EE641000 Quantum Information and Computation

Chung-Chin Lu

Department of Electrical Engineering

National Tsing Hua University

February 21, 2006

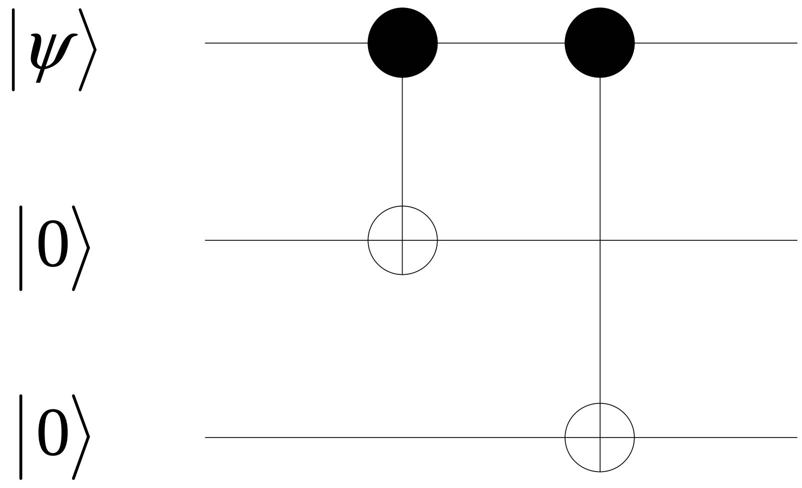
Unit Seven –
Quantum Error-Correcting Codes

A Three-Qubit Code over Bit Filp Channel

Obstacles

- No cloning : states cannot be cloned like in classical repetition codes
- Error is continuous : the "amount" of error a state (which is continuous in the state space of a quantum system) will face with is dependent on the state itself
  - The bit flip channel will not affect the state $(|0\rangle + |1\rangle)/\sqrt{2}$ of a qubit at all
  - The bit flip channel will change the state $|0\rangle$ of a qubit to the state $|1\rangle$ (and vice versa) totally
- Measurement may destroy quantum information : decoding procedure needs observation of the channel output, which may destroy the quantum state under observation and make recovery impossible

Encoding Algorithm



- $|0\rangle \mapsto |000\rangle$
- $|1\rangle \mapsto |111\rangle$
- $a|0\rangle + b|1\rangle \mapsto a|000\rangle + b|111\rangle$

Output of the Bit Flip Channel

- Assumption : each of the three encoded qubits is affected by a bit flip channel independently
- $E_{ijk} = E_i \otimes E_j \otimes E_k$ with $i, j, k \in \{0, 1\}$: a list of linear operators on the three-qubit system
  - $E_0 = \sqrt{1-p}I$ and $E_1 = \sqrt{p}\sigma_x$:

$$E_0^\dagger E_0 = (1-p)I, \quad E_1^\dagger E_1 = pI$$

  - Completeness identity :

$$\begin{aligned} \sum_{ijk} E_{ijk}^\dagger E_{ijk} &= \sum_{ijk} E_i^\dagger E_i \otimes E_j^\dagger E_j \otimes E_k^\dagger E_k \\ &= \sum_{ijk} (1-p)^{1-i} p^i (1-p)^{1-j} p^j (1-p)^{1-k} p^k I \otimes I \otimes I \\ &= ((1-p)+p)^3 I = I \end{aligned}$$

- $\mathcal{E}$: quantum operation which describes the three-qubit bit flip channel

$$\mathcal{E}(\rho) = \sum_{ijk} E_{ijk} \rho E_{ijk}^{\dagger}$$

- Input state of the channel : $|\psi\rangle = a|000\rangle + b|111\rangle$
- Output state of the channel : a mixed state

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_{ijk} E_{ijk}|\psi\rangle\langle\psi|E_{ijk}^{\dagger}$$

with ensemble $\{\lambda_{ijk}, E_{ijk}|\psi\rangle/\lambda_{ijk}\}$ where

$$E_{ijk}|\psi\rangle = aE_i|0\rangle E_j|0\rangle E_k|0\rangle + bE_i|1\rangle E_j|1\rangle E_k|1\rangle$$

and

$$\lambda_{ijk} = \langle\psi|E_{ijk}^{\dagger}E_{ijk}|\psi\rangle = (1-p)^{1-i}p^i(1-p)^{1-j}p^j(1-p)^{1-k}p^k$$

  - When $a = b$, $E_{ijk}(|\psi\rangle) = E_{1-i,1-j,1-k}(|\psi\rangle)$ and the ensemble of the mixed state $\mathcal{E}(|\psi\rangle\langle\psi|)$ can be simplified

Syndrome Measurement and Syndrome

- A thinking : each intact or corrupted state in the ensemble $\{\lambda_{ijk}, E_{ijk}|\psi\rangle/\lambda_{ijk}\}$ of the channel output state $\mathcal{E}(|\psi\rangle\langle\psi|)$ is in one of the following *orthogonal* subspaces of the state space of the three-qubit system

$$G_0 = \mathrm{Span}\{|000\rangle, |111\rangle\}, \quad G_1 = \mathrm{Span}\{|100\rangle, |011\rangle\},$$
$$G_2 = \mathrm{Span}\{|010\rangle, |101\rangle\}, \quad G_3 = \mathrm{Span}\{|001\rangle, |110\rangle\}$$

