Quantum Error Correction

PROFESSOR: RITUMONI SHARMA

STUDENTS:

Akshay Reddy Vellapalem
2020MT10868

Dayal Kumar
2020MT10797

Linear Algebra Notations

Notation	Description
z^*	Complex conjugate of complex number z
$\lvert\psi\rangle$	Vector (*ket*)
$\langle\psi\rvert$	Vector dual to $\lvert\psi\rangle$ (*bra*)
$\langle\phi\vert\psi\rangle$	Inner product between the vectors $\lvert\phi\rangle$ and $\lvert\psi\rangle$
$\lvert\psi\rangle \otimes \lvert\phi\rangle = \lvert\psi\rangle\lvert\phi\rangle = \lvert\psi\phi\rangle$	Tensor product of $\lvert\psi\rangle$ and $\lvert\phi\rangle$
A^*	Complex conjugate of the A matrix
A^T	Transpose of the A matrix
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix. $A^\dagger = (A^T)^*$
$\langle\phi\vert A\vert\psi\rangle$	Inner product between $\lvert\phi\rangle$ and $A\lvert\psi\rangle$

Recap: Qubit

A qubit is a quantum superposition of 2 states i.e., 0 and 1. We can represent a qubit $|\psi\rangle$ as a normal vector in $\mathbb{C}^2$ i.e.,

$$|\psi\rangle = (a_0, a_1) = |\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

$$p(|\psi\rangle \text{ is measured as bit } b) = \ |a_b|^2$$

A state containing n qubits is the tensor product of the individual qubits.
For example: Let

$$|\psi_x\rangle = x_0|0\rangle + x_1|1\rangle \quad \text{and} \quad |\psi_y\rangle = y_0|0\rangle + y_1|1\rangle\,,$$

The state having the qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ is:

$$|\psi_x\rangle \otimes |\psi_y\rangle = x_0y_0|00\rangle + x_0y_1|01\rangle + x_1y_0|10\rangle + x_1y_1|11\rangle$$

Recap: Quantum Gate

A quantum gate over n qubits is defined as a unitary operation:

$$U: \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n} \text{ such that } U^\dagger U = I$$

Any evolution of a closed quantum system is defined by a quantum gate.

Useful Results:

- **Permutation:** Any permutation of n bits can be implemented as a quantum gate in an n qubit system.
- $|+\rangle$ **and** $|-\rangle$**:** Using $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, we can transform $(|0\rangle, |1\rangle)$ to $(|+\rangle, |-\rangle)$:

$$a|0\rangle + b|1\rangle \xrightarrow{H} a|+\rangle + b|-\rangle \xrightarrow{H} a|0\rangle + b|1\rangle$$

Recap: Measurement

Measurement operators: A collection of operators $\{M_m\}_m$ such that $\sum_m M_m^\dagger M_m = I$.

We define a measurement on a quantum state $|\psi\rangle$ as an experiment with possible outcomes$\{m\}_m$.

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

The state of the system after the measurement m is: $\dfrac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$

Recap: Density Operator

Suppose a quantum system is in one of a number of states $|\psi_i\rangle$ with respective probabilities p_i.

$\{p_i, |\psi_i\rangle\}$ is called an $ensemble\ of\ pure\ states$.

The density operator for the system is defined as: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

If a quantum system is in state ρ_j with probability q_j, the resulting density operator is:

$$\rho = \sum_j q_j \rho_j$$

ρ is a density operator $\Leftrightarrow \rho$ is positive and $tr(\rho) = 1$

Recap: Density Operator (Theorem)

For any ensamble $\{p_i, |\psi_i\rangle\}$, define $|\widetilde{\psi_i}\rangle \coloneqq \sqrt{p_i}|\psi_i\rangle$

Theorem

The sets $\{|\widetilde{\psi_i}\rangle\}$ and$\{|\widetilde{\phi_j}\rangle\}$ generate the same density operator if and only if

$$|\widetilde{\psi_i}\rangle = \sum_j u_{ij}|\widetilde{\phi_j}\rangle, \qquad \text{where } U = [u_{ij}] \text{ is a unitary matrix}$$

