ON THE STUDY OF ERROR CORRECTING QUANTUM CODES AND GENERALIZED ENTROPIC UNCERTAINTY RELATION

Thesis Submitted to the University of Calicut in partial fulfillment of the requirements for degree of
DOCTOR OF PHILOSOPHY
IN MATHEMATICS

M.P. SIVARAMAKRISHNAN

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALICUT

MARCH 2002

DECLARATION

I do hereby declare that the present work is original and has not been published or submitted in part or full for any degree or prize.

30.3.2002

M.P.Sivaramakrishnan

CERTIFICATE

This is to certify that the material presented on the thesis **"ON THE STUDY OF ERROR CORRECTING QUANTUM CODES AND GENARALIZED ENTROPIC UNCERTAINTY RELATION"**,of Sri.M.P.Sivaramakrishnan is a bonafide record of the work done under my supervision and no part of this has been presented elsewhere for any degree or prize.

30.3.2002

Research Supervisor

ACKNOWLEDGEMENT

This thesis "ON THE STUDY OF ERROR CORRECTING QUANTUM CODES AND ENTROPIC UNCERTAINTY RELATION", has been undertaken under the supervision of Dr.M.S.BALASUBRAMANI, Reader in Mathematics, University of Calicut. I would like to express my deep sense of gratitude to him for all his help.

I am truly indebted to Prof. B.V. Rajarama Bhat, Indian Statistical Institute, Bangalore who had given me the initiation into this area and Prof. K.R.Parthasarathy, Institute of Mathematical Sciences, Chennai for suggesting some nice aspects of this subject.

I would like to express my sincere thanks to Prof. V.Krishnakumar, Head of the Department of Mathematics, University of Calicut for all the help and encouragement he gave me during this period. Also I take this opportunity to thank all the teaching and nonteaching staff of the department for their help.

Finally I place on records my sincere thanks to the University Grants Commission, New Delhi for allotting me a teacher fellowship under the Faculty Improvement Programme and the University of Calicut for providing the facilities.

M.P.Sivaramakrishnan

CONTENTS

INTRODUCTION

M.P. Sivaramakrishnan "On the study of error correcting quantum codes and genaralized entropic uncertainty relation" Thesis. Department of Mathematics , University of Calicut, 2002

INTRODUCTION

We are in the computer age. For each and everything we wish we had a computer !

It is said, 'To err is human'. Well this suits the computers also. Computers work on electricity. In an electric circuit, either current flows or not, i.e., the 'on' and 'off' positions. This is beautifully associated with the binary system. Using the binary system one tries to express as many things as possible. This is precisely the construction of '***codes***'.

Suppose we encode SUN as 10 and MOON as 01.While sending these two words, assume some error occurs say, instead of sending 01, 10 is transmitted. The MOON becomes a SUN! This in circuits mean the following. SUN is allotted two switches, first switch must be in the 'on' position and the second switch in 'off' position. For the MOON , the otherway. Because of a fault - error, the roles get reversed. This is quite possible since the components in a computer are man made and subjected to

wear and tear. Thus evolved the theory of detecting and correcting codes.

Suppose we now encode SUN as 000 and MOON as 010, i.e., we add one redundant digit. While transmitting SUN suppose only one error has occurred. Then the received code will be either 100 or 010 or 001.Still we cannot be sure that the transmitted message is SUN. Add two redundant digits. SUN will have the encoding 0000 and MOON has 0100. Again suppose only one error has occurred. Then the received message will have the encoding:1000, 0100, 0010, 0001. By imposing a condition like : In the received message look at the digits from left to right. Choose that message in which the maximum number of digits from left to right do not change, to be the correct message. Thus we can be sure that the transmitted message was SUN.

Looking at this in a different way, the digits 0000 and 0100 can be considered as vectors in $\mathbf{R}^4$ and moreover they are orthogonal vectors. The digits 1000 , 0100, 0010, 0001 are also an orthogonal set of vectors in $\mathbf{R}^4$. Transmitting message now becomes an operator acting on $\mathbf{R}^4$. Original coding is in $\mathbf{R}^2$. We get a mapping from $\mathbf{R}^2$ to $\mathbf{R}^4$. This is the crux of the

coding theory. By introducing some extra coordinates one tries to detect and correct errors.

The present nomenclature to this type of study is '***Information Theory***'. What we have discussed above has already become ***Classical.***

In 1994, ***Peter Shor [Sh3]*** discovered a quantum algorithm which enables to factorise an integer significantly faster than what a classical digital analog computer can do. This discovery has paved way for the rapid flourishing of the branch of '***Quantum Information Theory*** '. This is the area of our research and is a recent upstart, more precisely an outcome of the ***last decade.***

Now about the thesis. The thesis has five chapters.

In chapter one we have the introductory notions. The first section contains certain ideas from the Classical Information Theory. Even though Quantum Information Theory is essentially different from it's classical counterpart, there are several features in it analogous to classical theory. We include some basic definitions and properties from classical setting. The second section involves mainly the characteristics , definitions and some important theorems of the quantum information theory. It gives an

overall picture of how quantum computation is distinguished from the classical one. Some theorems like ***Knill-Laflamme Criterion***, ***CSS code*** construction are discussed here. In the last section we learn about the uncertainty principle and ***Shannon entropy*** and how they can be fruitfully combined.

There are three sections in Chapter Two, which is a round up on quantum codes. The first section concerns with the ***CSS (Calderbank-Steane-Shor)*** construction of quantum codes. The important result of this section is constructing a more general code over a finite field.

Section two is about developing the Knill-Laflamme criterion of code construction to symmetric and antisymmetric tensor products of Hilbert spaces. These two spaces have great quantum relevance since they represent particles in the two categories namely ***Bosons*** and ***Fermions***. We use equivalent ***Weyl operators*** as in the t-error correcting quantum code in this situation.

The last section is on perfect codes. ***Laflamme*** et al [LMPZ] proved that the 5-qubit code is perfect and is the minimal one compared to the 7-qubit and 9-qubit codes. We have proved that 5-qubit code is perfect by

using the technique of error basis of Weyl operators in the Knill-Laflamme theorem as is given in [Pa2].

In Chapter Three. the higher spin systems are analysed. By higher spin we mean that it is higher than the ½ spin systems with a two element basis. In his work ***Chau*** [Ch2], has constructed a 5-quantum register code and has shown that it is optimal. By using the method given in ***Parthasarathy*** [Pa2] we prove this result . By the same method we also prove that the five register code is optimal. Using the same criterion we have been able to show that the the 9-register code of Chau [Ch2] give an error correcting code. We also develop an encoding to the case of 7-register code.

The Fourth Chapter is on two specific applications of the Knill-Laflamme criterion. In the first section we have discussed how a convex state may be recovered . In particular this leads to the question of recovering a mixed state, for which we have been able to give an affirmative answer, of course using some conditions.. The second section is on the recovery of a pure state not directly but through a 'representation' of the pure state.

We conclude our thesis by considering the uncertainty relation. Here Shannon entropy is involved and we improve a result of ***Massen and Uffink*** to a situation in which eigenvalues of the observable have degeneracy.

We consider our thesis as a very very small step in making a little contribution to a current vibrant topic. But for the time constraint, we believe, we could have attempted some more deeper results.

Preliminaries

M.P. Sivaramakrishnan "On the study of error correcting quantum codes and genaralized entropic uncertainty relation" Thesis. Department of Mathematics , University of Calicut, 2002

Chapter 1 Preliminaries

In this chapter we give an overview of the known ideas that we have used in our work.

1.1 Classical Information Theory

The fundamental problem of ***communication*** or ***information theory*** is to reproduce at one point either exactly or approximately a message selected at another point [Sh]. There is a source containing ***messages*** and it is transmitted to a ***destination*** through a ***channel*** or a ***noisy medium***. The message is ***encoded*** before sending it through the noisy medium and from the output the receiver has to decode it and recover the message. In classical setting the encoding is performed by using binary digits 0 ,1 which are usually called ***bits***.

1.1.1 *Definitions* [Va 3 : MS1]

A finite set of cardinality N is called an ***alphabet*** of N ***letters***. We write $\#A = N$.

A sequence $\mathbf{a} = (a_1, a_2, \ldots\ldots, a_n)$, $a_i \in A \; \forall$ i, is called a ***word of length n*** from alphabet A. Thus $\mathbf{a} \in A^n$.

If $\mathbf{a}, \mathbf{b} \in A^n$ the ***Hamming distance*** between **a** and **b** , denoted by d (**a**, **b**), is defined as : $d(\mathbf{a}, \mathbf{b}) = \#\{ i \ni a_i \neq b_i, 1 \leq i \leq n\}$. This is in fact a

metric on A^n .For a subset $C \subset A^n$ of cardinality M, the ***minimum distance*** d(C) of C is defined as, $d(C) = \min_{a,b \in C, a \neq b} d(\mathbf{a},\mathbf{b})$. If $d(C) = d$, we say C is a ***code*** with ***alphabet*** A , ***length*** n , ***size*** M and ***minimum distance*** d or that C is an $(n, M, d)_A$ ***code***. If A is {0,1} of binary digits, we say C is a ***binary code***. The ***Hamming weight*** of a word ***a*** is the number of nonzero a_i`s and is denoted by wt (a). We have d (**a**, **b**) = wt (**b** - **a**).For any nonnegative integer t and $\mathbf{a} \in A^n$, the ***Hamming sphere*** of radius t and center **a**, denoted by S(**a**, t), is defined as :

$$S(\mathbf{a}, t) = \{ \mathbf{x} \ni \mathbf{x} \in A^n, d(\mathbf{a}, \mathbf{x}) \leq t \}.$$

1.1.2 ***Property*** **[Va 3.1]**

The Hamming spheres are pairwise disjoint if and only if $d \geq 2t+1$.

1.1.3 ***Theorem*** **[MS 1.3]**

A code with a minimum distance d can correct [(d-1)/2] errors. If d is even it can both correct [(d-1)/2] errors and detect d/2 errors. (Here [.] is the greatest integer function).

1.1.4 ***Significance of Code*** **[Va,MS]**

Suppose we communicte letters from the alphabet A through a channel.

If $x \in A$ is an input letter fed into the channel we get an output $y \in A$.. But y need not be the same as the input x. Now if we use a string of letters $\mathbf{x} = x_1x_2....x_n \in A^n$ and transmit it successively, we obtain another string $\mathbf{y} = y_1y_2....y_n \in A^n$. Then the number of errors is the Hamming distance $d(\mathbf{x}, \mathbf{y})$ between the input word and the output word. If M messages are communicated and we have at our disposal an $(n,M,d)_A$ code C with $d \geq 2t+1$, then list the M messages 1, 2,....., M in correspondence with the codewords $\mathbf{c}^{(1)}, \mathbf{c}^{(2)}, ..., \mathbf{c}^{(M)}$. To communicate message number i, transmit the codeword $\mathbf{c}^{(i)}$. Then the output word x lies in $S(\mathbf{c}^{(i)}, t) = S_i$, say. By property of the spheres, S_i's are disjoint. This will yield the decoding procedure as : if the output sequence falls in sphere S_i decide that the message transmitted is numbered i. Thus error free transmission is ensured as long as $d \geq 2t+1$ or $t \leq \left[\frac{d-1}{2}\right]$. We say an $(n,M,d)_A$ code is a $\left[\frac{d-1}{2}\right]$ ***error correcting code.***

1.1.5 *Some Examples.*

A single error correcting code which sends two messages without any error if the channel makes at most one error in transmitting three binary digits successively is as follows:

We number the messages as 0 , 1. Define the encoding map as

$$0 \longrightarrow 000$$

$$1 \longrightarrow 111 .$$

Suppose the channel makes at most one error in three transmissions. If 000 is transmitted , the output belongs to $\{000,100,010,001\} = S_0$, say. If 111 is transmitted , the output belongs to $\{111,011,101,110\} = S_1$, say. S_0 and S_1 are disjoint spheres of radius unity with centers 000 and 111 respectively. The decoding is as follows: If the output falls in S_0 the message is decoded as 0 and if the output falls in S_1 the message is decoded as 1.

The code described here is called the ***repetition code***.

1.1.6 *Linear Codes* [MS 1]

We consider vectors and binary codes over F_2.

A binary vector $v \in F_2^n$, with d 1's has Hamming weight d. The Hamming distance $d_H(v,w)$ between two binary vectors is the Hamming weight of $v + w$. A code C of length n is a set of binary vectors of length n called ***codewords***. A ***linear code*** is a code whose words are those vectors in subspace of F_2^n, the n-dimensional vector space over the field F_2. The minimum distance $d = d(C)$ of a binary code is the minimum distance between two distinct codewords. If C is linear, the minimum distance is

the minimum Hamming weight of a nonzero codeword.

A ***generator matrix*** for a code C is an k×n matrix whose row space consists of codewords of C. A ***parity check matrix*** for this code is an (n-k)× n matrix H such that $Hx^{Tr} = 0$ for every $x \in C$. In other words the row space of H is the subspace of F_2^n perpendicular to C.

The ***dual code***, $C^{\perp}$ of a code C is the set of vectors perpendicular to C ie., $C^{\perp} = \{v \in F_2^n \ni v.c = 0 \ \forall c \in C\}$.

If G, H are the generator and parity check matrices of a code C, then H and G are generator and parity check matrices of $C^{\perp}$.

For a code C with minimum weight d, any vector in F_2^n is within Hamming distance $t = [(d-1)/2]$ of at most one codeword. Thus a code with minimum weight d can correct t errors in codeword. Such a code is a ***t-error correcting code***.

Similarly we can define a ***q-ary code*** if the base field is $\mathbf{F}_q$ rather than $\mathbf{F}_2$. We note that linear **[n,k,d]** ***code***, with length n, dimension k and minimum weight d is nothing but a $(n, 2^k, d)$ binary code. If the code is q-ary, it is denoted as $(\mathbf{n}, \mathbf{q}^{\mathbf{k}}, \mathbf{d})$ ***code***.

1.1.7 *Perfect code and Sphere-packing Condition* [Va 3.1.6]

In the case when $A^n = S_1 \cup S_2 \cup \ldots\ldots \cup S_m$, we say the $(n,M,d)_A$

code is ***perfect***. In general if an $(n,M,d)_A$ code is q-ary (i.e., over a field with q elements), the following inequality holds.

$$M \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n$$

If the code is perfect then equality holds here.

1.1.8 *Group code and Simplex code* [Va 1.4]

If the alphabet A has a group structure then a subgroup $C \subset A^n$ is a code called a ***group code***.

A code in which the distance between any two codewords is a constant is called a ***simplex code***.

1.1.9 *Finite field* [MS 4]

A finite field F_q where $q = p^m$, a prime power is called a ***finite field*** or a ***Galois field*** of dimension q. We may also denote F_q as F_{p^m}, GF (q) or GF (p^m) . The finite number of elements in the field is called the order of the field.

We have :

$$GF(4) = F_2^2 = \{00, 01, 10, 11\}$$

$$GF(9) = F_3^2 = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}$$

Now consider GF(16)

It consists of 4-tuples over {0,1}. The 16 elements can also be represented by polynomials over {0,1} :

The field operations in GF(16) can now be obtained by addition and multiplication of the polynomials, as indicated below, modulo $\pi(\alpha)$ (where $\pi(\alpha)$ is a suitable irreducible polynomial over F_2). We denote the field as GF(16) or GF (2^4). We note that the nonzero elements of the field form a cyclic group of order 15 with generator α where $\alpha^{15}=1$ under multiplication. We call α as the primitive element of GF(2^4).

4-tuple	Polynomial
0000	0
1000	1
0100	α
1100	$1+\alpha$
0010	α^2
1010	$1+\alpha^2$
0001	α^3
....	.....
1111	$1+\alpha+\alpha^2+\alpha^3$

GF(2) is the ***binary*** field {0,1}, GF(3) is the ***ternary*** field {0,1,2}. In general GF(p) is the ***p-ary*** field {0,1,2,...., p-1}.

As in the case of $GF(2^4)$, in general $GF(p^m)$ is constructed using a polynomial $\pi(x)$ which is irreducible over GF(p).

1.2 Quantum Information Theory

Quantum information theory is the quantum counterpart of classical information theory. In an error correcting quantum code information is stored in set of ***qubits*** , quantum binary digits, in such a way that information can be extracted even after a subset of this set has changed in an unknown way. The important distinguishing features of quantum information theory over the classical theory are the following. In quantum discussion the beginning point is a Hilbert space which is not present in classical theory. Here instead of the bits we have qubits , which are essentially different from classical case and are more powerful. There are also certain vulnerability to quantum communication like the '***no cloning principle***', '***decoherence***' etc. Quantum error correction coding has two distinct parts.

(i) How to apply error correction in a physical situation

(ii) To find good error correcting codes

1.2.1 *Error correction* [Pi]:

While we transmit a message through a medium , noise in it will damage the information conveyed. The task is to reconstruct the original message by some means.

In classical coding theory it is manipulated in the following manner.

Initially we encode the given message and send it through the medium where the errors creep in and something else is conveyed instead of the original thing. Then we decode this received data and make an estimate of the original input to it's best level.

In quantum setting this cannot be performed arbitrarily , primarily due to the 'no-cloning' property and the 'decoherence'. Anyhow some error correcting codes viz. 9-qubit ,7-qubit and 5-qubit error correcting quantum codes have been constructed , which can overpower the two afore mentioned drawbacks.

By error correcting quantum code we mean an appropriate subspace C of a suitable Hilbert space **H** , such that the input state vectors (or input density matrices) can be recovered by means of a suitable collection of recovery operators subsequently acting upon the error operators on the input vectors.

The fundamental error operators are the Pauli matrices namely,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The strategy adopted in the above error correcting quantum code is to use an ancillary space , say **H**(anc) , and error operators are performed on **H** $\otimes$ **H**(anc) to itself . Subsequently we make measurements on the ancillary space and based on these measurements we obtain the corrective mappings.

A quantum error correcting code is a way of encoding quantum states into qubits (two state quantum systems) so that error or decoherence in a small number of individual qubits has little or no effect on the encoded data.

1.2.2 *Basics in Quantum Information Theory* [Di,Pa2]:

Quantum Information Theory or communication through a quantum channel should satisfy three basic conditions:

(i) Messages are encoded as states of a quantum system with finite number of levels.

Example:

A single particle spin system with two levels, spin up and spin down are labeled as 0,1. A bunch of n such independent systems are combined to form a quantum system with 2^n levels, each level labeled by a word of

length n, from the binary alphabet {0,1}.

(ii) Encoded states are the inputs of the quantum channel and they are to be transmitted.

But due to the presence of 'noise' or 'decoherence' in the channel the output differs.

(iii) A collection of '***good***' states are those input states which when transmitted lead to output states from which input states can be reconstructed without any error or with a small error.

Thus 'good' states can be used to encode the message for transmission through a channel. In the Theory of quantum error correcting codes proper identification of the 'good' states are made and also suitable algorithm for an almost error free reconstruction of the input state are worked out.

A ***quantum system*** with n-levels is given by an n-dimensional complex vector space of coloumn vectors of the form

$$|u\rangle = \begin{bmatrix} z_1 \\ z_2 \\ . \\ . \\ z_n \end{bmatrix}$$, where $z_j \in \mathbf{C} \; \forall \; j$, is called a ***ket*** vector.

To such a ket vector is associated a ***bra*** vector $\langle u| = |u\rangle^{\dagger} = (\overline{z_1}, \overline{z_2}, ..., \overline{z_n})$, the conjugate transpose of $|u\rangle$.

For two ket vectors $|u\rangle$ and $|v\rangle$ their ***inner product*** is given by $\langle u||v\rangle = \langle u|v\rangle$.