- Syndrome measurement : a measurement which is able to tells us what error, if any, occurred on the quantum state *without destroying the quantum state*

– $\{P_0, P_1, P_2, P_3\}$: a legitimate projective measurement where P_i is the projector of the subspace G_i

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|, \quad P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|,$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|, \quad P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

- Syndrome : the result of the syndrome measurement
  - Syndrome 0 : with probability

$$\begin{aligned} \mathrm{tr}(P_0\mathcal{E}(|\psi\rangle\langle\psi|)P_0) &= \mathrm{tr}(E_{000}|\psi\rangle\langle\psi|E_{000}^\dagger + E_{111}|\psi\rangle\langle\psi|E_{111}^\dagger) \\ &= (1-p)^3 + p^3 \end{aligned}$$

and the state after the syndrome measurement is

$$\frac{E_{000}|\psi\rangle\langle\psi|E_{000}^\dagger + E_{111}|\psi\rangle\langle\psi|E_{111}^\dagger}{(1-p)^3 + p^3}$$

- Syndrome 1 : with probability

$$\begin{aligned} \mathrm{tr}(P_1\mathcal{E}(|\psi\rangle\langle\psi|)P_1) &= \mathrm{tr}(E_{100}|\psi\rangle\langle\psi|E_{100}^\dagger + E_{011}|\psi\rangle\langle\psi|E_{011}^\dagger) \\ &= (1-p)^2p + (1-p)p^2 = (1-p)p \end{aligned}$$

and the state after the syndrome measurement is

$$\frac{E_{100}|\psi\rangle\langle\psi|E_{100}^\dagger + E_{011}|\psi\rangle\langle\psi|E_{011}^\dagger}{(1-p)p}$$

- Syndrome 2 : with probability

$$\begin{aligned} \mathrm{tr}(P_2\mathcal{E}(|\psi\rangle\langle\psi|)P_2) &= \mathrm{tr}(E_{010}|\psi\rangle\langle\psi|E_{010}^\dagger + E_{101}|\psi\rangle\langle\psi|E_{101}^\dagger) \\ &= (1-p)^2p + (1-p)p^2 = (1-p)p \end{aligned}$$

and the state after the syndrome measurement is

$$\frac{E_{010}|\psi\rangle\langle\psi|E_{010}^\dagger + E_{101}|\psi\rangle\langle\psi|E_{101}^\dagger}{(1-p)p}$$

– Syndrome 3 : with probability

$$\begin{aligned} \mathrm{tr}(P_3\mathcal{E}(|\psi\rangle\langle\psi|)P_3) &= \mathrm{tr}(E_{001}|\psi\rangle\langle\psi|E_{001}^\dagger + E_{110}|\psi\rangle\langle\psi|E_{110}^\dagger) \\ &= (1-p)^2p + (1-p)p^2 = (1-p)p \end{aligned}$$

and the state after the syndrome measurement is

$$\frac{E_{001}|\psi\rangle\langle\psi|E_{001}^\dagger + E_{110}|\psi\rangle\langle\psi|E_{110}^\dagger}{(1-p)p}$$

- Ambiguity : two intact or corrupted states in the ensemble $\{\lambda_{ijk}, E_{ijk}|\psi\rangle/\lambda_{ijk}\}$ of the channel output state $\mathcal{E}(|\psi\rangle\langle\psi|)$ will produce the same syndrome measurement output, called *syndrome*
  – Syndrome 0 : $E_{000}|\psi\rangle/\lambda_{000}$ and $E_{111}|\psi\rangle/\lambda_{111}$
  – Syndrome 1 : $E_{100}|\psi\rangle/\lambda_{100}$ and $E_{011}|\psi\rangle/\lambda_{011}$
  – Syndrome 2 : $E_{010}|\psi\rangle/\lambda_{010}$ and $E_{101}|\psi\rangle/\lambda_{101}$
  – Syndrome 3 : $E_{001}|\psi\rangle/\lambda_{001}$ and $E_{110}|\psi\rangle/\lambda_{110}$

- Cosets : a coset is the set of all states in the ensemble $\{\lambda_{ijk}, E_{ijk}|\psi\rangle/\lambda_{ijk}\}$ of the channel output state $\mathcal{E}(|\psi\rangle\langle\psi|)$ which will result in the same syndrome

Undetectable Error Probability

- Undetectable error patterns : event patterns other than $E_{000}|\psi\rangle/\lambda_{000}$ in the coset of $E_{000}|\psi\rangle/\lambda_{000}$, which is just $E_{111}|\psi\rangle/\lambda_{111}$
- Undetectable error probability : $\lambda_{111} = p^3$

Uncorrectable Error Probability

- Correctable error patterns : (error) patterns each of which is selected from distinct cosets of the ensemble of the channel output states
  - We usually select a pattern with the largest probability of occurrence from a coset as a correctable error pattern
  - If $p \leq 0.5$, we select the following correctable error patterns

$$E_{000}|\psi\rangle/\lambda_{000}, E_{100}|\psi\rangle/\lambda_{100}, E_{010}|\psi\rangle/\lambda_{010}, E_{001}|\psi\rangle/\lambda_{001}$$