$\big($Pad whichever set $\{|\widetilde{\psi_i}\rangle\}$ or $\{|\widetilde{\phi_j}\rangle\}$ is smaller with aditional $\mathbf{0}$ vectors$\big)$

$Proof$:

$(\Leftarrow)$

$$\sum_i |\widetilde{\psi_i}\rangle\langle\widetilde{\psi_i}| = \sum_i \left(\sum_j u_{ij}|\widetilde{\phi_j}\rangle\right)\left(\sum_k u_{ik}^*\langle\widetilde{\phi_k}|\right) = \sum_{i,j,k} u_{ij}u_{ik}^*|\widetilde{\phi_j}\rangle\langle\widetilde{\phi_k}|$$

$$= \sum_{j,k}\left(\sum_i u_{ki}^\dagger u_{ij}\right)|\widetilde{\phi_j}\rangle\langle\widetilde{\phi_k}| = \sum_{j,k}\delta_{jk}|\widetilde{\phi_j}\rangle\langle\widetilde{\phi_k}| = \sum_j |\widetilde{\phi_j}\rangle\langle\widetilde{\phi_j}|$$

Recap: Density Operator (Theorem) (cont.)

$Proof$:

(⇒)

$$A = \sum_i |\widetilde{\psi_i}\rangle\langle\widetilde{\psi_i}| = \sum_j |\widetilde{\phi_j}\rangle\langle\widetilde{\phi_j}| \text{ such that } A \text{ is positive with trace 1.}$$

$$\text{By spectral decomposition, } A = \sum_k \lambda_k |k\rangle\langle k| = \sum_k |\tilde{k}\rangle\langle\tilde{k}| \quad \left(|\tilde{k}\rangle = \sqrt{\lambda_k}|k\rangle\right)$$

$$\text{Let } |\omega\rangle \perp span\left(|\tilde{k}\rangle\right)_k \Rightarrow \langle\omega|A|\omega\rangle = 0$$

$$0 = \sum_i \langle\omega|\widetilde{\psi_i}\rangle\langle\widetilde{\psi_i}|\omega\rangle = \sum_i \left|\langle\omega|\widetilde{\psi_i}\rangle\right|^2 \Rightarrow |\omega\rangle \perp span\left(|\widetilde{\psi_i}\rangle\right)_i \Rightarrow span\left(|\tilde{k}\rangle\right)_k = span\left(|\widetilde{\psi_i}\rangle\right)_i$$

$$|\widetilde{\psi_i}\rangle = \sum_k c_{ik}|\tilde{k}\rangle \Rightarrow \sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_i |\widetilde{\psi_i}\rangle\langle\widetilde{\psi_i}| = \sum_{k,l}\left(\sum_i c_{ik}c_{il}^*\right)|\tilde{k}\rangle\langle\tilde{l}| \Rightarrow \sum_i c_{ik}c_{il}^* = \delta_{kl}$$

So, the columns of $C = [c_{ik}]$ form an orthonormal set.

Extend these columns to make an orthonormal basis which, when used as columns, create a unitary matrix $V = [v_{ik}]$

$$\text{So, } |\widetilde{\psi_i}\rangle = \sum_k v_{ik}|\tilde{k}\rangle \text{ and similarly, } |\widetilde{\phi_i}\rangle = \sum_k w_{ik}|\tilde{k}\rangle$$

$$\therefore |\widetilde{\psi_i}\rangle = \sum_j u_{ij}|\widetilde{\phi_j}\rangle, \qquad \text{with } U = VW^\dagger \text{ being unitary}$$