The set of ket vectors $\mathbf{C}^n$ is an n-dimensional Hilbert space is denoted by **H**. Also $|u\rangle$ as a function of u on $\{1, 2....., n\}$ is given by $u(i) = z_i$ for i=1,2,.....,n

If $v(i) = t_i$,I=1,2,.....,n then $\langle u|v\rangle = \sum_{i=1}^{n} \overline{u(i)}v(i) = \sum_{i=1}^{n} \overline{z_i}t_i$.

Here {1,2,....,n} is the ***alphabet***.

1.2.3 *States and Observable* [Di]:

An n×n matrix over **C** , defines a linear transformation T on the Hilbert space by $|u\rangle \rightarrow T|u\rangle$. The space $M_n(\mathbf{C})$ of all $n \times n$ matrices is an algebra with involution $T \rightarrow T^{\dagger}$, the conjugate transpose of T.

We call T ***hermitian*** if $T = T^{\dagger}$ and T is ***positive semidefinite*** denoted by $T \geq 0$, if $\langle u|T|u\rangle \geq 0 \ \forall$ u. T is called a ***projection*** if $T = T^2 = T^{\dagger}$.The ***trace*** of T , denoted by TrT, is the sum of the eigenvalues of T or the sum of its diagonal elements.

A positive semidefinite matrix ρ i.e., $\rho \geq 0$ with unit trace is called a ***state*** or a ***density matrix.***

A hermitian matrix is an ***observable*** for any state ρ if the scalar

$Tr(\rho T)$ is the expectation of T in the state ρ.

1.2.4 ***Theorem(Spectral Theorem)*** **[Co]:**

If T is an observable (or a Hermitian matrix) then

$$T = \sum_{i=1}^{k} \lambda_i E_i \tag{1}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_k$ are the distinct real scalars and $E_1, E_2, \ldots, E_k$ are the projections such that $\sum_{i=1}^{k} E_i = I$, $E_i E_j = 0$, if $i \neq j$. The set $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ is called the spectrum of T, the scalars λ_i are the ***eigenvalues*** of T and E_i are the ***spectral projections*** or ***eigen spaces*** of T and (1) is called the ***spectral resolution*** of T.

Remark **:**

Since every projection E can be represented as

$$E = \sum_{i=1}^{d} |u_i\rangle\langle u_i|$$

where $\{|u_i\rangle, i = 1, 2 \ldots, d\}$ is any orthonormal basis for the subspace $\{|u\rangle | E|u\rangle = |u\rangle\}$ of all ket vectors fixed by E, it follows that any state ρ can be expressed as

$$\rho = \sum_{i=1}^{n} p_i |v_i\rangle\langle v_i| \tag{2}$$

where $\{ p_1, p_2, \ldots\ldots, p_n \}$ is the probability distribution on $\{1,2,\ldots\ldots,n\}$ and $\{ |v_i\rangle , i = 1,2\ldots,n \}$ is an orthonormal basis for the Hilbert space $\mathbf{C}^n$. i.e., $\langle v_i | v_j \rangle = \delta_{ij} \quad \forall \; i , j = 1, 2,\ldots, n.$

In the state ρ, the probability that the observable T assumes the value λ_i is given by

$$Pr_{\psi}(T = \lambda_i) \quad = \quad Tr\, \rho E_i \qquad \forall \quad i = 1, 2\ldots, k$$

and the expectation of T is

$$\sum_{i=1}^{k} \lambda_i \, Tr\, \rho E_i \quad = \quad Tr\rho \sum_{i=1}^{k} \lambda_i E_i$$

$$= \; Tr \; \rho T.$$

If $|u\rangle$ is any unit vector in $\mathbf{C}^n$, then $|u\rangle \langle u|$ is a one dimensional projection and is a state called a ***pure state***. By (2) every state ρ can be expressed as a linear combination of states which are one dimensional projections $| v_i \rangle \langle v_i |$, then ρ is called a ***mixed state*** . So every state is a convex combination or a mixture of pure states .

We call (H , ρ) as the ***quantum probability space***.

1.2.5 *Completely positive map* [Da]:

Let $A = B(\mathbf{H})$ and $B = B(\mathbf{K})$ and $\varphi : A \rightarrow B$ be a linear map. Then we can define $\varphi_n : M_n(A) \rightarrow M_n(B)$ as $\varphi_n(a_{ij}) = (\varphi(a_{ij}))$. The map φ is

positive if it maps positive elements of A into positive elements of B and φ is ***completely positive*** if every φ_n is positive.

1.2.6 *Tensor product of Hilbert spaces* [Ka,Pa1]:

Let $\mathbf{H}_i$, $1 \leq i \leq k$ be Hilbert spaces . For any $u_i \in \mathbf{H}_i$, $1 \leq i \leq k$ the multilinear functional $\overset{k}{\underset{i=1}{\otimes}} u_i : \mathbf{H}_1 \times \mathbf{H}_2 \times \ldots\ldots \times \mathbf{H}_k \rightarrow \mathbf{C}$ is defined as

$$\overset{k}{\underset{i=1}{\otimes}} u_i (v_1, v_2, \ldots, v_k) = \prod_{i=1}^{k} \langle v_i, u_i \rangle .$$

This collection of functionals generate a manifold M such that $u_1 \otimes \ldots . \otimes u_{i-1} \otimes (\alpha u_i + \beta v_i) \otimes u_{i+1} \otimes \ldots . \otimes u_k = \alpha\, u_1 \otimes \ldots\ldots \otimes u_k + \beta u_1 \otimes \ldots \otimes u_{i-1} \otimes v_i \otimes u_{i+1} \otimes \ldots \otimes u_k$, extended by sesquilinearity to a pre-Hilbert space. Then it's completion is a Hilbert space called the ***tensor product*** of the Hilbert spaces , denoted as $\overset{k}{\underset{i=1}{\otimes}} \mathbf{H}_i$.

Let $\{e_{ij} , j = 1,2,\ldots.\}$ be an orthnormal basis of $\mathbf{H}_i$, $i = 1,2,\ldots,k$. Then the set $\{e_{1j_1} \otimes e_{2j_2} \otimes \ldots\ldots \otimes e_{kj_k} , j_1 = 1,2..;\ j_2 = 1,2,\ldots;\ldots;j_k = 1,2,..\}$ is an orthonormal basis for $\overset{k}{\underset{i=1}{\otimes}} \mathbf{H}_i$

If $\dim \mathbf{H}_i = m_i < \infty$ then $\dim \overset{k}{\underset{i=1}{\otimes}} \mathbf{H}_i = m_1 m_2 \ldots . m_k$

1.2.7 Combination of Quantum States [Pa 2]:

A ***combination of quantum systems*** can be represented by a tensor product of quantum states. The tensor product of the operators A_i , which is equivalent to $n_i \times n_i$ matrices , is defined as the product linear operator

$A_1 \otimes A_2 \otimes \ldots\ldots\ldots \otimes A_k$ on $\mathbf{H}_1 \otimes \mathbf{H}_2 \otimes \ldots\ldots\ldots \otimes \mathbf{H}_k$ as

$$A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_k \,|\, u_1, u_2, \ldots, u_k\rangle \;=\; |A_1 u_1, A_2 u_2, \ldots\ldots\ldots A_k u_k\,\rangle.$$

With this definition we have:

$$(A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_k)\,(B_1 \otimes B_2 \otimes \ldots\ldots \otimes B_k) \;=\; (A_1 B_1 \otimes A_2 B_2 \otimes \ldots\ldots \otimes A_k B_k),$$

$$(A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_k)^{\dagger} \;=\; (A_1^{\dagger} \otimes A_2^{\dagger} \otimes \ldots\ldots\ldots \otimes A_n^{\dagger}),$$

$$A_1 \otimes A_2 \otimes \ldots\ldots \otimes (\alpha A_i + \beta B_i) \otimes \ldots\ldots \otimes A_k \;=$$

$$A_1 \otimes A_2 \otimes \ldots \otimes A_{i-1} \otimes A_i \otimes A_{i+1} \ldots \otimes A_k)$$

$$+\; (\,\beta A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_{i-1} \otimes B_i \otimes A_{i+1} \otimes \ldots\ldots \otimes A_k\,).$$

$$\mathrm{Tr}\,(A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_k) \;=\; \prod_{i=1}^{k} \mathrm{Tr}\, A_i.$$

If ρ_i is a state on $\mathbf{H}_i$ then $\rho_1 \otimes \rho_2 \otimes \ldots\ldots \otimes \rho_k$ represents a state on $\mathbf{H}_1 \otimes \mathbf{H}_2 \otimes \ldots\ldots \otimes \mathbf{H}_k$ such that the expectation of the observable $A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_k$ in the product state $\rho_1 \otimes \rho_2 \otimes \ldots\ldots\ldots \otimes \rho_k$ is

$$\mathrm{Tr}\;(\rho_1 \otimes \rho_2 \otimes \ldots\ldots \otimes \rho_k)\,(A_1 \otimes A_2 \otimes \ldots\ldots \otimes A_k)$$

$$= \mathrm{Tr}\rho_1 A_1 \otimes \rho_2 A_2 \otimes \ldots\ldots \otimes \rho_k A_k$$

$$= \prod_{i=1}^{k} \mathrm{Tr}\, \rho_i A_i \ , \text{ the product of individual expectations.}$$

1.2.8 *High Level Systems* [Pa2]:

We combine several systems into a single system. Suppose $\mathbf{H}_j = \mathbf{C}^{nj}$ where j = 1,2,.....,k are the Hilbert spaces describing k quantum systems numbered 1,2,.....,k respectively. By means of tensor Product of spaces $\mathbf{H}_j$ we combine them into a single system.

If $|u_j\rangle \in \mathbf{H}_j$ is given by

$$|u_j\rangle = \begin{bmatrix} z_{j1} \\ z_{j2} \\ . \\ . \\ z_{jm_j} \end{bmatrix} \quad \text{, where} \quad 1 \le j \le k \quad \text{and } z_{jl} \in \mathbf{C} \text{ ,}$$

then the tensor product $|u_1\rangle \otimes |u_2\rangle \otimes \ldots\ldots \otimes |u_k\rangle$ (also denoted as $|u_1\rangle|u_2\rangle \ldots\ldots |u_k\rangle$ or $|u_1\, u_2 \ldots\ldots u_k\rangle$) of the u_i's defined as the coloumn vector

$$|u_1\, u_2 \ldots\ldots u_k\rangle = \begin{pmatrix} . \\ z_i \\ . \end{pmatrix} \quad , \ \mathbf{i} = i_1 i_2 \ldots\ldots i_k \qquad (3)$$

where $z_{\mathbf{i}} = z_{1i_1} z_{2i_2} \ldots\ldots\ldots z_{ki_k} \quad 1 \leq i_r \leq n_r \;,\; r = 1,2,\ldots\ldots,k$

and the multiindex $\mathbf{i}$ ranges through in the lexicographic order.

Similarly we have $\langle u_1 u_2 \ldots\ldots u_k| = \langle u_1| \langle u_2| \ldots\ldots \langle u_k|$

$$= \langle u_1| \otimes \langle u_2| \otimes \ldots \otimes \langle u_k|$$

$$= (\ldots\ldots, \overline{z_i}, \ldots\ldots)$$

The ***Inner product*** between two product vectors

$|u_1 u_2 \ldots u_k\rangle$ and $|v_1 v_2 \ldots\ldots\ldots v_k\rangle$ is $\prod_{i=1}^{k} \langle u_i, v_i \rangle$.

All product vectors of the form (3) span the Hilbert space $\mathbf{C}^{n_1 n_2 \ldots\ldots n_k}$ and is denoted by $\mathbf{H}_1 \otimes \mathbf{H}_2 \otimes \ldots\ldots \otimes \mathbf{H}_k$

Example:

For the 2-level quantum system of dimension 2, the Hilbert space is $\mathbf{H} = \mathbf{C}^2$.

We write $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and

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

as an orthonormal basis for $\mathbf{C}^2$ and the levels are called ***spin up*** and ***spin down*** respectively of the two level spin system.

If $a_1,a_2,\ldots,a_k$ is a binary sequence i.e., each a_i is either 0 or 1 we write

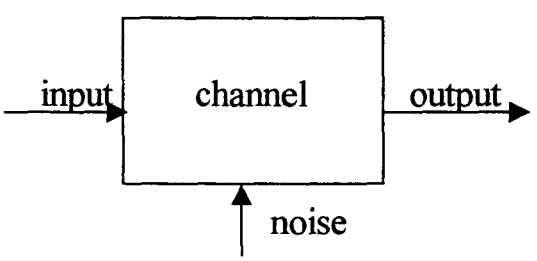
$$|a_1a_2\ldots.a_k\rangle = |a_1\rangle|a_2\rangle\ldots..|a_k\rangle = |a_1\rangle \otimes |a_2\rangle \otimes\ldots..\otimes|a_k\rangle \qquad (4)$$

As all words $a_1a_2\ldots.a_k$ of length k runs through the binary alphabet $\{0,1\}$, the equation (3) runs through an orthonormal basis for $\mathbf{H} \otimes \mathbf{H} \otimes\ldots\ldots\otimes \mathbf{H} = \mathbf{H}^{\otimes k}$.

A state in $\mathbf{C}^2$ is called a ***one qubit state*** and a state in $\mathbf{H}^{\otimes k}$ is called a ***k-qubit state.***

A state of a quantum mechanical particle with ***spin q*** corresponds to a 1-dimensional subspace of the Hilbert space $\mathbf{H} = \mathbf{C}^{2q+1}$ and is represented by a vector in that subspace.

1.2.10 *Quantum Noisy Channels* [NC]:



Let T be a linear operator on **H** such that for each 'signal' or input state ρ on **H** there is an output state $T\rho$. In our context we choose the linear transformation to be '***affine linear***' i.e.,

$T(p\rho_1 + q\rho_2) = pT\rho_1 + qT\rho_2$ for any two states ρ_1, ρ_2 on **H** and nonnegative scalars p,q satisfying $p+q = 1$

Example **[Pa2]:**

Suppose U is a unitary operator such that $T\rho = U\rho U^\dagger$. Here T is reversible transformation and the inverse is $T^{-1}\rho = U^\dagger\rho U$. Such a T transforms pure states into pure states.

Now suppose there is a collection of unitary operators $U_1, U_2, \ldots, U_k$ with probabilities $p_1, p_2, \ldots, p_k$ and applied to a state ρ.

Then $T\rho = \sum_{j=1}^{k} p_j U_j \rho U_j^\dagger$.

Such a T is not reversible and it transforms a pure state into a mixed state.More generally we consider maps of the form

$$T\rho = \sum_{j=1}^{k} L_j \rho L_j^\dagger \qquad \text{where} \qquad \sum_{j=1}^{k} L_j^\dagger L_j = I$$

We note that if each ρ is a positive semidefinite matrix, so is each $L_j\rho L_j^\dagger$ and so is their sum. Thus $T\rho$ is again a state. Further this gives a characterization of a completely positive map.

The matrices L_j are said to ***corrupt*** the input state ρ and are called ***error operators***. A ***noise*** in the channel is a class A of matrices operating as linear operators on **H** of the quantum system and A is called the ***errorspace***.

1.2.11 *Error Correcting Quantum Codes* [Pi]:

The input state is reconstructed from the received output state by decoding.We seek a '***recovery operator***' or '***superoperator***' R which when applied to the output state will reproduce the input state i.e., $R(\sum_{j=1}^{k} Lj\rho Lj^{\dagger}) = \rho$. Such an R will also be a completely positive map. The R need not exist generally but when the input states are restricted to a class of 'good' operators i.e., to a particular subspace of **H** it works.

1.2.12 *Definition* [Pa2]:

Let $C \subset \mathbf{H}$ be a subspace. A state ρ is said to have its ***support*** in C if $Tr\rho P = 1$, where P is the projection on C. The ***orthogonal complement*** $C^{\perp} = \{|v\rangle \; | \langle u|v\rangle = 0 \;\; \forall \;\; |u\rangle \in C\}$ of C , is a subspace of **H**.

1.2.13 ***Definition*** **[Pa2]:**

Let **A** be the space of error operators of a quantum channel whose input and output states are defined on the Hilbertspace **H** of dimension N. A subspace $C \subset \mathbf{H}$ is called an **A** ***correcting quantum code*** if there exist matrices $M_1, M_2, \ldots\ldots, M_n$ (acting as linear operators on **H**) and satisfying:

(a) $\sum_{i=1}^{n} M_i^{\dagger} M_i = I$

(b) If k is any positive integer, $L_1, L_2, \ldots\ldots, L_k \in \mathbf{A}$ satisfy

$\sum_{j=1}^{k} L_j^{\dagger} L_j = I$ and ρ is any input state with support in C

then $\sum_{i=1}^{n} \sum_{j=1}^{k} Mi\,(Lj\rho Lj^{\dagger}) Mi^{\dagger} = \rho.$

Remark:

Thus a state ρ with it's support in an **A**-correcting quantum code C is a ***good state*** i.e., if such a ρ is transmitted through a channel, the output is

$\tilde{\rho} = \sum_{j=1}^{k} L_j \rho L_j^{\dagger}$ where $L_j \in \mathbf{A}$ and $\sum_{j=1}^{k} L_j L_j^{\dagger} = I.$

If the recovery operator R is defined by

$$R\tilde{\rho} = \sum_{i=1}^{n} M_i \rho M_i^{\dagger}$$

then we can recover the input state ρ.

In the case of abstract error correcting code the measurements and corrective actions are modeled by 'Recovery operators' as given below.

If $\{A_a\}$, $\{R_r\}$ are the collections of error operators and recovery operators respectively and if $|k_0\rangle$ is an input state vector ,what we desire for is

$|k_0\rangle = \sum_r R_r A_a |k_0\rangle$ for every a.

More generally if ρ_i is any density matrix defined by states in C such that $\rho_i = \sum_{k_0} p_{k_0} |k_0\rangle\langle k_0|$ then the condition becomes

$\alpha(a,\rho_i)\rho_i = S(A_a \rho_i A_a^{\dagger}) = \sum_r R_r A_a \rho_i A_a^{\dagger} R_r^{\dagger}$ for each a , where

S is the superoperator defined on densities ρ as $S(\rho) = \sum_r R_r \rho R_r^{\dagger}$,

and $\alpha(a,\rho_i)$ is a positive constant and ρ_i is any C density.

The recovery superoperator S is a completely positive map.There is a nice criterion due to Knill and Lafflamme , a necessary and sufficient condition for a subspace to be an error correcting quantum code.

1.2.14 ***Theorem (Knill-Lafflamme Criterion)*** **[KL]:**

For a subspace C of a Hilbert space **H** to be an **A** correcting quantum

code, a necessary and sufficient condition is that C has an orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots\ldots, |\psi_d\rangle\}$ such that for error operators A_a, A_b in the errorspace **A** :

(i) $\langle\psi_i|A_a^{\dagger}A_b|\psi_j\rangle = 0$ if $i \neq j$

(ii) $\langle\psi_i|A_a^{\dagger}A_b|\psi_j\rangle$ is a scalar independent of $i = 1, 2, \ldots\ldots, d$

1.2.15 *t-error correcting quantum codes*[Pa2]:

We consider the input states and output states in the tensor product $\mathbf{H}^{\otimes n}$ of the Hilbert space **H**. The corresponding operator in this case has the form $A_1 \otimes A_2 \otimes \ldots \otimes A_n$ and if at most t-errors occur, except t of the operators A_i, $1 \leq i \leq n$,the others are equal to the identity operator.

If $\mathbf{A}_t$ denotes a linear span of such product operators then the $\mathbf{A}_t$ -error correcting quantum code C is called a ***t-error correcting quantum code.***

1.2.16 *Group representation as a tool in error correcting codes* [Pa2]:

Let A be a finite additive abelian group with null element 0. Let r be the smallest positive integer with the property $rx = 0 \ \forall\ x$. Let $\omega = \exp 2\pi i/r$ be the primitive r th root of unity. Then $\{1, \omega, \omega^2, \ldots, \omega^{r-1}\}$, the set of all r th roots of unity is an abelian group under multiplication.