- Uncorrectable error probability : the sum of the probability of occurrence of each uncorrectable error pattern, which is

$$\lambda_{110} + \lambda_{011} + \lambda_{101} + \lambda_{111} = 3(1-p)p^2 + p^3$$

Decoding Algorithm

- Conditioned on the syndrome, the decoding procedure takes the following actions
  - Syndrome 0 : do nothing
  - Syndrome 1 : flip qubit one
  - Syndrome 2 : flip qubit two
  - Syndrome 3 : flip qubit three
- All correctable error patterns can be completely removed and in those cases, the original state is recovered perfectly

Alternative Syndrome Measurements by Two Observables

- $Z_1Z_2(= Z \otimes Z \otimes I)$: the first observable with spectral decomposition

$$
\begin{aligned}
Z_1Z_2 &= (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes I \\
&= (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I
\end{aligned}
$$

  – A projective measurement with projectors $P_{12}^{+1} = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I, P_{12}^{-1} = (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$
  – Outcome (syndrome) +1 : when the values of the first and the second qubits are the same
  – Outcome (syndrome) -1 : when the values of the first and the second qubits are different
  – The observable Z_1Z_2 provides one bit of information about the error pattern without destroying the channel output

quantum state

- $Z_2Z_3(= I \otimes Z \otimes Z)$: the second observable with spectral decomposition

$$
\begin{aligned}
Z_2Z_3 &= I \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \\
&= I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)
\end{aligned}
$$

  - A projective measurement with projectors $P_{23}^{+1} = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|), P_{23}^{-1} = I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)$
  - Outcome (syndrome) +1 : when the values of the second and the third qubits are the same
  - Outcome (syndrome) -1 : when the values of the second and the third qubits are different
  - The observable Z_2Z_3 provides one bit of information about the error pattern without destroying the channel output quantum state

- Syndrome +1+1 : with probability

$$
\begin{aligned}
& \mathrm{tr}(P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1}) \cdot \mathrm{tr}\left(P_{23}^{+1}\frac{P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1}}{\mathrm{tr}(P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1})}P_{23}^{+1}\right) \\
= \; & \mathrm{tr}\left(P_{23}^{+1}P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1}P_{23}^{+1}\right) \\
= \; & \mathrm{tr}(E_{000}|\psi\rangle\langle\psi|E_{000}^{\dagger} + E_{111}|\psi\rangle\langle\psi|E_{111}^{\dagger}) \\
= \; & (1-p)^3 + p^3
\end{aligned}
$$

and the state after the two projective measurements

$$
\frac{P_{23}^{+1}\frac{P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1}}{\mathrm{tr}(P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1})}P_{23}^{+1}}{\mathrm{tr}\left(P_{23}^{+1}\frac{P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1}}{\mathrm{tr}(P_{12}^{+1}\mathcal{E}(|\psi\rangle\langle\psi|)P_{12}^{+1})}P_{23}^{+1}\right)} = \frac{E_{000}|\psi\rangle\langle\psi|E_{000}^{\dagger} + E_{111}|\psi\rangle\langle\psi|E_{111}^{\dagger}}{(1-p)^3 + p^3}
$$

  - This is the same as when syndrome 0 is produced by the previous syndrome measurement

- Syndrome -1+1 : the same as syndrome 1 in the previous syndrome measurement

- Syndrome -1-1 : the same as syndrome 2 in the previous syndrome measurement
- Syndrome +1-1 : the same as syndrome 3 in the previous syndrome measurement

A Three-Qubit Code over Phase Filp Channel

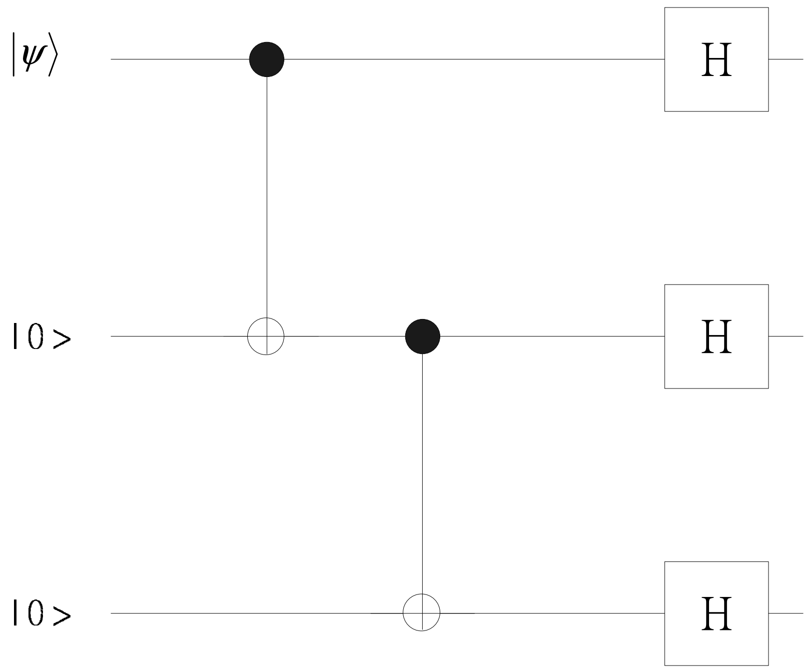
Turning Phase Flip Channel to Bit Flip Channel