Recap: Postulates

Postulate	In terms of vectors	In terms of density operator
Postulate 1: State Space	System is defined by unit vector in the state space (complex Hilbert Space)	System is defined by density operator in the state space (complex Hilbert Space)
Postulate 2: Evolution	$\lvert\psi\rangle \overset{U}{\rightarrow} \mathrm{U}\lvert\psi\rangle$	$\rho \overset{U}{\rightarrow} U\rho U^{\dagger}$
Postulate 3: Measurement	$\lvert\psi\rangle \overset{m}{\rightarrow} \frac{M_m\lvert\psi\rangle}{\sqrt{\langle\psi\lvert M_m^{\dagger}M_m\rvert\psi\rangle}}$ with $p(m) = \langle\psi\lvert M_m^{\dagger}M_m\rvert\psi\rangle$	$\rho \overset{m}{\rightarrow} \frac{M_m\rho M_m^{\dagger}}{tr(M_m^{\dagger}M_m\rho)}$ with $p(m) = tr(M_m^{\dagger}M_m\rho)$
Postulate 4: Composite Systems	$(\lvert\psi_1\rangle, \lvert\psi_2\rangle, \dots, \lvert\psi_n\rangle) \rightarrow \lvert\psi_1\rangle \otimes \cdots \otimes \lvert\psi_n\rangle$	$(\rho_1, \rho_2, \dots, \rho_n) \rightarrow \rho_1 \otimes \cdots \otimes \rho_n$

Reduced Density Operator

Let ρ^{AB} correspond to the density operator for the composite system of A and B.

Then, the density operator corresponding to the system A is given by:

$$\rho^{A} = tr_B(\rho^{AB})$$

For example, let A and B be 1 qubit systems and AB be the composite system.
Wrt to the basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$, let:

$$\rho^{AB} = \begin{bmatrix} 0.5 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0.5 \end{bmatrix}$$

$$\rho^{A} = tr_B(\rho^{AB}) = \begin{bmatrix} tr\begin{pmatrix} 0.5 & 0 \\ 0 & 0 \end{pmatrix} & tr\begin{pmatrix} 0 & 0.5 \\ 0 & 0 \end{pmatrix} \\ tr\begin{pmatrix} 0 & 0 \\ 0.5 & 0 \end{pmatrix} & tr\begin{pmatrix} 0 & 0 \\ 0 & 0.5 \end{pmatrix} \end{bmatrix} = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix}$$

Quantum Operation

We want to model how a quantum system interacts with its environvent.

$$\rho \equiv \text{Density operator of the system}$$

$$\rho_{env} \equiv \text{Density operator of environment}$$

$$\rho \otimes \rho_{env} \equiv \text{Composite density operator}$$

$$U(\rho \otimes \rho_{env})U^{\dagger} \equiv \text{Density operator after evolution}$$

$$\mathcal{E}(\rho) = tr_{env}\left(U(\rho \otimes \rho_{env})U^{\dagger}\right) \equiv \text{Density operator of system after evolution}$$

$\mathcal{E}$,as defined above, is called a quantum operation.

If U is unitary, $tr\left(\mathcal{E}(\rho)\right) = tr(\rho) = 1$
If, the evolution of the system involves loss of information(such as measurement), then:

1. $tr\left(\mathcal{E}(\rho)\right) < 1$
2. Density operator after interaction is given by: $\rho' = \frac{\mathcal{E}(\rho)}{tr\left(\mathcal{E}(\rho)\right)}$

Quantum Operation (Theorem 1)

Theorem (Operator Sum Representation)

$\forall$ quantum operation $\mathcal{E}$, $\exists$ $\{E_k\}_k$ such that: $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$

Let $\{|e_k\rangle\}_k$ and $\{|v_j\rangle\}_j$ be an orthonormal basis for the environment and system respectively.

