QUANTUM CODES OVER FINITE FROBENIUS RINGS

A Thesis

by

ANURUPA SARMA

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

August 2012

Major Subject: Computer Science

QUANTUM CODES OVER FINITE FROBENIUS RINGS

A Thesis

by

ANURUPA SARMA

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,	Riccardo Bettati
	Laszlo Kish
Head of Department,	Hank Walker

August 2012

Major Subject: Computer Science

ABSTRACT

Quantum Codes over Finite Frobenius Rings. (August 2012)
Anurupa Sarma, B.Tech, National Institute of Technology, Silchar, India
Chair of Advisory Committee: Dr. Andreas Klappenceker

It is believed that quantum computers would be able to solve complex problems more quickly than any other deterministic or probabilistic computer. Quantum computers basically exploit the rules of quantum mechanics for speeding up computations. However, building a quantum computer remains a daunting task. A quantum computer, as in any quantum mechanical system, is susceptible to decohorence of quantum bits resulting from interaction of the stored information with the environment. Error correction is then required to restore a quantum bit, which has changed due to interaction with external state, to a previous non-erroneous state in the coding subspace. Till now the methods for quantum error correction were mostly based on stabilizer codes over finite fields. The aim of this thesis is to construct quantum error correcting codes over finite Frobenius rings. We introduce stabilizer codes over quadratic algebra, which allows one to use the hamming distance rather than some less known notion of distance. We also develop propagation rules to build new codes from existing codes. Non binary codes have been realised as a gray image of linear Z_4 code, hence the most natural class of ring that is suitable for coding theory is given by finite Frobenius rings as it allow to formulate the dual code similar to finite fields. At the end we show some examples of code construction along with various results of quantum codes over finite Frobenius rings, specially codes over Z_m.

To My family.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor, Dr. Andreas Klappenecker, for his guidance and much useful advice. I would also like to thank my committee members, Dr. Richardo Bettati and Dr. Laszlo Kish, who assisted me throughout this process. A special thanks to the NSF for their financial support for this project. This work would not have been possible without unwavering and undiminishing support and prayers of my family. Finally, I would like to thank my dearest friend, Shardul, for his love and support throughout this period. This research was partially supported by NSF grant CCF 1018500.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER I

INTRODUCTION

A. Introduction

Noise is a bane of information processing system. Error correction is an important aspect of classical information processing that protects the classical bits against errors, similarly quantum error correction is an important aspect of quantum information processing. Quantum information is represented by the states of quantum mechanical systems. Since the information carrying quantum systems will inevitably interact with their environment, one has to deal with decoherence effects that tend to destroy the stored information. Hence, it is infeasible to perform quantum computations without introducing techniques to remedy this dilemma.

It is conjectured that quantum computers are able to solve certain problems more quickly than any deterministic or probabilistic computer. For instance, Shors algorithm is able to factor large integers in polynomial time on a quantum computer. Therefore it is of considerable interest to build quantum computer. However, it is a formidable task, since the quantum mechanical systems storing the information unavoidably interact with their environment. Therefore, one has to mitigate the resulting noise and decoherence effects to avoid computational errors.

The space in which quantum error correcting codes exist is the Quantum state space of n quantum digits. The space is represented as $\mathbf{C}^{q^n}$ and is a tensor product of n copies of C^q where each copies corresponds to one qubit. The idea of Quantum error correction is to encode k quantum digits to n quantum digit which is nothing but a linear mapping of $\mathbf{C}^{q^n}$ onto a q^k dimensional subspace of $\mathbf{C}^{q^n}$.

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

B. Motivation and problem

1. As it is known that quantum computer are able to solve certain problems more quickly than classical computer. However quantum computer is highly prone to noise and decoherence which is a major hurdle in this field. Quantum Error correcting code can save it from this problem and it is worth exploring.

2. The ability to correct quanutum errors without any cloning or disturbing the state of computation was assumed to be close to impossible and hence coming up with a good quantum code is a challenging and exciting area of research.

3. Stabilizer codes form an important class of quantum codes and have a close relationship with classical codes. The first examples of quantum code found by Shor [1] and Steane [2, 7] were quantum stabilizer codes. Binary stabilizer codes are well established. Ashikman and Knill initiated the study of non binary stabilizer codes over finite field [3]. This inspired me to verify whether the well established theory of non binary stabilizer codes over finite fields can be extended for finite rings.

4. Currently in classical computing there is an upsurge of interest in codes over rings, since non binary codes has been realised as the gray image of linear Z_4 code. So the most natural class of ring that is suitable for coding theory is given by finite Frobenius rings as it allow to formulate the dual code similar to finite fields. So it is worth to delve into codes over finite frobenius ring.

C. Outline of thesis

In the chapter II we include basic of quantum mechanics, basics of classical error correction and quantum error correction and detection. We also include algebraic preliminaries which is required for the rest of our thesis.

In Chapter III we walk through the theory of binary and non binary stabilizer codes. Here we also make our reader familiar with finite Frobenius rings, error bases, error groups and discuss the theory of codes over finite Frobenius rings.

In Chapter IV we introduce quadratic algebra and explain how we establish theory of stabilizer codes over quadratic algebra, relation to classical coding theory and codes over ring with q^2 elements.

In Chapter V we use the relation between classical and quantum codes and derive propagation rules that allow one to obtain new codes from existing codes. Lastly, product codes and how quantum codes can be built from product codes. Furthermore in last chapter we show some examples of code construction along with various results of quantum codes over finite Frobenius rings, specially codes over Z_m.

CHAPTER II

BACKGROUND ON QUANTUM AND CLASSICAL CODES

To make the thesis self contained we try to provide a general idea of quantum computing. As this domain is vast it isn't possible for us to include everything in detail. We recommend the reader to go through the textbook by Nielsen and Chaung [4] and lecture notes by Preskill [5].

Quantum Computer requires the control and manipulation of a large number of sensitive quantum mechanical systems. A quantum computer would inevitably interact with the environment which results in decoherence and eventually would decay the quantum information stored in the device. So successfully combating decoherence is a major need. But even though we can fix the decoherence by perfectly isolating the computer from the environment, we have other hurdles to overcome. Quantum gates are unitary transformation chosen from a continuum of possible values. It is not possible to build quantum gates with perfect accuracy, so small imperfections in the gates would accumulate resulting in serious failure. Therefore any practical quantum computer would need the ability to fix not only errors due to noise but also from the quantum gates that accompany it in its processing. Peter schor [6] and Andrew Steane [7] independently proposed schemes to protect quantum information from noise and operational errors. Gottesman [8] and indpendently Calderbank et al., [9] proposed methods to construct quantum codes from classical codes which added up tremendously to the literature of quantum coding theory leading a lots of scholars to research in this domain. These codes are known as stabilizer codes and are the most studied class of quantum codes. We introduce this class of codes in the next chapter.

With this fundamental results in place the focus of quantum coding theory shifted to the design of good codes with systematic methods of code construction.

A. Quantum computation

Classical computer works on the well understood laws of classical physics whereas Quantum computer behaves according to quantum mechanics.

1. Qudits

Qudits are the mathematical models for quantum systems which are used to store quantum information. General state of a quantum digit is represented as

$$|\psi\rangle = \sum_{i=1}^{q} \alpha_i |x_i\rangle$$

where α_i are complex numbers satisfying $\sum_{i=1}^{q} |\alpha_i|^2 = 1$. We define a orthonormal basis $\{|x_1\rangle, |x_2\rangle, \cdots, |x_q\rangle\}$ which is called computational basis. Each element x_i belongs to ring R with q elements.

For example, when $q = 2$ we call it qubit. The state of the qubit is a normalized vector over C^2. The computational basis over C^2 as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{(ket zero)}, \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{(ket one)}$$

which are simple column vectors.

The the state of a qudit must be a normalized vector and $|\psi\rangle$ is a superposition. We know in classical information theory, we never have any problem in measuring the state of a bit and measurement is not considered as a part of a classical information theory. If the measurement gives us result 0 the digit we are measuring is in the state

0 if it gives us 1 and then the digit is in state 1 etc. But things are not same in the quantum domain. Not only we cannot trust the measurements results but measurement is itself a essential part of quantum information theory. When we measure $|\psi\rangle$ in computational basis we may obtain a measurement result corresponding to the state $|x_i\rangle$ with probability $|\alpha_i|^2$ for all i ranging from $1 \leq i \leq q$. The sum of the probabilities should be equal to 1, thus we get the equation $\sum_{i=1}^{q} |\alpha_i|^2 = 1$. This is the reason why the state of a qudit must be a normalized vector. The sign "+" in the state $|\psi\rangle$ means "or", i.e the state is either in any of the state $|x_i\rangle$. or in the state $|1\rangle$. This is why we call the state $|\psi\rangle$ superposition. For example, suppose there is a state in computational basis $\{|0\rangle, |1\rangle\}$ over C^2

$$\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

Once we measure the state we will either get $|0\rangle$ with probability 0.5 or $|1\rangle$ with probability 0.5. The state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ along with the state $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ forms another orthonormal basis over C^2. The coefficients of the state $|\psi\rangle$ can be any values as long they satisfy the equation $|\alpha|^2+|\beta|^2 = 1$. This means a qudit can be in any of infinite possible states. However, after they are measured they collapses to two possible states. The amount of information we can store on one qudit is given by Schumacher [10], is one two-system's worth.

In quantum information theory frequently used quantum systems to represent are:-

1. Ground and excited states of ions stored in a linear ion trap, with interactions between ions provided through a joint vibration mode.

2. Photons in either polarization, with interactions via cavity QED.

3. Nuclear spin states in polymers, with interactions provided by nuclear magnetic resonance technique.

In point 1 the ground state or the excited state corresponds to $|0\rangle$ or $|1\rangle$, respectively. Radiating the atom with a ray of light with an appropriate frequency we can force the electron to jump from $|0\rangle$ to the state $|1\rangle$. But we can also reduce the duration of the radiation, the electron in the state $|0\rangle$ could then move to a middle state between $|0\rangle$ and $|1\rangle$ which is $|+\rangle$

2. Quantum registers

An n-qudit register is just a name for the sequence of n qudits. Such a q-register has q^n different base states. Again as in the case of single qudit, any normalized linear superposition of q^n different base states can be in q-register. There is a significant difference between classical and quantum register like classical register are all independent of its digits, we can read or manipulate each digit without any inference to other digits. Whereas in q-registers the situation is bit different. For example, consider a 3 qudit register over C^2 in state $|\psi_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |1\rangle$. The operator $\otimes$ above is called tenser product. The tensor product is a way of putting vector spaces together to form larger vector spaces. The notation $|111\rangle$ is shorter form of exact notation: $|1\rangle \otimes |1\rangle \otimes |1\rangle$. Well we see a third qudit of $|\psi_3\rangle$ in the form $|1\rangle$ but we cannot interchange the third qudit to make it appear in the first place. that is we cannot rewrite $|\psi_3\rangle$ in the form $|1\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we cannot say in what state the first qudit is. Again the first and second qudits are entangled so we cannot get any description of any one of them without mentioning the second. Though we can get partial description of this qudits using the density operators [4].

3. Hilbert space and linear operators

Hilbert space gives a mathematical apparatus need to describe and formulate operations in quantum computing. In general, it extends the methods of vector of algebra and calculus from the two-dimensional euclidean plane and three-dimensional space to spaces with any finite or infinite number of dimensions.

A Hilbert space H is a real or complex inner product space that is also a complete metric space with respect to the distance function induced by the inner product. H is a complex inner product space means that H is a complex vector space on which there is a inner product $\langle x, y\rangle$ associating a complex number to each pair of element x, y of H which satisfies the following properties:

1. $\langle y, x\rangle$ is a complex conjugate of $\langle x, y\rangle$

$$\langle y, x\rangle = \overline{\langle x, y\rangle}$$

2. $\langle x, y\rangle$ is linear in first argument. For all complex number a and b

$$\langle ax_1 + bx_2, y\rangle = a\langle x_1, y + b\langle x_2, y\rangle\rangle$$

3. The inner product $\langle ., .\rangle$ is positive definite:

$$\langle x, x\rangle \geq 0,$$

where the case of equality holds precisely when x = 0.

In addition to measurements that can be done on quantum digit, there are operators which transverse one normalized state to another normalized state [11]. This operators tends to be normal. Let us assume there are two elements p and q in C^n, the hermitian inner product is defined as $\langle p|q\rangle = \overline{p_0}q_0 + \overline{p_1}q_1 + \cdots + \overline{p_{n-1}}q_{n-1}$. The norm $||p||$ of a vector $p \in C^n$ is defined as $||p|| = \sqrt{\langle p|p\rangle}$. 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 linear operator transforms the quantum bit $a|0\rangle + b|1\rangle$ to $a|\phi\rangle + b|\psi\rangle$. The linear operator U is nothing but a 2×2 matrix. This kind of linear mapping which takes a unit vector in C^n to unit vector in C^n is called unitary mapping. So, the operator U is a unitary operator, the matrix U satisfies the condition $UU^\dagger = I$. This kind of unitary matrix satisfies $\langle Up|Uq\rangle = \langle p|q\rangle$ for $p, q \in C^n$.

