

Title: IQC - Quantum Error Correction - Lecture 1

Date: Jan 04, 2018 02:00 PM

URL: <http://pirsa.org/18010047>

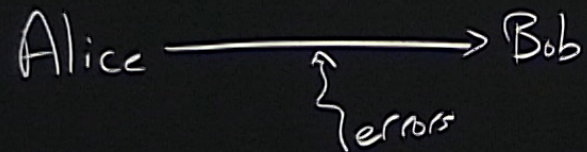
Abstract:

Quantum Error Correction and Fault Tolerance

Class web page: <http://perimeterinstitute.ca/personal/dgottesman/QECC2018>

Quantum Error Correction and Fault Tolerance

Class web page: <http://perimeterinstitute.ca/personal/dgottesman/QECC2018>



Quantum Error Correction and Fault Tolerance

Class web page: <http://perimeterinstitute.ca/personal/dgottesman/QECC2018>

error correction: Alice $\xrightarrow{\quad \uparrow \text{errors} \quad}$ Bob

fault tolerance: fault tolerant protocols
threshold theorem

topological codes

CPTP map $\rho \mapsto S(\rho)$

1) Positive $\rho \geq 0 \Rightarrow S(\rho) \geq 0$

2) Completely positive: σ st. $\text{tr}_R \sigma = \rho$, $\sigma \geq 0$
 $\Rightarrow (I \otimes S)(\sigma) \geq 0$

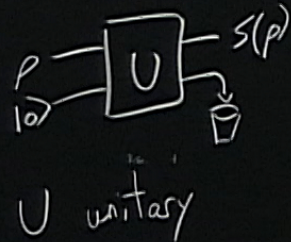
3) Trace preserving $\text{tr} S(\rho) = \text{tr} \rho$

CPTP map $\rho \mapsto S(\rho)$

1) Positive $\rho \geq 0 \Rightarrow S(\rho) \geq 0$

2) Completely positive: σ st. $\text{tr}_R \sigma = \rho$, $\sigma \geq 0$
 $\Rightarrow (I \otimes S)(\sigma) \geq 0$

3) Trace preserving $\text{tr} S(\rho) = \text{tr} \rho$



Kraus representation

$$S(\rho) = \sum_k A_k \rho A_k^\dagger$$

$$\text{with } \sum_k A_k^\dagger A_k = I$$

Unitary $S(\rho) = U\rho U^\dagger$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{Bit flip} \quad \begin{array}{l} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{array}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{Phase flip} \quad \begin{array}{l} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow -|1\rangle \end{array}$$

$$Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \begin{array}{l} |0\rangle \rightarrow i|1\rangle \\ |1\rangle \rightarrow -i|0\rangle \end{array}$$

$$R_\theta = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Dephasing channel:

$$S(\rho) = (1-p)\rho + pZ\rho Z$$

$$p = \frac{1}{2}: |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$S(|\psi\rangle\langle\psi|) = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$$

Unitary $S(\rho) = U\rho U^\dagger$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{Bit flip} \quad \begin{array}{l} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{array}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{Phase flip} \quad \begin{array}{l} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow -|1\rangle \end{array}$$

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

$$R_\theta = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

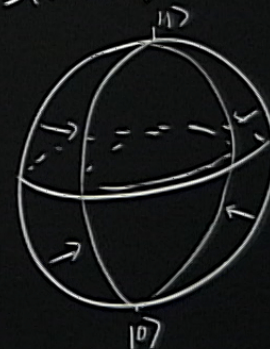
$$\begin{array}{l} |0\rangle \rightarrow i|1\rangle \\ |1\rangle \rightarrow -i|0\rangle \end{array}$$

Dephasing channel:

$$S(\rho) = (1-p)\rho + pZ\rho Z$$

$$p = \frac{1}{2}: |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

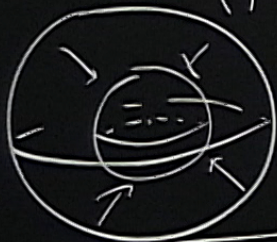
$$S(|\psi\rangle\langle\psi|) = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$$