WLOG, let $\rho_{env} = |e_0\rangle\langle e_0|$

$$\mathcal{E}(\rho) = tr_{env}\left(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right) = \sum_k \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle$$

$$= \sum_k \langle e_k|U|e_0\rangle\, \rho\, \langle e_0|U^\dagger|e_k\rangle = \sum_k E_k \rho E_k^\dagger$$

$$(E_k = \langle e_k|U|e_0\rangle)$$

$$Note: \langle e_k|\left(\sum_{j,k'} a_{jk'}|v_j\rangle|e_{k'}\rangle\right) = \sum_j a_{jk}|v_j\rangle$$

Quantum Operation (Theorem 2)

Theorem

Let $\mathcal{E} \equiv \{E_1, \dots, E_m\}$ and $\mathcal{F} \equiv \{F_1, \dots, F_n\}$ be 2 quantum operations.
By appending 0s to te shorter list, let $m = n$.

$$\mathcal{E} = \mathcal{F} \Leftrightarrow E_i = \sum_j u_{ij} F_j \text{ for some unitary matrix } u$$

($\Rightarrow$)Let $\{|k\rangle\}_k$ be an orthonormal basis for the state space. Define:

$$|e_i\rangle = \sum_k |k\rangle(E_i|k\rangle) \qquad \text{and} \qquad |f_j\rangle = \sum_k |k\rangle(F_j|k\rangle)$$

Observe that $\sum_i |e_i\rangle\langle e_i| = \sum_j |f_j\rangle\langle f_j| \Rightarrow |e_i\rangle = \sum_j u_{ij}|f_j\rangle$ (u is unitary)

$$\forall\ |\psi\rangle, \qquad |\psi\rangle = \sum_k \langle\psi^*|k\rangle|k\rangle \Rightarrow E_i|\psi\rangle = \sum_k \langle\psi^*|k\rangle E_i|k\rangle = \langle\psi^*|e_i\rangle = \sum_j u_{ij}\langle\psi^*|f_j\rangle = \sum_j u_{ij}\ F_j|\psi^*\rangle$$

$$\Rightarrow E_i = \sum_j u_{ij} F_j$$

($\Leftarrow$)

Basic algebra shows

that:

$$\sum_i E_i \rho E_i^\dagger = \sum_j F_j \rho F_j^\dagger$$

Theory Of Error Correction

State space$(\boldsymbol{V} \cong \mathbb{C}^{\boldsymbol{2^n}})$: Complex Hilbert space corresponding to the n qubit system.

Codespace$(\boldsymbol{C})$: Subspace of codewords

Projector$(\boldsymbol{P})$: Projector onto the codespace C. If $\{|v_k\rangle\}_k$ is orthonormal basis of C, then $\mathrm{P} \equiv \sum_k |v_k\rangle\langle v_k|$

Noise$(\boldsymbol{\mathcal{E}})$: Quantum operation corresponding to the error in the sent codeword (May not be trace preserving).

Error Correction$(\boldsymbol{\mathcal{R}})$: Trace preserving quantum opperation such that:

$$\mathcal{R} \circ \mathcal{E}\,(\rho) \propto \rho$$
$$\forall \rho \text{ whose support is in } C$$

Existence of Error Correction

Theorem

Let $\{E_i\}_i$ be the operation elements of $\mathcal{E}$.

$\exists$ error correction $\mathcal{R}$ for noise $\mathcal{E}$ $\Leftrightarrow PE_i^\dagger E_j P = \alpha_{ij} P$ for some Hermitian matrix α

$(\Rightarrow)$ Let $\{R_j\}_j$ be the operation elements of $\mathcal{R}$.

$\forall\, \rho$, $P\rho P$ is a density operator in or codespace C

$$\Rightarrow \mathcal{R}\big(\mathcal{E}(P\rho P)\big) \propto P\rho P$$
$$\Rightarrow \sum_{i,j} R_j E_i P\rho P E_i^\dagger R_j^\dagger = cP\rho P$$
$$\Rightarrow \{R_j E_i P\}_{i,j} \equiv \{\sqrt{c}P\}$$

So, $\exists$ complex numbers c_{ki} such that: $R_k E_i P = c_{ki} P \Rightarrow PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$

$$\Rightarrow \left(\sum_k c_{ki}^* c_{kj}\right) P = PE_i^\dagger \left(\sum_k R_k^\dagger R_k\right) E_j P = PE_i^\dagger (I) E_j P = PE_i^\dagger E_j P$$

So, $PE_i^\dagger E_j P = \alpha_{ij} P$, with $\alpha_{ij} = \sum_k c_{ki}^* c_{kj}$

Existence of Error Correction (cont.)