Let $\alpha : A \to \{1, \omega, \omega^2, \ldots, \omega^{r-1}\}$ be a map satisfying $\alpha(a)\alpha(b) = \alpha(a+b)$ $\forall\ a, b \in A$. Then α is called a ***character*** of A and let $\hat{A}$ denotes the multiplicative group of characters.

On the Hilbert space $\mathbf{H} = L^2(A)$ of complex valued functions on A, define the unitary operators,

U_a, $a \in A$ and V_α, $\alpha \in \hat{A}$ by

$$(U_a f)(x) = f(x+a) \qquad \forall\ x \in A, f \in \mathbf{H}$$

$$(V_\alpha f)(x) = \alpha(x) f(x).$$

We have the ***Weyl commutation relations,***

$$U_a U_b = U_{a+b}, \qquad V_\alpha V_\beta = V_{\alpha\beta}, \qquad U_a V_\alpha = \alpha(a) V_\alpha U_a.$$

The correspondence $(a,\alpha) \to U_a V_\alpha$ is an irreducibile unitary representation of $A \times \hat{A}$.

Now consider $H^{\otimes n}$. The Weyl operators generalizes to

$$U_{\mathbf{a}} = U_{a_1 a_2 \ldots a_n} = U_{a_1} \otimes U_{a_2} \otimes \ldots\ldots \otimes U_{a_n}$$

$$V_{\alpha} = V_{\alpha_1 \alpha_2 \ldots \alpha_n} = V_{\alpha_1} \otimes V_{\alpha_2} \otimes \ldots\ldots \otimes V_{\alpha_n}$$

where A is the encoding space such that $(\mathbf{a},\alpha) \in A^n \times \hat{A}^n$.

Then the Weyl commutation relations are

$$U_{\mathbf{a}} U_{\mathbf{b}} = U_{\mathbf{a}+\mathbf{b}}, \quad V_\alpha V_\beta = V_{\alpha\beta} \quad \text{and}$$

$$V_\alpha U_a = \prod_{i=1}^{n} \alpha_i(a_i)\, U_a V_\alpha$$

Here $(\mathbf{a},\alpha)$ is said to have weight t , if $\#\{ i \mid (a_i,\alpha_i) \neq (0,1), 1 \leq i \leq n \} = t$ and it is denoted as $w(\mathbf{a},\alpha) = t$

1.2.17 ***Proposition*** **[Pa2]:**

The set $\{ U_a V_\alpha \mid w(\mathbf{a}, \alpha) \leq t \}$ is a basis of unitary operators for the error space $\mathbf{A}_t$

Remark:The following theorem gives an important connection between error correcting quantum codes and the Weyl operators.

1.2.18 Theorem **[Pa2]:**

For a subspace $C \subset \mathbf{H}^{\otimes n}$ is a t-error correcting quantum code , a necessary and sufficient condition is that : C has an orthonormal basis $\{ |\psi_i\rangle , i = 1,2,\ldots k\}$ where $|\psi_i\rangle = \sum_{a_1,a_2,\ldots a_n \in A} \psi_i(a_1,a_2,\ldots,a_n) \mid a_1,a_2,\ldots,a_n \rangle$

(is equal to $\sum_{a \in A^n} \psi_i(\mathbf{a}) \mid \mathbf{a} \rangle$) and $\forall$ $(\mathbf{a} ,\alpha) \in A^n \times \hat{A}^n$ (Here A is the additive group encoding the Hilbert space $\mathbf{H}$ and $\hat{A}$ is the multiplicative group of the characters of A) with weight $w(\mathbf{a} ,\alpha) \leq 2t$ one has

(i) $\sum_{x \in A^n} \alpha(\mathbf{x})\, \psi_i(\mathbf{x}+\mathbf{a})\, \psi_j(\mathbf{x}) = 0$ if $i \neq j$

(ii) $\sum_{x \in A^n} \alpha(\mathbf{x})\, \psi_i(\mathbf{x}+\mathbf{a})\, \psi_i(\mathbf{x})$ is independent of $i = 1,2,\ldots,k$

with $\alpha(\mathbf{x}) = \prod_{i=1}^{n} \alpha_i(x_i)$.

1.2.19 *CSS CODE (Calderbank-steane-shor code)*[CS ,St1,2]

In this method the scheme of classical error correcting codes are implemented in the general quantum error correcting quantum codes .The idea behind is to use two classical codes ,one to correct σ_x errors and the other to correct σ_z errors in such a manner that the corrections of one type of error will not effect the corrections of the other type of error.

Let E = lin.span $\{U_a V_\alpha \mid a\in A, \alpha\in \hat{A}\}$. We define the E-corrrcting quantum code by subgroups $C_1 \subset C_2 \subset A$. Let S be the cross section for C_2/C_1 such that $C_2 = \bigcup_{a\in S} C_1 + a$, the coset decomposition of C_2 by C_1 cosets.

1.2.20 *Theorem*[CS,St1,2,Pa3]:

The lin.span $\{\psi_a \mid a\in S\}$ is an E-correcting quantum code of dimension $\frac{\#C_2}{\#C_1}$ where $\psi_a(x) = (\#C_1)^{-1/2} I_{C_1+a}(x)$, $a\in S$, I is the indicator function.

1.3 Uncertainty and Entropy

In this section we consider some results pertaining to uncertainty and entropy and how they are interrelated.

1.3.1 *Uncertainty Principle* [Is]:

The Heisenberg uncertainty relation in wave mechanics is

$$\Delta_\psi x \Delta_\psi p \geq \tfrac{1}{4}([x,p] = i)$$

which expresses indeterminacy of position and momentum in terms of the second moments of the corresponding distributions.

If A and B are two observable whose probability distributions cannot be both arbitrarily peaked and they are noncommuting then the uncertainty principle is given by the Robertson relation [Ro],

$$\Delta_\psi A \, \Delta_\psi B \geq \tfrac{1}{2} \left| \langle [A,B] \rangle \right|,$$

where $\Delta_\psi A$ and $\Delta_\psi B$ denote the standard deviations of the distributions:

$$(\Delta_\psi A)^2 = \langle A^2 \rangle_\psi - (\langle A \rangle_\psi)^2$$

$$(\Delta_\psi B)^2 = \langle B^2 \rangle_\psi - (\langle B \rangle_\psi)^2$$

In general there is an irreducible lower bound on the uncertainty in the result of a simultaneous measurement of noncommuting observables or equivalently there is an upper bound on the accuracy with which values of noncommuting observables can be simultaneously prepared.

The right hand side of the relation depends on the state ψ and so it has no fixed lower bound.

1.3.2 Shannon entropy [NC]:

Shannon [Sh] introduced the concept of entropy of a probability distribution (already it was there in thermodynamics) as a measure of information gained in a communication . The amount of information gained after an experiment is same as the amount of uncertainty prevailed before the experiment This is the crux of the connection between Shannon Entropy and Uncertainty principle.

1.3.3 *Definition*:

For every probability distribution $P = (p_1, p_2, \ldots, p_n)$ with $p_i \geq 0$ and $\sum_{i=1}^{n} p_i = 1$, the *Shannon entropy* is defined as

$$H(P) = -\sum_{j=1}^{n} p_j \log p_j$$

1.3.4 *Properties*:

(i) H(P) is invariant under permutation since it depends only on the probabilities.

(ii) $H(P) \geq 0$

(iii) H(P) is a concave function ie., if P and Q are two distributions ,

$$H(\lambda P + (1-\lambda) P) \geq \lambda H(P) + (1-\lambda) H(Q) \text{ for } 0 \leq \lambda \leq 1$$

(iv) If P,Q are two distributions then P×Q is also a distribution and

$$H(P\times Q) = -\sum_{i,j} p_i q_j \log p_i q_j.$$

Then $H(P\times Q) = H(P) + H(Q)$

(v) $H(P) = 0$ if and only if P is a Dirac distribution

i.e., when $p_i = 0$ or $p_i = 1$

i.e., when the distribution is deterministic.

(vi) $H(P)$ is maximum for a fixed n if and only if $p_1 = p_2 = \ldots = p_n = \frac{1}{n}$.

On Quantum Codes

M.P. Sivaramakrishnan "On the study of error correcting quantum codes and genaralized entropic uncertainty relation" Thesis. Department of Mathematics , University of Calicut, 2002

Chapter 2 On Quantum Codes

In the first section of this chapter we have a generalization of the CSS code from $\mathbf{F}_2^3$ to $\mathbf{F}_q^n$ and in the second section we discuss that the 5-qubit code is a perfect code whereas the 7-qubit and 9-qubit codes are not. In the last section we get the Knill-Laflamme criterion in the case of symmetric and antisymmetric tensor product spaces.

2.1 Genaralisation of the Calderbank-Steane-Shor Quantum Error Correcting Code

The Calderbank - Steane - Shor (CSS) quantum code is obtained the by Calderbank and Shor and independently by Steane. The seven qubit code was developed by Steane by considering the elements over the finite field $\mathbf{F}_2$ and the encoding has been done as elements of $\mathbf{F}_2^3 = \mathbf{Z}_2^3$.

In this section we work out a genaralisation of this to the case of $\mathbf{F}_q^n$, over any finite field $\mathbf{F}_q$, where we assume that $q = p^m$, an integer power of a prime p. In terms of the entries of $\mathbf{F}_q^n$ we construct a table whose (i, j) th entry is the usual innerproduct of these entries over $\mathbf{F}_q$.

Let C be the set of all row vectors from the table leaving the first coloumn. We , in Theorem 2.1 get a $(q^n-1,\ q^n,\ q^n-q^{n-1})$ simplex code [1.1.8] .We will quantize this by applying theorem [1.2.19] and get

$$|\Psi_0\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C} |\underline{x}\rangle \quad , \quad |\Psi_1\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C+(1,1,1,\ldots,1)} |\underline{x}\rangle,$$

$$|\Psi_\omega\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C+(\omega,\omega,\omega\ldots,\omega)} |\underline{x}\rangle,\ldots\ldots,$$

$$|\Psi_{\omega^{q-2}}\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C+(\omega^{q-2},\omega,^{q-2}\ldots,\omega^{q-2})} |\underline{x}\rangle.$$

is an orthonormal basis for the error correcting quantum code of dimension q and it can correct $[(q^n-q^{n-1}-1)/2]$ errors [1.2.20 ,1.1.4] with $\mathbf{F}_q = \{0, 1, \omega, \omega^2, \ldots\ldots, \omega^{q-2}\}$.

We start with an example as given in [Pa2] which gives a method to construct quantum codes from classical codes.

2.1.1 ***Proposition***:

Consider triples in F_2^3 $(= Z_2^3)$ over the finite field F_2. Then there exists an error correcting quantum code of dimension 2.

Proof:

We construct the following table .On the entries of F_2^3, we use the usual inner product as the composition. ie. abc . xyz = ax+by+cz (mod 2) where the entries in the table are over $F_2 = Z_2$

	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0
001	0	1	0	1	0	1	0	1
010	0	0	1	1	0	0	1	1
011	0	1	1	0	0	1	1	0
100	0	0	0	0	1	1	1	1
101	0	1	0	1	1	0	1	0
110	0	0	1	1	1	1	0	0
111	0	1	1	0	1	0	0	1

Then the portion inside the box is the (7, 8 ,4) = [7,3, 4] simplex code [1.1.8] and it's row vectors form a vector space over F_2 Let C be the set of all row vectors inside the box.

Define

$$|\Psi_0\rangle = \frac{1}{2\sqrt{2}}\sum_{\underline{x}\in C}|\underline{x}\rangle \quad , \quad |\Psi_1\rangle = \frac{1}{2\sqrt{2}}\sum_{\underline{x}\in C+(1,1,1,1,1,1,1,1)}|\underline{x}\rangle \ .$$

Then $\{ |\Psi_0\rangle , |\Psi_1\rangle \}$ is an orthonormal basis [1.2.20] for the error correcting quantum code of dimension 2 and since d = 4, it can correct one error [1.1.4].

We use this method and construct some more quantum codes over other finite fields.

2.1.2 ***Proposition*:**

Consider two tuples of elements in F_3^2 $(= Z_3^2)$ over the finite field F_3. Then there exists a 2 error correcting quantum code of dimension 3.

***Proof*:**

We construct the table as follows .On the entries of F_3^2 over F_3, we apply the standard inner product as ab . xy = ax+by (mod 3) so that the entries of the table are over $F_3 = Z_3$

	00	01	02	10	11	12	20	21	22
00	0	0	0	0	0	0	0	0	0
01	0	1	2	0	1	2	0	1	2
02	0	2	1	0	2	1	0	2	1
10	0	0	0	1	1	1	2	2	2
11	0	1	2	1	2	0	2	0	1
12	0	2	1	1	0	2	2	1	0
20	0	0	0	2	2	2	1	1	1
21	0	1	2	2	0	1	1	2	0
22	0	2	1	2	1	0	1	0	2

The row vectors inside the box form a vector space over $\mathbf{F}_3$ and this portion inside the box is an (8 , 9 , 6) = [8 ,2 ,6] simplex code [1.1.8].

Let C denote the set of all row vectors inside the box.

Define

$$|\Psi_0\rangle = \frac{1}{3}\sum_{\underline{x}\in C} |\underline{x}\rangle \quad , \quad |\Psi_1\rangle = \frac{1}{3}\sum_{\underline{x}\in C+(1,1,1,1,1,1)} |\underline{x}\rangle ,$$

$$|\Psi_2\rangle = \frac{1}{3}\sum_{\underline{x}\in C+(2,2,2,2,2,2)} |\underline{x}\rangle .$$

Then $\{ |\Psi_0\rangle , |\Psi_1\rangle , |\Psi_2\rangle \}$ is an orthonormal basis [1.2.20] for the error correcting quantum code of dimension 3 and since d = 6, it can correct 2 errors [1.1.4].

2.1.3 ***Proposition*:**

Consider all the tuples of elements in $F_4^{\,2}$ ($= Z_4^{\,2}$) over the finite field $\mathbf{F}_4$. Then a quantum code of dimension 4 exists.

***Proof*:**

We construct the following table. Apply the usual inner product on the entries of $F_4^{\,2}$ as the composition. Then ab . xy = ax+by (mod 4) over the field $\mathbf{F}_4 = \mathbf{Z}_4$

	00	01	0ω	$0\omega^2$	10	11	1ω	$1\omega^2$	ω0	ω1	ωω	$\omega\omega^2$	$\omega^2 0$	$\omega^2 1$	$\omega^2\omega$	$\omega^2\omega^2$
00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01	0	1	ω	ω^2	0	1	ω	ω^2	0	1	ω	ω^2	0	1	ω	ω^2
0ω	0	ω	ω^2	1	0	ω	ω^2	1	0	ω	ω^2	1	0	ω	ω^2	1
$0\omega^2$	0	ω^2	1	ω	0	ω^2	1	ω	0	ω^2	1	ω	0	ω^2	1	ω
10	0	0	0	0	1	1	1	1	ω	ω	ω	ω	ω^2	ω^2	ω^2	ω^2
11	0	1	ω	ω^2	1	0	ω^2	ω	ω	ω^2	0	1	ω^2	ω	1	0
1ω	0	ω	ω^2	1	1	ω^2	ω	0	ω	0	1	ω^2	ω	1	0	ω
$1\omega^2$	0	ω^2	1	ω	1	ω	0	ω^2	ω	1	ω^2	ω^2	ω^2	0	ω	1
ω0	0	0	0	0	ω	ω	ω	ω	ω^2	ω^2	ω^2	ω^2	1	1	1	1
ω1	0	1	ω	ω^2	ω	ω^2	0	1	ω^2	ω	1	0	1	0	ω^2	ω
ωω	0	ω	ω^2	1	ω	0	1	ω^2	ω^2	1	0	ω^2	1	ω^2	ω	0
$\omega\omega^2$	0	ω^2	1	ω	ω	ω^2	ω^2	0	ω^2	1	ω	ω	1	ω	0	ω^2
$\omega^2 0$	0	0	0	0	ω^2	ω^2	ω^2	ω^2	1	1	1	1	ω	ω	ω	ω
$\omega^2 1$	0	1	ω	ω^2	ω^2	ω	1	0	1	0	ω^2	ω	ω	ω^2	0	1
$\omega^2\omega$	0	ω	ω^2	ω	ω^2	1	0	ω	1	ω^2	ω	0	ω	0	1	ω^2
$\omega^2\omega^2$	0	ω^2	1	1	ω^2	0	ω	1	1	ω	0	ω^2	ω	1	1	0

The row vectors inside the box form a vector space over $\mathbf{F}_4$ and they form a (15 , 16 , 12) = [15 ,4 ,12] simplex code [1.1.8].

Let C denote the set of all row vectors inside the box.

Define

$$|\psi_0\rangle = \frac{1}{4}\sum_{\underline{x}\in c} |\underline{x}\rangle \quad , \quad |\psi_1\rangle = \frac{1}{4}\sum_{\underline{x}\in C+(1,1,\ldots,1)} |\underline{x}\rangle \quad ,$$

$$|\psi_2\rangle = \frac{1}{4}\sum_{\underline{x}\in C+(\omega,\omega,\ldots,\omega)} |\underline{x}\rangle \quad , \quad |\psi_3\rangle = \frac{1}{4}\sum_{\underline{x}\in C+(\omega^2\omega^2,\omega^2,\ldots,\omega^2)} |\underline{x}\rangle$$

Then { $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ } is an orthonormal basis[1.2.20] for the five error correcting four dimensional quantum code[1.1.4].

2.1 Theorem (The general case F_q^n):

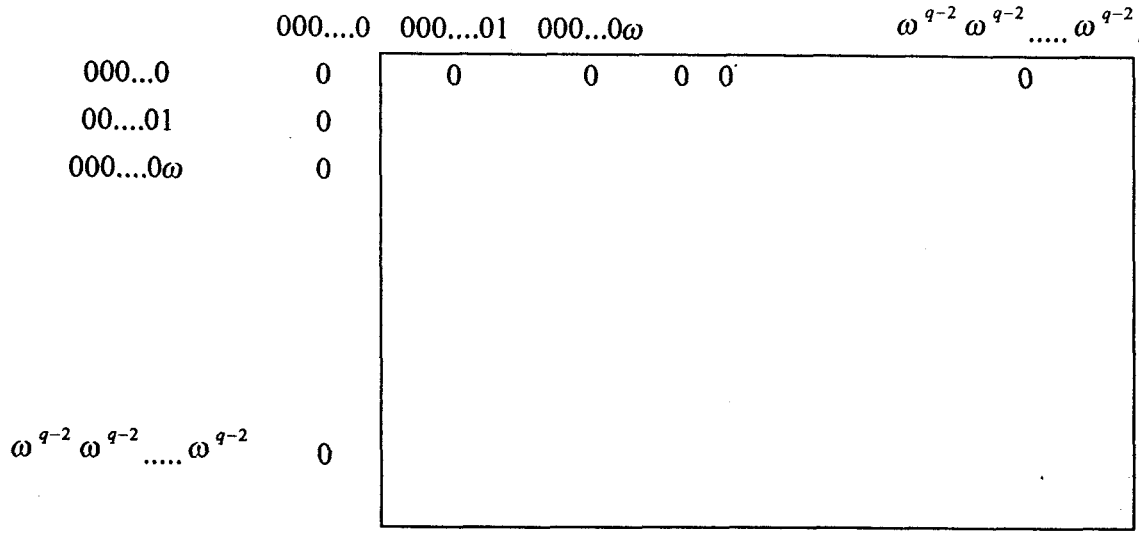
Consider the elements of $\mathbf{F}_q^n$ which are the n-ary vectors over the finite field F_q .Then there exists an error correcting quantum code of dimension (q^n-1 ,q^n , q^n-q^{n-1}) which can correct $[(q^n-q^{n-1}-1)/2]$ errors.