- $\{|0\rangle, |1\rangle\}$: the computational basis of a qubit
- $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$: another orthonormal basis of the state space of the qubit
- $|\psi\rangle = a|+\rangle + b|-\rangle$: a state of the qubit as channel input state
- Phase flip channel $\mathcal{E}_{pf}$: with probability $1 - p$, the output state is the same as the input state and with probability p, the output state becomes

$$\sigma_z|\psi\rangle = a|-\rangle + b|+\rangle$$

  - The effect of the phase flip channel is to exchange the two states $|+\rangle$ and $|-\rangle$, similar to the bit flip channel to exchange the two states $|0\rangle$ and $|1\rangle$

Encoding Algorithm



- $|0\rangle \mapsto |+++\rangle$
- $|1\rangle \mapsto |---\rangle$
- $a|0\rangle + b|1\rangle \mapsto a|+++\rangle + b|---\rangle$

Output of the Phase Flip Channel

- Assumption : each of the three encoded qubits is affected by a phase flip channel independently
- $E_{ijk} = E_i \otimes E_j \otimes E_k$ with $i, j, k \in \{0, 1\}$: a list of linear operators on the three-qubit system
  - $E_0 = \sqrt{1-p}I$ and $E_1 = \sqrt{p}\sigma_z$:

$$E_0^\dagger E_0 = (1-p)I, \quad E_1^\dagger E_1 = pI$$

  - Completeness identity :

$$\begin{aligned} \sum_{ijk} E_{ijk}^\dagger E_{ijk} &= \sum_{ijk} E_i^\dagger E_i \otimes E_j^\dagger E_j \otimes E_k^\dagger E_k \\ &= \sum_{ijk} (1-p)^{1-i} p^i (1-p)^{1-j} p^j (1-p)^{1-k} p^k I \otimes I \otimes I \\ &= ((1-p)+p)^3 I = I \end{aligned}$$

- $\mathcal{E}$: quantum operation which describes the three-qubit phase flip channel
$$\mathcal{E}(\rho) = \sum_{ijk} E_{ijk} \rho E_{ijk}^{\dagger}$$
- Input state of the channel : $|\psi\rangle = a|+++\rangle + b|---\rangle$
- Output state of the channel : a mixed state
$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_{ijk} E_{ijk}|\psi\rangle\langle\psi|E_{ijk}^{\dagger}$$

  with ensemble $\{\lambda_{ijk}, E_{ijk}|\psi\rangle/\lambda_{ijk}\}$ where
$$E_{ijk}|\psi\rangle = aE_i|+\rangle E_j|+\rangle E_k|+\rangle + bE_i|-\rangle E_j|-\rangle E_k|-\rangle$$

  and
$$\lambda_{ijk} = \langle\psi|E_{ijk}^{\dagger} E_{ijk}|\psi\rangle = (1-p)^{1-i}p^i(1-p)^{1-j}p^j(1-p)^{1-k}p^k$$
  - When $a = b$, $E_{ijk}(|\psi\rangle) = E_{1-i,1-j,1-k}(|\psi\rangle)$ and the ensemble of the mixed state $\mathcal{E}(|\psi\rangle\langle\psi|)$ can be simplified

Syndrome Measurement and Syndrome

- A thinking : each intact or corrupted state in the ensemble $\{\lambda_{ijk}, E_{ijk}|\psi\rangle/\lambda_{ijk}\}$ of the channel output state $\mathcal{E}(|\psi\rangle\langle\psi|)$ is in one of the following *orthogonal* subspaces of the state space of the three-qubit system

$$G'_0 = \mathrm{Span}\{|+++\rangle, |---\rangle\}, \quad G'_1 = \mathrm{Span}\{|-++\rangle, |+--\rangle\},$$
$$G'_2 = \mathrm{Span}\{|+-+\rangle, |-+-\rangle\}, \quad G'_3 = \mathrm{Span}\{|++-\rangle, |--+\rangle\}$$

- $\{P'_0, P'_1, P'_2, P'_3\}$: a legitimate syndrome measurement where P'_i

is the projector of the subspace G_i'

$$P_0' = |+++\rangle\langle+++| + |---\rangle\langle---| = HP_0H,$$
$$P_1' = |-++\rangle\langle-++| + |+--\rangle\langle+--| = HP_1H,$$
$$P_2' = |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-| = HP_2H,$$
$$P_3' = |++-\rangle\langle++-| + |--+\rangle\langle--+| = HP_3H$$

- $H^{\otimes 3}Z_1Z_2H^{\otimes 3} = X_1X_2$ and $H^{\otimes 3}Z_2Z_3H^{\otimes 3} = X_2X_3$: two consecutive observables as an alternative syndrome measurement
  - X_1X_2 : comparing the sign of the first two qubits with spectral decomposition