An operator P which maps an Hilbert space to another Hilbert space is called projection operator if it satisfies the following conditions i.e $P = P^\dagger$, $P^2 = P$

4. Density operators

Here we consider the quantum state space as C^2. Suppose we have two vectors $|\psi\rangle$ and $|\phi\rangle$, let us define the outer product of $|\psi\rangle$ and $|\phi\rangle$ as $|\phi\rangle\langle\psi|$. So for instance if $|\psi\rangle = |0\rangle$ and $|\phi\rangle = |1\rangle$, then $|1\rangle\langle 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. If the outer product is formed with itself then it is called the density matrix, which is denoted by $\rho = |\psi\rangle\langle\psi|$. This density matrix $\langle\psi|\rho|\psi\rangle \geq 0$ is positive definite and $\mathrm{Tr}(\rho) = 1$, where Tr is the sum of the diagonal matrix. The density operators are matrices of size $2^n \times 2^n$, which allows to view the state as being operators on the Hilbert space. We can thus say if a system can be found in any of the states $|\psi_i\rangle$ with probability p_i, the density operator associated to this system is given by

$$\rho = \sum_i p_i |\psi\rangle\langle\psi|$$

A state is considered as pure if $\mathrm{Tr}(\rho^2) = 1$ and mixed otherwise.

B. Linear algebra

In this section we review necessary mathematical knowledge for the study of quantum mechanics and quantum error correction theory. Here we only scan through the necessary results and conclusion by omitting the proofs.

Vector Space : Vector space over a field F is a set V which is closed under finite vector addition and scalar multiplication.

Tensor products : Tensor product is important concept in the study of multi-particle systems as it merges small vector space into large vector spaces. Let H_1 and H_2 be two Hilbert spaces of dimension n_1 and n_2 respectively. Then $H_1 \otimes H_2$ is a Hilbert space of $n_1 n_2$ dimension. So, if $|x\rangle$ is a vector of H_1 and $|y\rangle$ is a vector of H_2 then, $|x\rangle \otimes |y\rangle$ is a vector of $H_1 \otimes H_2$. Tensor product of two matrices is defined as

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n} \\ a_{21}B & a_{22}B & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Tensor product satisfies the following properties :

1)For any scalar z any element $|x\rangle$ of H_1 and any element $|y\rangle$ of $|H_2\rangle$:

$$z(|x\rangle \otimes |y\rangle) = (z|x\rangle) \otimes |y\rangle = |x\rangle \otimes (z|y\rangle)$$

2)For any $|x_1\rangle, |x_2\rangle$ in H_1 and any $|y\rangle$ in H_2

$$(|x_1\rangle + |x_2\rangle) \otimes |y\rangle = |x_1\rangle \otimes |y\rangle + |x_2\rangle \otimes |y\rangle$$

3)For any $|y\rangle$ in H_2 and $|y_1\rangle, |y_2\rangle$ in $|H_2\rangle$:

$$|x\rangle \otimes (|y_1\rangle + |y_2\rangle) = |x\rangle \otimes |y_1\rangle + |x\rangle \otimes |y_2\rangle$$

4)Let A and B be two arbitrary linear operators defined on H_1 and H_2, respectively. Let $|x_i\rangle$ and $|y_i\rangle$ be sets of vectors in H_1 and H_2. Then,

$$(A \otimes B)(\sum a_i |x_i\rangle \otimes |y_i\rangle) = \sum a_i (A|x_i\rangle) \otimes (B|y_i\rangle)$$

The inner product in the space $H_1 \otimes H_2$ can be defined by the inner products in the H_1 and H_2. Suppose that $\{|x_i\rangle\}$ is an orthonormal basis for H_1 and $\{|y_k\rangle\}$ is an orthonormal basis for H_2, then we can prove that $\{|x_i y_k\rangle\}$ is an orthonormal basis for $H_1 \otimes H_2$.

The inner product of two vectors $|x_i y_k\rangle$ and $|x_j y_l\rangle$ is:

$$\langle x_i y_k | x_j y_l \rangle = \langle x_i | x_j \rangle \langle y_k | y_l \rangle = \delta_{i,j} \delta_{k,l}$$

If $i = j \; and \; k = l$, the value is equal to 1. Otherwise the value is 0.

Let us consider A and B be two linear operators defined on spaces H_1 and H_2 respectively, then the following properties hold:

$$(A \otimes B)^* = A^* \otimes B^*$$
$$(A \otimes B)^T = A^T \otimes B^T$$
$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$$

where $A*$ is the conjugate of a matrix A, A^T is the transpose of matrix A and $A^\dagger$ is the hermitian conjugate of the matrix A. Suppose a be either a linear operator or a state then, $a^{\otimes k}$ means a tensor product with itself k times. For example, $A^{\otimes 4} = A \otimes A \otimes A \otimes A$

Commutator : The commutator of two same size square matrices A and B is defined as:

$$[A, B] \equiv AB - BA$$

If $[A, B] = 0$, then we say A commutes with B. Whereas the anti-commutator of two matrices A and B is defined as:

$$\{A, B\} \equiv AB + BA$$

If $\{A, B\} = 0$, we say A anti-commutes with B.

Pauli matrices : The four important matrices in quantum mechanics are Pauli matrices which is frequently used in quantum information theory.

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

Important operators : Hermitian operator on a matrix M is denoted by $M^\dagger$ and is defined as $M^\dagger = (M^*)^T$, where M^* is the conjugate of matrix M. This operator is also called adjoin operator. For square matrix M, N it has the following properties:

$$(MN)^\dagger = N^\dagger M^\dagger \ (M^\dagger)^\dagger) = M$$

For the outer products like $|\psi\rangle\langle\psi|$, it is easy to prove that $(|\psi\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\psi|$. If $M^\dagger = M$, then a linear operator M is called self adjoin hermitian. Projectors are important class of hermitian operators.

Gram-Schmidt procedure is a important tool to convert between inner product space. Suppose V be a n-dimensional vector space and let W be a m-dimensional subspace of V. It is easy to form a orthonormal basis $\{|g_i\rangle\}$, $1 \leq i \leq m$ whose first m elements are basis of W. The projector onto the subspace W is defined as

$$P = \sum_{i=1}^{m} |g_i\rangle\langle g_i|$$

The P defined above is a hermitian operator and it acts as a filter. For example, suppose $|v\rangle$ be a vector in the space V, now if we apply $P|v\rangle$, then the part of the vector of $|v\rangle$ which is not in subspace W is been cut off and that only belong to W remains. Thus the vector $|v\rangle$ has been filtered. So, the projector is only determined by orthonormal basis of the subspace instead of the V.

For any non zero vector $|v\rangle$ if the inner product $\langle v|M|v\rangle$ is always > 0, then the operator M is called positive definite. A normal operator is an operator satisfying

$MM^\dagger = M^\dagger M$. Hermitian operator are a subclass of normal operator. A square operator U is called a unitary operator if $UU^\dagger = I$. And the unitary operator preserves the inner product of two vectors.

Eigenvectors : Let us consider a square matrix M, eigen value of the square matrix is a non-zero complex value λ such that it satisfies the equation $M|v\rangle = \lambda|v\rangle$, where $|v\rangle$ is a non-zero vector. This vector is called the eigen vector of the linear operator M associated with eigenvalue λ The equation $c(\lambda) \equiv |M - \lambda I|$ is called the characteristic equation. The roots of this characteristic equation are the eigenvalues of the linear operator M. To find eigenvector $|v\rangle$, corresponding to a eigenvalue λ, we simply solve the systems of linear equations given by $(M - \lambda I)|v\rangle = 0$. The set of all vectors $|v\rangle$ satisfying the equation $M|v\rangle = \lambda|v\rangle$ is called the eigenspace of M corresponding to λ.

C. Classical error correction

Important elements and concepts of classical error correction are explained in this section.

Additive Code : Let F_q denote a finite field with q elements. We have $q = p^m$ for some prime p. A subset $C \subseteq F_q^n$ is an additive code if for any x, y in C, $x + y$ also in C. Additive code plays an important role in quantum computing. If in addition to being additive, C also satisfies $sc \in C$ for any s in F_q and $c \in C$, then C is called F_q linear code.

Linear Code : Linear code is error correcting code for which any linear combination of codewords is also a codeword. A linear code of length n and rank k is a subspace of a vector space over F_q^n, where k is the dimension of the code and d which is the minimum difference between two codewords is the distance of the code.

Block code : All codewords have the same length n, i.e. $C \subseteq V^n$.

Error : While the message is transmitted through a binary symmetric channel, it is probable that some codewords are changed. That is the receiver does not get the same message as it has been transmitted. All codewords have the same probability of being changed.

Error Detection : It is the technique by which we can detect the garbled message.

Error Correction : Technique to correct the garbled message. The codewords have to be "suciently dierent" from each other so that we can still tell them apart even when "a few" errors occurred.

Hamming Distance : Hamming distance between two codewords is the number of positions between two code words which differ and hamming distance between of a code C is the minimum hamming distance between two codewords in the code.

Hamming weight : The number of non zero entries in a codeword.

Theorem C.1 *A code with distance d is a $d-1$ error detecting and $\lfloor \frac{d-1}{2} \rfloor$ error correcting code.*

A classical $(n, K, d)_q$ code $C \subseteq F_q^n$, is a code of size $|C| = K$ and distance $d = wt(C)$, where wt is the hamming weight of C. If $|C| = q^k$, then we denote it by $[n, k, d]_q$. If C is also F_q-linear code, then C is a $k-$ dimensional subspace of F_q^n. Linear codes are also defined with the help of generator matrix. Generator matrix G is a basis of codewords. A linear code consists of linear combination of G. When the generator matrix is of the form $[I|P]$ we say that it is in the standard form.

Encoding : Suppose C contains q^k codewords each of which are distinct messages that need to be transmitted. Each of these messages are identified as $k-tuple$ of F_q^k. Each message m is encoded as codeword length n which is obtained by multi-

plying the message with the generator matrix on the right. The encoded message is then $mG = (g_0 + g_1 + \cdots + g_i)$ where each g_i are the rows of the generator matrix.

Parity check matrix and Dual Codes : 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 row vector w of the generator matrix of C, i.e $vH = 0$, where H is the transpose of G and the generator matrix of the dual code $C^{\perp}$. This is called as the parity check matrix. $C^{\perp}$ has the parameters $[n, n-k]$. A code with minimum distance d has a parity check matrix in which any arbitrary set of $d-1$ columns are linearly independent.

The parity check matrix can be used for error detection as the parity check matrix nullifies all the codeword in C, i.e $Hc = 0$, where $c \in C$ Now suppose c is a vector which is transmitted through a communication channel, that is corrupted with an error e, then the vector or codeword becomes $c^{'} = c \oplus e$. When such a corrupted vector is multiplied with the parity check matrix H, we get the error syndrome, $Hc' = H(c \oplus e) = He$. If the syndrome $Hc^{'} = 0$, then $c^{'}$ is called valid codeword else the codeword is corrupted.

D. Quantum error correction

Errors are the major factor which we need to address while building a quantum communication device. Any qudit stored without any protection or one transmitted in a communication channel will inevitably come out with slight change. The theory of quantum error correcting code is to remove noise introduced in this way. Again we cannot use the techniques used by classical error correction mechanism as we have two hurdles in quantum computing. Firstly, we cannot clone quantum state. Secondly,

it is quite likely that measurement of a quantum state would collapse the original state and thus the original information would be lost. So the first fact restrains us from adding the redundant information and the second fact seems to prevent us from detecting the quantum state.

1. Independent error model

By independent error model, we mean the interactions between the qudits and the channels are independent from qudit to qudit. In another words, each operator from the operator sum representation for quantum noise is a tensor product of one qubit operators. For example, an operator E_i for a two qudit system may be $E_i = X \otimes Y$. This error model is very often analogous to the one used in classical theory of error correction.

2. Properties of quantum codes

As we have already mentioned a code to encode k qudits in n qudits will have 2^k basis codewords corresponding to the basis of original states. Linear combination of these basis codewords is also a valid codewords. Subspace C of valid codewords is a Hilbert space in its own right , a subspace of the full 2^n dimensional Hilbert space. We only need to consider whether a code can correct a basis of errors. Because if we can correct errors E and F, we can correct $\alpha E + \beta F$.

One very convenient basis which we have used in our work is the set of tensor products of error operators. The set of all these tensor products with a possible overall factor of -1 or $\pm i$ forms a group G under multiplication. In general, there are three kinds of error which occurs in codewords. Let E be the error affecting the codes pace and $|v\rangle$ and $|w\rangle$ be two code vectors.

1. The first kind is one which does not effect the codeword. i.e is $E|v\rangle = |v\rangle$.

2. Error which acting on a codeword produce invalid codeword.

3. Error which converts the codeword to a different codeword in the same codespace. i.e $E|v\rangle = |w\rangle$.

The first kind of errors does not produce any harm so it falls under detectable error. The second kind of error is also detectable but the third kind of error is not detectable as it is in the same space. Thus the condition for error detection is $E|v\rangle \neq |w\rangle$. *If $|i\rangle$ and $|j\rangle$ be two quantum digits then, an error E_a is detectable if and only if E_a satisfies the condition $\langle j|E_a|i\rangle = C_a\delta_{ij}$. This is the necessary and sufficient condition for an error E_a to be detectable.*

In order for the code to correct error E_a and E_b, we must be able to distinguish error E_a acting on one basis codeword $|i\rangle$ from error E_b acting on a different basis codeword $|j\rangle$. That is,

$$\langle i|E_a^\dagger E_b|j\rangle = 0,$$

where $i \neq j$. However this is insufficient to guarantee a code will work as a quantum error-correcting code. When we make a measurement to find out about the error, we must learn nothing about the actual state of the code within the coding space. Because if we did learn something, we will be disturbing superpositions of the basis states, so while we might correct the basis states, we will not be correcting an arbitrary valid codeword. We usually learn information about the error by measuring $\langle i|E_a^\dagger E_b|i\rangle$ for all errors E_a, E_b, where this quantity must be the same for all basis codewords:

$$\langle i|E^\dagger F|i = \langle j|E_a^\dagger E_b|j$$

Therefore,

$$\langle i|E_a^\dagger E_b|i\rangle = C_{ab}\delta_{ij}$$

for all i, j ranges in basis codewords and E_a, E_b be all possible errors. C_{ab} is independent of i, j [12] 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.