Proof:

We identify F_q with $\{0,1,\omega,\ldots,\omega^{q-2}\}$ where ω is the q th root of unity. We consider the usual inner product namely

$$a_1a_2\ldots a_n \;.\; b_1b_2\ldots b_n = a_1b_1+a_2b_2+\ldots+a_n b_n \;(\text{mod } q)$$

Under this composition we get a table whose entries will make a $q^n \times q^n$ matrix over F_q.



Consider the row vectors inside the box .Their entries are from $\{0,1,\omega,\ldots,\omega^{q-2}\}$.

***Claim* 1:**

These row vectors form a vector space over $\mathbf{F_q}$.

***Proof*:**

A multiplication of any of these rows by an element of $\mathbf{F_q}$ gives

again a row inside the box. Consider the rows corresponding to $\alpha_1,\alpha_2,\ldots,\alpha_n$ and $\beta_1, \beta_2,\ldots\ldots, \beta_n$ where α_i's and β_i's are in $\mathbf{F}_q$.These rows are given by taking the inner product of $\alpha_1, \alpha_2,\ldots\ldots, \alpha_n$ and $\beta_1, \beta_2,\ldots\ldots, \beta_n$ with the n tuples appearing at the top of the table. Hence the sum of these two rows is given by taking the inner product of $\alpha_1, \alpha_2,\ldots\ldots, \alpha_n + \beta_1, \beta_2,\ldots\ldots, \beta_n$ with the n tuple appearing at the top of the table. But

$\alpha_1, \alpha_2,\ldots\ldots, \alpha_n +\beta_1, \beta_2,\ldots\ldots, \beta_n$ is again of the form $\gamma_1, \gamma_2,\ldots\ldots, \gamma_n$ where $\gamma_I \in \mathbf{F}_q$ and corresponding to $\gamma_1, \gamma_2,\ldots\ldots, \gamma_n$ we have a row inside the box. This implies that the sum of rows corresponding to $\alpha_1, \alpha_2,\ldots\ldots, \alpha_n$ and $\beta_1, \beta_2,\ldots\ldots, \beta_n$ lies inside the box. Hence the claim.

***Claim* 2:**

The number of 0's in each nonzero row is q^{n-1}.

We use the following theorem to prove this claim:

***Theorem* [Hu]:**

An if and only if condition for the congruence $a_1x_1+a_2x_2+\ldots..+a_nx_n+b \equiv 0 \pmod m$ to have a solution $(x_1,x_2,\ldots,x_n)$ is that g.c.d $(a_1,a_2,\ldots..,a_n,m) \mid b$. If this condition is satisfied then the number of incongruent (mod m) solutions is $m^{n-1}(a_1,a_2,\ldots..,a_n, m)$

***Proof*:**

If an entry inside the box is zero implies that it is the composition of some $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots\ldots, \beta_n$ such that $\alpha_1\beta_1+\alpha_2\beta_2+\ldots\ldots+\alpha_n\beta_n = 0(\text{mod } q)$ or $\alpha_1\beta_1+\alpha_2\beta_2+\ldots\ldots+\alpha_n\beta_n = tq$

By Theorem [Hu], it happens if and only if g.c.d $(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n, q) = 1 \mid 0$, which is true since $q = p^m$, p is a prime. Hence the number of incongruent solutions (mod q)is equal to $q^{n-1}.1 = q^{n-1}$

If we consider any element of $\mathbf{F}_q^n$ we have shown that there exists exactly q^{n-1} elements of $\mathbf{F}_q^n$ such that the inner product $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ with these q^{n-1} elements is zero, which implies the distance between any two row vectors inside the box is $q^n - q^{n-1}$

Hence the row vectors inside the box is a vector space over $\mathbf{F}_q$ and they form a $(q^n-1, q^n, q^n-q^{n-1}) = [q^n-1, n, q^n-q^{n-1}]$ simplex code [1.1.8] i.e., an n-dimensional (or it has q^n rows), q^{n-1} long vectors with a minimum distance q^n-q^{n-1} so that it can correct $[(q^n-q^{n-1}-1)/2]$ errors [1.2.20 ,1.1.4]

Now let C denote the set of row vectors inside the box .

Define

$$|\Psi_0\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C} |\underline{x}\rangle \quad , \quad |\Psi_1\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C+(1,1,1,\ldots,1)} |\underline{x}\rangle,$$

$$|\Psi_\omega\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C+(\omega,\omega,\omega\ldots\ldots,\omega)} |\underline{x}\rangle,\ldots\ldots,$$

$$|\Psi_{\omega^{q-2}}\rangle = \frac{1}{\sqrt[n]{q}} \sum_{\underline{x}\in C+(\omega^{q-2},\omega,\omega^{q-2}\ldots\ldots,\omega^{q-2})} |\underline{x}\rangle.$$

Then $\{ |\Psi_0\rangle , |\Psi_1\rangle ,\ldots\ldots, |\Psi_{\omega^{q-2}}\rangle \}$ is an orthonormal basis [1.1.20] for the q- dimensional quantum code that can correct $[(q^n-q^{n-1}-1)/2]$ errors [1.1.4].

We conclude this section by asking the following simple yet important question: In quantum studies since unpredictable things happen, is it necessary to consider the usual or standard inner product always ? In the following result we show that by changing the 'product' we can still obtain a quantum code.

2.2 ***Theorem***:

Consider the triples in F_2^3 over the finite field $\mathbf{F}_2$.Then under the 'product' abc . xyz = ax + by (mod2) ,there exists a single error correcting

quantum code of dimension 2.

***Proof*:**

We have $F_2^3 = Z_2^3$

With the 'product' defined as $abc \,.\, xyz = ax + by \pmod 2$,

we obtain the following table.

	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0
001	0	0	0	0	0	0	0	0
010	0	0	1	1	0	0	1	1
011	0	0	1	1	0	0	1	1
100	0	0	0	0	1	1	1	1
101	0	0	0	0	1	1	1	1
110	0	0	1	1	1	1	0	0
111	0	0	1	1	1	1	0	0

Choose C as the four nonrepeated rows inside the box.

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Over $\mathbf{F}_2$, the row vectors in C form a vector space .Hence the rows of C gives a (7 , 4 , 4) = [7 , 2, 4] simplex code [1.1.8].

Now define

$$|\psi_0\rangle = \frac{1}{2}\sum_{\underline{x}\in C} |\underline{x}\rangle \quad , \quad |\psi_1\rangle = \frac{1}{2}\sum_{\underline{x}\in C+(1,1,\ldots,1)} |\underline{x}\rangle.$$

Then $\{ |\psi_0\rangle , |\psi_1\rangle \}$ is an orthonormal basis [1.1.20] for the error correcting quantum code of dimension 2 and it can correct one error[1.1.4].

2.3 ***Theorem*:**

Consider triples in F_2^3 over the finite field $\mathbf{F}_2$.Then under the 'product' abc . xyz = by + cz (mod2).there exists an error correcting quantum code of dimension 2.

***Proof*:**

We have $F_2^3 = Z_2^3$

and the scalar product as abc . xyz = by + cz (mod2)

We obtain the following table.

	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0
001	0	1	0	1	0	1	0	1
010	0	0	1	1	0	0	1	1
011	0	1	1	0	0	1	1	0
100	0	0	0	0	0	0	0	0
101	0	1	0	1	0	1	0	1
110	0	0	1	1	0	0	1	1
111	0	1	1	0	0	1	1	0

Choose C as

$$C = \begin{array}{|ccccccc|} \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline \end{array}$$

It gives a $(7, 4, 4) = [7, 2, 4]$ simplex code[1.1.8].

Define

$$|\psi_0\rangle = \frac{1}{2}\sum_{\underline{x}\in C} |\underline{x}\rangle \quad , \quad |\psi_1\rangle = \frac{1}{2}\sum_{\underline{x}\in C+(1,1,\ldots,1)} |\underline{x}\rangle$$

Then $\{|\psi_0\rangle, |\psi_1\rangle\}$ is an orthonormal basis [1.1.20] for the error correcting code of dimension 2 and it can correct one error [1.1.4].

***Remark*:**

So the above results show that it is possible to change the scalar product and still obtain quantum codes . However we note that with these products we may have to work with a smaller vector space or in other words to work with a lesser number of code words.

2.2 The 5-qubit code is perfect

In determining quantum single error correcting codes the three major breakthroughs are by the 9-qubit case of Shor [Sh2], 7-qubit case of Calderbank, Steane, Shor [CS,St1,2] and the 5-qubit case of Laflamme et al [LMPZ]. The 5- qubit code has some nice features over the other two codes. It required a smaller number of qubits in encoding. Indeed it is the minimum bound in terms of the number of qubits.

For a single quantum quantum error correcting code using n qubits means one can make n-1 measurements and so there are 2^{n-1} error patterns. .But in terms of Pauli matrices the number of error patterns is 3n+1. In general the inequality $3n+1 \leq 2^{n-1}$ holds .

In the 9-qubit and 7-qubit cases this inequality is very well satisfied and the equality itself holds in the 5-qubit case. Moreover for no $n \leq 5$ the inequality does hold. Thus it is the least n where equality holds. When the equality holds, the code is called a perfect code. In fact we can prove that apart from the 5-qubit case the 7-qubit and 9-qubit cases are not perfect.

***Remark*:**

An error correcting quantum code C is a subspace of the Hilbert space H. Roughly speaking, the error operators will cause error by mapping this subspace onto subspaces of H. If the code is perfect then these subspaces will make up the whole Hilbert space H. If the code is not perfect then the sum of these subspaces will not give us the whole H.

2.2.1 *Theorem*:

The error space of the single error correcting 5-qubit code with an orthonormal basis $\{ |\psi_0\rangle , |\psi_1\rangle \}$ given by

$$|\psi_0\rangle = \tfrac{1}{4}\{ |00000\rangle + [|11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle]$$
$$- [|01010\rangle + |00101\rangle + |10010\rangle + |01001\rangle]$$
$$- [|11110\rangle + |01111\rangle + |10111\rangle + |11011\rangle]$$
$$|\psi_1\rangle = \tfrac{1}{4}\{ |11111\rangle + [|00111\rangle + |10011\rangle + |11001\rangle + |11100\rangle]$$

$$-[|10101\rangle + |11010\rangle + |01101\rangle + |10110\rangle]$$

$$-[|00001\rangle + |10000\rangle + |01000\rangle + |00100\rangle] \qquad (**)$$

(Laflamme's encoding) has dimension equal to 16.

***Proof*:**

We know the error space A_t of the t-error correcting code has the basis $\{ U_a V_\alpha \mid w(\mathbf{a},\alpha) \leq t \}$ where $\mathbf{a} = a_1 a_2 \ldots . a_n$ and $\alpha = \alpha_1 \alpha_2 \ldots . \alpha_n$ with $U_a V_\alpha = U_{a_1} V_{\alpha_1} \otimes U_{a_2} V_{\alpha_2} \otimes \ldots . \otimes U_{a_n} V_{\alpha_n}$ and $w(\mathbf{a},\alpha) = t$ means $t = \#\{i \mid (a_i,\alpha_i) \neq (0,1) \text{for } 1 \leq i \leq n\}$ [1.2.17]

Thus except for t terms in the tensor product all the rest are identity. In our 5-qubit single error correcting code

$$U_a V_\alpha = U_{a_1} V_{\alpha_1} \otimes U_{a_2} V_{\alpha_2} \otimes \ldots . \otimes U_{a_5} V_{\alpha_5}$$

$$\#\{i \mid (a_i,\alpha_i) \neq (0,1) \text{for } 1 \leq i \leq 5\} = 1$$

Here the possible choices of (a_i,α_i) are $(0,-1)$, $(1,1)$ and $(1,-1)$ since $A = \{0,1\}$ and $\hat{A} = \{1,-1\}$. Thus in the tensor product of 5 factors we make errors but we cannot make errors in more than one factor. In other words except for one factor the remaining factors are identity. Hence the possible

choices of entries in the basis of the error space are $\{U_{a_1} V_{\alpha_1} \otimes I \otimes I \otimes I \otimes I$, $I \otimes U_{a_2} V_{\alpha_2} \otimes I \otimes I \otimes I$, $I \otimes I \otimes U_{a_3} V_{\alpha_3} \otimes I \otimes I$, $I \otimes I \otimes I \otimes U_{a_4} V_{\alpha_4} \otimes I$, $I \otimes I \otimes I \otimes I \otimes U_{a_5} V_{\alpha_5}\}$ where $(a_i,\alpha_i) \in \{(0,-1),(1,1),(1,-1)\}$ (1)

The Laflamme's 5-qubit single error correcting 2 dimensional quantum code has the orthonormal basis $\{|\psi_0\rangle, |\psi_1\rangle\}$ as given in (**) above.

Now $U_{a_i} V_{\alpha_i} |x\rangle = \alpha_i(x_i) |x+a_i\rangle$ since the actions of the two unitary operators U_a and V_α are given by

$$U_a |\mathbf{x}\rangle = |\mathbf{x}+\mathbf{a}\rangle \quad \text{and} \quad V_\alpha |\mathbf{x}\rangle = \alpha(\mathbf{x}) |\mathbf{x}\rangle$$

Now to prove that the 5 qubit code is perfect it is sufficient if we prove Span $\{U_a V_\alpha |\psi_0\rangle | w(\mathbf{a},\alpha) \leq 1\}$ + Span $\{U_a V_\alpha |\psi_1\rangle | w(\mathbf{a},\alpha) \leq 1\}$ = $\mathbf{H}^{\otimes 5}$, the whole 32- dimensional Hilbert space.

This will mean that the 5-qubit code is perfect since the (code $H_0)^\perp = \{0\}$

We have this following table associating A and $\hat{A}$,

	0	1
1	1	1
-1	1	-1

Except for identity , the options of (a_i,α_i) are (0,-1), (1,1), (1,-1).With this choice of (a_i,α_i), (1) gives 243 unitary operators.

Further we have :

(1) $U_0V_1|x\rangle = |x\rangle$ i.e.,

$U_0V_1|0\rangle = |0\rangle$ and $U_0V_1|1\rangle = |1\rangle$

(2) $U_0V_{-1}|x\rangle = -1(x)|x\rangle$ i.e.,

$U_0V_{-1}|0\rangle = |0\rangle$ and $U_0V_{-1}|1\rangle = -|1\rangle$

(3) $U_1V_1|x\rangle = |x+1\rangle$ i.e.,

$U_1V_1|0\rangle = |1\rangle$ and $U_1V_1|1\rangle = |0\rangle$

(4) $U_1V_{-1}|x\rangle = -1(x)|x+1\rangle$ i.e.,

$U_1V_{-1}|0\rangle = |1\rangle$ and $U_1V_{-1}|1\rangle = -|0\rangle$

The 243 unitary operators carry the orthonormal set$\{|\psi_0\rangle, |\psi_1\rangle\}$ to an orthonormal set of H. Out of this collection, we can pick out 32, which will form a basis of $\mathbf{H}^{\otimes 5}$. In other words the action of merely 16 of these operators can give an orthonormal basis for $\mathbf{H}^{\otimes 5}$.

2.2.2 ***Corollary*** **:**

The five qubit error correcting quantum code is perfect.

***Proof*:**

By theorem [2.2.1] only 16 operators are needed to span the errorspace so that they will make a decomposition of the Hilbert space as the union of these subspaces. This property proves that the 5-qubit quantum code is perfect.

***Remark*:**

On the other hand in the case of 7-qubit code we have to check the action of a total 2187 unitary operators and in the case of 9-qubit code the action of a total 19683 unitary operators .But in both cases what we conclude is that even after ignoring the multiplicities in the resulting vectors, there are vectors left out so as to make up the orthonormal basis for $\mathbf{H}^{\otimes 7}$ and $\mathbf{H}^{\otimes 9}$ with respective dimensions 128 and 512 .

2.2.3 *Corollary* :

The seven qubit and the nine qubit quantum codes are not perfect. Even if we make use of all the 2187 (19683) error operators and get subspaces , they will not combine to form the whole $\mathbf{H}^{\otimes 7}$ ($\mathbf{H}^{\otimes 9}$) spaces.

2.3 Symmetric and Antisymmetric Tensor product (Regarding Bosons and Fermions)

If $\mathbf{H}$ is a Hilbert space we denote by $\mathbf{H}^{\otimes n}$, $\mathbf{H}^{s^n}$, $\mathbf{H}^{a^n}$ as the n th tensor, symmetric tensor, antisymmetric tensor products respectively.

Example:

If $\{e_1,e_2\}$ is a basis for $\mathbf{H}$ then $\mathbf{H}^{\otimes 2}$ has dimension 4 with basis $\{e_1\otimes e_2,\ e_1\otimes e_1,\ e_2\otimes e_2,\ e_2\otimes e_1\}$, $\mathbf{H}^{s^n}$ has dimension 3 with basis $\{e_1\otimes e_1,\ e_2\otimes e_2,\ e_1\otimes e_2+e_2\otimes e_1\}$ and $\mathbf{H}^{a^n}$ has dimension 1 with basis $\{e_1\otimes e_2 - e_2\otimes e_1\}$

2.3.1 ***Definition*** **[Pa 1]**:

Let S_n be the group of permutations of the set $\{1,2,\ldots,n\}$ and $U(\mathbf{H}^{\otimes n})$ be the unitary group of $\mathbf{H}^{\otimes n}$.

For $\sigma \in S_n$, define the map U_σ on $U(\mathbf{H}^{\otimes n})$ as

$$U_\sigma\, u_1\otimes u_2\otimes \ldots..\otimes u_n = u_{\sigma^{-1}(1)} \otimes u_{\sigma^{-1}(2)} \otimes \ldots.\otimes u_{\sigma^{-1}(n)},$$

where σ^{-1} is the inverse of σ. The map $\sigma \to U_\sigma$ is a map from the finite group S_n into $U(\mathbf{H}^{\otimes n})$.

The subspaces $\mathbf{H}^{s^n}$, $\mathbf{H}^{a^n}$ of $\mathbf{H}^{\otimes n}$ are given by

$\mathbf{H}^{s^n} = \{u \in \mathbf{H}^{\otimes n} \mid U_\sigma u = u \ \forall \sigma \in S_n\}$ and

$\mathbf{H}^{a^n} = \{u \in \mathbf{H}^{\otimes n} \mid U_\sigma u = \varepsilon(\sigma) u \ \forall \sigma \in S_n\}$, where $\varepsilon(\sigma) = \pm 1$ according as σ is even or odd.

These are the n-fold symmetric and antisymmetric tensor products of **H**.

Remark:

If the Hilbert space **H** has dimension N then the dimensions of

$$\dim \mathbf{H}^{\otimes n} = N^n \quad , \quad \dim \mathbf{H}^{s^n} = \binom{N+n-1}{n} \text{ and}$$

$$\dim \mathbf{H}^{a^n} = \begin{cases} \binom{N}{n} & , \text{if } n \le N \\ 0 & , \text{if } n > N \end{cases}$$

respectively.

Let A be the additive abelian group of order N with identity 0 and let $\hat{A}$ be the multiplicative group of its characters with unit element 1.

By assuming that there are no repetitions , we encode the orthonormal basis for $\mathbf{H}^{\otimes n}$ with the entries of A as $\{|a_1 a_2 \ldots a_n\rangle \ , a_i \in A \ , 1 \le i \le n.\}$

We note that $(a,\alpha) \rightarrow U_a V_\alpha$ is a unitary representation of $A \times \hat{A}$ and the dimension of $B(\mathbf{H}) = N^2$

Similarly $(\mathbf{a},\alpha) \rightarrow U_a V_\alpha$ is a unitary representation of $A^n \times \hat{A}^n$ and the dimension of $B(\mathbf{H}^{\otimes n}) = N^{2n}$.