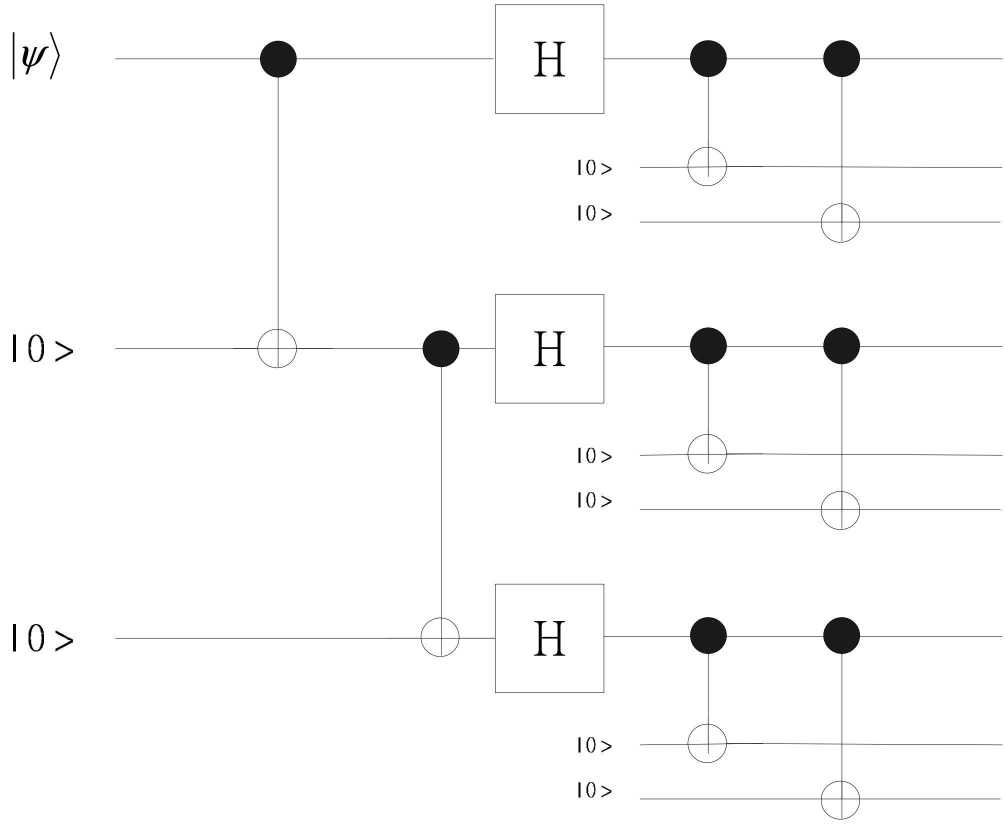
    $$X_1X_2 = (|++\rangle\langle++|+|--\rangle\langle--|)\otimes I-(|+-\rangle\langle+-|+|-+\rangle\langle-+|)\otimes I$$

  - X_2X_3 : comparing the sign of the last two qubits with spectral decomposition

$$X_2X_3 = I\otimes(|{+}{+}\rangle\langle{+}{+}|+|{-}{-}\rangle\langle{-}{-}|) - I\otimes(|{+}{-}\rangle\langle{+}{-}|+|{-}{+}\rangle\langle{-}{+}|)$$

The Shor Code

- Correct an arbitrary error on a single qubit
- The encoding circuit diagram



The Encoding Algorithm

There are two stages

- 1st stage : three-qubit phase flip code

$$|0\rangle \mapsto |+++\rangle, \quad |1\rangle \mapsto |---\rangle$$

- 2nd stage : three-quit bit flip code

$$|+\rangle \mapsto \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \quad |-\rangle \mapsto \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

- A nine-qubit code

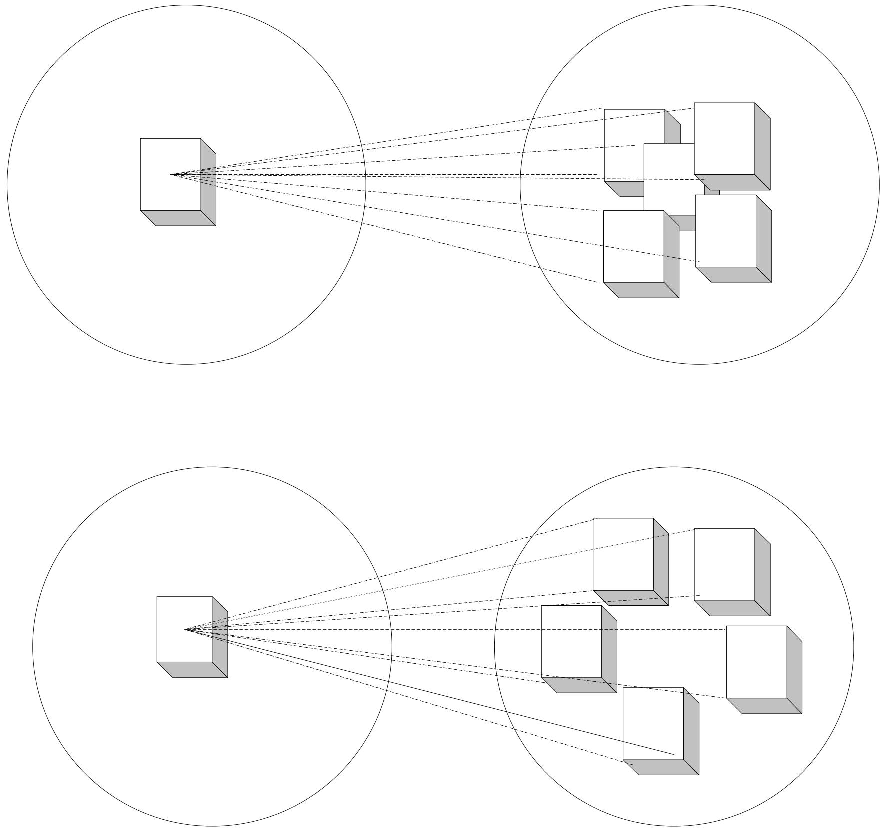
$$\begin{aligned} |0\rangle \quad &\mapsto \quad |0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}, \\ |1\rangle \quad &\mapsto \quad |1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \end{aligned}$$