3. Quantum error correction

Suppose the quantum channel is transmitting encoded quantum digit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ over quantum state C^2, subjected to error operator X which has following effect on single qudit:

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

The error is called digit flip as it flips between $|0\rangle$ and $|1\rangle$ here. Simple idea how to protect data against digit flip errors consists in encoding logical qudit $\alpha|0\rangle + \beta|1\rangle$ as three entangled qudits,

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|000\rangle + \beta|111\rangle.$$

As we have discussed earlier that we have two insurmountable problem in quantum computing. One is the no-cloning theorem because of which we cannot directly do $|\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$. We can introduce some auxilary qubits and make them entangled with the qubits we want to transmit. By using quantum circuit controlled not gate we can encode in the following ways $\alpha|0\rangle + \beta|1\rangle \otimes |0\rangle^2 \longrightarrow \alpha|000\rangle + \beta|111\rangle$. There can be two kinds of error which can occur in the quantum state - bit flip and phase flip error. Though here we are confined to bit flip errors but can refer to both bit and phase flip errors explained in shor's 9 bit code [4]. For example, if the bit flip occurs on second qudit of encoded data, the state will be $|\psi_2\rangle = \alpha|010\rangle + \beta|101\rangle$. The error correction is based on two procedures, error detection detects the error and then second recovery procedure from error, using the information gained by error detection recovers the initial state. Error detection procedure can be performed by projective measurement, with four projection operators:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \text{ (no error)}$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \text{ (bit flip on first qubit)}$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \text{ (bit flip on second qubit)}$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \text{ (bit flip on third qubit).}$$

If an error on i-th quantum digit occurs on the state $|\psi\rangle$ and transforms the three qubits to the state $|\psi_i\rangle$ then $\langle\psi_i|P_j|\psi_i\rangle = \delta_{ij}$. The outcome of error detection on the state $|\psi_i\rangle$ is certainly i. This measurement never changes the state of measured system since $P_i|\psi_i\rangle = |\psi_i\rangle$ The recovery action is following: if output of the error detection is 0 no action is needed, otherwise if output i is obtained then we will flip i-th qudit back to its initial encoded state.

The problem of quantum error correcting code is more complicated if we want to protect data against arbitrary error on single qudit. It turns out that a code which can correct both quantum digit flip and phase flip errors is able to correct an arbitrary error on single qudit [13]. The first solution of this problem was provided by Peter Shor by introducing so known 9-qubits Shor code which protects against arbitrary error on a single qubit [14].

4. Error operators

Error acting on a quantum digit is a linear operator that takes the quantum digit from one state to another. The most commonly used error basis acting on a two dimensional Hilbert space is Pauli bases. Let P be a set of pauli matrices given by I, X, Z, Y. So, in general a quantum error E acting on a quantum digit can be represented as linear combination of qudit flip, qudit shift and qudit flip + phase flip errors. Error basis provides a convenient way to confine to only the errors that are the basis of error vector space. Because of the fundamental linear property of quantum

mechanics any code that can correct errors E_a and E_b are very likely to correct errors $E_a + E_b$. Thus if we can correct errors in the basis set then we can correct any error that can be written as the linear span of this set.[15] Let us consider the errors that form a basis of vector space of linear operators acting on C_p^m Let

$$\mathcal{E} = \{e_1, e_2, e_3....e_{p^{2m}}\}$$

form such basis. If $|\psi\rangle$ represents a state of n p^m-ary systems it can be altered by error operator of the form $E = \sigma_1 \otimes \sigma_2 \otimes ..... \otimes \sigma_n$, where $\sigma_1 \in \{E_1, E_2, ..., E_{p^{2m}}\}$ From the general theory of quantum code it is well known that if a code can correct a given set $\mathcal{E}$ of error operators then it can correct the linear span of $\mathcal{E}$. So it makes sense to concentrate on operators $\mathcal{E}$.

CHAPTER III

THEORY OF STABILIZER CODES

The most important class of quantum code is binary stabilizer code. An appealing aspect for which they are studied so much is that there exists link to classical coding theory that facilitates the construction of good codes. This construction takes a classical binary code, self-orthogonal under a certain symplectic inner product and produces a quantum code, with minimum distance determined from the classical code [9]. They were first formalised by Daniel Gottesman. The theory of binary stabilizer code is well developed. More recently some results were generalized to the case of non binary stabilizer codes [3, 13]. Non binary stabilizer codes over finite field [15] has inspired us to work on non binary stabilizer codes over Finite Frobenius rings. This chapter has two main goals. Initially, we review the theory of stabilizer codes formulated in [16] and additionally we generalize some results.

A. Stabilizer codes

A stabilizer code is defined as 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 error operator. Stabilizer code are characterized by the error operators that stabilize them.

Let G_n be the error group generated by the error bases and let S be the subgroup of G_n. Therefore the stabilizer code is defined as,

$$Q = \{|v\rangle | s|v\rangle = |v\rangle, \forall s \in S\} \text{ where, } S \text{ is a subgroup of } G_n$$

All operators in the stabilizer must commute with each other otherwise the code space will only contain zero codeword. For example, if A and B are two operators in the

stabilizer which do not commute with each other, then $|\psi\rangle = AB|\psi\rangle = -BA|\psi\rangle = -|\psi\rangle$.

Thus in gist, to encode k qudits in n, Q has q^k dimensions and S has q^{n-k} elements. The stabilizer S must be an abelian subgroup of the error group G_n. Because only commuting operators can have simultaneous eigenvectors, but as it is abelian and neither -1 nor i is in S, the space Q have dimension q^k.

B. Theory of stabilizer codes over finite Frobenius ring

The most natural class of rings that is suitable for coding theory is given by finite Frobenius rings as they allow us to formulate the dual codes as in the case of codes over finite fields.

There is a well developed theory of stabilizer codes over finite fields. Here we consider the construction of quantum codes over Frobenius rings based on the same idea of classical self-orthogonal codes over ring. The self-orthogonality notion is identified with the symplectic inner product. Self-orthogonal codes with respect to this inner product are used in constructing the quantum Stabilizer codes.

Finite Frobenius rings are considered appropriate for constructing quantum codes, because two classical theorems which are the extension theorem and the MacWilliams identities, are generalized to these rings.

Notation Let R be 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 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 C is defined as $C^{\perp} = \{v \mid (u,v) = 0 \; for \; all \; u \in C\}$ [4]. In this section, we establish the details required to establish a theory of quantum codes over Frobenius ring.

1. Frobenius rings and the concept of generating character

Let R be a finite ring with identity. The character group of the additive group of R which is $(R,+)$ is denoted by $\widehat{R} := Hom_z(R, C^{\times})$. This group has the structure of $R \setminus R$ bimodule. By defining $\chi^r(m) := \chi(rm)$ and ${}^r\chi(m) := \chi(mr)$ for all $\chi \in \widehat{R}$ and for all $r \in R, m \in M$ where M is the module over ring R. A finite ring R is called a Frobenius ring if $R^{\widehat{R}} = R^R$. A character χ is called a generating character if for every $\psi \in \widehat{R}$ there exists a $r \in R$ such that $\psi = \chi^r(a)$ and $a \in R$. A finite ring is called a Frobenius ring if and only if it admits right or left generating character [16].

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

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

Examples of Frobenius rings are [17]: i) A finite field is a Frobenius ring with generating character being defined as $\chi(a) = e^{2\pi itr(a)}/p$, where p is the primitive of the field and tr is the trace of the homomorphism $F \rightarrow F_p$ and F_p is the prime subfield.

ii) Ring of integers modulo m denoted as $R = Z/m$ belong to this class. Suppose $\xi = e^{(2\pi i/m)}$, then generating character is $\chi(x) = \xi^x$.

iii) Any Galois ring is a Frobenius ring. A Galois ring is a Galois extension of $Z/(p^n)$ and is given by $GR(p^n, r) = Z/(p^n)[x]/(f)$ where f belongs to $Z/(p^n)$ is a

monic irreducible polynomial $\sum_{i=1}^{r} a_i X^{r-i}$ where $a_i \in Z/(p^n)$. Let $\xi = exp(2\pi i/p^n)$ then, $\chi(a) = \xi^a$ is a generating character.

2. Inner product

Symplectic inner product Let $(a|b)$ and $(a^{'}|b^{'})$ denote two codewords in the code C. Then the symplectic inner product of the two vectors is defined as $\chi(b.a^{'} - b^{'}.a)$. If C is the code then its dual $C^{\perp}$ is defined as $C^{\perp} = \{(a|b)|\chi(b.a' - b'.a) = 1 for all (a'|b') \in C\}$

Lemma 1 *Let χ be a character of a finite frobenius ring R. Then χ is a right generating character if and only if $ker(\chi)$ contains no non-zero ideals.*

Proof Let us define a homomorphic function $\phi : R \to \widehat{R}$ by $\phi(r) = \chi^r$ As we know $|\widehat{R}| = |R|$, $\phi : R \to \chi^r$ is an isomorphism if and only if ϕ is injective. We have $r \in ker(\phi)$ if and only if $\chi^r(x) = \chi(rx) = 1$ for all $x \in R$ if and only if the right ideal $rR \subset ker(\chi)$.

The symplectic inner product over Frobenius ring is non-degenerate. Because $\chi(\langle (a|b)|(c|d)\rangle) = 1$ for all $(a|b), (c|d) \in R^{2n}$ and $(a|b) = 0$ else if $(a|b) \neq 0$ then $\chi(a_i d_i) = 1$ for some $(a_i, 0, 0, \cdots, 0)$ which implies kernel of the character contains the right ideal. This contradicts our above theorem. If C is a free code then $C^{\perp}$ is also free with respect to symplectic inner product.

Hilbert-Schmidt inner product Let us define the normalized Hilbert-Schmidt inner product on the set of linear operators of C^q as

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

where tr is the trace of the matrix and $A^{\dagger}$ is the adjoint of the linear operator A.

3. Nice error bases

An error basis $\mathcal{E}$ is called a nice error basis if it satisfies the following conditions [16]:

1. It contains the identity matrix.

2. The product of any two elements should be a scalar multiple of some element of the error basis.

3. For any two distinct elements E_i, E_j of $\mathcal{E}$, $tr(E_i^\dagger E_j = 0)$.

Here we construct the error base and prove that it is a nice error bases. Suppose R be a finite Frobenius ring with q elements. The addition and multiplication in the ring R will be used to define an unitary shift and a multiplication operator on C^q. For each a, b in R, we define a shift operator $X(a) : C^q \to C^q$ and multiplication operator $Z(b) : C^q \to C^q$ by

$$X(a)|x\rangle = |x + a\rangle$$
$$Z(b)|x\rangle = \chi(bx)|x\rangle$$

where x is in R and χ is an irreducible character of the additive abelian group $(R, +)$. We form the set

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

This set has some interesting properties as follows:

1. It contains the identity matrix as in the matrix $X(0)Z(0)$ is a identity matrix.

2. The product of two matrices in ε is a scalar multiple of another element in $\mathcal{E}$.

We know $\chi(ba)X(a)Z(b) = Z(b)X(a)$ which implies that the product of two operators is given by

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

which implies our statement.

3.The trace $Tr(A^\dagger B) = 0$ for distinct elements $A, B \in \mathcal{E}$. A finite set of q^2 unitary

matrices that satisfy $1, 2, 3$ is called nice error bases. The set $\mathcal{E}$ of error operators forms a basis of the set of complex $q \times q$ matrices due to property 3. Let R be a finite ring. Denote $Irr(R) = Hom((R, +), C^{\times})$, the set of irreducible characters of the additive group $(R, +)$. An irreducible character χ is generating if and only if $Irr(R) = \{\chi_b | b \in R\}$ where $\chi_b(x) = \chi(bx)$ for all $x \in R$. All finite ring does not necessarily have a generating character. We call a ring nice if it has a generating character. From the definition of Frobenius ring which tells that a ring is Frobenius if and only if it admits left and right generating character, thus Frobenius ring is a nice ring [18].

Let $A = X(a)Z(b)$ and $B = X(a')Z(b')$ are two error operators and $C = \{\chi_b | b \in R\}$ be the set of all irreducible characters. Then we have,

$$Tr(A^{\dagger}B) = \begin{cases} 0 & \text{if } a \neq a' \\ \sum_{x \in R} \overline{\chi(b'x)}\chi(bx) = \langle \chi_{b'} | \chi_b \rangle & \text{if } a = a' \end{cases}$$

which implies character χ_b and $\chi_{b'}$ are orthogonal when $b \neq b'$ and thus $\mathcal{E}$ is an orthonormal basis. We can state that

Proposition B.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 $C = \{\chi_b |\, b \in R\}$ is the set of all irreducible characters of the additive group of R [16].*

As R is a nice ring thus $\mathcal{E} = \{X(a)Z(b) | a, b \in R\}$ is a nice error basis on C^q and the above discussion justifies the statement.