Depolarizing channel:

$$S(\rho) = (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z$$

$$= (1 - \frac{4}{3}p)\rho + \frac{4}{3}p(\frac{I}{2})$$



Pauli channel:

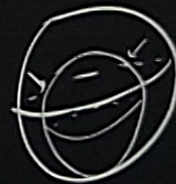
$$S(\rho) = (1-p_x-p_y-p_z)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$$

Amplitude damping channel:

$$S(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger$$

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 0 & \gamma \\ 0 & 0 \end{pmatrix}$$



Def. Let $M = M_1 \otimes M_2 \otimes \dots \otimes M_n$. The weight of M is the $\text{wt}(M)$ number of non-identity tensor factors. A CPTP on n qubits that can be written w/ Kraus operators each of which is a sum of operators w/ $\text{wt} \leq t$, is a t -qubit error.

Def. Let $M = M_1 \otimes M_2 \otimes \dots \otimes M_n$. The weight of M is the number of non-identity tensor factors. A CPTP on n qubits that can be written w/ Kraus operators each of which is a sum of operators w/ $wt < t$, is a t -qubit error.

Prob. p per bit of error
Prob. of bit flips on t bits: $\binom{n}{t} p^t (1-p)^{n-t}$
 $n \gg 1 \Rightarrow$ peaked at $t \approx pn$

Thm. Let $\mathcal{E}$ be a single-qubit quantum channel close to the identity $\|\mathcal{E} - I\|_\diamond < \epsilon$ (for small ϵ). Then $\exists$ t -qubit error channel $\tilde{\mathcal{E}}$ s.t.
 $\|\mathcal{E}^{\otimes n} - \tilde{\mathcal{E}}\|_\diamond = O\left(\binom{n}{t+1} \epsilon^{t+1}\right)$

Repetition code

$$0 \rightarrow 000$$

$$1 \rightarrow 111$$

$$010 \rightarrow 000$$

Quantum repetition code

$$|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$$

No cloning theorem

Barriers to QECC:

1) No cloning

2) Measuring qubits to identify errors would collapse superpositions

3) Need to correct phase errors as well as bit flips

4) Need to handle continuous rotations, decohering maps,...

$$|0\rangle \rightarrow |000\rangle$$

$$|1\rangle \rightarrow |111\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

$$\neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

B: + flip on 2nd qubit

$$\rightarrow \alpha|010\rangle + \beta|101\rangle$$

$$|0\rangle \rightarrow |000\rangle$$

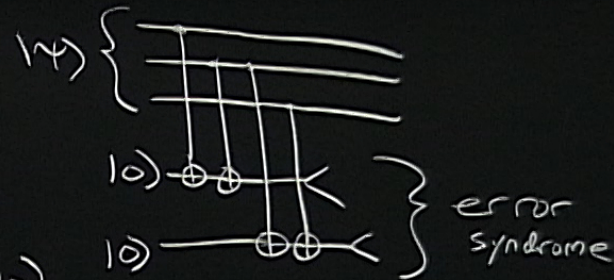
$$|1\rangle \rightarrow |111\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

$$\neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

Bit flip on 2nd qubit

$$\rightarrow \alpha|010\rangle + \beta|101\rangle$$



00	no error
10	1st qubit
01	3rd qubit
11	2nd qubit

Phase error correction:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$X|+\rangle = |+\rangle \quad Z|+\rangle = |-\rangle$$

$$X|-\rangle = -|-\rangle \quad Z|-\rangle = |+\rangle$$

$$|0\rangle \rightarrow |+\rangle|+\rangle|+\rangle$$

$$|1\rangle \rightarrow |-\rangle|-\rangle|-\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|+++\rangle + \beta|---\rangle$$



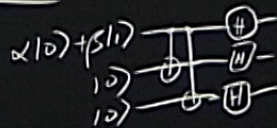
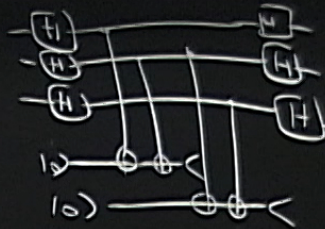
Phase error correction:

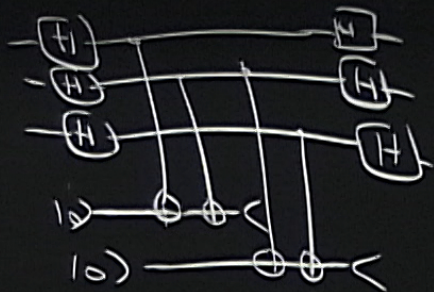
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\begin{aligned} X|+\rangle &= |+\rangle & Z|+\rangle &= |-\rangle \\ X|-\rangle &= -|-\rangle & Z|-\rangle &= |+\rangle \end{aligned}$$

$$\begin{aligned} |0\rangle &\rightarrow |+\rangle|+\rangle|+\rangle \\ |1\rangle &\rightarrow |-\rangle|-\rangle|-\rangle \\ \alpha|0\rangle + \beta|1\rangle &\rightarrow \alpha|+++ \rangle + \beta|--- \rangle \end{aligned}$$



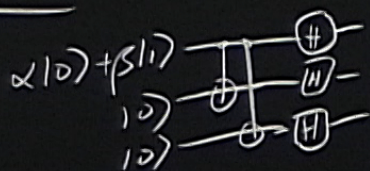


9-qubit code
(Shor):

$$|\bar{0}\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|\bar{1}\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Corrects X : look in each set of 3
Corrects Z : compare phases between sets of 3.

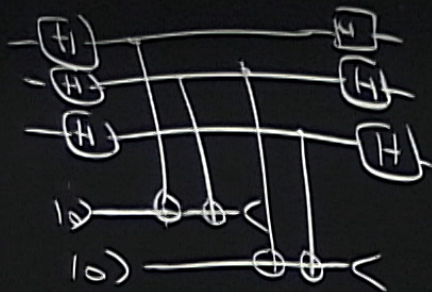


Repetition

0 → 00

1 → 11

Qua



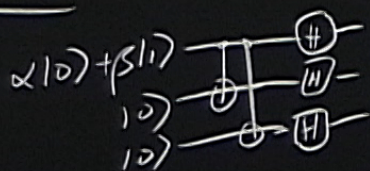
9-qubit code
(Shor):

$$|\bar{0}\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|\bar{1}\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Corrects X: look in each set of 3
Corrects Z: compare phases between sets of 3.

Corrects Y: Do both



Repetition

0 → 00

1 → 11

Quant

$$R_{\theta} = \cos \theta \underline{I} - i \sin \theta \underline{Z} \quad \text{error}$$

$$R_{\theta}^{(i)} |\psi\rangle = \cos \theta |\psi\rangle - i \sin \theta \underline{Z}^{(i)} |\psi\rangle$$

$$R_{\theta}^{(i)} |\psi\rangle |0\rangle \xrightarrow{\text{extract syndrome}} \cos \theta |\psi\rangle | \text{no error} \rangle - i \sin \theta \underline{Z}^{(i)} |\psi\rangle | \underline{Z}^{(i)} \rangle$$

Measure syndrome Prob. $|\cos^2 \theta|$: no error, $|\psi\rangle$

Prob. $|\sin^2 \theta|$: error $\underline{Z}^{(i)}$, $\underline{Z}^{(i)} |\psi\rangle$

Quantum Error Correction and Fault Tolerance

Class web page: <http://perimeterinstitute.ca/personal/dgottesman/QECC2018>

Def: A QECC $(U, \mathcal{C})$ is unitary encoding map $U: \mathcal{H}^K \rightarrow \mathcal{H}^N$
with set $\mathcal{C}$ of correctable errors st.