Theory of Quantum Error-Correcting Codes

Key Features of Quantum Error-Corretion

- Encoding : a unitary transformation which maps the state space of a k-qubit quantum system (embeded as a subspace of the state space H of an n-qubit quantum system, called the information space A) into a quantum error-correcting code C (also as a subspace of H, called the code space)
  - H : the state space of a 3-qubit quantum system
  - $A = \{(a|0\rangle + b|1\rangle) \otimes |0\rangle \otimes |0\rangle\}$: the information space
  - $C = \{a|000\rangle + b|111\rangle\}$: the code space
  - P : the projector from H to the code space C
- Noise : described by a quantum operation $\mathcal{E}$ with operation elements $\{E_i\}$, which may not be trace-preserving
  - E_i : correctable error patterns which map the code spaces into undeformed and orthogonal subspaces of H

* Orthogonality : Reliable distinguishability by the syndrome measurement
* Undeformation : each error pattern E_i maps orthogonal codewords to orthogonal states in order to be able to recover codewords from the error



- Error-correction operation : a trace-preserving quantum operation $\mathcal{R}$ such that for any state ρ whose support lies in the code space C, we have

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho$$

Quantum Error-Correting Conditions

- C : a quantum code
- P : the projector onto C
- $\mathcal{E}$: a quantum operation with operation elements $\{E_i\}$

A neccesary and sufficient codition for the *existence* of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C is that

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

for some Hermitian matrix α of complex numbers

- E_i : (noise $\mathcal{E}$) error patterns and if such an error-correction operation $\mathcal{R}$ exists, correctable error patterns

- $d = u^\dagger \alpha u$: a diagonalization of the Hermitian matrix α by the unitary matrix u
- $F_k \stackrel{\triangle}{=} \sum_i u_{ik} E_i$: a unitary equivalent set of operation elements for the noise $\mathcal{E}$

$$PF_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger u_{jl} P E_i^\dagger E_j P = \sum_{ij} u_{ki}^\dagger \alpha_{ij} u_{jl} P = d_{kl} P$$

  - $d_{kk} \geq 0$: $PF_k^\dagger F_l P$ is a positive operator
    - α : a positive operator
  - If $d_{kk} = 0$ then F_k is the zero operator and will be ignored

- $F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P$: left polar decomposition of $F_k P$, where U is a unitary operator
  - F_k : rotating the code space $C = P(H)$ into the subspace defined by the projector

$$P_k = U_k P U_k^\dagger = F_k P U_k^\dagger / \sqrt{d_{kk}}$$

- $\{P_k(H)\}$: a collection of orthogonal subspaces of H

$$P_k P_l = P_k^\dagger P_l = \frac{U_k P F_k^\dagger F_l P U_l^\dagger}{\sqrt{d_{kk} d_{ll}}} = \frac{d_{kl} U_k P U_l^\dagger}{\sqrt{d_{kk} d_{ll}}}$$

- $\{P_k\}$: a projective measurement as a syndrome measurement, where additional projectors $P_{k'}$ may be augmented to satisfy the completeness relation $\sum_k P_k + \sum_{k'} P_{k'} = I$
- $U_k^\dagger$: recovery operator when the syndrome is k

- $\mathcal{R}(\sigma) = \sum_k U_k^\dagger P_k \sigma P_k U_k$: the error-correction operation
- ρ : a density operator whose support is in the code space C, i.e., $\rho = P\rho$ and then $\sqrt{\rho} = P\sqrt{\rho}$, which implies

$$
\begin{aligned}
U_k^\dagger P_k F_l \sqrt{\rho} &= U_k^\dagger P_k^\dagger F_l P \sqrt{\rho} \\
&= U_k^\dagger U_k P F_k^\dagger F_l \sqrt{\rho} / \sqrt{d_{kk}} \\
&= \delta_{kl} \sqrt{d_{kk}} P \sqrt{\rho} \\
&= \delta_{kl} \sqrt{d_{kk}} \sqrt{\rho}
\end{aligned}
$$

- $\mathcal{R}(\mathcal{E}(\rho)) \propto \rho$:

$$
\begin{aligned}
\mathcal{R}(\mathcal{E}(\rho)) &= \sum_{kl} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k \\
&= \sum_{kl} \delta_{kl} d_{kk} \rho = \left(\sum_k d_{kk} \right) \rho \propto \rho
\end{aligned}
$$