Lemma 2 *If $\mathcal{E}_1$ and $\mathcal{E}_2$ are nice error bases then,*

$$\mathcal{E} = \{E_1 \otimes E_2 | E_1 \in \mathcal{E}_1, E_2\mathcal{E}_2\}$$

is a nice error bases as well.

The lemma can be proved directly from the definition.

Let $a = (a_1, \cdots, a_n) \in R^n$. We can write $X(a) = X(a_1) \otimes \cdots \otimes X(a_n)$ and $Z(a) = Z(a_1) \otimes \cdots \otimes Z(a_n)$ for the tensor product of n operators over C^{q^n}. After defining the operators on C^{q^n}, we can state the following Corollary.

Corollary B.2 *The set $\mathcal{E}_n = \{X(a)Z(b)|a, b \in R^n\}$ is also a nice error basis on C^{q^n}.*

4. Stabilizer codes

Let G_n be the error group generated by the nice error basis. By including all the scalar multiples of the operators of the error basis, we get the error group

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

We call G_n be the error group associated with the nice error basis $\mathcal{E}_n$. A non-zero subspace of C^{q^n} is called Stabilizer code Q that satisfies

$$Q = \bigcap_{E \in S} \{v \in C^{q^n} | Ev = v\}$$

Where S is a subgroup of G_n. Q is the joint eigenspace of a subgroup S with eigenvalue 1. A stabilizer code contains all joint eigenvectors of S with eigenvalue 1. If it does not, then it is not a stabilizer code for S.

C. Commutativity of operators

Commutativity of operators of the error group plays a crucial role to understand the relation between classical and stabilizer codes. Let E_a be a error operator and $a = (a_1, a_2, \cdots, a_n)$. Suppose the error operator is acting on n bit quantum state. The operator can be either a bit flip or a phase flip error or both. So, in case of bit

flip it can be denoted as X_a and decomposed as $X^{a_1} \otimes X^{a_2} \otimes \cdots \otimes X^{a_n}$. Similarly if the operator is a phase flip, it is denoted as Z_b where $b = (b_1, b_2, \cdots, b_n)$. This operator can be expanded to act on n bit quantum state as $Z^{b_1} \otimes Z^{b_2} \otimes \cdots \otimes Z^{b_n}$. Any error operator can be represented as $X_a Z_b = X^{a_1} Z^{b_1} \otimes X^{a_2} Z^{b_2} \otimes X^{a_n} Z^{a_n}$. The main relation between stabilizer and classical code is that the errors in the error group can be characterized by the classical codes. Now we represent the error $X_a Z_b$ by a vector $(a|b)$ which is nothing but a vector over a field or a ring. So, the classical code related to stabilizer code can be denoted by

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

C is a additive code as it needs to have the property that any two vectors in it are close under vector addition. Let C' be the dual of the code C with respect to the inner product $\langle (a|b), (a'|b') \rangle = (b.a' + a'.a) \, mod \, 2$. We denote C' to be the centralizer of the stabilizer as it has the property that it commutes with every element of S. Let it be defined as below

$$C^{'} = \{(a'|b')|b.a' + b'.a = 0 \, mod \, 2, \; for \; all \; (a|b) \in C\}$$

Since stabilizer is contained in its $C^{'}$ therefore C should be a self orthogonal code with respect to the above inner product. Thus there is a relation between quantum stabilizer code and classical code.

1. Relation to classical codes

The condition for two error operators to commute with each other is given by the following lemma.

Lemma 3 *Two elements $X(a)Z(b)$ and $X(a')Z(b')$ of the error group commute if and only if*

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

Proof Let $x \in R^n$, we have $X(a)Z(b)|x\rangle = X(a)\chi(b.x)|x\rangle = \chi(b.x)|x + a\rangle$ and $Z(b)X(a)|x\rangle = Z(b)|x + a\rangle = \chi(b.x)\chi(b.a)|x + a\rangle$. Therefore $\chi(b.a)X(a)Z(b) = Z(b)X(a)$. Thus it follows that

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

and

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

From both the equation we can say that $X(a)Z(b)$ and $X(a')Z(b')$ will commute only if $\chi(b.a' - b'.a) = 1$

We define the symplectic weight swt of a vector $(a|b)$ in R^{2n} as

$$swt((a|b)) = |\{k \mid (a_k, b_k) \neq (0, 0),\ for\ 1 \leq k \leq n\}|$$

The weight $wt(E)$ in the group G_n is defined to be the number of non-identity tensor components. Thus $wt(E) = swt((a|b))$.

Minimum distance of quantum code is d if it can detect all errors in G_n of weight less than d but cannot detect some errors of weight d. We say that Q is an $((n, K, d))_q$ code if and only if Q is a $k-$dimensional subspace of C^{q^n} with minimum distance d.

2. Additive codes

Relation between stabilizer codes and classical codes comes from the fact that the errors in the error group G_n that are detectable by the stabilizer codes can be characterized by the classical codes. If S is a subgroup of G_n, then C_{G_n} denote the centralizer of S in G_n

$$C_{G_n} = \{E \in G_n \mid EF = FE \; for \; all \; F \in S\}$$

and $SZ(G_n)$ denotes the group generated by S and the center $Z(G_n)$ of the group G_n

Lemma 4 *Suppose that $S \leq G_n$ is the stabilizer group of a stabilizer code Q_s of dimension $dim Q_s > 1$. An error E in G_n is detectable by the quantum code Q_s if and only if either E is an element of $SZ(G_n)$ or E does not belong to the centralizer of $C_{G_n}(S)$.*

Proof Any element E in $SZ(G_n)$ is a scalar multiple of stabilizer S, E acts on a quantum state by multiplication with a scalar λ_E on Q and hence the error E is detectable. Suppose E is an element of G_n, that does not commute with some element F of the stabilizer S. Therefore $EF = \lambda FE$ where $\lambda \neq 1$. For any vector u and v in Q_s we have $\langle u|E|v\rangle = \langle u|EF|v\rangle = \lambda\langle u|FE|v\rangle = \lambda\langle u|E|v\rangle$ which implies that $\langle u|E|v\rangle = 0$ since $\lambda \neq 1$. Thus we can say that the error E is detectable.

Remark: We say that a quantum code Q is pure to t if and only if its stabilizer group S does not contain non-scalar matrices of weight less than t. A quantum code is called pure if and only if it is pure to its minimum distance. It is always assumed that an $((n, 0, d))_q$ code has to be pure [15].

Corollary C.1 *If a stabilizer code Q has a minimum distance d and is pure t, then all errors $E \in G_n$ with $1 \leq wt(E) < min\{t, d\}$ satisfy $\langle u|E|v\rangle = 0$ for all u, v in Q.*

Proof Since the weight of the error is less than the minimum distance, it follows that error E is detectable. Since the $wt(E) < t$ and the quantum code is pure to t, it implies that E is not an element of $SZ(Gn)$. Hence E does not belong to the centralizer $C_{G_n}(S)$. Thus the fact $\langle E\rangle = 0$ follows from the above lemma.

3. Codes over ring R with q elements

Let R be a nice ring. The errors in the error group G_n that are detectable by the stabilizer are characterized by the additive codes over R. Let χ be a character in $Hom(R, C^{\times})$. For each χ in $Hom(R, C^{\times})$ there exists a unique function

$$\psi : R \to Q/Z$$

such that

$$\chi(x) = exp(2\pi\psi(x)),\ x \in R.$$

Let $\langle\cdot|\cdot\rangle_\chi : R^{2n} \times R^{2n} \to Q/Z$. Therefore,

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

for all $(a|b)$ and $(a'|b')$ in R^{2n}. The $\langle u|v\rangle_\chi$ is called the bilinear inner product.

Lemma 5 *Let R be a nice ring with χ be the generating character and $u_1, u_2, v, v_1, v_2, u \in R^{2n}$ and $n \in Z$. Then the following conditions holds [16]*

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. $\langle nu|v\rangle_\chi = \langle u|nv\rangle_\chi = n\langle u|v\rangle_\chi$,
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* $v = 0$.

Let us also define another form called symplectic form $\langle\cdot|\cdot\rangle_s : R^{2n} \times R^{2n} \to R$ by

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

both the forms can be related as

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

and the inner product is called the symplectic inner product. Suppose C be a subgroup of $(R^{2n}, +)$. The relationship between the cardinality of two codes C and $C^{\perp}$ is given by [16]

$$|C||C^{\perp}| = |R^{2n}|.$$

Likewise if we impose C to be linear, which is when C is sub-module of the R^{2n} module, then the following lemma can be stated.

Lemma 6 *Suppose R be a finite (commutative) chain ring with generating character χ. Let C and D be $R-$sub-modules of R^{2n}. Then,[16]*

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

CHAPTER IV

THEORY OF STABILIZER CODES OVER QUADRATIC ALGEBRA

Let R be a commutative ring satisfying $1 \neq 0$. A free algebra of rank 2 over R is called a **quadratic algebra** over R. Recall that for elements x, y of the algebra A and a scalar r in R, we have

$$r(xy) = (rx)y = x(ry).$$

Since A is a free R-algebra, the ring R can be understood as a subring of A by identifying the ring element r with the element $r1_A$ of the center of the algebra A.

A quadratic algebra A over R contains an element x such that $B = \{1_A, x\}$ is a basis of A. Thus, there exist elements a, b in R such that $x^2 = a1_A + bx$. This equation completely determines the multiplication in A. Indeed, given two elements y_1 and y_2 of A, we can express them in the form $y_1 = a_1 1_A + b_1 x$ and $y_2 = a_2 1_A + b_2 x$ for some elements a_1, b_1, a_2, b_2 in R; multiplication yields

$$\begin{aligned} y_1 y_2 &= (a_1 1_A + b_1 x)(a_2 1_A + b_2 x) \\ &= a_1 a_2 1_A + (a_1 b_2 + a_2 b_1)x + b_1 b_2 x^2 \\ &= a_1 a_2 1_A + (a_1 b_2 + a_2 b_1)x + b_1 b_2 (a1_A + bx) \\ &= (a_1 a_2 + b_1 b_2 a)1_A + (a_1 b_2 + a_2 b_1 + b_1 b_2 b)x. \end{aligned}$$

Since R is commutative, it follows from this expression that $y_1 y_2 = y_2 y_1$ holds, that is, A must be a commutative algebra.

Lemma 7 *Let A be a quadratic algebra over R with basis $\{1_A, x\}$ such that $x^2 = a1_A + bx$ for some a, b in R, and A' a quadratic algebra over R with basis $\{1_{A'}, x'\}$ such that $x'^2 = a'1_{A'} + b'x'$ for some a', b' in R. Let $\varphi : A' \to A$ be an A-linear map satisfying $\varphi(1_{A'}) = 1_A$ and $\varphi(x') = v$ for some element v of A. Then φ is an*

A-algebra homomorphism if and only if

$$v^2 = a'1_A + b'v$$

holds.

Proof See [19].

Conjugation : Let A be a quadratic algebra over commutative ring R with basis $\{1_A, x\}$, where $x^2 = a + bx$. The element $y := b - x$ satisfies

$$y^2 = (b - x)(b - x) = a + b(b - x)$$

Thus there exists an A algebra automorphism σ on A satisfying

$$\sigma(1_A) = 1_A \text{ and } \sigma(x) = b - x$$

σ^2 is an identity map on A and σ is an **involution**. We call σ the **conjugation map** on A. For c, d in R, we have

$$\sigma(c + dx) = (c + d(b - x)) = (c + db) - dx$$

Norm : We can define the **norm** N of an element $y = c + dx$ by

$$\begin{aligned} \mathrm{N}(y) &= y\sigma(y) = (c + dx)(c + db - dx) \\ &= c(c + db) - cdx + dx(c + db) - d^2(a + bx) \\ &= c^2 + cdb - d^2a \end{aligned}$$

Thus, the norm is a map from A to R.

Lemma 8 *Let A be a quadratic algebra over a commutative ring R. Then*

(i) The norm is multiplicative (ii) An element y in A is a unit if and only if $N(y)$ is a unit in R.

Proof (i) Suppose that u, v are elements of A. Then

$$\mathrm{N}(uv) = uv\sigma(uv) = uv\sigma(u)\sigma(v) = u\sigma(u)v\sigma(v) = \mathrm{N}(u)\,\mathrm{N}(v).$$

(ii) Suppose that z is an element in A such that $yz = 1$. Then $\mathrm{N}(yz) = \mathrm{N}(y)\,\mathrm{N}(z) = 1$, so $\mathrm{N}(y)$ is a unit in R. Conversely, suppose that $\mathrm{N}(y)$ is a unit in R. Then $\mathrm{N}(y)^{-1}\sigma(y)$ is a multiplicative inverse of y.

Trace : We can define the **trace** tr of an element $y = c + dx$ of A by

$$\mathrm{tr}(y) = y + \sigma(y) = c + dx + c + db - dx = 2c + db.$$

Thus, the trace maps elements from the algebra A to R.