$\exists$ quantum channel $\mathcal{D}$ (decoder) st. $\forall E \in \mathcal{C}, \forall |\psi\rangle \in \mathcal{H}^K$

$$\mathcal{D}(E U |\psi\rangle \langle \psi| U^\dagger E^\dagger) = c(E, |\psi\rangle) |\psi\rangle \langle \psi|$$

The code corrects E if $E \in \mathcal{C}$.

Quantum Error Correction and Fault Tolerance

Class web page: <http://perimeterinstitute.ca/personal/dgottesman/QECC2018>

Def: A QECC $(U, \mathcal{C})$ is unitary encoding map $U: \mathcal{H}^K \rightarrow \mathcal{H}^N$ with set $\mathcal{C}$ of correctable errors st.

$\exists$ quantum channel $\mathcal{D}$ (decoder) st. $\forall E \in \mathcal{C}, \forall |\psi\rangle \in \mathcal{H}^K$

$$\mathcal{D}(E U |\psi\rangle \langle \psi| U^\dagger E^\dagger) = c(E, |\psi\rangle) |\psi\rangle \langle \psi|$$

The code corrects E if $E \in \mathcal{C}$.

Usually $N=2^n, K=2^k$

logical Hilbert space

physical Hilbert space

Thm If a QECC corrects E and F , it also corrects $\alpha E + \beta F$

Cor A QECC that corrects all weight $\leq t$ tensor products of I, X, Y, Z corrects any t -qubit error.

CAUTION

$$\{E_b|\psi\rangle\}$$

To distinguish E_a & E_b ,

$$\langle\phi|E_a^\dagger E_b|\psi\rangle = \delta_{ab} \langle\phi|\psi\rangle$$

(sufficient for Paulis)

$$\{E_b|\psi\rangle\}$$

To distinguish E_a & $E_b \in \mathcal{E}$,

$$\langle \phi | E_a^\dagger E_b | \psi \rangle = c_a \delta_{ab} \langle \phi | \psi \rangle$$

(sufficient conditions)

$\{F_a\}$ basis for $\mathcal{E}$

$$F_a = \sum_c \alpha_{ac} E_c$$

$$\begin{aligned} \langle \phi | F_a^\dagger F_b | \psi \rangle &= \sum_{cd} \alpha_{ac}^* \alpha_{bd} \langle \phi | E_c^\dagger E_d | \psi \rangle \\ &= \sum_d \alpha_{ad}^* \alpha_{bd} c_d \langle \phi | \psi \rangle = c_{ab} \langle \phi | \psi \rangle \end{aligned}$$

Thm. A subspace Q is a QEC for the set of errors $\mathcal{E}$ iff $\langle \phi | E_a^\dagger E_b | \psi \rangle = c_{ab} \langle \phi | \psi \rangle$

$\forall |\phi\rangle, |\psi\rangle \in Q, \forall E_a, E_b \in \mathcal{E}$

Note that c_{ab} don't depend on $|\psi\rangle$ or $|\phi\rangle$

$$= \left(\sum_d \alpha_{ad} \alpha_{bd} \right) d$$

Thm: For subspace Q , ^{linear space} errors $\mathcal{C}$, the following are equivalent

$$1) \langle \phi | E_a^\dagger E_b | \psi \rangle = c_{ab} \langle \phi | \psi \rangle \quad \forall |\phi\rangle, |\psi\rangle \in Q, \text{ basis } \{E_a\} \text{ of } \mathcal{C}$$

$$2) \langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = c_{ab} \delta_{ij}$$

$$3) \langle \psi | E_a^\dagger E_b | \psi \rangle = c_{ab}$$

$$4) \langle \psi | E^\dagger E | \psi \rangle = c(E)$$

for basis $\{|\psi_i\rangle\}$ of Q , basis $\{E_a\}$ of $\mathcal{C}$

$\forall |\psi\rangle \in Q$, basis $\{E_a\}$ of $\mathcal{C}$

$\forall |\psi\rangle \in Q, \forall E \in \mathcal{C}$

$$= \sum_d \alpha_d \alpha_{bd} \alpha_d \langle \psi | \psi \rangle = C_{ab} \langle \psi | \psi \rangle$$