Knowing that dim $\mathbf{H}^{s^n} = \binom{N+n-1}{n}$ and dim $\mathbf{H}^{a^n} = \binom{N}{n}$ we look for the appropriate Weyl unitary representations for $\mathbf{H}^{s^n}$ and $\mathbf{H}^{a^n}$.

We first consider a simple case.

Let dim(**H**) =3 ,N =3 ,n = 2 then dim $\mathbf{H}^{s^2} = \binom{4}{2} = 6$.

If the orthonormal basis for **H** is $\{e_1,e_2,e_3\}$,then the orthonormal basis for $\mathbf{H}^{s^2}$ is

$\{ |e_1e_1\rangle, |e_2e_2\rangle, |e_3e_3\rangle, |e_1e_2\rangle+|e_2e_1\rangle, |e_2e_3\rangle+|e_3e_2\rangle, |e_1e_3\rangle+|e_3e_1\rangle\}$

Encode the basis of **H** by $A = \{a_1,a_2,a_3\}$ and $\hat{A} = \{\alpha_1,\alpha_2,\alpha_3\}$.

Then the orthonormal basis of $\mathbf{H}^{s^2}$ encoded by the alphabet of A is

$\{ |a_1a_1\rangle, |a_2a_2\rangle, |a_3a_3\rangle, |a_1a_2\rangle+|a_2a_1\rangle, |a_2a_3\rangle+|a_3a_2\rangle, |a_1a_3\rangle+|a_3a_1\rangle\}$

Let $\varphi^{(2)}_{\alpha_i,\alpha_j} = (\varphi_{\alpha_i},\varphi_{\alpha_j})$, $\varphi_{\alpha_i}, \varphi_{\alpha_j} \in A$

Then we define $\varphi^{s^2} = (\varphi_{\alpha_i},\varphi_{\alpha_j}) = \varphi^{(2)}_{\alpha_i,\alpha_j}$ if i = j and

$\varphi^{s^2} = \sum_{p\in\wp(3)} |\varphi^{(2)}_{P,i,j}\rangle$, (where $\varphi^{(2)}_{P,i,j} = (\varphi_{\alpha_i}, \varphi_{\alpha_j})$ and P varies over all permutations of 1,2,3 taken two at a time), otherwise.

With this notation for denoting entries of $\mathbf{H}^{s^2}$ where **H** is encoded by A, we now define operators $U_{\mathbf{a}}$ and V_α on $\mathbf{H}^{s^2}$ as

$$U_{\mathbf{a}}|\mathbf{x}\rangle = |\mathbf{x}+\mathbf{a}\rangle \text{ and } V_\alpha|\mathbf{x}\rangle = \alpha(\mathbf{x})|\mathbf{x}\rangle$$

where $\mathbf{a} = a_ia_j + a_ja_i$, $\mathbf{x} = x_ix_j + x_jx_i$ are in A^{s^2} and $\alpha = \alpha_i\alpha_j$ in $\hat{A}^{s^2}$. Then $\mathbf{x}+\mathbf{a} = (x_i+a_i)(x_j+a_j) + (x_j+a_j)(x_i+a_i) \in A^{s^2}$ and $\alpha(\mathbf{x}) = \alpha_i(x_i)\alpha_j(x_j)$ (By A^{s^2}, $\hat{A}^{s^2}$ we mean terms from A^n and $\hat{A}^n$ which are symmetric in nature).

Thus $\{U_{\mathbf{a}}V_\alpha | \mathbf{a} \in A^{s^2}, \alpha \in \hat{A}^{s^2}\}$ is a basis for the t-error correcting quantum code if $w(\mathbf{a}, \alpha) \le t$. [1.2.17]

We observe that dim $B(\mathbf{H}^{s^2}) = 6^2 = 36$.

In the general case ,

Let $\varphi^{(n)}_{\alpha_1,\alpha_2,..,\alpha_n} = (\varphi_{\alpha_1}, \varphi_{\alpha_2}, ..., \varphi_{\alpha_n})$ where $\varphi_{\alpha_i} \in A$

Define $\varphi^{s^n} = (\varphi_{\alpha_1}, \varphi_{\alpha_2}, ..., \varphi_{\alpha_n}) = \varphi^{(n)}_{\alpha_1,\alpha_2,..,\alpha_n}$, if all φ_{α_i} are equal and

$\varphi^{s^n} = \sum_{P\in\wp(n)} |\varphi^{(n)}_{P,\alpha_1,\alpha_2,..,\alpha_n}\rangle$, where $\varphi^{(n)}_{P,\alpha_1,\alpha_2,..,\alpha_n} = (\varphi_{\alpha_1}, \varphi_{\alpha_2}, ..., \varphi_{\alpha_n})$ and

summation is taken over all permutations P of N indices taken n at a time, otherwise.

With this notation of denoting entries of $\mathbf{H}^{s^n}$ where **H** is encoded by A, we now define operators $U_{\mathbf{a}}$ and V_α on $\mathbf{H}^{s^n}$ as

$U_{\mathbf{a}}|\mathbf{x}\rangle = |\mathbf{x}+\mathbf{a}\rangle$ and $V_\alpha|\mathbf{x}\rangle = \alpha(\mathbf{x})|\mathbf{x}\rangle$ over all symmetric terms **x**, **a** in A^n and α in $\hat{A}^n$ which we denote as A^{s^n} and $\hat{A}^{s^n}$ respectively. Then $\{U_{\mathbf{a}}V_\alpha \mid \mathbf{a} \in A^{s^n}, \alpha \in \hat{A}^{s^n}\}$ is a basis for the t-error correcting quantum code if $w(\mathbf{a}, \alpha) \leq t$. [1.2.17]

By making such a selection of the error space we can equivalently state the version of Knill-Laflamme criterion [1.2.18] for a symmetric tensor product of Hilbert spaces.

2.3.2 ***Theorem*:**

A subspace $C \subset \mathbf{H}^{s^n}$ ($\mathbf{H}^{a^n}$) is a t-error correcting quantum code , a necessary and sufficient condition is that if C has an orthonormal basis $\{|\psi_i\rangle, I = 1,2,\ldots k\}$ where $|\psi_i\rangle = \sum_{a_1,a_2,\ldots a_n \in A} \psi_i(a_1,a_2,\ldots,a_n) \mid a_1,a_2,\ldots,a_n\rangle$ (is equal to $\sum_{a \in A^{s^n}} \psi_i(\mathbf{a}) \mid \mathbf{a}\rangle$) and $\forall (\mathbf{a},\alpha) \in A^{s^n} \times \hat{A}^{s^n}$ ($A^{a^n} \times \hat{A}^{a^n}$) (Here A is the additive group encoding the Hilbert space H , $\hat{A}$ is the multiplicative

group of thecharacters of A and by A^{s^n}, $\hat{A}^{s^n}$ we mean terms of symmetric nature from A^n, $\hat{A}^n$. A parellel structure may be used for antisymmetric case.) with weight $w(\mathbf{a}, \alpha) \leq 2t$ one has,

(i) $\sum_{x \in A^n} \alpha(\mathbf{x})\, \overline{\psi_i(\mathbf{x}+\mathbf{a})}\, \psi_j(\mathbf{x}) = 0 \quad \text{if} \quad i \neq j$

(ii) $\sum_{x \in A^n} \alpha(\mathbf{x})\, \overline{\psi_i(\mathbf{x}+\mathbf{a})}\, \psi_i(\mathbf{x})$ is independent of $i = 1,2,\ldots,k$

with $\alpha(\mathbf{x}) = \prod_{i=1}^{n} \alpha_i(x_i)$.

***Proof*:**

We have proved the theorem in the case of symmetric product. Now we have to prove the theorem for an antisymmetric product.

Consider the example discussed above.

If $\dim \mathbf{H} = N = 3$, $n = 2$. Then $\dim \mathbf{H}^{a^2} = \binom{3}{2} = 3$

The orthonormal basis of $\mathbf{H}^{a^2}$ encoded by the alphabet of A is

$$\{|a_1a_2\rangle - |a_2a_1\rangle, |a_1a_3\rangle - |a_3a_1\rangle, |a_2a_3\rangle - |a_3a_2\rangle\}$$

Let $\varphi^{(2)}_{\alpha_i,\alpha_j} = (\varphi_{\alpha_i}, \varphi_{\alpha_j})$, $\varphi_{\alpha_i}, \varphi_{\alpha_j} \in A$

Then we define $\varphi^{a^2} = \sum_{P\in\wp(3)} \varepsilon(p)\,|\varphi^{(2)}_{P,i,j}\rangle$: where $\varphi^{(2)}_{P,i,j} = (\varphi_{\alpha_i}, \varphi_{\alpha_j})$ and summation is taken over all permutations P of three indices 1,2,3 taken two at a time and $\varepsilon(p) = \pm 1$ according where $i \neq j$

With this notation for denoting entries of $\mathbf{H}^{a^2}$ where **H** is encoded by A, we now define operators $U_{\mathbf{a}}$ and V_α on $\mathbf{H}^{a^2}$ as :

Define operators $U_{\mathbf{a}}$ and V_α as

$$U_{\mathbf{a}}\,|\mathbf{x}\rangle = |\mathbf{x}+\mathbf{a}\rangle \qquad \text{and} \quad V_\alpha\,|\mathbf{x}\rangle = \alpha(\mathbf{x})\,|\mathbf{x}\rangle$$

where $\mathbf{a} = a_i a_j - a_j a_i$, $\mathbf{x} = x_i x_j - x_j x_i$ are in A^{a^2} and $\alpha = \alpha_i\alpha_j$ in $\hat{A}^{a^2}$. Then $\mathbf{x}+\mathbf{a} = (x_i+a_i)(x_j+a_j) - (x_j+a_j)(x_i+a_i) \in A^{a^2}$ and $\alpha(\mathbf{x}) = \alpha_i(x_i)\alpha_j(x_j)$ (By A^{a^2}, $\hat{A}^{a^2}$ we mean terms from A^n and $\hat{A}^n$ which are antisymmetric in nature).

Thus $\{U_{\mathbf{a}}V_\alpha\,|\,\mathbf{a}\in A^{a^2},\ \alpha\in\hat{A}^{a^2}\}$ is a basis for the t-error correcting quantum code if $w(\mathbf{a},\alpha)\leq t$.

We observe that $\dim B(\mathbf{H}^{a^2}) = 3^2 = 9$.

In the general case ,

Let $\varphi^{(n)}_{\alpha_1,\alpha_2,\ldots,\alpha_n} = (\varphi_{\alpha_1}, \varphi_{\alpha_2}, \ldots\ldots, \varphi_{\alpha_n})$ where $\varphi_i \in A$

Define $\varphi^{s^n} = \sum_{P\in\wp(n)} \varepsilon(p) \left| \varphi^{(n)}_{P,\alpha_1,\alpha_2,..,\alpha_n} \right\rangle$ where $\varphi^{(n)}_{P,\alpha_1,\alpha_2,..,\alpha_n} = (\varphi_{\alpha_1},\varphi_{\alpha_2},.....,\varphi_{\alpha_n})$,

summation is taken over all permutations P of N indices taken n at a time and $\varepsilon(p) = \pm 1$ according as the permutation is even or odd .

With this notation of denoting entries of $\mathbf{H}^{a^n}$, we now define operators $U_{\mathbf{a}}$ and V_α on $\mathbf{H}^{a^n}$ as

$U_{\mathbf{a}} |\mathbf{x}\rangle = |\mathbf{x}+\mathbf{a}\rangle$ and $V_\alpha |\mathbf{x}\rangle = \alpha(\mathbf{x}) |\mathbf{x}\rangle$ over all antisymmetric terms $\mathbf{x}$, $\mathbf{a}$ in A^n and α in $\hat{A}^n$ which we denote as A^{a^n} and $\hat{A}^{a^n}$ respectively. Then $\{U_{\mathbf{a}}V_\alpha \mid \mathbf{a}\in A^{s^n}, \alpha\in \hat{A}^{s^n}\}$ is a basis for the t-error correcting quantum code if $w(\mathbf{a}, \alpha) \leq t$. [1.2.17]

Hence the theorem.

Error Correcting Quantum Codes in Higher Spin Systems

M.P. Sivaramakrishnan "On the study of error correcting quantum codes and genaralized entropic uncertainty relation" Thesis. Department of Mathematics , University of Calicut, 2002

Chapter 3 Error Correcting Quantum Codes in Higher Spin Systems

Normally error correcting quantum codes are discussed in a framework where quantum particles have two possible eigenstates, otherwise termed as spin-1/2 particles. Here we consider a construction of error correcting quantum codes for a higher spin system i.e., spin greater than ½ .Such codes were considered by Chau [Ch2].He had constructed five register and nine register error correcting quantum codes for a higher spin system. His codes are described for a quantum particle with N possible eigen states or the particle has an (N-1)/2 spin.

In his work Chau has used the direct version of the Knill-Laflamme theorem. In our work we use [1.2.18] which is the modified version of the Knill-Laflamme criterion done by K.R.Parthasarathy [Pa2]. Moreover in the last part we make use of this criterion again to check that the five register quantum code is optimal or equivalently that there does not exist a four register quantum code. We have applied a similar method to verify the 9-qubit quantum code. We also construct a seven qubit code following the method discussed by Chau [Ch1].

Chau's theorem says,

3.1 ***Theorem*** **[Ch 2]:**

Consider a quantum particle with N eigen states. Suppose the N mutually orthogonal eigen states that are used to construct the five quantum register code are given by $|0\rangle$, $|1\rangle$, ..., $|N\text{-}1\rangle$ .Then the encoding scheme that can correct at most one quantum error occurring in one of the quantum registers is

$$|k\rangle \rightarrow |k_L\rangle$$

$$= \sum_{p,q,r=0}^{N-1} \omega_N^{k(p+q+r)+pr} \; |p+q+k\rangle\,|p+r\rangle\,|q+r\rangle\,|p\rangle\,|q\rangle$$

$$= \sum_{p,q,r=0}^{N-1} \omega_N^{k(p+q+r)+pr} \; |p+q+k\,,\, p+r,\, q+r,\, p,\, q\,\rangle$$

for $k = 0,1,\ldots..,N\text{-}1$, where additions in the state kets are modulo N and ω_N is the primitive Nth root of unity. (Here $|k_L\rangle$ stands for encoded $|k\rangle$)

Now we have the following version of the Knill-Laflamme criterion [1.2.18] for a t-error error correcting quantum code.

3.2 ***Theorem*****:**

Suppose **H** is a Hilbert space of spin (N-1)/2 i.e., **H** has dimension N.

Let C be a subspace of $\mathbf{H}^{\otimes 5}$ consisting of all vectors of the form $x = |p+q+k, p+r, q+r, p, q\rangle$ with p, q, r, k = 0,1,2.....,N-1. Let $A = \mathbf{Z}_N$, $\hat{A}$ it's group of characters. For $|\mathbf{x}\rangle = |p+q+k, p+r, q+r, p, q\rangle$, set $\psi_k(\mathbf{x}) = \omega_N^{k(p+q+r)+pr}$ and $|\psi_k\rangle = \sum_{x\in A^5} \psi_k(\mathbf{x})|\mathbf{x}\rangle$ for k =0,1,...,N-1. Then this collection is an orthonormal set. Let C be the span of this collection. Then for all $(\mathbf{a}, \alpha)$ in $A^5 \times \hat{A}^5$ with $w(\mathbf{a}, \alpha) \leq 2$, C is a single error correcting quantum code if the following hold :

(i) $\sum_{x\in A^n} \alpha(\mathbf{x})\, \psi_k\, \overline{(\mathbf{x}+\mathbf{a})\, \psi_{k'}}(\mathbf{x}) = 0$ if $k \neq k'$

(ii) $\sum_{x\in A^n} \alpha(\mathbf{x})\, \psi_k\, \overline{(\mathbf{x}+\mathbf{a})\, \psi_k}(\mathbf{x})$ is independent of k =0, 1,2,...., N-1

with $\alpha(\mathbf{x}) = \prod_{i=1}^{n} \alpha_i(x_i)$.

Remark:

By Knill-Laflamme criterion [1.2.18] the subspace C as given in the above theorem will be a single error correcting quantum code.

Proof:

The collection $|\psi_k\rangle$ an orthonormal set in C [Ch2].

Assume $w(\mathbf{a}, \alpha) \leq 2$

Corresponding to $|p+q+k, p+r, q+r, p, q\rangle$ we have

$$\psi_k(p+q+k, p+r, q+r, p, q) = \frac{1}{N^{3/2}}\omega_N^{k(p+q+r)+pr}$$

So for an arbitrary $|x_1,x_2,x_3,x_4,x_5\rangle$ we have

$$k = x_1 - p - q = x_1 - x_4 - x_5$$

$$r = x_2 - p = x_3 - q$$

$$\text{i.e., } r = \begin{cases} x_2 - x_4 \\ x_3 - x_5 \end{cases}$$

$$\text{Hence, } k(p+q+r)+pr = \begin{cases} (x_1 - x_4 - x_5)[x_4 + x_5 + (x_2 - x_4)] + x_4(x_2 - x_4) \\ (x_1 - x_4 - x_5)[x_4 + x_5 + (x_3 - x_5)] + x_4(x_3 - x_5) \end{cases} \quad (1)$$

$$\psi_k(x_1,x_2,x_3,x_4,x_5) = \begin{cases} \frac{1}{N^{3/2}}\omega_N^{(x_1-x_4-x_5)[x_4+x_5+(x_2-x_4)]+x_4(x_2-x_4)} \\ \frac{1}{N^{3/2}}\omega_N^{(x_1-x_1-x_5)[x_4+x+5(x_3-x_5)+x_4(x_3-x_5)} \end{cases}$$

Since $w(\mathbf{a},\alpha) \leq 2$, we need to consider only two cases, when $w(\mathbf{a},\alpha) = 1$ and $w(\mathbf{a},\alpha) = 2$

Now the sum $\sum_{x \in A^n} \alpha(\mathbf{x})\,\psi_k(\mathbf{x}+\mathbf{a})\,\psi_{k'}(\mathbf{x})$ reduces to

$$\frac{\alpha(x)}{N^3}\sum_{p,q,r=0}^{N-1}\omega_N^{P-P_e} \quad (2)$$

where

$$P - P_e = [k(p+q+r) + pr] - [k'_e(p_e+q_e+r_e) + p_e r_e] \quad (3)$$

where the second term is consequent to error.

We discuss all possibilities, since there is no uniformity.

Case 1: (when w(a ,α) = 1)

Weight w(**a** ,α) = 1 implies #{i | $(a_i,\alpha_i) \neq (0,1)$,1≤ i≤ 5 } = 1.Then except for one term in the five tuple (a_1,a_2,a_3,a_4,a_5) the rest are zeroes. It's corresponding character is the only one different from one out of all the five characters.

We have the following subcases.