Different and Discriminant : Let A be a quadratic R-algebra with basis $B = \{1, x\}$. The element $x - \sigma(x)$ is called the **different** with respect to the basis B. The different with respect to different bases just differ by a factor that is a unit in R.

The **discriminant** of A with respect to the basis B is the element

$$\delta := b^2 + 4a = -\,\mathrm{N}(x - \sigma(x)).$$

The principal ideal δR generated by a discriminant is called the **discriminant ideal**. The discriminants of A with respect to two different bases just differ by a factor that is the square of a unit in R. Thus, even though the discriminants of A with respect to different bases may differ, their discriminant ideals are the same.

A quadratic R-algebra A is called **unramified** if and only if its discriminant ideal is equal to R.

Lemma 9 *Let A be a quadratic R-algebra such that its discriminant is not a zero divisor. For all y in A, we have $y = \sigma(y)$ if and only if $y \in R$.*

Proof Let $B = \{1, x\}$ be a basis of A with $x^2 = a+bx$. The discriminant d of A with respect to the basis B is not a zero divisor. Since $\mathrm{N}(x - \sigma(x)) = -d$, the different $x - \sigma(x) = 2x - b$ cannot be a zero divisor either.

Suppose that y is an element of the algebra A satisfying $y = \sigma(y)$. If we write y in the form $y = c+dx$ for some c, d in R, then $c+dx = c+db-dx$, hence $d(2x-b) = 0$. Since $2x-b$ is not a zero divisor, this means that d must be 0. Hence, y is an element of R, as claimed. The proof of the converse is straightforward.

Examples : Let us exemplify the concept and see what will be the outcome if we play around with the values of a and b. Suppose we take A as a quadratic algebra over commutative Ring R with basis $\{1_A, x\}$ where $x^2 = x$. Then the ring A is isomorphic $R \oplus R$. That is the cartesian product ring $R \times R$ made into an R algebra via the diagonal map $R \to R \times R$ we have $\sigma(1_A) = 1_A$ and $\sigma(x) = 1 - x$. Here σ is again a involution. In this case Norm is 0 since, let $y = dx$ then, Norm $= y.\sigma(y) = (dx)(d - dx) = d^2x - d^2x^2$ But we know here $x^2 = x$ therefore Norm $= 0$. Trace is $tr(y) = y + \sigma(y) = dx + d - dx = d$, which belongs to R. And Discriminant is 1

Example 1 : For basis $\{1_A = (1, 1), x = (0, 1)\}$ of $R \oplus R$. We have $\phi A \to R \oplus R$ by $\phi(1_A) = (1, 1)$ and $(0, 1)^2 = (0, 1)$. Clearly ϕ is a isomorphism. Conjugation is $\sigma(x) = 1 - x = (1, 0)$ Suppose $y = (1, 0)$ then $y^2 = (1, 0)$ i.e it satisfies $y^2 = y$ In this case Norm is 0 and trace is 1 and discriminant is 1

Example 2 : If $t \in R^*$ then, $x^2 = bx + a = tbx + t^2a$

Example 3 : Let A be a quadratic algebra over R where $x^2 = bx + a$ and B be any quadratic algebra over R where $x^2 = dx - c$ then we can say both of the algebra are

isometric to each other if there exists r in R and u in R^*, ring which are units such that

$$d = ub + 2r \text{ and } c = u^2 arub - r^2$$

Example 4 : IF $R = C$ be the algebra over complex numbers. Quadratic algebra over C is isomorphic to either the trivial algebra $C[X]/X^2 - X$ or the algebra of dual numbers $C[X]/(X^2)$

Example 5 : Let A be a quadratic algebra over Z/mZ with basis $\{1, x\}$ and $x^2 = -1$.

Lemma 10 *Let i denote the solution of equation $x^2 = -1$. Let us define the set $A = \{a+ib|a, b \in R\}$ of q^2 elements such that addition is given by $(a+ib)+(c+id) = (a+c)_q+i(b+d)_q$ and multiplication is given by $(a+ib).(c+id) = (ac-bd)_q+i(bc-ad)_q$. The set A is a commutative ring.*

Proof It is clear from the theorem that any element $u = e + if, v = j + ik$ and $w = x + iy$ satisfies $u + (v + w) = (u + v) + w, u + v = v + u, u.(v + w) = u.v + u.w$ and $uv = vu$

Conjugation of x is $-x$

Discriminant in this case is > 0 i.e $b^2 + 4a < 0$. Both trace and norm maps from A to R. Let $q_1, \cdots, q_r$ be a sequence of prime numbers such that (-1) is quadratic non residue of q_j such that $j = 1, 2, \cdots, r$. Let $q = \prod_{j=1}^{r} q_j$. A be a R algebra as defined above i.e $A = \{a + ib|a, b \in R_q\}$ with respect to addition and multiplication *modq*.

Theorem .2 *Direct sum of Galois fields $S_{q^2=F_{q_1^2}+\cdots+F_{q_r^2}=\{(a_1,a_2,\cdots,a_r)|a_j \in F_{q_j}^2}, j = 1, \cdots, r\}$ where $(a_1, a_2, \cdots, a_r) + (b_1, b_2, \cdots, b_r) = (a_1 + b_1, \cdots, a_r + b_r)$ and $(a_1, a_2, \cdots, a_r).(b_1, b_2, \cdots, b_r) = ((a_1b_1, \cdots, a_rb_r)$. S is a ring with q^2 element which is isomorphic to the ring A.*

Proof If $(a+ib) \in A$ then let $\phi : a+ib \rightarrow (a+ib)modq_1, (a+ib)modq_2, \cdots, (a+ib)modq_r$ be the mapping. Since j is a solution of $x^2 = -1$, it is identically the solution of $x^2 = -1 modq_j$ for $k = 1, 2, \cdots, r$. The residue $a_{q_j} + ib_{q_j}$ of $(a+ib)modq_j$ is an element of $F_{q_j^2}$ for $j = 1, 2, \cdots, r$ Thus, ϕ is a mapping of A into the ring $S = \sum_{j=1}^{n} F_{q_j^2}$ which implies $\phi : A \rightarrow F_{q_1^2} + F_{q_2^2} + \cdots + F_{q_j^2}$. If $u = e+if, v = j+ik$ are arbitrary elements in A , then

$$\phi(u+v) = \phi(u) + \phi(v)$$

and

$$\phi(u.v) = \phi(u).\phi(v).$$

ϕ is a homomorphic function. $\phi(u)$ maps the ring A into the direct sum of Galois fields S i.e

$$\phi(u) = \phi(e+if) = (e_{q_1} + if_{q_1}, e_{q_2} + if_{q_2} + \cdots, e_{q_r} + if_{q_r})$$

$a \equiv e_{qj} modq_j$

and $b \equiv e_{q_j} modq_j$ for $j = 1, 2, \cdots, r$ It each element in S is a image of a unique element in A which follows that the function ϕ is one to one and hence an isomorphic mapping of S to A.

Isometric isomorphism : Let R be a nonzero commutative ring, and A a quadratic R-algebra, that is, A is a free algebra of rank 2 over R. Let $B = \{1, x\}$ be a basis of A over the ring R such that $x^2 = \alpha + \beta x$ for some α, β in R. We can define a map ϕ: $R^{2n} \rightarrow A^n$ by

$$\phi((a|b)) = a + bx \tag{4.1}$$

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

Lemma 11 *The map ϕ given in (4.1) is an R-linear isomorphism of R-modules that is isometric in the sense that*

$$\mathrm{swt}((a|b)) = \mathrm{wt}(\phi((a|b))).$$

In other words, a vector of symplectic weight d is mapped by ϕ to a vector of Hamming weight d.

Proof It is clear that ϕ is an R-linear map. The map is isometric, since for a vector $(a|b)$ in R^{2n}, we have

$$\begin{aligned} \mathrm{swt}((a|b)) &= |\{i|1 \leq i \leq n, (a_i|b_i) \neq (0,0)\}| \\ &= |\{i|1 \leq i \leq n, a_i + b_i x \neq 0\}| \\ &= \mathrm{wt}(\phi((a|b))), \end{aligned}$$

as claimed.

A. Alternating form

We introduce an alternating form that will enable us to obtain stabilizer codes from classical codes over quadratic $R-$algebra A. A quadratic algebra unramified if and only if $x - \sigma(x)$ is a unit. For $w, v \in A^n$ we define,

$$\langle v|w\rangle_a = (\frac{v.\sigma(w) - \sigma(v).w}{x - \sigma(x)})$$

If we define a map $\phi : R^n \times R^n$ such that $\phi(v_X|v_Z) = v_X + xv_Z$ where $(v_X|v_Z \in R^{2n}$

Theorem A.1 *Suppose that $C \leq R^{2n}$ and $D \leq A^n$ is a R linear code. According to the above mapping ϕ let us consider $\phi(C) = D$ satisfying $D \subseteq D^{\perp_a}$. Then $C \leq C^{\perp_a}$. Also $D^{\perp_a} = D^{\perp_{\langle\cdot|\cdot\rangle_s}}$*

Proof Let $(v_X|v_Z) in C$ and $(w_X|w_Z)$ in $C^{\perp}$. Clearly if $\phi(C) \leq \phi(C^{\perp_a})$ then, $C \leq C^{\perp_a})$.

$\langle \phi(v_X|v_Z)|\phi(w_X|w_Z)\rangle_a = 0$
i.e. $(\dfrac{\phi(v_X|v_Z)\sigma(\phi(w_X|w_Z) - \sigma(\phi(v_X|v_Z))\phi(w_X|w_Z}{x-\sigma(x)})$
$= (\dfrac{v_X w Z(x-\sigma(x)) - v_Z w_X(x-\sigma(x))}{x-\sigma(x)})$
$= (\dfrac{(x-\sigma(x))(v_X w_Z - v_Z w_X)}{x-\sigma(x)})$
$= (v_X w_Z - v_Z w_X)$

This proves the theorem.

Lemma 12 *The form defined in equation (??) satisfies*

(i) $\langle v_1 + v_2|w\rangle_a = \langle v_1|w\rangle_a + \langle v_2|w\rangle_a$

(ii) $\langle v|w_1 + w_2\rangle_a = \langle v|w_1\rangle_a + \langle v|w_2\rangle_a$

(iii) $\langle rv|w\rangle_a = \langle v|w\rangle_a = r\langle v|w\rangle_a$

(iv) $\langle v|v\rangle_a = 0$

for all v, v_1, v_2, w, w_1, w_2 in A^n, and all r in R. Thus, it is an R-linear alternating form.

Proof (i) Since σ is linear, we have

$$\begin{aligned}\langle v_1 + v_2|w\rangle_a &= \frac{(v_1+v_2)\cdot\sigma(w) - \sigma(v_1+v_2)\cdot w}{x-\sigma(x)} \\ &= \frac{v_1\cdot\sigma(w) - \sigma(v_1)\cdot w}{x-\sigma(x)} + \frac{v_2\cdot\sigma(w) - \sigma(v_2)\cdot w}{x-\sigma(x)} \\ &= \langle v_1|w\rangle_a + \langle v_2|w\rangle_a.\end{aligned}$$

The proof of the properties (ii) and (iii) is similar. Since A is commutative, we have $v\cdot\sigma(v) = \sigma(v)\cdot v$, which implies property (iv).

Let R be a nonzero commutative ring. In the construction of quantum stabilizer codes, a different $R-$linear from played a significant role, namely the symplectic form $\langle\cdot|\cdot\rangle_s : R^{2n}\times R^{2n}\to R$ defined by

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

for all $(a|b)$ and $(a'|b')$ in R^{2n}. The symplectic form over R^{2n} and the alternating form over quadratic algebra over R are closely related, as the next theorem shows.

Theorem A.2 *Let R be a nonzero commutative ring, and A an unramified quadratic R-algebra. For all elements $(a|b)$ and $(a'|b')$ in R^{2n}, we have*

$$\langle (a|b)|(a'|b')\rangle_s = \langle \phi((a|b)|\phi((a|b))\rangle_a,$$

where ϕ is the isometry defined in (4.1). In particular, for all v, w in A^n, the value of the alternating form $\langle v|w\rangle_a$ is in R.

Proof We have

$$\phi((a|b)) \cdot \sigma\phi((a'|b')) = a \cdot a' + (b \cdot a')x + (a \cdot b')\sigma(x) + (b \cdot b')\,\mathrm{N}(x)$$
$$\sigma\phi((a|b)) \cdot \phi((a'|b')) = a \cdot a' + (b \cdot a')\sigma(x) + (a \cdot b')x + (b \cdot b')\,\mathrm{N}(x)$$

Taking the difference of these terms yields

$$\phi((a|b)) \cdot \sigma\phi((a'|b')) - \sigma\phi((a|b)) \cdot \phi((a'|b')) = (b \cdot a')(x - \sigma(x)) + (a \cdot b')(\sigma(x) - x).$$

It follows from this calculaton that

$$\begin{aligned}\langle \phi((a|b)|\phi((a|b))\rangle_a &= \frac{(b \cdot a')(x - \sigma(x)) + (a \cdot b')(\sigma(x) - x)}{x - \sigma(x)} \\ &= (b \cdot a') - (a \cdot b') \\ &= \langle (a|b)|(a'|b')\rangle_s,\end{aligned}$$

as claimed. Since the isometry ϕ is surjective, it follows that the values of the alternating form are in R for all pairs of arguments.