- $\{E_i\}$: correctable (noise $\mathcal{E}$) error patterns
- $\mathcal{R}$: error-correction operation with operation elements $\{R_j\}$
- $\mathcal{E}_C$: a quantum operation such that for any density operator ρ, not necessarily having support in the code space C, we have

$$\mathcal{E}_C(\rho) = \mathcal{E}(P\rho P)$$

- $\mathcal{R}(\mathcal{E}_C(\rho)) = \mathcal{R}(\mathcal{E}(P\rho P)) \propto P\rho P$: the operator $P\rho P$ has suport in C and the proportional positive constant c is independent of ρ since both $\mathcal{R} \circ \mathcal{E}_C$ and $P \cdot P$ are linear maps, we have

$$\sum_{ij} R_j E_i P\rho P E_i^\dagger R_j^\dagger = cP\rho P$$

for any density operator ρ

- $\{R_j E_i P\}$ and $\{\sqrt{c}P\}$: two sets of operation elements for the same quantum operation and by the unitary freedom, we have

  $$R_k E_l P = \beta_{kl} P,$$

  where β_{kl} are complex numbers, and then

  $$P E_i^\dagger R_k^\dagger R_k E_j P = \beta_{ki}^* P \beta_{kj} P = \beta_{ki}^* \beta_{kj} P$$

  and summing over k, we have

  $$P E_i^\dagger E_j P = (\sum_k \beta_{ki}^* \beta_{kj}) P = \alpha_{ij} P$$

  with $\alpha_{ij} = \sum_k \beta_{ki}^* \beta_{kj}$ a Hermitian matrix, since

  $$\sum_k R_k^\dagger R_k = I$$

The Error Discretization Theorem

- C : a quantum code
- P : the projector onto C
- $\mathcal{R}$: the error-correction operation
- $\mathcal{E}$: a quantum operation with correctable error patterns (operation elements) $\{E_i\}$
- $\mathcal{F}$: a quantum operation with error patterns (operation elements) $\{F_j\}$ which are *linear combinations* of the correctable error patterns E_i, i.e, $F_j = \sum_i \beta_{ji} E_i$ for any complex numbers β_{ji}

Then for any density operator ρ whose support is in C, we have

$$\mathcal{R}(\mathcal{F}(\rho)) \propto \rho$$

Proof

- $PE_i^\dagger E_j P = d_{ij} P$: the matrix $[d_{ij}]$ is diagonal with positive entries
- $\{U_k^\dagger P_k\}$: operation elements of the error-correction operation $\mathcal{R}$ such that for any density operator ρ whose support is in the code space C

$$U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho}$$

which implies that

$$U_k^\dagger P_k F_j \sqrt{\rho} = \sum_i \beta_{ji} \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} = m_{jk} \sqrt{d_{kk}} \sqrt{\rho}$$

and thus

$$\mathcal{R}(\mathcal{F}(\rho)) = \sum_{kj} U_k^\dagger P_k F_j \sqrt{\rho} F_j^\dagger P_k U_k = \sum_{jk} |m_{jk}|^2 d_{kk} \rho \propto \rho$$

A Theory of Classical Binary Linear Block Codes

Binary Linear Block Codes

Construction of Quantum Error-Correcting Codes

Calderbank-Shor-Steane Codes

- C_1 and C_2 : $[n, k_1]$ and $[n, k_2]$ classical binary linear codes with
  - $C_2 \subset C_1$
  - C_1 and $C_2^{\perp}$ both correct t errors
- $\bar{x} = x + C_2$: a coset of C_2 in C_1 containing $x \in C_1$
- H : the state space of an n-qubit quantum system
- $|\bar{x}\rangle = |x + C_2\rangle$: a state in H corresponding to the coset $\bar{x} = x + C_2$

$$|\bar{x}\rangle = |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

- The $[n, k_1 - k_2]$ quantum code $\mathrm{CSS}(C_1, C_2)$: the subspace of H spanned by the orthonormal set $\{|\bar{x}\rangle, \bar{x} \in C_1/C_2\}$

Error Model

- Independent error model : error affects each qubit independently
- The error discretization theorem : an arbitrary single-qubit error pattern (a linear combination of the error patterns $I, \sigma_x, \sigma_z, \sigma_x\sigma_z$) is correctable if $\{I, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$ are correctable error patterns
  - The error pattern $\sigma_x\sigma_z$ is the total effect of firstly applying error pattern σ_z and then secondly applying error pattern σ_x
- e_z : n-bit phase flip (error pattern) indicator with 1s where phase flip occur and 0s otherwise
- e_x : n-bit bit flip (error pattern) indicator with 1s where bit flip occur and 0s otherwise

- An error pattern with which each qubit is affected by any of the single qubit error patterns $I, \sigma_x, \sigma_z, \sigma_x\sigma_z$ can be represented by an indicator as the concatenation $e_x \circ e_z$ of an bit flip indicator e_x and an phase flip indicator e_z
  - An example : $(1,0,0,1) \circ (0,1,0,1)$ means that the first qubit is affected by a bit flip error, the second qubit is affected by a phase flip error, the third qubit is error-free, and the last qubit is affected by a bit and phase flip error
  - The effect of error pattern with indicator $e_x \circ e_z$: for a computational basis $\{|l\rangle\}$ of H, we have

$$|l\rangle \xrightarrow{e_x \circ e_z} (-1)^{l \cdot e_z} |l + e_x\rangle$$

- Correctable error patterns : all error patterns with indicator $e_x \circ e_z$ such that $w_H(e_x) \le t$ and $w_H(e_z) \le t$