$(\Leftarrow)$ α is Hermitian $\Rightarrow$ $\exists$ unitary matrix u such that: $d = u\alpha u^\dagger$ is a diagonal matrix

$$\Rightarrow \mathcal{E} \equiv \{E_i\}_i \equiv \left\{F_k = \sum_i u_{ik} E_i\right\}_k$$

Observe that: $PF_k^\dagger F_l P = \sum_{i,j} u_{ki}^\dagger \alpha_{ij} u_{jl} P = d_{kl} P = \delta_{kl} d_{kk} P$

By polar decomposition, $F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P$, for some unitary U_k. Define: $P_k = (U_k P) U_k^\dagger = \left(F_k P / \sqrt{d_{kk}}\right) U_k^\dagger = F_k P U_k^\dagger / \sqrt{d_{kk}}$

$$U_k^\dagger P_k F_l P = U_k^\dagger P_k^\dagger F_l P = \frac{1}{\sqrt{d_{kk}}} U_k^\dagger U_k P F_k^\dagger F_l P = \delta_{kl} \sqrt{d_{kk}} P$$

Define $\tilde{\mathcal{R}} \equiv \left\{U_k^\dagger P_k\right\}_k$ $\Rightarrow \tilde{\mathcal{R}}\big(\mathcal{E}(P\rho P)\big) = \sum_{k,l} U_k^\dagger P_k F_l P \rho P F_l^\dagger P_k^\dagger U_k = \sum_{k,l} \delta_{kl} d_{kk} P \rho P \propto P\rho P$

Discretization Of Errors

Theorem
Let $\mathcal{E} \equiv \{E_i\}_i$ be a correctable noise, and let $\tilde{\mathcal{R}}$ be the standard error corrector described above. Then, $\tilde{\mathcal{R}}$ also corrects $\mathcal{F} \equiv \left\{F_j = \sum_i m_{ji} E_i\right\}_j$ $\forall$ non − zero matrix m

$\mathcal{E}$ is correctable $\Rightarrow PE_i^\dagger E_j P = \alpha_{ij} P$. WLOG, let $\alpha = d$ be diagonal.

From previous results, we get $U_k^\dagger P_k E_i P = \delta_{ki} \sqrt{d_{kk}} P$

$$\Rightarrow U_k^\dagger P_k F_j P = \sum_i m_{ji} U_k^\dagger P_k E_i P = \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} P = m_{jk} \sqrt{d_{kk}} P$$

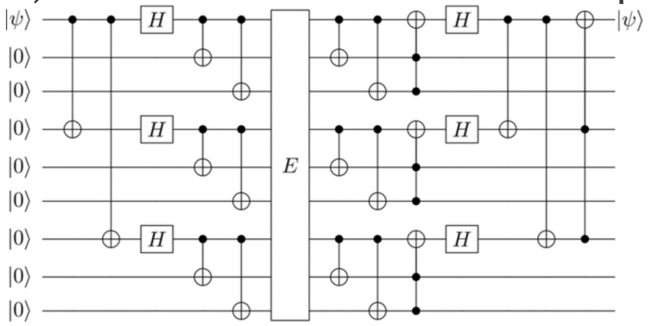
$$\tilde{\mathcal{R}}\big(\mathcal{F}(P\rho P)\big) = \sum_{k,j} U_k^\dagger P_k F_j P \rho P F_j^\dagger P_k^\dagger U_k = \sum_{k,l} \left|m_{jk}\right|^2 d_{kk} P \rho P \propto P \rho P$$

Discretization Of Errors (cont.)

Consider the matrices: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

They form a basis for $M_{2\times 2}(\mathbb{C})$.

So, any code that can handle a single X, Y or Z error can handle all 1 qubit errors. (Eg: Shor Code)



Shor Code Circuit

Generalizing, any code that can handle t X, Y and Z errors combined can handle all possible t qubit errors.
We call such codes as $t-$ error correcting codes.
We will next discuss a family of codes called **Stabilizar Codes**.