Subcase **(i)**

If the error is in the first register, then $(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1+a_1, x_2, x_3, x_4, x_5)$

So $k = x_1 - x_4 - x_5 + a_1$

$$r = \begin{cases} x_2 - x_4 \\ x_3 - x_5 \end{cases}$$

from (1) we get $k(p+q+r) + pr = (k+a_1)(p+q+r)+pr$

Using this in (3) we get $P - P_e = [\, k(p+q+r) + pr \,] - [\, (k'+a_1)(p+q+r)+pr]$

$$= (k-k')(p+q+r) - a_1(p+q+r)$$

Thus sum in (2) reduces to $\alpha_1(x_1)\delta_{k,k'}$

Subcase **(ii)**

If the error is in the second register then $(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_2+a_2, x_3, x_4, x_5)$

So $k = x_1 - x_4 - x_5$

$$r = \begin{cases} x_2 - x_4 + a_2 \\ x_3 - x_5 \end{cases}$$

$$\text{Hence} \quad (p+q+r)+pr = \begin{cases} k(p+q+r)+pr \\ k(p+q+r)+p(r+a_2) \\ k(p+q+r+a_2)+pr \\ k(p+q+r+a_2)+p(r+a_2) \end{cases}$$

$$\text{Thus} \qquad P - P' = \begin{cases} (k-k')(p+q+r) \\ (k-k')(p+q+r)-pa_2 \\ (k-k')(p+q+r)-ka_2 \\ (k-k')(p+q+r)-ka_2-pa_2 \end{cases}$$

Again from (3) the sum in (2) reduces to $\alpha_2(x_2)\delta_{k,k'}$

Subcase **(iii)**

If the error is in the third register then $(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_2, x_3+a_3, x_4, x_5)$

So $k = x_1 - x_4 - x_5$

$$r = \begin{cases} x_2 - x_4 \\ x_3 - x_5 + a_3 \end{cases}$$

Hence $k(p+q+r)+pr = \begin{cases} k(p+q+r)+pr \\ k(p+q+r)+p(r+a_3) \\ k(p+q+r+a_3)+pr \\ k(p+q+r+a_3)+p(r+a_3) \end{cases}$

Thus $P\text{-}P' = \begin{cases} (k-k')(p+q+r) \\ (k-k')(p+q+r)-pa_3 \\ (k-k')(p+q+r)-ka_3 \\ (k-k')(p+q+r)-ka_3-pa_3 \end{cases}$

Again sum in (2) reduces to $\alpha_3(x_3)\delta_{k,k'}$

Subcase **(iv)**

If the error is in the fourth register then $(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_2, x_3, x_4, x_5)$

So $k = x_1 - x_4 - x_5 - a_4$

$$r = \begin{cases} x_2 - x_4 - a_4 \\ x_3 - x_5 \end{cases}$$

$$k(p+q+r)+pr = \begin{cases} (k-a_4)(p+q+r)+pr \\ (k-a_4)(p+q+r)+p(r-a_4) \\ (k-a_4)(p+q+r-a_4)+pr \\ (k-a_4)(p+q+r-a_4)+p(r-a_4) \end{cases}$$

$$P\text{-}P' = \begin{cases} (k-k')(p+q+r)+a_4(p+q+r) \\ (k-k')(p+q+r)+a_4(p+q+r)+pa_4 \\ (k-k')(p+q+r)+a_4(p+q+r-a_4) \\ (k-k')(p+q+r)+a_4(p+q+r-a_4)+pa_4 \end{cases}$$

This again gives $\alpha_4(x_4)\,\delta_{k,k'}$ on substitution in (2).

Subcase **(v)**

If the error is in the fifth register then $(x_1, x_2, x_3, x_4, x_5+a_5) \rightarrow (x_1, x_2, x_3, x_4, x_5+a_5)$

So $k = x_1 - x_4 - x_5 - a_5$

$$r = \begin{cases} x_2 - x_4 \\ x_3 - x_5 - a_5 \end{cases}$$

$$\text{Hence } k(p+q+r)+pr = \begin{cases} (k-a_5)(p+q+r)+pr \\ (k-a_5)(p+q+r)+p(r-a_5) \\ (k-a_5)(p+q+r-a_5)+pr \\ (k-a_5)(p+q+r-a_5)+p(r-a_5) \end{cases}$$

$$\text{and} \qquad P - P' = \begin{cases} (k-k')(p+q+r)+a_5(p+q+r) \\ (k-k')(p+q+r)+a_5(p+q+r)+pa_5 \\ (k-k')(p+q+r)+a_5(p+q+r-a_5) \\ (k-k')(p+q+r)+a_5(p+q+r-a_5)+pa_5 \end{cases}$$

We again get $\alpha_5(x_5)\delta_{k,k'}$ in (2).

Case (ii)

In this case $w(\mathbf{a}, \alpha) = 2$. It implies $\#\{i \mid (a_i, \alpha_i) \neq (0,1), 1 \leq i \leq 5\} = 2$. Then except for two terms in the five tuple $(a_1, a_2, a_3, a_4, a_5)$ the rest are zeroes and the corresponding two characters are only those different from 1.

Here also we have the following subcases.

Subcase **(i)**

The two errors are in the first and second registers. Then

$$(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1+a_1, x_2+a_2, x_3, x_4, x_5)$$

So $k = x_1 - x_4 - x_5 + a_1$

$$r = \begin{cases} x_2 - x_4 + a_2 \\ x_3 - x_5 \end{cases}$$

$$\text{Hence, } k(p+q+r) + pr = \begin{cases} (k+a_1)(p+q+r) + pr \\ (k+a_1)(p+q+r) + p(r+a_2) \\ (k+a_1)(p+q+r+a_2) + pr \\ (k+a_1)(p+q+r+a_2) + p(r+a_2) \end{cases}$$

$$\text{and} \quad P - P_e = \begin{cases} (k-k')(p+q+r) - a_1(p+q+r) \\ (k-k')(p+q+r) - a_1(p+q+r) - pa_2 \\ (k-k')(p+q+r) - a_1(p+q+r+a_2) \\ (k-k')(p+q+r) - a_1(p+q+r+a_2) - pa_2 \end{cases}$$

which gives $\alpha_1(x_1)\alpha_2(x_2)\delta_{k,k'}$ in (2).

Subcase **(ii)**

The two errors are in the second and third registers. Then

$$(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_2+a_2, x_3+a_3, x_4, x_5)$$

So $k = x_1 - x_4 - x_5$

$$r = \begin{cases} x_2 - x_4 + a_2 \\ x_3 - x_5 + a_3 \end{cases}$$

$$\text{Hence} \quad k(p+q+r)+pr = \begin{cases} k(p+q+r+a_2)+p(r+a_2) \\ k(p+q+r+a_2)+p(r+a_3) \\ k(p+q+r+a_3)+p(r+a_2) \\ k(p+q+r+a_3)+p(r+a_3) \end{cases}$$

$$\text{and} \qquad P - P_e = \begin{cases} (k-k')(p+q+r)-k'a_2-pa_2 \\ (k-k')(p+q+r)-k'a_2-pa_3 \\ (k-k')(p+q+r)-k'a_3-pa_2 \\ (k-k')(p+q+r)-k'a_3-pa_3 \end{cases}$$

(2) reduces to $\alpha_2(x_2)\alpha_3(x_3)\delta_{k,k'}$

Subcase **(iii)**

The two errors are in the third and fourth registers. Then

$$(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_2, x_3+a_3, x_4+a_4, x_5)$$

So $k = x_1 - x_4 - x_5 - a_4$

$$r = \begin{cases} x_2 - x_4 - a_4 \\ x_3 - x_5 + a_3 \end{cases}$$

$$\text{Hence} \quad k(p+q+r)+pr = \begin{cases} (k-a_4)(p+q+r+a_3)+p(r+a_3) \\ (k-a_4)(p+q+r+a_3)+p(r-a_4) \\ (k-a_4)(p+q+r-a_4)+p(r+a_3) \\ (k-a_4)(p+q+r-a_4)+p(r+a_3) \end{cases}$$

$$P - P_e = \begin{cases} (k-k')(p+q+r) - k'a_3 + a_4(p+q+r+a_3) - pa_3 \\ (k-k')(p+q+r) - k'a_3 + a_4(p+q+r+a_3) + pa_4 \\ (k-k')(p+q+r) + k'a_4 + a_4(p+q+r-a_4) - pa_3 \\ (k-k')(p+q+r) + k'a_4 + a_4(p+q+r-a_4) - pa_3 \end{cases}$$

This gives $\alpha_3(x_3)\alpha_4(x_4)\delta_{k,k'}$ in (2).

Subcase **(iv)**

The two errors are in the fourth and fifth registers. Then

$$(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_2, x_3, x_4+a_4, x_5+a_5)$$

So $k = x_1 - x_4 - x_5 - a_4 - a_5$

$$r = \begin{cases} x_2 - x_4 - a_4 \\ x_3 - x_5 - a_5 \end{cases}$$

$$\text{Hence } k(p+q+r) + pr = \begin{cases} (k-a_4-a_5)(p+q+r-a_4) + p(r-a_4) \\ (k-a_4-a_5)(p+q+r-a_4) + p(r-a_5) \\ (k-a_4-a_5)(p+q+r-a_5) + p(r-a_4) \\ (k-a_4-a_5)(p+q+r-a_5) + p(r-a_5) \end{cases}$$

$$P - P_e = \begin{cases} (k-k')(p+q+r) + k'a_4) + (a_4+a_5)(p+q+r-a_4) + pa_4 \\ (k-k')(p+q+r) + k'a_4 + (a_4+a_5)(p+q+r-a_4) + pa_5 \\ (k-k')(p+q+r) + k'a_5 + (a_4+a_5)(p+q+r-a_5) + pa_4 \\ (k-k')(p+q+r) + k'a_5 + (a_4+a_5)(p+q+r-a_5) + pa_5 \end{cases}$$

Substituting gives $\alpha_4(x_4)\alpha_5(x_5)\delta_{k,k'}$ in (2).

Subcase **(v)**

The two errors are in the first and fifth registers. Then

$$(x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1+a_1, x_2, x_3, x_4, x_5+a_5)$$

So $k = x_1 - x_4 - x_5 + a_1 - a_5$

$$r = \begin{cases} x_2 - x_4 \\ x_3 - x_5 - a_5 \end{cases}$$

$$\text{Hence} \quad k(p+q+r) + pr = \begin{cases} (k+a_1-a_5)(p+q+r) + pr \\ (k+a_1-a_5)(p+q+r) + p(r-a_5) \\ (k+a_1-a_5)(p+q+r-a_5) + pr \\ (k+a_1-a_5)(p+q+r-a_5) + p(r-a_5) \end{cases}$$

$$\text{and} \qquad P - P_e = \begin{cases} (k-k')(p+q+r) - (a_1-a_5)(p+q+r) \\ (k-k')(p+q+r) - (a_1-a_5)(p+q+r) + pa_5 \\ (k-k')(p+q+r) + k'a_5 - (a_1-a_5)(p+q+r-a_5) \\ (k-k')(p+q+r) + k'a_5 - (a_1-a_5)(p+q+r-a_5) + pa_5 \end{cases}$$

which again gives $\alpha_1(x_1)\alpha_5(x_5)\delta_{k,k'}$ in (2).

The following theorem shows that five quantum register code is optimal.

Theorem :

The five quantum register code is optimal i.e., at least five register encoding is needed for error correction.

Proof:

We prove that the five quantum code is optimal or equivalently

a four quantum register code is insufficient for single error correction. If possible suppose the encoding is

$$|k\rangle \rightarrow |k_L\rangle = \sum_{p,q,r=0}^{N-1} \alpha_{pqrs} |p,q,r,s\rangle \quad \text{and}$$

$$|k'\rangle \rightarrow |k'_L\rangle = \sum_{p,q,r=0}^{N-1} \beta_{pqrs} |p,q,r,s\rangle |$$

Define $\rho^{k}_{p'q'pq} = \sum_{r,s} \overline{\alpha_{p'q'rs}} \alpha_{pqrs}$ and $\rho^{k'}_{p'q'pq} = \sum_{r,s} \overline{\beta_{p'q'rs}} \beta_{pqrs}$ (4)

Now we use the two conditions of error correction by Knill-Laflamme in [1.2.18] under the following assumptions.

Case **(i)**

Assume the two errors occur in the last two registers and using condition (i) in [1.2.18] we get

$$\sum_{p,q} \overline{\beta_{pq(r+l')(s+m)}} \alpha_{pqrs} = 0 \quad \text{Similarly} \sum_{p,q} \overline{\alpha_{pq(r+l')(s+m)}} \beta_{pqrs} = 0 \qquad (5)$$

Now assume the two errors occurred in first two registers and applying condition (ii) in [1.2.18] we get

$$\sum_{r,s} \beta \overline{_{(p+l')(q+m')rs}} \beta_{pqrs} = \sum_{r,s} \overline{\alpha_{(p+l')(q+m')rs}} \alpha_{pqrs} \qquad (6)$$

Now we consider the following,

$$[\sum_{r,s}\alpha_{(p+l')(q+m')(r+l)(s+m)}\sum_{p,q}\overline{\alpha_{pq(r+l)(s+m)}}\beta_{pqrs}\overline{\beta_{(p+l')(q+m')rs}}\ ] \qquad (7)$$

In terms of (4) expression (7) is $\rho_k\rho_{k'}$. Then $\rho_k\rho_{k'}=0$ since the middle part is zero by (5)

On the other hand by putting $\beta=\alpha$ in (7) gives $\rho_k\rho_{k'}=1$, which is a contradiction.

3.4 ***Theorem :***

Consider H as in Theorem [3.2]. Let C be the subspace of $H^{\otimes 9}$ consisting of all vectors of the form $|$ pppqqqrrr$\rangle$ such that p, q, r varies over 0,1,..., N-1. Let $A = Z_N$ and $\hat{A}$ be it's group of characters. For $|\mathbf{x}\rangle = |$ pppqqqrrr$\rangle$, set $\psi_k(\mathbf{x}) = \omega_N^{k(p+q+r)}$ and $|\psi_k\rangle = \sum_{x\in A^3}\psi_k(\mathbf{x})|\mathbf{x}\rangle$ for $k = 0,1,..,N-1$. Then this collection is an orthonormal set. Then for all (a,α) in $A^9\times\hat{A}^9$ with $w(a,\alpha)\le 2$, C is a single error correcting quantum code if it satisfies,

(i) $\sum_{x\in A^n}\alpha(\mathbf{x})\,\psi_k\,\overline{(\mathbf{x}+\mathbf{a})\,\psi_{k'}}(\mathbf{x})=0$ if $k\neq k'$

(ii) $\sum_{x\in A^n}\alpha(\mathbf{x})\,\psi_k\,\overline{(\mathbf{x}+\mathbf{a})\,\psi_k}(\mathbf{x})$ is independent of $k=0,1,2,\ldots,N-1$

with $\alpha(\mathbf{x}) = \prod_{i=1}^{n}\alpha_i(x_i)$.

Proof :

The nine quantum register code in Higher Spin system was developed by Chau [Ch1]. He gave an encoding that can correct error in atmost one register as the following.

$$|k\rangle \rightarrow |k_L\rangle = \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{(p+q+r)k} \, |pppqqqrrr\rangle |$$

for all k = 0,1,...., N-1 and ω_N is the N-th root of unity.

We verify that this indeed satisfy the criterion as in [1.2.18] . If $(x_1,x_2, \ldots,x_9)$ represents (pppqqqrrr) then their association is

$$x_1 = x_2 = x_3 = p \, , \; x_4 = x_5 = x_6 = q \, , \; x_7 = x_8 = x_9 = r.$$

Since the code is single error correcting, the weight $w(\mathbf{a},\alpha) \leq 2$.

First we consider the case that $w(\mathbf{a},\alpha) = 1$

Subcase **(i)**

Suppose the error occurs in the first register. Then

$(x_1, x_2, \ldots, x_9) \rightarrow (x_1+a_1, x_2, \ldots, x_9)$.

So,

$$x_1 = \begin{cases} p \\ p - a_1 \end{cases} \quad x_2 = x_3 = p \, , \; x_4 = x_5 = x_6 = q \, , \; x_7 = x_8 = x_9 = r.$$

$$\text{Then } P - P_e = \begin{cases} k(p+q+r) - k'(p+q+r) \\ k(p+q+r) - k'(p-a_1+q+r) \end{cases}$$

$$= \begin{cases} (k-k')(p+q+r) \\ (k-k')(p+q+r) + k'a_1 \end{cases}$$

Applying the criterion we get the sum to be $\delta_{k,k'}\alpha_1(x_1)$

Cases where the errors occur in the second and third registers follow similarly..

***Subcase* (ii)**

If the error occurs in the fourth register. Then

$(x_1, x_2, x_3, x_4, \ldots, x_9) \rightarrow (x_1, x_2, x_3, x_4+a_4, \ldots, x_9)$.

So $x_1 = x_2 = x_3 = p$, $x_4 = \begin{cases} q \\ q-a_4 \end{cases}$, $x_5 = x_6 = q$, $x_7 = x_8 = x_9 = r$.

$$\text{Then } P - P_e = \begin{cases} k(p+q+r) - k'(p+q+r) \\ k(p+q+r) - k'(p+q-a_4+r) \end{cases}$$

$$= \begin{cases} (k-k')(p+q+r) \\ (k-k')(p+q+r) + k'a_4 \end{cases}$$

Applying the criterion we get $\delta_{k,k'}\alpha_4(x_4)$ for the sum.

All the subcases of one register error follow similarly.

Case(ii)

Here we consider the case that $w(\mathbf{a},\alpha) = 2$

Subcase **(i)**

Error occur in the first and second registers. Then

$$(x_1, x_2, \ldots, x_9) \rightarrow (x_1+a_1, x_2+a_2, \ldots, x_9).$$

So $x_1 = \begin{cases} p \\ p-a_1 \end{cases}, x_2 = \begin{cases} p \\ p-a_2 \end{cases}, x_3 = p, x_4 = x_5 = x_6 = q, x_7 = x_8 = x_9 = r.$

Then $$P - P_e = \begin{cases} k(p+q+r) - k'(p+q+r) \\ k(p+q+r) - k'(p-a_2+q+r) \\ k(p-a_1+q+r) - k'(p+q+r) \\ k(p-a_1+q+r) - k'(p-a_2+q+r) \end{cases}$$

$$= \begin{cases} (k-k')(p+q+r) \\ (k-k')(p+q+r) + k'a_2 \\ (k-k')(p+q+r) - ka_1 \\ (k-k')(p+q+r) - ka_1 + k'a_2 \end{cases}$$

Applying the criterion we get $\delta_{k,k'}\alpha_1(x_1)\alpha_2(x_2)$ for the sum.

Subcase **(ii)**

Error occur in the third and fourth registers. Then

$$(x_1,., x_3, x_4, \ldots, x_9) \rightarrow (x_1,., x_3+a_3, x_4+a_4, \ldots, x_9).$$

So $x_1 = p, x_2 = p, x_3 = \begin{cases} p \\ p-a_3 \end{cases}, x_4 = \begin{cases} q \\ q-a_3 \end{cases}, x_5 = x_6 = q, x_7 = x_8 = x_9 = r.$

$$\text{Then} \quad P - P_e = \begin{cases} k(p+q+r) - k'(p+q+r) \\ k(p+q-a_4+r) - k'(p+q-a_4+r) \\ k(p-a_3+q+r) - k'(p-a_3+q+r) \\ k(p-a_3+q-a_4+r) - k'(p-a_3+q-a_4+r) \end{cases}$$

$$= \begin{cases} (k-k')(p+q+r) \\ (k-k')(p+q+r) - ka_4 + k'a_4 \\ (k-k')(p+q+r) - ka_3 + k'a_3 \\ (k-k')(p+q+r) - k(a_3+a_4) + k'(a_3+a_4) \end{cases}$$

Applying the criterion we get $\delta_{k,k'}\alpha_3(x_3)\,\alpha_4(x_4)$ for the sum.

All the remaining subcases are either of these two types.

3.3 ***Theorem :***

Consider **H** as in Theorem [3.2]. A subspace C of $\mathbf{H}^{\otimes 7}$ with the orthonormal basis $|\psi_k\rangle = \sum_{x \in A^7} \psi_k(\mathbf{x})|\mathbf{x}\rangle$ where $\psi_k(\mathbf{x}) = \omega_N^{kN(p+q+r)}$ and $x = |p+q+r+k,\ p+r+k,\ q+r+k,\ p+q+k,\ q+k,\ p+k\rangle$ is a single error correcting quantum code.

***Proof*:**

In this construction of the code we use the rule that

$$\sum_{m=0}^{N-1} \omega_N^{mk} = \begin{cases} N & \text{if } k = 0 \bmod N \\ \\ \\ 0 & \text{if } k = 1,2,\ldots,N\text{-}1 \bmod N \end{cases}$$

where ω_N is the primitive N th root of unity.