Thm: For subspace Q , ^{linear space} errors E , the following are equivalent

- 1) $\langle \phi | E_a^\dagger E_b | \psi \rangle = C_{ab} \langle \phi | \psi \rangle \quad \forall |\phi\rangle, |\psi\rangle \in Q$, basis $\{E_a\}$ of E
- 2) $\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij}$ for basis $\{|\psi_i\rangle\}$ of Q , basis $\{E_a\}$ of E
- 3) $\langle \psi | E_a^\dagger E_b | \psi \rangle = C_{ab} \quad \forall |\psi\rangle \in Q$, basis $\{E_a\}$ of E
- 4) $\langle \psi | E^\dagger E | \psi \rangle = C(E) \quad \forall |\psi\rangle \in Q, \forall E \in E$

Def: Let Q be a subspace of an n -qubit Hilbert space. The distance of Q is the minimum weight d of a tensor product F such that $\langle \psi | F | \psi \rangle \neq C(F)$.

If $\dim Q = K$, we say this is an $((n, K, d))$ code.

To correct t -qubit errors, we want a code of distance $\geq 2t+1$.

Thm: For subspace Q , ^{linear space} errors $\mathcal{C}$, the following are equivalent

$$1) \langle \phi | E_a^\dagger E_b | \psi \rangle = c_{ab} \langle \phi | \psi \rangle \quad \forall |\phi\rangle, |\psi\rangle \in Q, \text{ basis } \{E_a\} \text{ of } \mathcal{C}$$

$$2) \langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = c_{ab} \delta_{ij}$$

$$3) \langle \psi | E_a^\dagger E_b | \psi \rangle = c_{ab}$$

$$4) \langle \psi | E^\dagger E | \psi \rangle = c(E)$$

for basis $\{|\psi_i\rangle\}$ of Q , basis $\{E_a\}$ of $\mathcal{C}$

$\forall |\psi\rangle \in Q$, basis $\{E_a\}$ of $\mathcal{C}$

$\forall |\psi\rangle \in Q, \forall E \in \mathcal{C}$

Def: Let Q be a subspace of an n -qubit Hilbert space. The distance of Q is the minimum weight d of a tensor product F such that

$$\langle \psi | F | \psi \rangle \neq c(F)$$

If $\dim Q = K$, we say this is an $((n, K, d))$ code.

To correct t -qubit errors, we want a code of distance $\geq 2t+1$.

Thm: If a QECC corrects E and F , it also corrects EF

Cor: A QECC that corrects all weight ≤ 1 tensor products of I, X, Y, Z corrects any 1-qubit error.

Def. An erasure error is an error on a known set of qubits

$\{E_a\}$ is constrained to the erased qubits

$$\text{wt}(E_a^\dagger E_b) \leq \# \text{ of erased qubits}$$

Cor. A distance d code corrects $d-1$ erasure errors.

Cor. A QECC $\mathcal{Q}$ corrects for erasures on a set S of qubits
iff $\text{tr}_S |\Psi\rangle\langle\Psi|$ is independent of $|\Psi\rangle \in \mathcal{Q}$

Def. An erasure error is an error on a known set of qubits

$\{E_a\}$ is constrained to the erased qubits

$$\text{wt}(E_a^\dagger E_b) \leq \# \text{ of erased qubits}$$

Cor. A distance d code corrects $d-1$ erasure errors.

Cor. A QECC $\mathcal{Q}$ corrects for erasures on a set S of qubits
iff $\text{tr}_S |\Psi\rangle\langle\Psi|$ is independent of $|\Psi\rangle \in \mathcal{Q}$
 $\uparrow$
 $\langle\Psi|E|\Psi\rangle$ independent of $|\Psi\rangle \forall E$ acting on S

Def. A QECC is degenerate if C_{ab} is not full rank when $\{E_a\}$ are linearly independent errors. Otherwise it is non-degenerate.

$$E.g. : E|\psi\rangle = F|\psi\rangle \rightarrow (E-F)|\psi\rangle = 0$$