Pairings : Let R be a nonzero commutative Frobenius ring with generating character χ. Let A be an unramified quadratic R-algebra. We define a pairing $\langle \cdot \,|\, \cdot \rangle_{s,\chi} \colon R^{2n} \times R^{2n} \to \mathbf{C}$ by

$$\langle u|u' \rangle_{s,\chi} = \chi(\langle u|u' \rangle_s)$$

for all $u, u' \in R^{2n}$, and a pairing $\langle \cdot \,|\, \cdot \rangle_{a,\chi} \colon A^n \times A^n \to \mathbf{C}$ by

$$\langle v|w \rangle_{a,\chi} = \chi(\langle v|w \rangle_a)$$

for all v, w in A^n. Thus, these pairings are simply obtained by applying the character χ to the corresponding bilinear forms. We write

$$u \perp_{s,\chi} u' \text{ if and only if } \langle u|u' \rangle_{s,\chi} = 1,$$

$$v \perp_{a,\chi} w \text{ if and only if } \langle v|w \rangle_{a,\chi} = 1.$$

Lets now relate the stabilizer code to that of the classical code.

Theorem A.3 *Let R be a finite commutative Frobenius ring with generating character χ. Let A be an unramified quadratic R-algebra. An $((n, K, d))_R$ stabilizer code exists if and only if there exists an additive code $D \subseteq A^n$ such that*

a) the cardinality of D is given by $|D| = |R|^n/K$,

b) the code is self-orthgonal, $D \subseteq D^{\perp}$,

c) and $d = \begin{cases} \mathrm{wt}(D^{\perp_{a,\chi}} \setminus D) & \text{if } K > 1, \\ \mathrm{wt}(D^{\perp_{a,\chi}} - \{0\}) & \text{if } K = 1. \end{cases}$

Proof If an $((n, K, d))$ stabilizer code exists, then there exists an additive code $C \subseteq R^{2n}$ such that a') $|C| = |R|^n/K$, b') $C \subseteq C^{\perp_{s,\chi}}$, and c)'

$$d = \begin{cases} \mathrm{swt}(C^{\perp_{s,\chi}} \setminus C) & \text{if } K > 1, \\ \mathrm{swt}(C^{\perp_{s,\chi}} - \{0\}) & \text{if } K = 1, \end{cases}$$

see Theorem[8] [16]. Applying the isometric isomorphism ϕ yields an additive code D with the claimed properties a), b), and c).

Conversely, if there exists an additive code $D \subseteq A^n$ satisfying a), b), and c), then the code $C = \phi^{-1}(D)$ satisfies the properties a'), b'), and c') above. Therefore, an $((n, K, d))_R$ stabilizer code exists by Theorem[8] [16].

Corollary A.4 *If there exists a classical $[n, k]_{q^2}$ additive code $D \leq A$ such that $D \leq D^{\perp_a}$ and $d^{\perp_a} = wt(D^{\perp_a})$ then there exists an $((n, n-2k, \geq d^{\perp_a}))$ stabilizer code that is pure to $d^{\perp}$.*

Hermitian inner product of two vectors x and y in A is $\sigma(x).y$. Two vectors are $x \perp_h y$ if and only if $\sigma(x)y = 0$ Here we relate our trace alternating inner product with hermitian inner product.

Lemma 13 *If two vectors x and y in A satisfy $x \perp_h y$, then they satisfy $x \perp_a y$. In particular if $D \leq A^n$ then $D\perp_h \leq D^{\perp_a}$*

Proof If $\sigma(x).y = 0$ then $x.\sigma(y) = 0$ holds therefore

$$\langle x|y\rangle_a = (\frac{x.\sigma(y) - \sigma(x).y}{\sigma(x) - x}) = 0$$

Thus the theorem holds. Therefore any self-orthogonal code with respect to the hermitian inner product is self-orthogonal with respect to the trace alternating form.

CHAPTER V

CODE CONSTRUCTION RULES OVER FINITE FROBENIUS RINGS

A. Introduction

Here we leverage the theory of stabilizer codes over finite Frobenius ring using trace symplectic form, to establish a set of rules for constructing new codes from old codes. That is, we define and show how to construct new non binary quantum stabilizer codes over Frobenius rings by considering the relation of quantum stabilizer codes to classical codes. Our approach is based on non binary error bases. We generalize the relation between self-orthogonal codes over finite fields to non binary quantum codes to self orthogonal codes over Frobenius ring to non binary quantum codes. As we know constructing a good quantum code is a difficult task. So, using old codes for finding new codes can simplify the task of finding codes which can otherwise be quite a daunting task. There are number of simple modification which we can make to existing codes to produce new codes with different parameters. We have used the theory of stabilizer codes over Frobenius rings defined in [16] to formulate the set of rules.

B. Relation of stabilizer codes to additive codes.

A code C over the ring R is a subset of R^n module of rank n. Additive code is defined as the additive subgroup of R^n. Associating with every element $\chi(c)X(a)Z(b)$ of G_n, an element $(a|b)$ of R^{2n} forms an additive code C. The dual $C^{\perp}$ of the code C, is defined as

$$C^{\perp} = \{u|\langle u|w\rangle_{\chi} = 0 \; for \; all \; w \in C\}.$$

Suppose R be a nice ring with generating character χ. Let C be a subgroup of $(R^{2n}, +)$. Then the relation between the cardinality of the two codes is given by

$$|C||C^{\perp}| = |R|^{2n}$$

Let R be a nice ring and n be a positive number and let us consider a group which has exponent m denoted by

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

Considering $\omega = exp(2\pi i/m)$, be a primitive mth root of unity. We now define the error group

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

generated by the error operators $X(a)Z(b)$ such that $a, b \in R^n$. As we have already mentioned that the symplectic weight $swt(a|b)$ is the number of indices i such that $a_i \neq 0$ or $b_i \neq 0$, where $a, b \in R^n$ and $(a|b) \in R^{2n}$. We define a weight of an element $e \in G_n$ where $e = \omega^c X(a)Z(b)$ to be the number of non-scalar tensor products of e. Thus it is implied that

$$wt(e) = swt(a|b).$$

Let H be a subgroup of G_n. The stabilizer code $Q = Fix(H)$ associated with H is given by

$$Q = \{c \in C^{q^n} | Sc = c \, for \, all \, S \in H\}$$

Quantum code Q denoted by $((n, K, d))$ is the subspace of C^{q^n}. A quantum code is a stabilizer code if and only if we have a subgroup H of G_n such that $Fix(H) = Q$. So if a stabilizer code Q exists then it implies there exists a subgroup $H \in G_n$ of order $|R|^n/K$ where K is the dimension of the code. Let C be the subgroup of R^{2n}

given by $C \cong HZ(G_n)/Z(G_n)$, where $Z(G_n)$ is the center of the group G_n such that $Z(G_n) = \{\omega^c.1 | c \in Z\}$. Then $|C| = |H| = |R|^n/K$ and $C^\perp \cong C_{G_n}(H)/Z(G_n)$. As H is an abelian group, then $HZ(G_n) \leq C_{G_n}(H)$, which is why $C \leq C^\perp$. If $K = 1$ then Q is a pure quantum code, thus $wt(C_{G_n}\ Z(G_n)) = swt(C^\perp - 0) = d$. And if $K > 1$, then the elements if $C_{G_n}(H) \setminus HZ(G_n)$ have atleast weight d so that $swt(C^\perp \setminus C) = d$. Now supposedly C is an additive code of R^{2n} such that $|C| = |R|^n/K$, $C \leq C^\perp$, and $swt(C^\perp \setminus C) = d$ if $K \geq 1$ and for $K = 1$, $swt(C^\perp - \{0\}) = d$. Let $N = \{\omega^c X(a)Z(b) | c \in Z\ and\ (a|b) \in C\}$ be a normal abelian subgroup of G_n. It is normal because it is the pre-image of $C = N/Z(G_n)$ and abelian since C is self orthogonal. Let χ be a character of N such that $\chi(\omega^c 1) = \omega^c$ for $c \in Z$. Then

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

is a orthogonal projector onto a vector space Q because P_N is idempotent in the group ring $C[G_n]$ So,

$$dim(Q) = Tr[P_N] = |Z(G_N)||R^n|/|N| = K$$

Each coset of $N/Z(G_n)$ contains exactly one matrix E such that $Ev = v$ for all $v \in Q$. Let $H = \{E \in N | Ev = v\ for\ all\ Q\}$ is an abelian subgroup of G_n and its order is given by $|H| = |C| = |R|^n/K$. The vector space Q is clearly a subspace of $Fix(H)$ and $dim(Q) = |R|^s/|S|$, hence $Q = Fix(H)$. Again if $K \geq 1$, then an element $w^c X(a)Z(b)$ in $C_{G_n} \setminus HZ(G_n)$ cannot have weight less than d, else it will imply that $(a|b) \in C$, which is not possible. The above explanation answers the following theorem.

Note : From now onwards we will assume that $|R| = q$

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

[16]

Proof We can refer to the above explanation.

This theorem makes precise the relation between classical codes and stabilizer codes giving us a well known connection to symplectic codes. This theorem is the basic theorem over which formulation of propagation rule is done.

C. Pure vs impure codes

- A pure code is one in which different elements of the set of correctable errors produce orthogonal results.
- Pure code are usually easier to implement due to their simple decoding process while the degenerate ones has better error detecting capabilities.
- We say a stabilizer code is pure to t if and only if the stabilizer group S does not contain non-scalar matrices of weight less than t.
- A quantum code is called pure if and only if it is pure to its minimum distance.
- An $(n, 0, d)_q$ code is always pure.

D. Propagation rules

Using old codes to find new ones can simplify the task of finding codes, which can otherwise be quite a difficult problem. There are number of simple modifications we can make to existing codes to produce new codes with different parameters.

We can lengthen a stabilizer code to get a new code. The main trick here is how we append a scalar to get the new code. Suppose that an $(n, K, d)_q$ stabilizer code

exist, and let C be the corresponding additive code with cardinality $|C| = q^n/K$. If we append a scalar $(\alpha|0)$ to C we get the following code C'

$$C' = \{(a\alpha|b0) \mid \alpha \in R,\ (a|b) \in C\},$$

with cardinality q^{n+1}/K. In the next theorem we affirm that corresponding to the code C' there exist a impure stabilizer code of length $n+1$.

Theorem D.1 *Let $((n, K, d))$ stabilizer code exists for $K > 0$ then there exists an impure$((n+1, K, d))$ stabilizer codes*

Proof Above we have lengthened the additive code C to get C'. Suppose that $(a\alpha|b0)$ and $(a'\alpha'|b'0)$ are two arbitrary elements of C'. Then,

$$\Big\langle (a\alpha|b0)|(a'\alpha'|b'0) \Big\rangle_\chi = \psi(a\alpha|b0)|(a'\alpha'|b'0) = \psi(a\alpha b'0 - a'\alpha' b0) =$$
$$\psi(a.b' + \alpha.0 - a'.b + \alpha'.0) = \psi(a.b' - a'b) = \langle (ab|a'b') \rangle_\chi$$

Therefore, C' is self-orthogonal with respect to symplectic inner product.

A vector in the symplectic dual should be of the form $(a\alpha|b0)$ with $(a|b) \in C^\perp$ and $\alpha \in R$ Thus,

$$swt(C'^\perp \backslash C') = min\{swt(a\alpha|b0)|\alpha \in R, a, b \in C^\perp \setminus C\}$$

As α can be zero so, the $swt(C'^\perp \backslash C')$ coincides with $swt(C^\perp \backslash C)$. Therefore an $(n+1, k, d)_q$ stabilizer code exists by Theorem B.1. If $d > 1$, the code is impure because $C'^\perp$ has a vector $(0\alpha|00)$ of symplectic weight 1. So, we can conclude $(n+1, K, d)$ code exists, which is impure if $d > 1$.

Now we see if we puncture a stabilizer code we can get a new code. The following theorem shows the technique used while puncturing the code.

Theorem D.2 *If a pure* $((n, K, d))_q$ *stabilizer code exists with* $n > 2$ *and* $d > 2$ *then there exists a pure* $((n-1, K^*, d-1))_q$ *stabilizer code where* $K^* > K$.

Proof Let an $((n, K, d))_q$ stabilizer code Q exists and C be the corresponding additive subgroup of R^{2n} and size of $|C| = |R|^n/K$. Let $C \leq C^\perp$ and $swt(C^\perp \setminus C) = d$ if $K > 1$ and $swt(C^\perp) = d$ if $K = 1$ by the basic theorem defined above.

Suppose $C_0^\perp$ be code obtained by puncturing one coordinate from $C^\perp$. As minimum distance of $C^\perp$ is greater than or equal to 2, we have $|C_0^\perp| = |C^\perp| = |q^{2n}|/|C| = q^n K$ and note that the minimum distance is $d-1$. That is, dual of $C_0^\perp$ consists of all vectors $(u|v)$ in $(R \times R)^{n-1}$ such that $(0u|0v)$ consists in C. Hence C_0 is a self orthogonal additive code and the size of C_0 is

$$|R^{2n-2}|/|C_0^\perp| = q^{2n-2}/q^n K = q^{n-2}q/Kq = q^{n-1}/Kq$$

as $|C_0||C_0^\perp| = (R \times R)^{n-1}$. Therefore we see that $K^* = Kq$. Thus $((n-1, K^*, d-1))_q$ code exists where $K^* > K$.

