of the corresponding vector $(a|b)$. Also the minimum distance of the stabilizer code equals $swt(C^\perp - C)$. Let us denote $d(C^\perp - C)$ to be the minimum of all the $swt(a|b)$ where $(a|b) \in (C^\perp - C)$. Thus we are interested in estimating the $d(C^\perp - C)$ as this would directly relate to the minimum distance of the stabilizer code over the ring. The following lemmas establish all the conditions and

show that $d(C^{\perp} - C) \leq d(\overline{(C^{\perp} - (C : \alpha))}$ where $\overline{C^{\perp}}$ and $\overline{(C : \alpha)}$ denote orthogonal submodule quotients over the residue field $R/J(R)$. We state the conditions under which the equality can be achieved.

Proposition 18. *Let R be a finite local principal ideal ring, γ an element of R generating the Jacobson radical J of R, and ν the smallest positive integer such that $J^{\nu} = \{0\}$. Let C be an R-submodule of R^{2n} satisfying $C \leq C^{\perp}$, that is, C is a self-orthogonal linear code over the ring R. Then*

$$d(C^{\perp} - C) \leq d(\overline{(C^{\perp} - (C : \alpha))}$$

where $\alpha = \gamma^{\nu-1}$.

Proof. Let $C^{\perp} - (C : \alpha) = \{x | x \ \in C^{\perp} \text{ and } \alpha x \ \notin \ C\}$. Let us consider an element $x \ \in C^{\perp} - (C : \alpha)$, then $\alpha x \in C^{\perp} - C$. This implies that $\alpha(C^{\perp} - (C : \alpha)) \subset C^{\perp} - C$. Therefore we have $d(C^{\perp} - C) \leq d(\alpha(C^{\perp} - (C : \alpha)))$.

From the above we have $d(C^{\perp} - C) \leq d(\alpha(C^{\perp} - (C : \alpha)))$. Since R is a finite local ring with Jacobson radical J, its quotient ring $F = R/J$ is a finite field. We can define a map $\psi : \alpha R^{2n} \ \to F^{2n}$ by

$$\psi((\alpha r_1, \ldots, \alpha r_{2n})) = (r_1 + J, \ldots, r_{2n} + J).$$

Since the annihilator of α in R is given by J, this is a well-defined homomorphisms of R-modules. Since ψ is surjective and $\ker \psi = \{0\}$, it follows that ψ is an isomorphism.

We have $\psi(\alpha((C^{\perp} - (C : \alpha)) = \overline{(C^{\perp} - (C : \alpha))}$. Since $\mathrm{swt}(\alpha c) = \mathrm{swt}\, \psi(\alpha c)) = \mathrm{swt}(\overline{c})$, we have

$$d(C^{\perp} - C) \leq d(\alpha(C^{\perp} - (C : \alpha))) = d(\overline{(C^{\perp} - (C : \alpha)}.$$

Therefore, we can conclude that $d(C^{\perp} - C) \leq d(\overline{(C^{\perp} - (C : \alpha)}$, as claimed. □

The above bounds on the minimum distance have been established using the classical objects. However in order to generalize the comparison to stabilizer codes, we need the code over the field also to be self orthogonal. This is possible when the projected code over the field contains its dual, which is the case for free codes.

Theorem 19. *If an $(n, K, d)_R$ free stabilizer code exists over the ring, then a corresponding $(n, K, \geq d)$ stabilizer code exists over the field.*

Proof. Since $C^{\perp}$ is a free code, C is also a free code(Dual of a free module is also a free module) A code is free if and only if it is linear and it satisfies the property that $C \bigcap \gamma^i R^n = \gamma^i C$. Hence we have $\overline{(C : \gamma^i)} = \overline{C}$ for $i = 0, ..., v-1$. This implies that $\overline{(C^{\perp} - (C : \alpha)} = \overline{(C^{\perp} - C)}$. Hence $d(\overline{(C^{\perp} - (C : \alpha))} = d(\overline{(C^{\perp} - C)})$. Hence from the above theorem we have the following for free codes, $d(C^{\perp} - C) \leq d(\overline{C^{\perp} - C})$. Hence Proved. □

By restricting to the class of pure codes, we can preserve all the three parameters of the stabilizer code over the field. A quantum code is pure to d, if the stabilizer group does not contain any elements of weight less than d. Most of the bounds that have been proved, are for the class of pure codes. The popular codes that are constructed are the pure quantum codes. Hence the following theorem states the existence of a quantum code over the ring and the field with the same parameters.