We denote the N mutually orthogonal eigenstates in each quantum register by $|0\rangle, |1\rangle, \ldots\ldots, |N\text{-}1\rangle$. We define the following encoding scheme which can correct at most one error in the quantum registers as

$$|k\rangle \rightarrow |k_L\rangle = \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{(p+q+r)kN} \; |p+q+r+k\rangle \, |p+r+k\rangle \, |q+r+k\rangle \, |p+q+k\rangle \, |q+k\rangle \, |p+k\rangle$$

$$= \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{(p+q+r)kN} \; |p+q+r+k,\ p+r+k,\ q+r+k,\ p+q+k,\ q+k,\ p+k\rangle$$

for $k = 0,1,\ldots,N\text{-}1$ and addition in the state kets and in the sum are modulo N.

We prove that this is an encoding by applying the criterion. Suppose $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ be any 7-tuple that represents the (p+q+r+k, p+q+k, q+r+k, p+r+k, p+k, q+k,r+k)

Then

$$p = \begin{cases} x_4 - x_7 \\ x_2 - x_6 \\ x_1 - x_3 \end{cases}, \quad q = \begin{cases} x_3 - x_7 \\ x_2 - x_5 \\ x_1 - x_4 \end{cases}, \quad r = \begin{cases} x_4 - x_5 \\ x_3 - x_6 \\ x_1 - x_2 \end{cases}$$

Then P = (p+q+r)kN can take the above values.

Since the code is single error correcting the weight $w(\mathbf{a},\alpha) \leq 2$

Case (i)

First we consider the case that $w(\mathbf{a},\alpha) = 1$

Suppose the error occurs in the first register

Then $(x_1, x_2,\ldots,x_7) \rightarrow (x_1+a_1,x_2,\ldots,x_7)$. Choosing four choices from among the possible eight choices of P- P_e, then

$$\text{P- } P_e = \begin{cases} kN[(k-k')(p+q+r)] \\ kN[(k-k')(p+q+r)-a_1k'] \\ kN[(k-k')(p+q+r)-a_1k'-a_2k'] \\ kN[(k-k')(p+q+r)-a_1k'-a_2k'-a_3k'] \end{cases}$$

On applying the criterion we get $\alpha_1(x_1)\delta_{k,k'}$ for the sum.

Similarly we can deal with the remaining four choices.

All the single error register cases follow similarly.

Case (ii)

We consider the case that $w(\mathbf{a},\alpha) = 2$

Suppose the error occur in the first and second registers

Then $(x_1, x_2, \ldots,x_7) \rightarrow (x_1+a_1, x_2+a_2, \ldots,x_7)$

There are a large number of choices for P- P_e, for

$$P - P_e = \begin{cases} N(k-k')(p+q+r) \\ N(k-k')(p+q+r) - k'a_1 \\ N(k-k')(p+q+r) - k'a_1 - k'a_2 \\ \textit{etc.} \end{cases}$$

On applying the criterion we get $\alpha_1(x_1)\,\alpha_2(x_2)\delta_{k,k'}$ for the sum.

Two Nice Applications of the Knill-Laflamme Criterion

M.P. Sivaramakrishnan "On the study of error correcting quantum codes and genaralized entropic uncertainty relation" Thesis. Department of Mathematics , University of Calicut, 2002

Chapter 4 Two Nice Applications of the Knill-Laflamme Criterion

In the first section we look for the recovery of convex combination of states but in the worst case the extreme points, namely, the pure states are absent in the set. In the second section what is recovered after transmission is not the input state but a 'representation' of the state.

4.1 Recovery of Convex States

We seek the recovery of convex states after being transmitted through a noisy medium.

By a convex set D of states we mean that if ρ_1, ρ_2 are in D then $a_1\rho_1 + a_2\rho_2$ also is in D , if $a_1, a_2 \geq 0$ and $a_1 + a_2 = 1$. Now if ρ is any state in this convex set D of states and if $\rho = a_1\rho_1 + a_2\rho_2$, then by error correction procedure,

$$\sum_j L_j \rho L_j^\dagger = \sum_j L_j (a_1\rho_1 + a_2) \rho L_j^\dagger$$

$$= a_1 \sum_j L_j \rho_1 L_j^\dagger + a_2 \sum_j L_j \rho_2 L_j^\dagger$$

$$= a_1\rho_1 + a_2\rho_2 \quad \text{if} \quad \sum_j L_j^\dagger L_j = I$$

where $L_j = R_r A_a$, with A_a's as the error operators and R_r's as the recovery operators that satisfy

$$\sum_r R_r^{\dagger} R_r = I \quad \text{and} \quad \sum_a A_a^{\dagger} A_a = I$$

By spectral theorem [1.2.4] every state ρ can be expressed as $\rho = \sum_j p_j |u_j\rangle\langle u_j|$ where $p_j > 0$ and $\sum_j p_j = 1$ and u_j , j=1,2,...is an orthonormal set of eigenvectors of ρ such that $\rho u_j = p_j u_j$ for each j. This will imply that the extreme points [Co] of the convex set are precisely the one dimensional projections in **H**. Any one dimensional projection is a pure state.

Thus a pure state ρ always has the form $\rho = |u\rangle\langle u|$. But in the case of a state which is not a pure state i.e., for a mixed state [1.2.4] such a representation is not possible.

We have to consider both the cases.

Case (i)

The extreme points of the convex set are pure states. When the input states are pure states , they can be reconstructed by the original form of Knill-Laflamme criterion [KL].

Case (ii)

The extreme points are mixed states (i.e., not pure states) but they are diagonal states. This could happen if the set of convex states has no pure states in it.

We obtain a theorem to this effect in the case of diagonal states.

***Remark*:**

The diagonal states or diagonal density matrices are pure states or mixed states whose matrix representations are as diagonal matrices.

We prove the following.

4.1.1 *Theorem*:

Let $D_1, D_2,.....,D_d$ be a collection of orthogonal density matrices on the Hilbert space **H**. Fix a $|\psi\rangle$ in **H**. Let C be the span $D_1|\psi\rangle$, $D_2|\psi\rangle,.....,D_d|\psi\rangle$. Then C is an error correcting quantum code if for the error operators A_a , A_b in the errorspace **A** of **H** , the following conditions are satisfied:

(i) $\langle\psi| D_i^{\dagger}A_a^{\dagger}A_bD_j |\psi\rangle = 0$ and

(ii) $\langle\psi|D_i^{\dagger}A_a^{\dagger}A_bD_i |\psi\rangle = \sum_r$ t(r,a)t(r,b), a constant independent of density matrices D_i

***Proof*:**

We first prove the theorem for two dimensional diagonal states.

Let $E_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Choose a_1, a_2, b_1, b_2 such that $a_1^2+a_2^2=1$ and $b_1^2+b_2^2=1$.

Consider the sum

$$\sum_{r,a} \langle\psi | [(b_1 E_1 +b_2 E_2) R_r A_a (a_1E_1 +a_2 E_2)]$$

$$[(b_1 E_1 +b_2 E_2) R_r A_a (a_1E_1 +a_2 E_2)]^\dagger | \psi\rangle$$

$$= \sum_{r,a} \langle\psi | [(b_1 E_1 +b_2 E_2) R_r A_a (a_1 E_1 + a_2 E_2)]$$

$$[(a_1E_1 + a_2 E_2) A_a{}^\dagger R_r{}^\dagger (b_1 E_1 + b_2E_2)] | \psi\rangle$$

$$= \langle\psi | [(b_1 E_1 +b_2 E_2)[\sum_{r,a} R_r A_a (a_1 E_1 + a_2 E_2)]$$

$$[(a_1E_1 + a_2 E_2) A_a{}^\dagger R_r{}^\dagger](b_1 E_1 + b_2E_2)] | \psi\rangle$$

$$= \langle\psi | [(b_1 E_1 +b_2 E_2)[(a_1 E_1 +a_2 E_2)(a_1E_1 + a_2 E_2)] (b_1 E_1 + b_2E_2) | \psi\rangle$$

(Since by assumption diagonal states are recovered)

Now if $(a_1^2E_1+a_2^2E_2)$ is orthogonal to $(b_1^2E_1+b_2^2E_2)$,

i.e., $(a_1^2E_1+a_2^2E_2)(b_1^2E_1+b_2^2E_2) = \mathbf{0}$, the zero matrix, then

$\sum_{r,a} [(b_1E_1+b_2E_2)R_rA_a(a_1E_1+a_2E_2)] \ |\psi\rangle = \mathbf{0}$ which means

$(b_1E_1+ b_2E_2)[R_rA_a(a_1E_1+ a_2E_2)] \ |\psi\rangle = \mathbf{0}$

Hence

$$R_r A_a (a_1 E_1 + a_2 E_2) \ |\psi\rangle = t(r,a)(a_1 E_1 + a_2 E_2) |\psi\rangle \qquad (1)$$

where $t(r,a) \in \mathbf{C}$

Now,

$$\langle\psi | D_i^\dagger A_a^\dagger A_b D_j | \psi\rangle$$

$$= \sum_r \langle\psi | (a_i E_1 + a_i E_2) A_a^\dagger R_r^\dagger R_r A_b(a_jE_1+b_jE_2) |\psi\rangle$$

$$= \sum_r [R_rA_a(a_1E_1+a_2E_2) \ |\psi\rangle]^\dagger R_r A_b(a_jE_1+b_jE_2) \ |\psi\rangle$$

$$= \sum_r \overline{t(r,a)} \ t(r,b) \langle\psi | D_i^\dagger D_j \ |\psi\rangle \quad , \text{ by (1)}$$

$$= \begin{cases} 0 & , \text{if } i \neq j \\ \overline{t(r,a)} \ t(r,b) & , \text{if } i = j \text{ where} \\ t(r,a), \ t(r,b) & \text{are in } \mathbf{C} \end{cases}$$

In general for n dimensional diagonal states we can simply extend the above result as ,

$$E_1 = \begin{bmatrix} 1 & 0 & . & . & \\ 0 & 0 & & & \\ . & & . & & \\ . & & & . & \\ & & & & 0 \end{bmatrix}, E_2 = \begin{bmatrix} 0 & 0 & . & . & \\ 0 & 1 & & & \\ . & & . & & \\ . & & & . & \\ & & & & 0 \end{bmatrix}, \ldots\ldots\ldots, E_n = \begin{bmatrix} 0 & 0 & . & . & \\ 0 & 0 & & & \\ . & & . & & \\ . & & & . & \\ & & & & 1 \end{bmatrix}$$

Now consider the sum

$$\sum_{r,a} \langle\psi | [(b_1 E_1 + b_2 E_2 + \ldots\ldots + b_n E_n) R_r A_a (a_1 E_1 + a_2 E_2 + \ldots\ldots + a_n E_n)]$$

$$[(a_1 E_1 + a_2 E_2 + \ldots\ldots + a_n E_n) A_a^{\dagger} R_r^{\dagger} (b_1 E_1 + b_2 E_2 + \ldots\ldots + b_n E_n)]^{\dagger} | \psi\rangle$$

On simplification this will give,

$$R_r A_a (a_1 E_1 + a_2 E_2 + \ldots\ldots + a_n E_n) | \psi\rangle =$$

$$t(r,a) (a_1 E_1 + a_2 E_2 + \ldots\ldots + a_n E_n) | \psi\rangle , \quad \text{where } t(r,a) \in \mathbf{C}$$

***Remark*:**

If ρ is any nondiagonal state then we may diagonalise it as $\rho = UDU^{\dagger}$ (This is possible since ρ is hermitian and every hermitian

matrix is unitarily diagonalizable) where U is a unitary matrix. So we will deduce the same condition as we got above.

Then , $D = U^{\dagger}\rho U$

If we consider arbitrary mixed states ρ_1, ρ_2,....., ρ_{d-1} as an orthonormal basis for C. Suppose the diagonalising unitary operators are $U_1, U_2, \ldots\ldots, U_{d-1}$ respectively. Then suppose,

$D_1 = U_1\rho_1 U_1^{\dagger}$, $D_2 = U_2\rho_2 U_2^{\dagger}$,....., $D_{d-1} = U_{d-1}\rho_{d-1}U_{d-1}^{\dagger}$

Then the criterion becomes,

$U_i^{\dagger}\rho_i U_i A_a^{\dagger}A_b D U_j\rho_j U_j^{\dagger}$

$$= \begin{cases} 0 & , \text{if } i \neq j \\ \overline{t(r,a)}\, t(r,b) & , \text{if } i = j \text{ where} \\ & t(r,a),\ t(r,b) \text{ are in } \mathbf{C} \end{cases}$$

4.2 Recovery as a Representation

We look for a criterion in which if $\rho \otimes I$, ie ., a representation of the state ρ , is recovered after the input ρ is transmitted through a noisy medium. Since $\rho \otimes I$ can be thought of as ρ itself, for all practical

purposes, we will be recovering ρ itself.

In this case we define the error correcting quantum code as follows:

4.2.1 ***Definition*:**

A subspace C of the Hilbert space **H** is called an error correcting quantum code , if there exists recovery operators R_1, R_2,...such that for any ρ with support in C and any collection of error operators A_1, A_2,.... with $\sum_a A_a^\dagger A_a = I$, we have $\sum_{r,a} R_r A_a \rho A_a^\dagger R_r^\dagger = \rho \otimes I$ (here the recovery operators R_r satisfy $\sum_r R_r^\dagger R_r = I$)

***Remark*:**

Here the action of R_rA_a and $A_a^\dagger R_r^\dagger$ are considered as $R_rA_a(u\otimes v) = R_rA_au$ and $A_a^\dagger R_r^\dagger u = A_a^\dagger R_r^\dagger(u\otimes 0)$. With this interpretation we have $R_rA_a : \mathbf{H} \otimes \mathbf{K} \rightarrow \mathbf{H}$ and $A_a^\dagger R_r^\dagger : \mathbf{H} \rightarrow \mathbf{H} \otimes \mathbf{K}$,where **K** is a Hilbert space.

Since ρ is a state, ρ is positive semidefinite so also is $\rho \otimes I$ and $Tr(\rho \otimes I) = Tr\rho.TrI = 1$. Hence $\rho \otimes I$ is also a state. Thus what we prove is when ρ in **H** is transmitted, $\rho \otimes I$ can be recovered in $\mathbf{H} \otimes \mathbf{K}$, with suitable assumptions.

More specifically what we have is the following theorem.

4.2.2 ***Theorem:***

Let C be a subspace of **H** .Suppose in an error correction procedure an input state ρ in a Hilbert Space **H**, with support in C , is recovered as $\rho \otimes I$ of a Hilbert space $\mathbf{H} \otimes \mathbf{K}$ after transmitting through a noisy medium.Then C will be an error correcting quantum code if C has an orthonormal basis $|\psi_0\rangle, |\psi_1\rangle, \ldots\ldots, |\psi_{k-1}\rangle$ such that

(i) $\langle\psi_i | A_a^\dagger A_a A_b^\dagger A_b | \psi_j\rangle = 0$, for $i \neq j$

(ii) $\langle\psi_i | A_a^\dagger A_a A_b^\dagger A_b | \psi_i\rangle$ is a constant independent i = 0,1,.....,k-1

and A_a , A_b are error operators corrected by the recovery operators R_1 , R_2 ,....

We require the following results , which are consequences of Stinespring's dilation theorem [Sti].

4.2.3 ***Proposition*** **[Pa1]:**

Let $\mathbf{H}_1$, $\mathbf{H}_2$ be Hilbert spaces.Then an operator $T : B(\mathbf{H}_2) \rightarrow B(\mathbf{H}_1)$ is completely positive if and only if there exist operators $L_j : \mathbf{H}_1 \rightarrow \mathbf{H}_2$, $j = 1,2,\ldots$ such that $\sum_j L_j^\dagger L_j = I$ and $T(X) = \sum_j L_j^\dagger X L_j$ for all

$X \in B(\mathbf{H}_2)$. If dim $\mathbf{H}_j = n_j < \infty$, $j = 1, 2$ then the number of L_j's is $\leq n_1 n_2$.

4.2.4 ***Corollary*** **[Pa1]:**

Let T , $\{L_j\}$ be as in above proposition. Let T' be the map from the states in $\mathbf{H}_1$ into the states in $\mathbf{H}_2$ defined by $Tr\rho T(X) = Tr\, T'(\rho)\, X$ for all $X \in B(\mathbf{H}_2)$ .Then $T'(\rho) = \sum_j L_j \rho L_j^\dagger$

***Remark*:**

From the above two results if X in $B(\mathbf{H}_2)$ is mapped onto $T(X) = \sum_j L_j^\dagger X L_j$ then $\sum_j L_j\, T(X)\, L_j^\dagger$ gives X.

4.2.5 ***Theorem*** **[Ra1]:**

Let A, B be unital C^* algebras and α,β be completely positive maps from A to B such that $\alpha-\beta$ is completely positive. Now if α is a unital *-ho momorphism from A to B then $\beta(X) = \alpha(X)\beta(I) = \beta(I)\alpha(X) \quad \forall\ X \in A$..

For a Hilbert space $\mathbf{H}$, $B(\mathbf{H})$ is a unital C^* algebra.

4.2.6 ***Proposition*:**

Let $\mathbf{H}$,$\mathbf{K}$ be Hilbert spaces.Consider $B(\mathbf{H})$ and $B(\mathbf{H} \otimes \mathbf{K})$. Suppose

π , α_{ra} be completely positive maps from B(**H**) to B(**H** $\otimes$ **K**) given by $\alpha_{ra}(T) = R_r A_a T A_a^{\dagger} R_r^{\dagger}$ and $\pi(T) = T \otimes I$ then $\pi - \alpha_{ra}$ positive and for any state $\rho\alpha_{ra}(\rho) = \rho \otimes E_{ra}$ and if $\rho \otimes I$ is recovered out of ρ then $\sum_{r,a} E_{ra} = I$

***Proof*:**

We make use of the theorem [4.2.5].

We have

$\alpha_{ra}(\rho) = R_r A_a \rho A_a^{\dagger} R_r^{\dagger} \leq \sum_{r,a} R_r A_a \rho A_a^{\dagger} R_r^{\dagger} = \pi(\rho)$ for any state ρ [4.2.1].

Hence $\pi - \alpha_{ra}$ is completely positive and also π is unital.

By [4.2.5] we have $\alpha_{ra}(T) = \pi(T).\ \alpha_{ra}(I)\ \forall\ T \in B(H)$.

In particular we have $\alpha_{ra}(\rho) = \pi(\rho).\ \alpha_{ra}(I)$. Taking $D_{ra} = \alpha_{ra}(I)$,

We have $\alpha_{ra}(\rho) = \pi(\rho).D_{ra} = (\rho \otimes I)\ D_{ra}$.

Again by [4.2.5] $D_{ra}(\rho \otimes I) = (\rho \otimes I)\ D_{ra}$

Now we have the following result,

4.2.7 ***Property*** **[Ra2]:**

If a pn×pn matrix D commutes with all matrices of the form $I_p \otimes X$, then D

is of the form $A \otimes I_n$. So, $\alpha_{ra}(\rho) = (\rho \otimes I)\, D_{ra} = (\rho \otimes I)(I \otimes E_{ra})$ (since anything that commutes with $\rho \otimes I$ has the form $I \otimes E_{ra}$ by above property).

Hence $\alpha_{ra}(\rho) = \rho \otimes E_{ra} = \rho \otimes E_{ra}$

Thus $\alpha_{ra}(\rho) = R_r A_a \rho A_a^{\dagger} R_r^{\dagger}$

Now if $\rho \otimes I$ is recovered from ρ,

$$\rho \otimes I = \sum_{r,a} R_r A_a \rho A a^{\dagger} R_r^{\dagger} = \sum_{r,a} \alpha_{ra}(\rho)$$

$$= \sum_{r,a} \rho \otimes E_{ra} = \rho \otimes (\sum_{r,a} E_{ra})$$

This implies

$$\sum_{r,a} E_{ra} = I$$

Proof of the main theorem:

Since ρ and $\rho \otimes I$ can be identified, by Knill-Laflamme theorem, C has an orthonormal basis $|\psi_0\rangle, |\psi_1\rangle, \ldots\ldots, |\psi_{k-1}\rangle$.