Here we will discuss the condition of getting smaller code inside the bigger code.

Theorem D.3 *Suppose a (pure)* $((n, K, d))_q$ *stabilizer code exists with* $K \geq 2 (K \geq 1)$ *then there exists a (pure)* $((n, K^*, d^*)$ *stabilizer code such that* $d^* \geq d$ *and* $K^* \leq K$

Proof Suppose (n, K, d) be a stabilizer code then we can say an additive code $C \leq (R \times R)^n$ exists such that $C \leq C^\perp$ and $swt(C^{\perp_s} \setminus C) = d$ and $|C| = |R|^n/K$ Choose an additive code C_b be subgroup of $(R \times R)^n$ of size R^n/K^* such that $K^* < K$ and $C \leq C_b \leq C^\perp$. As $C \leq C_b$ we conclude that $C_b^\perp \leq C^\perp$.

The set $\sum_b = \{C_b^\perp \setminus C_b\}$ is a subset of $\{C^\perp \setminus C\}$. Thus the minimum weight of the set d^* is at least d. Thus we can conclude that an (n, K^*, d^*) code exists.

If the code is pure, then $swt(C^{\perp}) = d$, it follows as $C_b^{\perp} \leq C^{\perp}$, then $swt(C_b^{\perp})$ is greater than or equal to d. That is, smaller code should also be pure.

From above two theorem the corollary holds

Corollary D.4 *If a pure $((n, K, d))_q$ stabilizer code with $n \geq 2$ and $d \geq 2$ exists then there exists a pure $((n-1, K, d-1))_q$ stabilizer code.*

Concatenating two quantum codes gives us a new quantum code. Suppose that P_1 and P_2 are the orthogonal projectors onto the stabilizer codes $Q_1 = ((n_1, K_1, d_1))_q$ and $Q_2 = ((n_2, K_2, d_2))_q$. Then $P_1 \times P_2$ is an orthogonal projector onto a K_1K_2-dimensional subspace Q of $C^{q^{n_1+n_2}}$. Now if we consider S_1 and S_2 the stabilizer groups of the images of P_1 and P_2, respectively. Then $S = \{E_1 \times E_2 | E_1 \in S_1, E_2 \in S_2\}$ is the stabilizer group of Q. If an element $F_1 \times F_2$ of $G_{n_1} \times G_{n_2} = G_{n_1+n_2}$ is not detectable , then F_1 has to commute with all elements in S_1 and F_2 has to commute with all elements of S_2. As it is not possible that both $F_1 \in Z(G_{n_1})S_1$ and $F_2 \in Z(G_{n_2})S_2$ hold because which would imply that $F_1 \times F_2$ is detectable. Thus either F_1 or F_2 is not detectable which shows that the weight of $F_1 \times F_2$ is atleast $min(d_1, d_2)$.

The above explanation leads to the following theorem.

Theorem D.5 *Suppose an $((n_1, K_1, d_1))_q$ and $((n_2, K_2, d_2))_q$ stabilizer code exists. Then there exists an $((n_1 + n_2, K_1K_2, min(d_1, d_2))_q$ stabilizer code.*

Proof It can be easily proved from the explanation above.

Theorem D.6 *Let Q_1 and Q_2 be pure stabilizer codes that respectively have parameters $((n, K_1, d_1))_q$ and $((n, K_2, d_2))_q$. IF $Q_2 \subseteq Q_1$ then there exists a $((2n, K_1K_2, d))_q$ pure stabilizer code with minimum distance $d \geq min\{2d_2, d_1\}$.*

Proof Let us consider $D_1 \leq (R^n \times R^n)$, $D_2 \leq (R^n \times R^n)$ and suppose $D_1 \leq D_2$ such that $D_1 \leq D_1^{\perp}$ ($D_2 \leq D_2^{\perp}$) and size of $|D_1| = q^n/K_1$ ($|D_2| = q^n/K_2$). The additive code $D = \{(u, u+v) | u \in D_1, v \in D_2\} \leq (R^{2n} \times R^{2n})$ is of size $|D| = q^{2n}/K_1K_2$. The trace symplectic dual of the code is

$$D^{\perp} = \{(u' + v', v') \mid u' \in D_1^{\perp}, v' \in D_2^{\perp}\}.$$

We see that the vector on the right hand side are $\perp$ to the vectors in D because

$$\langle (u, u+v) | (u' + v', v') \rangle = \langle u | u' + v' \rangle + \langle u + v | v' \rangle = 0$$

then $u \in D_1$, $v \in D_2$ and $u' \in D_1^{\perp}$, $v' \in D_2^{\perp}$. We observe that D is self-orthogonal $D \leq D^{\perp}$. And the weight of a vector $(u' + v', v') \in D^{\perp} \setminus D$ is at least $min\{2d_2, d_1\}$.

Theorem D.7 *Let $|R| = q$ be an even prime number. If a pure $((n, K_1, d_1))_q$ stabilizer code Q_1 exists that has pure subcode $Q_2 \subseteq Q_1$ with parameters $((n, K_2, d_2))_q$ such that $K_1 > K_2$, then a pure $((2n, K_1/K_2, d))_q$ stabilizer code exists such that $d \geq min\{2d_1, d_2\}$.*

Proof The inclusion $Q_2 \subseteq Q_1$ implies that $D_1 \leq D_2$. Let D denote the additive code consisting of vectors of the form $(u, u+v)$ such that $u \in D_2^{\perp}$ and $v \in D_1$. We claim that $D^{\perp}$ consisting of vectors of the form $(u', u'+v')$ such that $u' \in D_1^{\perp}$ and $v' \in D_2$. And we have

$$\langle v_1 | v_2 \rangle = \langle u | u' \rangle + \langle u | v' \rangle + \langle v | u' \rangle + \langle v | v' \rangle = 0,$$

which implies that v_1 and v_2 are orthogonal. The set $\{(u', u'+v') | u' \in D_1^{\perp}, v' \in D_2\} \subseteq D^{\perp}$ has cardinality $q^{2n}K_1/K_2$. So, it must be equal to $D^{\perp}$ by dimension argument.

The hamming weight of a vector $(u', u'+v')$ in $D^{\perp}$ is at least $min\{2d_1, d_2\}$ because $u' \in D_1^{\perp}$ and $v' \in D_2 \leq D_2^{\perp}$.

1. Product codes

Let R be a ring with q elements then there is a subring R_0 which is isomorphic to Z/nZ where n is the characteristic of the ring. Suppose A be a unramified quadratic algebra $R-$algebra A. If we define the inner product product as $v \star w = \sum_{i=1}^{n} tr(v_i \sigma(w_i))$ for $v, w \in A^n$ tr maps elements from A to R.

Lemma 14 *Let w, w' be two elements of R^m which is a free module over R and v, v' be two elements over R^n which is a module over R_0, we have $(v \otimes w) \star (v' \otimes w') = (v.v')(w \star w')$*

[21]

Proof $(v \otimes w) \star (v' \otimes w') = \sum_{i=1}^{n} \sum_{j=1}^{m} tr(v_i w_j (\sigma(v_i') \sigma(w_j'))$ since $v, v' \in R^n$ so $\sigma(v) = v$ and $tr(\sum_{i=1}^{n} v.v'$ is equal to $\sum_{i=1}^{n} v.v'$. Therefore symplectic inner product is the product of the Eucledian inner product on the first space and "$\star$" inner product on the second space.

Let C_1 and C_2 be a linear $(n_1, k_1, d_1)_q$ and $(n_2, k_2, d_2)_q$ code over R, with generator matrices G_1 and G_2 respectively. Then, the product code $C_\pi = C_1 \otimes C_2$ is a linear code where $C_\pi = (n_1 n_2, k_1 k_2, d_1 d_2)$ generated by the matrix $G = G_1 \otimes G_2$.
If C_1 is a linear code over the S given by $(n_1, k_1, d_1)_p$ and C_2 is a additive code with $(n_2, p^{k_2}, d_2)_q$ over R with q elements where q is a power of prime p then, product code is defined by $c_\pi = C_1 \otimes_s C_2$ with parameters $(n_1 n_2, p^{k_1 k_2}, d_1 d_2)_q$.

Theorem D.8 *Let Q_1 and Q_2 be two quantum code and their corresponding additive code be $C_1 \leq R^{2n}, C_1 \subseteq C_1^\star$ and $C_2 \leq R^{2n}, C_2 \subseteq C_2^\star$ with parameters $((n_1, k_1, d_1))_R$ and $((n_2, k_2, d_2))_R$ respectively. Then there exists a quantum code Q with parameters $((n_1 n_2, n_1 n_2 - 2k_1 k_2, min(d_1, d_2))_R$ whose corresponding additive code be $C_\pi = C_1 \otimes_s C_2$*

Proof This can be constructed using CSS code construction.

CHAPTER VI

CODE CONSTRUCTION AND RESULTS

A. Introduction

In this chapter we show some code construction over Z_{p^s}. Our main strategy to build quantum code is by searching self-orthogonal classical codes and then construct the quantum counterpart using CSS code construction theorem. We mostly emphasize on simplex codes of type α and β over Z_{2^s} and Quasi twisted codes. However we also construct few other types of codes over Z_m where m is an odd prime.

B. CSS code construction

The CSS construction deals with self-orthogonal codes over the ring R with q elements. This construction was introduced in 1996 by Calderbank and Shor [20] and Steane [7]. Later this was redefined over Frobenius ring in [16]. It provides the most direct link to classical coding theory. The following theorem defines the CSS Code Construction. All our code construction is done on the basis of this theorem.

Theorem B.1 *Let C_1 and C_2 denote two classical linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ such that $C_2^{\perp} \leq C_1$. Then there exists a $[[n, k_1 + k_2 - n, d]]_q$ stabilizer code with minimum distance $d = min\{wt(c) \mid c \in (C_1 \setminus C_2^{\perp}) \cup (C_2 \setminus C_1^{\perp})\}$ that is pure to $min\{d_1, d_2\}$*

A special case that interests us is when $C_1 = C_2$ i.e when the code is self-orthogonal. This is particularly interesting because one can easily find codes which satisfy the self-orthogonality condition.

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

C. Self-orthogonal codes over Z_{2^s}

Let C be a linear code of length n over Z_{p^s}. The generator matrix of the code is given by [22].

$$G = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\ 0 & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1}s \end{pmatrix},$$

where A_{ij} are matrices over Z_{p^s} and the columns are grouped into blocks of size $k_0, k_1, ..., k_{s-1}, k_s$. Let $k = \sum_{i=0}^{s-1}(s-1)k_i$. Then $|C| = p^k$.

Lets exemplify the self-orthogonal codes over Z_{2^s} by self-orthogonal codes over Z_4 Let C be a linear code over Z_4. Then C has a generator matrix of the form

$$G = \begin{pmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 0 & 2I_{k_1} & 2C \end{pmatrix}$$

where A, B_1, B_2 and C are matrices with 0 or 1. And I_k is the identity matrix of order k. The dual code $C^\perp$ of C is defined as $\{x \in Z_4^n \mid x.y = 0,\ for\ all\ y \in C\}$. The code C is called self-orthogonal if $C \subseteq C^\perp$. Let d_H and d_L be the minimum Hamming and Lee distance of C. E. M. Rains has shown that $d_H \geq \lceil d_L/2 \rceil$. C is said to be of type α if $d_H = \lceil \frac{d_L}{2} \rceil$ and of type β if $d_H > \lceil \frac{d_L}{2} \rceil$. Let G_k^α be the generator matrices of simplex code of type α defined by

$$G_1^\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 \end{pmatrix}, G_k^\alpha = \begin{pmatrix} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 \\ G_{k-1} & G_{k-1} & G_{k-1} & G_{k-1} \end{pmatrix}.$$

G_k^α consists of all elements of Z_4^k.

Let G_k^β be defined inductively by

$$G_2^\beta = \begin{pmatrix} 1111 & 0 & 2 \\ 0123 & 1 & 1 \end{pmatrix}, \; G_k^\beta = \begin{pmatrix} 11\cdots1 & 00\cdots0 & 22\cdots2 \\ G_{k-1}^\beta & G_{k-1}^\beta & G_{k-1}^\beta \end{pmatrix}.$$

No two columns of G_k^β are multiples of each other. Both the codes generated by G_k^α and G_k^β over Z_4 is of type α and β and is called simplex code of type α and β. Their parameters are $[2^{2k},\, 2k,\, 2^{2k-1}]$ and $[2^{k-1}(2^k-1),\, 2k,\, 2^{2k-1}]$ respectively.

D. Simplex codes of type α, β over Z_{2^s}

Let G_k be a $k \times 2^{sk}$ matrix over Z_{2^s} defined inductively by

$$G_1^\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & \cdots & 2^s-1 \end{pmatrix}, \text{ for } k \geq 2,$$

$$G_k^\alpha = \begin{pmatrix} 00\cdots0 & 11\cdots1 & 22\cdots2 & \cdots & (2^s-1)(2^s-1)\cdots(2^s-1) \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & \cdots & G_{k-1}^\alpha \end{pmatrix}.$$

The code S_k^α generated by G_k^α over Z_{2^s} has length 2^{sk} and 2−dimension sk. Let G_k^β be the $k \times 2^{(s-1)(k-1)(2^{k-1})}$ matrix defined by

$$G_2^\beta = \begin{pmatrix} 111\cdots1 & 0 & 2 & 4 & 6 & \cdots & (2^s-2) \\ 0123\cdots(2^s-1) & 1 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}, \text{ and for } k > 2$$

$$G_k^\beta =$$

$$\begin{pmatrix} 111\cdots1 & 00\cdots0 & 22\cdots2 & 44\cdots4 & 66\cdots6 & \cdots & (2^s-2)(2^s-2)\cdots(2^s-2) \\ G_{k-1}^\alpha & G_{k-1}^\beta & G_{k-1}^\beta & G_{k-1}^\beta & G_{k-1}^\beta & \cdots & G_{k-1}^\beta \end{pmatrix}.$$

S_k^β is a $[2^{(s-1)(k-1)}, sk, 2^{(s-1)(k-1)-s}]$ code.