Theorem 20. *If an $(n, K, d)_R$ stabilizer code exists over the ring, then the parameters of the code remain preserved over the field, i.e., (n, K, d) exists over the field, provided the following conditions are satisfied.*

- $\overline{C^{\perp}}$ *is a pure code*
- $C^{\perp}$ *is a free code*

Proof. $C^{\perp} - C \subseteq C^{\perp}$. Hence we have $d(C^{\perp}) \leq d(C^{\perp} - C)$. For free codes we have $d(C^{\perp}) = d(\overline{C^{\perp}})$. Therefore, $d(\overline{C^{\perp}}) \leq d(C^{\perp} - C)$. Since $\overline{C^{\perp}}$ is a pure code, we have $d(\overline{C^{\perp}}) = d(\overline{C^{\perp} - C})$. This implies $d(\overline{C^{\perp} - C}) \leq d(C^{\perp} - C)$. From the above lemma we have $d(C^{\perp} - C) \leq d(\overline{C^{\perp} - C})$. Hence $d(C^{\perp} - C)$ has to be equal to $d(\overline{C^{\perp} - C})$. Hence Proved. □

Thus the minimum distance of the codes over these rings cannot exceed the minimum distance of the codes over the fields.

CHAPTER III

CONCLUSIONS

The theory of stabilizer codes over rings has been studied in this thesis. We established the existence of stabilizer codes over Frobenius rings. In particular, we related quantum codes over rings to classical codes. This allowed us to give the first systematic construction of quantum codes over rings. Subsequently, we studied the structure of stabilizer codes over finite chain rings. By developing the structure theory of modules over finite chain rings, we were able to obtain numerous structural results on stabilizer codes over finite chain rings. In particular, we established that the minimum distance of stabilizer codes corresponding to free codes over finite chain rings cannot exceed the minimum distance of stabilizer codes over finite field.

REFERENCES

[1] R. Hill, *A First Course in Coding Theory*, [2nd edition], New York: Oxford University Press, 1990.

[2] J. H. Van Lint, *Introduction to Coding Theory*, [2nd edition], New York: Springer-Verlag, 1992.

[3] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, New York: Cambridge University Press, 2004.

[4] D. W. Sharpe and P. Vamos, *Injective Modules*, Cambridge: Cambridge University Press, 2008.

[5] A. Ketkar, A. Klappenecker, S. Kumar, and P. Kiran Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, pp. 4892-4914, Nov 2006.

[6] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, pp. 3065-3072, Nov 2001.

[7] E. Knill, "Non-binary unitary error bases and quantum codes," Los Almos National Laboratory report LAUR-96-2712, Los Alamos, NM; June 1996.

[8] W. J. Martin, "A physics-free introduction to quantum error correcting codes," *Utilitas Mathematica*, vol. 65, pp. 133-158, 2004.

[9] G. H. Norton and A. Salagean, "On the hamming distance of linear codes over a finite chain ring," *IEEE Transaction On Information Theory*, vol. 46, no. 3, May 2000.

[10] G. H. Norton and A. Salagean, "On the structure of linear and cyclic codes over a finite chain rings," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, pp. 489–506, July 2001.

[11] T. Honold, I. Landjev, and Z. Mathematik, "Linear codes over finite chain rings," *Electronic Journal of Combinatorics*, vol. 7, pp. 116–126, 1998.

[12] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. Thesis, California Institute of Technology, Pasadena, CA, 1997.

[13] P. Majek, "Quantum error correcting codes," Ph.D. dissertation, Comenius University, Bratislava, 2005.

[14] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *The American Journal of Mathematics*, vol. 121, pp. 555–575, 1999.

[15] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, and W. H. Zurek, "Introduction to quantum error correction," Quantum Physics, Tech Report 0207170, Jul 2002.

[16] D. Bacon, "Stabilizer quantum error correcting codes," Lecture Notes, University of Washington, Seattle, WA.

VITA

Name: Sushma Nadella

Address: Department of Computer Science and Engineering
Texas A&M University,
College Station, TX 77843-3112.

Email Id: sushma.amicable@gmail.com

Education: B.Tech., International Institute of Information Technology, India,
May 2009
M.S., Texas A&M University , College Station, Texas,
May 2012