Suppose ρ is a pure state where $\rho = |\varphi_0\rangle\langle\varphi_0|$ with $|\varphi_0\rangle$ in H_0.

For any arbitrary state $|\psi\rangle$ consider the sum,

$$\sum_{r,a} |\langle\psi| A_a^\dagger R_r^\dagger R_r A_a \varphi_0\rangle|^2 = \sum_{r,a} \langle\psi| A_a^\dagger R_r^\dagger R_r A_a |\varphi_0\rangle\langle\psi| A_a^\dagger R_r^\dagger R_r A_a |\varphi_0\rangle^\dagger$$

$$= \sum_{r,a} \langle\psi| A_a^\dagger R_r^\dagger R_r A_a |\varphi_0\rangle\langle\varphi_0| A_a^\dagger R_r^\dagger R_r A_a |\psi\rangle$$

$$= \sum_{r,a} \langle\psi| A_a^\dagger R_r^\dagger R_r A_a \rho A_a^\dagger R_r^\dagger R_r A_a |\psi\rangle$$

$$= \sum_{r,a} \langle\psi| A_a^\dagger R_r^\dagger (\rho\otimes E_{ra}) R_r A_a |\psi\rangle \quad , \text{ by [4.2.6]}$$

$$= \langle\psi| \sum_{r,a} A_a^\dagger R_r^\dagger (\rho\otimes E_{ra}) R_r A_a |\psi\rangle$$

$$= \langle\psi|\rho|\psi\rangle \quad , \text{ by [4.2.4]}$$

$$= \langle\psi|\varphi_0\rangle\langle\varphi_0|\psi\rangle$$

$$= |\langle\psi|\varphi_0\rangle|^2$$

Now if $|\psi\rangle$ is orthogonal to $|\varphi_0\rangle$ then ,

$$A_a^\dagger R_r^\dagger R_r A_a |\varphi_0\rangle = t(r,a)|\varphi_0\rangle \qquad \text{where} \quad t(r,a)\in \mathbf{C}$$

By assumption If $\rho \otimes I$ is recovered for the input ρ and hence

$$\rho \otimes I = \sum_{r,a} R_r A_a \rho A_a^\dagger R_r^\dagger$$

Then by Proposition [4.2.4],

$$\sum_{r,a} A_a^\dagger R_r^\dagger (\rho \otimes I) R_r A_a = \rho$$

Thus,

$$\langle \psi_i | A_a^\dagger A_a A_b^\dagger A_b | \psi_j \rangle = \sum_r \langle \psi_i | A_a^\dagger R_r^\dagger R_r A_a A_b^\dagger R_r^\dagger R_r A_b | \psi_j \rangle$$

$$= \sum_r \langle \psi_i | A_a^\dagger R_r^\dagger R_r A_a A_b^\dagger R_r^\dagger R_r A_b | \psi_j \rangle$$

$$= \sum_r A_b^\dagger R_r^\dagger R_r A_b | \psi_j \rangle \overline{A_a^\dagger R_r^\dagger R_r A_a | \psi_i \rangle}$$

$$= \sum_r \overline{t(r,a)} t(r,b) \langle \psi_i | \psi_j \rangle$$

$$= \begin{cases} 0 \text{ , if } i \neq j \\ \\ \text{a constant(independent of i,j) , if } i = j \end{cases}$$

A More generalized Entropic Uncertainty Relation

M.P. Sivaramakrishnan "On the study of error correcting quantum codes and genaralized entropic uncertainty relation" Thesis. Department of Mathematics , University of Calicut, 2002

Chapter 5 A More generalized Entropic Uncertainty Relation

Massen and Uffink [MU] have proved a conjecture of Kraus [Kr] by providing a class of entropic uncertainty relations for a pair of observables that do not have any common eigenvector. In particular it is proved under the assumption that eigenvalues have no degeneracy. We improve this result to the case that the observable have degeneracy.

Let A and B be two hermition operators representing two observable in an N dimensional Hilbert space and let $|a_j\rangle$ and $|b_j\rangle$ be respectively the complete sets of normalized eigen vectors. For any quantum state ψ , if

$$P = (p_1,p_2,,\ldots,p_N) \quad \text{and} \quad Q = (q_1,q_2,\ldots\ldots,q_N)$$

are the two probability distributions , then

$$p_j = |\langle a_j | \psi \rangle|^2 \qquad \text{and} \qquad q_j = |\langle b_j | \psi \rangle|^2 \tag{1}$$

where both cannot be arbitrarily peaked.

The uncertainty principle is expressed by the Robertson relation [Ro] :

$$\Delta_\psi A \; \Delta_\psi B \geq \tfrac{1}{2} |\langle [A, B] \rangle_\psi| \tag{2}$$

where $\Delta_\psi A$ and $\Delta_\psi B$ are the standard deviations of the distributions in

(1) and $[A,B] = AB - BA$, the commutator of the observables. The right hand side has no fixed lower bound but depends on the state which is a drawback of the relation. To overcome this constraint, 'entropic' uncertainty relations were introduced which depends on Shannon entropy H as a measure of uncertainty.

Shannon entropy is defined for a probability distribution

$$P = (p_1, p_2, \ldots, p_N) \text{ with } p_i \geq 0 \text{ and } \sum_{i=1}^{N} p_i = 1$$

on a set of N possible outcomes as

$$H(P) = -\sum_{j=1}^{N} p_j \ln p_j \qquad (3)$$

Applying this notation to the probability distributions P and Q as given in (1), Kraus [Kr] had conjectured that the uncertainty relation is

$$H(P) + H(Q) \geq -2 \log c \qquad (4)$$

where $c = \max_{j,k} |\langle a_j | b_k \rangle|$

and it was later proved by Massen and Uffink [MU].

The inequality provides nontrivial information on probability distributions if $c < 1$ i.e., when A and B do not share any common eigen vector. Moreover the result was proved under the assumption of

nondegeneracy. By degeneracy it means that all the eigenvalues of the observables are not distinct.

We prove the inequality in the case of degenaracy. i.e., when the eigen values of the observables have multiplicities.

5.1 ***Theorem*** **:**

Let A ,B be two observables such that their eigen values have degeneracy. Suppose $A=(E_1, E_2, \ldots\ldots, E_m)$ and $B = (F_1, F_2, \ldots\ldots, F_n)$ be the spectral projections of A and B respectively. If ψ is any pure state on the Hilbert space , then

$$H(A) + H(B) \geq -2 \log c$$

$$\text{where } c = \max_{i,j} |\langle \psi | E_i F_j | \psi \rangle|$$

To prove this theorem we require the following theorem.

5.2 ***Riesz-Thorin Theorem*** **[RS , Ri]**

Let $T = (t_{ij})$ be an $m \times n$ matrix over **C**. Consider the p-norm on $\mathbf{C}^k$

$$\|x\|_p = \begin{cases} (\sum_{i=1}^{k} |x_i|^p)^{1/p}, 1 \leq p < \infty \\ \max_{1 \leq i \leq k} |x_i|, p = \infty \end{cases}$$

where $x = (x_1, x_2, \ldots, x_k)$

Consider the operator $T : \mathbf{C}^n \to \mathbf{C}^m$ given by

$$(Tx)_i = \sum_{j=1}^{n} t_{ij} x_j \quad , \quad \text{for} \quad i = 1,2,\ldots,m.$$

Define $\|T\|_{p,q} = \sup_{x:\|x\|_p=1} \|Tx\|_q \quad , \frac{1}{p} + \frac{1}{q} = 1$

Now we state the Riesz-Thorin theorem.

Suppose for $i \in \{0,1\}$, $p_i, q_i \in [1,\infty]$,

$$\frac{1}{p_i} + \frac{1}{q_i} = 1, \|T\|_{p_0,q_0} \le m_0, \|T\|_{p_1,q_1} \le m_1$$

Define $p_t, q_t, \quad 0 < t < 1$ by

$$\frac{1}{p_t} = t\frac{1}{p_1} + (1-t)\frac{1}{p_0}, \frac{1}{q_t} = t\frac{1}{q_1} + (1-t)\frac{1}{q_0}$$

Then $\|T\|_{p_t,q_t} \le m_t$ where $m_t = m_0^{1-t} m_1^{t} \quad \forall \quad 0 < t < 1$

Proof of the main theorem **:**

Let E_i and F_j be the projections associated with the eigenvalues λ_i and μ_j of the Hermitian operators A and B respectively where $i = 1, 2\ldots, m$ and $j = 1, 2\ldots, n$. Then by spectral theorem [Co],

$$A = \sum_{i=1}^{m} \lambda_i E_i \quad \text{and} \quad B = \sum_{j=1}^{n} \mu_j F_j$$

Suppose the probability that the observable A assumes the value in the state ψ is p_i, then

$$p_i = Pr_\psi(A=\lambda_i) = \langle\psi|E_i|\psi\rangle \quad (5)$$

Similarly if q_j is the probability with regard to the observable B in the same state ψ, then

$$q_j = Pr_\psi(B=\mu_j) = \langle\psi|F_j|\psi\rangle \quad (6)$$

so that the two probability distributions associated with A and B are

$P = (p_1, p_2, \ldots\ldots, p_m)$ and $Q = (q_1, q_2, \ldots.. q_n)$.

Choose $t_{ij} = Tr[(E_i F_j)|\psi\rangle\langle\psi|]$,

Let T be the linear transformation, $T : \mathbf{C}^n \rightarrow \mathbf{C}^m$

For any $x \in \mathbf{C}^n$ we have

$$\sum_{i=1}^{m}\left|\sum_{j=1}^{n} t_{ij}x_j\right|^2 = \sum_{i=1}^{m}\left|\sum_{j=1}^{n}[Tr(E_iF_j|\psi\rangle\langle\psi|)x_j\right|^2$$

$$= \sum_{i=1}^{m}\left|\sum_{j=1}^{n}\langle\psi|E_iF_j|\psi\rangle|)x_j\right|^2$$

$$= \sum_{i=1}^{m}\langle\psi\left|E_i(\sum_{j=1}^{n}x_jF_j|\psi\rangle)\right|^2$$

$$\leq \left| \sum_{i=1}^{m} \langle \psi | \; E_i \sum_{j=1}^{n} x_j | \psi \rangle \right|^2$$

$$= \; | \langle \psi \left| \sum_{j=1}^{n} x_j \right| \psi \rangle |^2$$

$$\leq \sum_{j=1}^{n} |x_j|^2$$

Thus T satisfies $\|T\|_{2,2} \leq 1$

Now $\|T\|_{1,\infty} \leq c$ where $c = \max_{i,j} |t_{i,j}|$

Using Riesz-Thorin Theorem, and substituting,

$p_0 = q_0 = 2$, $p_1 = q_1 = \infty$, $m_0 = 1$, $m_1 = c$

we get

$$\|T\|_{p_t, q_t} \leq c^t \qquad \text{for } 0 < t < 1 \tag{7}$$

where $p_t = \frac{2}{t+1}$, $q_t = \frac{2}{1-t}$

Define x_j as

$$x_j = \mathrm{Tr}(F_j |\psi\rangle\langle\psi|) = \langle \psi | F_j | \psi \rangle \qquad \text{for } 1 \leq j \leq n$$

Then $(Tx)_i = \sum_{j=1}^{n} t_{ij} x_j$

$$= \sum_{j=1}^{n} Tr(E_i F_j)|\psi\rangle\langle\psi| \; .Tr(F_j|\psi\rangle\langle\psi|)$$

$$= \sum_{j=1}^{n} Tr(E_i F_j|\psi\rangle\langle\psi| \otimes F_j|\psi\rangle\langle\psi|)$$

$$= Tr(E_i|\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|)$$

$$= \langle\psi| E_i |\psi\rangle$$

Applying (7)

$$(\sum_{i=1}^{m}(\langle\psi|E_i|\psi\rangle^{\frac{2}{1-t}})^{\frac{1-t}{2}} \leq c^t \sum_{j=1}^{n}(\langle\psi|F_j|\psi\rangle^{\frac{2}{1+t}})^{\frac{1+t}{2}} \quad \forall\, 0 \leq t \leq 1 \qquad (8)$$

i.e., $(\sum_{i=1}^{m} p_i^{\frac{2}{1-t}})^{\frac{1-t}{2}} (\sum_{j=1}^{n} q_j^{\frac{-t}{1+t}})^{\frac{-(1+t)}{t}} \leq c^t$, by (5) and (6)

Raising both sides to $\frac{2}{t}$,

$$(\sum_{i=1}^{m} p_i^{\frac{2}{1-t}})^{\frac{1-t}{t}} (\sum_{j=1}^{n} q_j^{\frac{-t}{1+t}})^{\frac{-(1+t)}{t}} \leq c^2$$

Taking logarithm, and in the limiting case as $t \to 0$, using L'Hospital's rule we get

$$\sum_{i=1}^{m} p_i \log p_i + \sum_{j=1}^{n} q_j \log q_j \leq 2\log c$$

where $c = \max_{i,j} |\langle\psi| E_i F_j |\psi\rangle|$

5.3 ***Corollary:***

Let A ,B be the two observables and let ψ be a pure state. Then

$H(A) + H(B) \geq -2 \log \max_{i,j} \|E_i F_j\|$

***Proof*:**

From the previous theorem we have

$$C = |\langle \psi | E_i F_j | \psi \rangle$$

$$= |\langle \psi E_i | E_i F_j | F_j \psi \rangle \text{ , since } E_i, F_j \text{ are projections.}$$

$$\leq \|E_i F_j\| \, \|E_i \psi\| \, \|F_j \psi\|$$

$$\leq \|E_i F_j\| .$$

Then the result from the previous theorem gives

$$-\sum_{i=1}^{m} p_i \log p_i \; -\sum_{j=1}^{n} q_j \log q_j \geq -2 \log \max_{i,j} |\langle \psi | E_i F_j | \psi \rangle|$$

$$\geq -2 \log \|E_i F_j\| .$$

i.e., $$H(A) + H(B) \geq -2 \log \max_{i,j} \|E_i F_j\|$$

Remark :

The inequality holds even in the case of a mixed state.

For suppose $W = \sum_k \alpha_k |\psi^{(k)}\rangle\langle\psi^{(k)}|$ with $\alpha_k \geq 0$ and $\sum_k \alpha_k = 1$ where $|\psi_k\rangle$ is a pure state.

Let $$\overline{p_i} = \sum_k \alpha_k \langle\psi^{(k)}|E_i|\psi^{(k)}\rangle = \sum_k \alpha_k p_i^{(k)}$$

$$\overline{q_j} = \sum_k \alpha_k \langle\psi^{(k)}|F_j|\psi^{(k)}\rangle = \sum_k \alpha_k q_j^{(k)}$$

Put $\overline{p} = (\overline{p_1}, \overline{p_2}, \ldots, \overline{p_m})$ and $\overline{q} = (\overline{q_1}, \overline{q_2}, \ldots, \overline{q_n})$

We write $\overline{A}$, $\overline{B}$ for the observable with regard to the mixed state and A , B with regard to the pure state.

Since entropy is a concave function [NC,1.3.5]

$$H(\overline{A})+H(\overline{B}) \geq \sum_k \alpha_k [H(A)+H(B)]$$

$$\geq -2 \ln \max_{i,j} \|E_i F_j\| .$$

BIBLIOGRAPHY

[BS] C.H.Bennett , P.W.Shor : Quantum Information Theory, IEEE transactions on Information Theory. vol **44**,no.6 (October 1996)

[Ch1] H.F.Chau : Correcting Quantum Errors in Higher Spin Systems, Phys.Rev.A **55** ,839 (1997)

[Ch2] H.F.Chau : Five quantum register error correction code for higher spin systems, Phys.Rev A,Vol.**56**.No1(July1997)

[CS] A.R.Calderbank , P.W.Shor : Good quantum error correcting codes exist , Phy. Rev .A .,**54** (1996)

[Da] K.R.Davidson : C^*-Algebras by Example, American Mathematical Society, USA (1996)

[Di] P.A.M Dirac : The Principles of Quantum Mechanics, Oxford University Press, London (1958)

[DS] D.Di Vincenzo,P.W.Shor : Fault-Taulerant error correction with efficient quantum codes, Phy.Rev.Lett.,vol.**77**,no.15(October 1996)

[Hu] Hua Loo Keng : Introduction to Number Theory, Springer

Verlag, Berlin (1982)

[Is] C.J.Isham : QuantumTheory, Mathematical and Structural Foundations, Imperial College Press, London (1995)

[KL] E.Knill and R.Laflamme : A Theory of Quantum error correcting codes, Phy.Rev.A **55** ,900 (1997)

[Kr] K.Kraus : Complementary observable and uncertainty relations, Phys .Rev .D **35**,3070 (1987)

[KR]R.V.Kadison and J.R.Ringrose : Fundamentals of the Theory of Operator algebras –Vol I, Academic Press (1983)

[LMPZ] R.Laflamme ,C.Miquel ,J.P.Paz,W.H.Zurek : A perfect quantum error correcting code , Phy.Rev.Lett.,Vol **7** (1996)

[MS] F.J.Macwilliams and N.J.A.Sloane : The Theory of Error correcting codes, North-Holland,Amsterdam (1977)

[MU] Hans Massen and J.B.M.Uffink : Generalized Entropic Uncertainty Relations, Phys.Rev .**60** ,12 (1988)

[NC] M.A.Nielson and I.L.Chuang : Quantum Computation and Quantum Information, Cambridge University Press, Cambridge (2000)

[Pa1] K.R.Parthasarathy : An introduction to Quantum Stochastic

Calculus (Birkhauser Verlag 1992)

[Pa2] K.R.Parthasarathy : The Mathematics of Error Correcting Quantum Codes,Resonance,Vol. ,6 ,2000 and Vol ,7,2000

[Pa3]K.R.Parthasarathy : Lectures on Quantum Computation and Quantum Error Correcting Codes , Preprint (2001)

[Pi] A.O.Pittenger : An introduction to Quantum Computing Algorithms, Birkhauser (2000)

[Ra1] B.V.Rajarama Bhat : Cocycles of CCR flows, American Mathematical Society, USA (2001)

[Ra2] B.V.Rajarama Bhat : Positive and completely positive maps on matrix algebras, Preprint (1998)

[Ri] M.Riesz : Acta Math .**49** ,465 (1926)

[Ro] H.P.Robertson : Phys.Rev.**34**,163 (1929)

[RS] M.Reed and B.Simon : Methods of Modern Mathematical Physics Vol.2 Academic Press, New York(1975)

[Sc] B.Schumacher : Quantum Coding,Phys.Rev .A, vol.**51** (April 1995)

[Sh] C.E.Shannon : A Mathematical Theory of Communication , Bell System Tech .J., Vol. **27** (1948)

[Sh1] P.W.Shor : Fault-taulerant quantum computation, in Proc .37th Symposium on Foundation of Computing,IEEE Computer Society Press (1996)

[Sh2] P.W.Shor : Scheme for reducing decohrence in quantum computer memory, Phys.Rev.A,vol.**52**.no.4(October 1995)

[Sh3] P.W.Shor : Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer , Siam.J. Comput., Vol.26,No.5(1997)

[St1] A.M.Steane : Error correcting codes in quantum theory, Phys. Rev .Lett. vol .**77** .no.5 (July 1996)

[St2] A.M.Steane : Multiple-particle interference and quantum error correction,Proc.Roy .Soc.London A,vol.**452**(1996)

[St3] A.M.Steane : Quantum computing,Rep.Prog.Phys.**61**(1998)

[Sti] W.Stinespring : Positive functions on C^*-algebras , Proc . Amer . Math Soc .(1955)

[Va] J.H.Vanlint : Introduction to Coding theory , Springer (1998)