E. Quantum codes from simplex codes

In this section we give some examples how to construct Quantum codes from simplex beta code and simplex alpha code both of degree 2.

Example 1 : Generator matrix of simplex beta code C is given by

$$\begin{pmatrix} 1 & 0 & 3 & 2 & 3 & 1 \\ 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}.$$

The direct sum of C with C gives the code which is self-orthogonal with respect to the symplectic inner product forms the stabilizer of the quantum code. The generator matrix of this code is given by

$$\begin{pmatrix} 1 & 0 & 3 & 2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}.$$

The corresponding quantum code $[[6, 2, 2]]_4$.

Example 2 Generator matrix of a self orthogonal simplex beta code C when $k = 3$ is:

$$G = \begin{pmatrix} 1 & 0 & 3 & 2 & 0 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 2 & 1 & 0 & 3 & 3 & 2 & 1 & 0 & 3 & 1 & 1 & 0 & 3 & 2 & 1 & 3 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 1 & 1 & 0 & 1 & 2 & 3 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 1 & 1 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 2 \end{pmatrix}.$$

The generator matrix of the code obtained by doing direct sum of C with itself is given by

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

The Quantum code obtained is $[[28, 22, 2]]_4$.

Example 3 Generator matrix of a simplex alpha code is given by

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

Direct sum of C with C gives the code which is self-orthogonal with respect to the symplectic inner product. The generator matrix of this code is given by

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 \end{pmatrix}$$

This is also the stabilizer matrix that stabilizes the quantum code $[[16, 12, 1]]_4$.

Simplex codes of degree 2 did not give any good quantum codes and going to higher degree will not be so helpful, as the dimension of the code grows exponentially which made it not suitable for building codes.

Similarly we can derive quantum codes from self-orthogonal codes over Z_{2^s} with $s > 2$ by the procedure mentioned above.

F. Quantum codes over finite rings Z_{p^m}

We present a method for constructing self-orthogonal quantum codes over finite rings Z_{p^m}, with p an odd prime and m a positive number. In the paper [23] they explained self-orthogonal codes over integer modulo odd primes. The "Building up construction" methodology is used to build self-orthogonal codes. Our construction of quantum codes is done by using these self-orthogonal classical codes over rings.

We skip through all the details of how the self-orthogonal classical codes over odd primes is built. Readers can refer to [23] for details. Building quantum codes is what we emphasize here.

Example 5 The following is a self-orthogonal almost MDR$[4, 2, 2]$ code over Z_{5^2} with generator matrix

$$G = \begin{pmatrix} 5 & 0 & 15 & 0 \\ 0 & 5 & 0 & 10 \end{pmatrix}.$$

The stabilizer is

$$G = \begin{pmatrix} 5 & 0 & 15 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 10 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 & 10 \end{pmatrix}.$$

The corresponding quantum code is $[[4, 0, 2]]_4$.

Example 6 For length $n = 6$ starting from a code with generator matrix G_5 with $x = \{14, 6, 21, 24\}$, we get a self-orthogonal MDR$[6, 3, 4]$ code over Z_{25} with a generator matrix

$$\begin{pmatrix} 5 & 0 & 0 & 15 & 20 & 15 \\ 0 & 5 & 0 & 5 & 10 & 15 \\ 0 & 0 & 5 & 10 & 15 & 20 \end{pmatrix}.$$

The corresponding quantum code is $[[6, 0, 2]]_4$.

Example 7 For length $n = 8$ a self orthogonal almost MDR$[8, 4, 4]$ code over Z_{25} with a generator matrix.

$$\begin{pmatrix} 5 & 0 & 0 & 0 & 15 & 20 & 0 & 15 \\ 0 & 5 & 0 & 0 & 0 & 20 & 15 & 15 \\ 0 & 0 & 5 & 0 & 15 & 20 & 15 & 0 \end{pmatrix}.$$

The corresponding generator matrix for quantum code is $[[8, 0, 1]]_(4)$ code.

Remark : An $[[n, 0, d]]$ code is pure by convention. $[[n, 0, d]]$ code is a single quantum state with the property that, when subjected to a decoherence of $[(d-1)/2]$ coordinates, it is possible to determine exactly which coordinates were decohered. Such a code might be useful for example in testing whether certain storage locations for qudits are decohering faster than they should.

Example 8 Another self-orthogonal MDR$[8, 5, 4]$ code over Z_{25} with generator matrix is

$$\begin{pmatrix} 1 & 3 & 0 & 2 & 2 & 22 & 13 & 23 \\ 0 & 5 & 0 & 0 & 4 & 11 & 3 & 2 \\ 0 & 0 & 1 & 1 & 3 & 17 & 9 & 12 \\ 0 & 0 & 0 & 5 & 2 & 13 & 14 & 16 \\ 0 & 0 & 0 & 0 & 5 & 20 & 10 & 15 \end{pmatrix}.$$

The corresponding quantum code is a $[[8, 2, 2]]_4$ code. We also have self orthogonal classical codes over integer modulo odd primes with length 10 and greater. However we won't be able to present those examples here as we do not have proper tool to find the distance of the quantum code.

G. Quantum codes from quasi twisted codes(QT)

A code is said to be Quasi Twisted codes (QT) if a consta-cyclic shift of any codeword by p positions is still a codeword. The length n of a QT code is a multiple of p, i.e $n = mp$. The constacyclic matrices are also called twistulant matrices and they form the basic components of a generator matrix for a Quasi Twisted code. The generator matrix G can be represented as

$$G = \begin{pmatrix} B_1 & B_2 & B_3 & \cdots & B_p \end{pmatrix},$$

where each B_i is a $m \times m$ $\eta-$twistulant matrix and is represented as below

$$B_i = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ \eta b_{m-1} & b_0 & b_1 & \cdots & b_{m-3} & b_{m-2} \\ \cdots & \cdots & \cdots & & & \\ \cdots & \cdots & \cdots & & & \\ \eta b_1 & \eta b_2 & \eta b_3 & \cdots & \eta b_{m-1} & b_0 \end{pmatrix},$$

Defining polynomials are used to represent the first row of the twistulant matrices. The QT form of the consta-cyclic matrix can be represented by these defining polynomials.

Let us exemplify the theory. The first row of the generator matrix for a $(6, 2)$ code is represented by $[1, 1, 13]$ The generator matrix of the Quasi Twisted code is given by

$$G = \begin{pmatrix} 0 & 1 & | & 0 & 1 & | & 1 & 3 \\ \eta.1 & 0 & | & \eta.1 & 0 & | & \eta.3 & 1 \end{pmatrix}$$

where $\eta = 3$. We use a brute force approach for exploring self orthogonal Quasi Twisted codes. Our general criteria is to check for codes which have good minimum distance.

Suppose the code which we have considered is C then the corresponding direct sum of C with C gives us the code which is self orthogonal with respect to symplectic inner product. The generator matrix of the code is given by

$$\begin{pmatrix} G & 0 \\ 0 & G \end{pmatrix},$$

where G is the generator matrix of the code C. This is also the stabilizer matrix that stabilizes the quantum code which we built with the help of the [16] Theorem[2].

Example 9 : A $(18, 6)$ Quasi Twisted Code with first row of the generator matrix is given by $[21, 111, 11321]$. The generator matrix of this code is given by the following

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 3 & 2 & 1 \\
3 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 0 & 1 & 1 & 3 & 2 \\
2 & 3 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 0 & 1 & 1 & 3 \\
0 & 2 & 3 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 0 & 1 & 1 \\
0 & 0 & 2 & 3 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 0 & 1 \\
0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 0
\end{pmatrix}.$$

The corresponding quantum code is $[[18, 6, 3]]_4$ with minimum distance 3.

Example 10 : Lets take another Self-orthogonal QT code is $(24, 8)$. The generator matrix is given below.

$$\begin{pmatrix}
0 & 0 & 0 & 1 & 2 & 1 & 0 & 3 & 0 & 0 & 0 & 1 & 1 & 0 & 3 & 1 & 0 & 0 & 2 & 1 & 3 & 1 & 1 & 3 \\
1 & 0 & 0 & 0 & 1 & 2 & 1 & 0 & 3 & 0 & 0 & 0 & 1 & 1 & 0 & 3 & 1 & 0 & 0 & 2 & 1 & 3 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 3 & 0 & 0 & 0 & 1 & 1 & 0 & 3 & 1 & 0 & 0 & 2 & 1 & 3 & 1 \\
3 & 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 & 1 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 3 & 1 & 0 & 0 & 2 & 1 & 3 \\
2 & 3 & 0 & 1 & 0 & 0 & 0 & 1 & 3 & 0 & 1 & 3 & 0 & 0 & 0 & 1 & 1 & 3 & 3 & 1 & 0 & 0 & 2 & 1 \\
3 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 3 & 3 & 0 & 1 & 3 & 0 & 0 & 0 & 3 & 1 & 3 & 3 & 1 & 0 & 0 & 2 \\
0 & 3 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 3 & 3 & 0 & 1 & 3 & 0 & 0 & 2 & 3 & 1 & 3 & 3 & 1 & 0 & 0 \\
0 & 0 & 3 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 3 & 3 & 0 & 1 & 3 & 0 & 0 & 2 & 3 & 1 & 3 & 3 & 1 & 0
\end{pmatrix}.$$

Quantum code constructed from this is $[[24, 8, 3]]_4$.

Similarly we have constructed quantum codes $[[32, 16, 4]]_4$ and $[[16, 2, 3]]_4$ from the classical code $(32, 16)$ and $(16, 2)$.

H. Conclusion

We provided a brief insight of constructing quantum codes over Z_{2^s} and Z_m rings where m is a odd prime. We presented a way of constructing quantum codes from existing self-orthogonal classical codes and we discussed few classes of self orthogonal codes and quoted few examples of quantum codes that have been constructed using these types.

REFERENCES

[1] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys, Rev. A*, vol. 52, no. 4, pp. 2493-2496, 1995.

[2] A. M. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, no. 6, pp. 793-797, 1996.

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

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

[5] J.Preskill, "Quantum computation," 2006, http://www.theory.caltech.edu/ people/preskill/ph229/.

[6] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys, Rev. A*, vol. 52, no. 4, pp. 2493-2496, 1995.

[7] A. Steane, "Multiple particle interference and quantum error correction," *Proc. Royal Society London A*, vol. 452, no. 1, pp. 2551-2577, 1996.

[8] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, 1997, Caltech Ph.D. Thesis, eprint: quant-ph/9705052.

[9] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via code over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 1369-1387, 1998.

[10] R. Jozsa and B. Schumacher, "A new proof of the quantum noiseless coding theorem," *J. Modern Optics*, vol. 41, no. 1, pp.2343-2349, 1994.

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

[12] D. Gottesman, "An introduction to quantum error correction and fault tolerant quantum computation," in *Proceedings of Symposia in Applied Mathematics*, vol. 68, no. 1, pp. 13-58, 2009.

[13] E. M. Rains, "Nonbinary quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 24812485, 1999.

[14] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys, Rev. A*, vol. 52, no. 4, pp. 2493-2496, 1995.

[15] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, "Non-binary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4892-4914, 2006.

[16] S. Nadella and A. Klappenecker, "Stabilizer codes over frobenius rings," in *Proceedings of International Symposium on Information Theory*, ISIT 2012, Cambridge, MA, 2012, IEEE Press.

[17] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *American Journal of Mathematics*, vol. 121, no. 3, pp. 555-575, 1999.

[18] A. Klappenecker, "Nice near-rings," in *Proceedings of International Symposium on Information Theory*, ISIT 2012, Cambridge, MA, 2012, IEEE Press.

[19] Scheja and Storch, *Lehrbuch der Algebra 3,* Teil 3, Stuttgart, B.G. Teubner.

[20] A. R. Calderbank and P. W. Shor. "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 4, pp. 10981105, 1996.

[21] M. Grassl and M. Rotteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *International Symposium on Information Theory*, pp. 1018-1022, 2007.

[22] M. K. Gupta, *On some linear codes over* Z_{2^s}, Ph.D. Thesis, Indian Institute of Technology, Kanpur, India, December, 1999.

[23] H. Lee, Y. Lee, "Construction of self-dual codes over finite rings Z_{p^m}," *Journal of Combinatorial Theory, Series A*, vol. 115, no. 1, pp. 407-422, 2008.

VITA

Name: Anurupa Sarma

Address: Intel Corporation, Robert Noyce Building, 2200 Mission College Blvd, Santa Clara, CA 95054-1537

Email Id: sarma.anurupa@gmail.com

Education: B.Tech., National Institute of Technology, Silchar, India - June 2007

M.S., Texas A&M University , College Station, Texas - August 2012