Pauli Matrices

The X, Y and Z matrices are called the Pauli matrices.
Properties:

1. $\forall\, A \in \{X, Y, Z\},\ A^2 = AA^\dagger = I$
2. $\forall\, A, B \in \{X, Y, Z\},\ A = B$ or $AB = -BA$
3. $XY = iZ, YZ = iX, ZX = iY$

Consider the set $G_1 = \left\{\omega M\colon \omega \in \{1, -1, i, -i\} \text{ and } M \in \{I, X, Y, Z\}\right\}$
$(G_1, \circ)$ is a group with the following property: $\forall\, A, B \in G_1, AB = BA$ or $AB = -BA$

We define the group G_n as $G_n := \left\{\omega M_1 \otimes M_2 \otimes \cdots \otimes M_n\colon\ \omega \in \{1, -1, i, -i\} \text{ and } M_i \in \{I, X, Y, Z\}\right\}$
Observe that G_n has the same property as G_1: $\forall\, A, B \in G_n, AB = BA$ or $AB = -BA$

Stabilizer Codes

Let $\mathcal{S}$ be a commutative subgroup of G_n such that $-I \ \notin \mathcal{S}$

Codespace: $C = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle\ \forall\ M \in \mathcal{S}\}$

Projector

Let $\mathcal{S} = \langle g_1, g_2, \dots, g_l \rangle$. Then $C = \bigcap_j Eig(g_j, +1)$

$P_j = \dfrac{I + g_j}{2}$ is the projector onto the subspace $Eig\left(g_j, +1\right)$. (Observe that all P_js commute)

$$P = \prod_j P_j = \prod_j \frac{I + g_j}{2}$$

Centralizer: $Z(\mathcal{S}) = \{E \in G_n:\ EM = ME\ \forall\ M \in \mathcal{S}\}$

Stabilizer Codes (cont.)

Theorem
Let $\mathcal{E} \equiv \{E_i\}_i$ be a noise such that $E_i \in G_n \; \forall\, i$. $E_j^\dagger E_k \notin Z(\mathcal{S}) \setminus \mathcal{S} \; \forall\, j,k \Rightarrow \mathcal{E}$ is correctable.

Case 1: $E_j^\dagger E_k \in \mathcal{S}$: $\forall |\psi\rangle,\; P|\psi\rangle \in C \Rightarrow PE_j^\dagger E_k P|\psi\rangle = P|\psi\rangle \Rightarrow PE_j^\dagger E_k P = P \Rightarrow \alpha_{jk} = 1$

Case 2: $E_j^\dagger E_k \in G_n \setminus Z(\mathcal{S})$

$$E_j^\dagger E_k \notin \mathcal{S} \Rightarrow \exists\, g_i \text{ such that } E_j^\dagger E_k g_i = -g_i E_j^\dagger E_k. \text{ WLOG, let } i = 1$$

$$E_j^\dagger E_k g_1 = -g_1 E_j^\dagger E_k \Rightarrow E_j^\dagger E_k \frac{I+g_1}{2} = \frac{I-g_1}{2} E_j^\dagger E_k \quad ; \quad \frac{I+g_1}{2} \circ \frac{I-g_1}{2} = 0 \Rightarrow P \circ \frac{I-g_1}{2} = 0$$

$$PE_j^\dagger E_k P = PE_j^\dagger E_k \prod_j \frac{I+g_j}{2} = P \circ \frac{I-g_1}{2} E_j^\dagger E_k \prod_{j=2}^{l} P_j = 0$$

$$PE_j^\dagger E_k P = 0P \Rightarrow \alpha_{jk} = 0$$

APPENDIX

Quantum Hamming Bound

Degenerate Code

Suppose $\exists\ E_1 \neq E_2 \in G_n$ such that $E_1(C) = E_2(C) \neq C$.

Such a code is called a degenerate code.