Error-Detection and Error-Correction

- $|\bar{x}\rangle = |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$: the transmitted codeword
- $e_x \circ e_z$: the correctable error pattern occurred
- $|r\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_z} |x + y + e_x\rangle$: the received (corrupted) state
- Two stages : firstly detect and correct the bit flip error indicator e_x and secondly detect and corrrect the phase flip error indicator
- A_1 : a k_1-qubit ancillary quantum system to store the syndrome of C_1, whose initial state is set to $|0\rangle$
- H_1 : a parity-check matrix of the classical binary linear code C_1
- C_1-syndrome calculation : a unitary operator on the

$(n+k_1)$-qubit composite system

$$|x+y+e_x\rangle|0\rangle \longrightarrow |x+y+e_x\rangle|H_1(x+y+e_x)\rangle = |x+y+e_x\rangle|H_1e_x\rangle$$

- Since $x+y \in C_1$, we have $H_1(x+y) = 0$
- Since C_1 can correct up to t classical errors, $x+y+e_x$ are all different for different coset leader x in C_1/C_2, different $y \in C_2$ and different e_x with $w_H(e_x) \le t$

• $\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_z}|x+y+e_x\rangle|H_1e_x\rangle$: the state of the $(n+k_1)$-qubit composite system after C_1-syndrome calculation

• Detection of the Bit flip error indicator e_x : projective measuremnet on the computational basis of the ancilla

- The outcome is H_1e_x with probability 1 which is used to find the correctable error pattern e_x by any calssical error-correcting procedure

– The state of the n-qubit system after the measurement is

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_z} |x + y + e_x\rangle$$

- Correction of the Bit flip error indicator e_x : applying a bit flip operator σ_x to each qubit where a bit flip occurred and resulting in the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_z} |x + y\rangle$$

- $H^{\otimes n}$: applying a Hadamard gate to each qubit (to convert phase flip errors to bit flip errors) and leaving the state

$$\frac{1}{\sqrt{|C_2| 2^n}} \sum_{k=0}^{2^n - 1} \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_z + k} |k\rangle$$

$$= \frac{1}{\sqrt{|C_2|2^n}} \sum_{k'=0}^{2^n-1} \sum_{y \in C_2} (-1)^{(x+y)\cdot k'} |k' + e_z\rangle, \text{where } k' = e_z + k$$

$$= \frac{1}{\sqrt{2^n}/|C_2|} \sum_{k' \in C_2^{\perp}} (-1)^{x \cdot k'} |k' + e_z\rangle$$

– When $k' \in C_2^{\perp}$, we have $y \cdot k' = 0$ for all $y \in C_2$ and then

$$\sum_{y \in C_2} (-1)^{y\cdot(k'} = |C_2|$$

– When $k' \notin C_2^{\perp}$, we have $y \cdot k' = 0$ for half of $y \in C_2$ and $y \cdot k' = 1$ for half of $y \in C_2$ and then

$$\sum_{y \in C_2} (-1)^{y\cdot(k'} = 0$$

- A_2 : a $(n - k_2)$-qubit ancillary quantum system to store the syndrome of $C_2^{\perp}$, whose initial state is set to $|0\rangle$

- H_2 : a parity-check matrix of the classical binary linear code $C_2^\perp$
- $C_2^\perp$-syndrome calculation : a unitary operator on the $(2n-k_2)$-qubit composite system

$$|k'+e_z\rangle|0\rangle \longrightarrow |k'+e_z\rangle|H_2(k'+e_z)\rangle = |k'+e_z\rangle|H_2e_z\rangle$$

  – Since $k' \in C_2^\perp$, we have $H_2k' = 0$
  – Since $C_2^\perp$ can correct up to t classical errors, $k'+e_z$ are all different for different $k' \in C_2^\perp$ and different e_z with $w_H(e_z) \le t$
- $\frac{1}{\sqrt{2^n/|C_2|}}\sum_{k'\in C_2^\perp}(-1)^{x\cdot k'}|k'+e_z\rangle|H_2e_z\rangle$: the state of the $(2n-k_2)$-qubit composite system after $C_2^\perp$-syndrome calculation
- Detection of the Bit flip error indicator e_z : projective measuremnet on the computational basis of the ancilla

- The outcome is $H_2 e_z$ with probability 1 which is used to find the correctable error pattern e_z by any calssical error-correcting procedure
- The state of the n-qubit system after the measurement is

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{k' \in C_2^{\perp}} (-1)^{x \cdot k'} |k' + e_z\rangle$$

- Correction of the phase flip error indicator e_z : applying a bit flip operator σ_x to each qubit where a bit flip occurred and resulting in the state

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{k' \in C_2^{\perp}} (-1)^{x \cdot k'} |k'\rangle = \frac{1}{\sqrt{|C_2| 2^n}} \sum_{k'=0}^{2^n - 1} \sum_{y \in C_2} (-1)^{(x+y) \cdot k'} |k'\rangle$$

- $H^{\otimes n}$: applying a Hadamard gate to each qubit again and recovering the state

$$|\bar{x}\rangle = |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

An Example : the Steane Code

- $C_1 = C$: the [7,4,3] Hamming code with parity-check matrix

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

- $C_2 = C^{\perp}$: a [7,3,4] linear code with parity-check matrix

$$H' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- $C_2 \subset C_1$

- $C_2^\perp = C$
- Both C_1 and $C_2^\perp$ are 1-error-correcting codes
- The Steane code is a $[7, 1]$ CSS quantum code which can correct one arbitrary error