Quantum Hamming Bound

If we want to encode k qubits into n qubits such that it can correct upto t Pauli errors using a non $-$ degenerate code. Then:

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n$$

Quantum Hamming Bound (Proof)

First, we count the total possible no. of j errors ($j \leq t$)

Out of n qubits, the error can occour at any j qubits $\Rightarrow \binom{n}{j}$ possibilities

At each position, one of X, Y or Z can occour $\Rightarrow \binom{n}{j} 3^j$ possibilities

$$\text{Total no. of errors} = \sum_{j=0}^{t} \binom{n}{j} 3^j$$

Each error reversibly maps our codespace $C(\dim = 2^{\mathrm{k}})$ onto a unique disjoint orthogonal subspace.

Dimension of each subspace $= 2^{\mathrm{k}}$

$$\text{Dimension of their direct sum} = \sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n = \text{Dimension of state space}$$

Calderbank Shor Stean Code

Let C_1 and C_2 be two classical $[n, k_1]$ and $[n, k_2]$ binary linear codes respectively such that:

1. $C_2 \subset \mathrm{C}_1$
2. C_1 and $C_2^{\perp}$ are $t-$ error correcting codes

$CSS(C_1, C_2)$ is a quantum $[n, k_1 - k_2]$ code defined as:

$$CSS(C_1, C_2) = span(\{|x + C_2\rangle : x \in C_1\}),$$

$$\text{where} |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum\nolimits_{y \in C_2} |x + y\rangle$$

Calderbank Shor Stean Code: Error

Sent word: $|\psi_s\rangle = \sum_i a_i \, |x_i + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_i \sum_{y \in C_2} a_i |x_i + y\rangle$

Error
During transmission, suppuse that r_1 bit flips(X) and r_2 phase flips (Z) occour. $(r_i \leq t)$
(If both bit flip and phase flip occour, it is a Y error)

Define 2 binary vectors of length n: e_1 and e_2

$$(e_1)_i = \begin{cases} 1 & \text{bit flip at } i^{th} \text{ position} \\ 0 & \text{otherwise} \end{cases} \quad ; \quad (e_2)_i = \begin{cases} 1 & \text{phase flip at } i^{th} \text{ position} \\ 0 & \text{otherwise} \end{cases}$$

Recieved word: $|\psi_r\rangle = \frac{1}{\sqrt{|C_2|}} \sum_i \sum_{y \in C_2} (-1)^{(x_i + y) \cdot e_2} a_i |x_i + y + e_1\rangle$

CSS Code: Bit Flip Correction

Let S_1 be the syndrome function of C_1.

$$\text{Define } \sigma: \mathbb{Z}_2^n \times \mathbb{Z}_2^{n-k_1} \to \mathbb{Z}_2^n \times \mathbb{Z}_2^{n-k_1}$$
$$\sigma(a,b) = (a, S_1(a) + b)$$

Add $n - k_1$ $|0\rangle$ qubits to $|\psi_r\rangle$ and apply U_σ(quantum gate version of σ):

$$U_\sigma|\psi_r\rangle|0\rangle = \frac{1}{\sqrt{|C_2|}}\sum_i \sum_{y \in C_2} (-1)^{(x_i+y)\cdot e_2} a_i |x_i + y + e_1\rangle\, |S_1(x_i + y + e_1) + 0\rangle$$
$$= \frac{1}{\sqrt{|C_2|}}\sum_i \sum_{y \in C_2} (-1)^{(x_i+y)\cdot e_2} a_i |x_i + y + e_1\rangle\, |S_1(e_1)\rangle = |\psi_r\rangle|S_1(e_1)\rangle$$

So, we can read $S_1(e_1)$and subsequently find e_1 using syndrome decoding table.

Upon correcting the bit flip, we get: $\left|\psi_p\right\rangle = \frac{1}{\sqrt{|C_2|}}\sum_i \sum_{y \in C_2} (-1)^{(x_i+y)\cdot e_2} a_i |x_i + y\rangle$

CSS Code: Phase Flip Correction

Applying $H^{\otimes n}$ to $\left|\psi_p\right\rangle$, we get:

$$H^{\otimes n}\left|\psi_p\right\rangle = \frac{1}{\sqrt{|C_2|}}\sum_i \sum_{y\in C_2} (-1)^{(x_i+y)\cdot e_2} a_i H^{\otimes n}|x_i + y\rangle$$

$$= \frac{1}{\sqrt{2^n|C_2|}}\sum_i \sum_{y\in C_2} (-1)^{(x_i+y)\cdot e_2} a_i \sum_{z\in\mathbb{Z}_2^n} (-1)^{(x_i+y)\cdot z}\,|z\rangle$$

$$= \frac{1}{\sqrt{2^n|C_2|}}\sum_i \sum_{y\in C_2} \sum_{z\in\mathbb{Z}_2^n} (-1)^{(x_i+y)\cdot(z+e_2)} a_i|z\rangle$$

$$= \frac{1}{\sqrt{2^n|C_2|}}\sum_i \sum_{z\in\mathbb{Z}_2^n} \left(\sum_{y\in C_2} (-1)^{y\cdot z}\right)(-1)^{x_i\cdot z} a_i|z + e_2\rangle$$

$$\sum_{y\in C_2} (-1)^{y\cdot z} = \begin{cases} |C_2| & z \in C_2^{\perp} \\ 0 & \text{otherwise} \end{cases}$$

CSS Code: Phase Flip Correction (cont.)

$$H^{\otimes n}|\psi_p\rangle = \sqrt{\frac{|C_2|}{2^n}}\sum_i \sum_{z\in C_2^\perp}(-1)^{x_i\cdot z} a_i|z+e_2\rangle$$

We converted phase flip error to bit flip error. On correcting it, we get:

$$|\psi_h\rangle = \sqrt{\frac{|C_2|}{2^n}}\sum_i \sum_{z\in C_2^\perp}(-1)^{x_i\cdot z} a_i|z\rangle$$

Applying $H^{\otimes n}$ to $|\psi_h\rangle$, we get:

$$H^{\otimes n}|\psi_h\rangle = \frac{1}{\sqrt{|C_2|}}\sum_i \sum_{y\in C_2} a_i|x_i+y\rangle = |\psi_s\rangle$$

Fidelity

Fidelity is a measure of how close two density operators are

Classical Fidelity: Let $\{p_x\}_x$ and $\{q_x\}_x$ be two distributions. $F(p,q) = \sum_x \sqrt{p_x q_x}$

Quantum Fidelity: Let ρ and σ be two density operators. $F(\rho,\sigma) = tr\left(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right)$

If $\rho = \sum_i r_i |i\rangle\langle i|$ and $\sigma = \sum_i s_i |i\rangle\langle i|$ for some orthogonal basis i:

$$F(\rho,\sigma) = tr\left(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right) = tr\left(\sqrt{\sum_i r_i s_i |i\rangle\langle i|}\right) = tr\left(\sum_i \sqrt{r_i s_i}|i\rangle\langle i|\right) = \sum_i \sqrt{r_i s_i} = F(r,s)$$

Fidelity between a pure state $|\psi\rangle\langle\psi|$ and $\rho = F(|\psi\rangle\langle\psi|\,,\rho) = tr\left(\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|}\right) = \sqrt{\langle\psi|\rho|\psi\rangle}$

Fidelity Example: 3 Qubit Flip Code

Without Code: $|\psi\rangle = a|0\rangle + b|1\rangle$

Sent: $|\psi\rangle\langle\psi|$; Recieved: $\rho = pX|\psi\rangle\langle\psi|X + (1-p)|\psi\rangle\langle\psi|$

Fidelity: $F(|\psi\rangle\langle\psi|, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{1 - p + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle} \geq \sqrt{1-p}$

With Code: $|\psi\rangle = a|000\rangle + b|111\rangle$

Sent: $|\psi\rangle\langle\psi|$; Recieved: $\rho = [(1-p)^3 + 3p(1-p)^2]|\psi\rangle\langle\psi| + \cdots$

Fidelity: $F(|\psi\rangle\langle\psi|, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle} =\geq \sqrt{(1-p)^3 + 3p(1-p)^2}$