Quantum computation

Lectures 20b-21

Reversible operations and quantum error correction

Setting:

Quantum operation $\mathcal{Q} = \underbrace{\sum_\alpha A_\alpha \odot A_\alpha^\dagger}_{\text{Kraus decomposition}} = \sum_\alpha |A_\alpha)(A_\alpha|$

A_α are Kraus operators

$$\rho' = \frac{\mathcal{Q}(\rho)}{\mathrm{tr}(\mathcal{Q}(\rho))}, \quad \mathrm{tr}(\mathcal{Q}(\rho)) = \begin{pmatrix}\text{probability for "outcome"} \\ \text{corresponding to } \mathcal{Q}\end{pmatrix} \le 1 \quad \forall \rho$$

$$\mathrm{tr}(\mathcal{Q}^*(I)\rho), \quad \mathcal{Q}^* = \sum_\alpha A_\alpha^\dagger \odot A_\alpha$$

$$\Longleftrightarrow \quad \mathcal{Q}^*(I) = \sum_\alpha A_\alpha^\dagger A_\alpha \le I$$

Trace-preserving operation: $\mathrm{tr}(\mathcal{Q}(\rho)) = 1 \quad \forall \rho$

$$\Longleftrightarrow \quad \mathcal{Q}^*(I) = \sum_\alpha A_\alpha^\dagger A_\alpha = I$$

① Measurement model:

$$\mathcal{Q}(\rho) = \mathrm{tr}_A\left(P_A\, U(\rho \otimes \sigma) U^\dagger\right) \qquad \sigma = \sum_l \lambda_l |f_l\rangle\langle f_l|, \quad P_A = \sum_k |g_k\rangle\langle g_k|$$

$$= \sum_{k,l} \underbrace{\sqrt{\lambda_l}\langle g_k|U|f_l\rangle}_{A_{kl} = A_\alpha}\, \rho\, \underbrace{\langle f_l|U^\dagger|g_k\rangle\sqrt{\lambda_l}}_{A_{kl}^\dagger = A_\alpha^\dagger}$$

$$= \sum_\alpha A_\alpha \rho A_\alpha^\dagger$$

② Extension: $\mathcal{I}_R \otimes \mathcal{Q}(\rho_{RQ}) \ge 0 \quad \forall R$ and $\forall \rho^{RQ}$

$$\sum_\alpha I_R \otimes A_\alpha\, \rho_{RQ}\, I_R \otimes A_\alpha^\dagger$$

$$|\tilde{\Psi}\rangle = \sum_j \underset{\substack{\uparrow \\ R}}{|f_j\rangle} \otimes \underset{\substack{\uparrow \\ Q}}{|e_j\rangle}$$

Jamiolkowski isomorphism

$$(\mathcal{I}_R \otimes \mathcal{A})(|\tilde{\Psi}\rangle\langle\tilde{\Psi}|) = \sum_{j,k} |f_j\rangle\langle f_k| \otimes \underbrace{\mathcal{A}(|e_j\rangle\langle e_k|)}_{\text{specifies } \mathcal{A}}$$

$$= \sum_\alpha I_R \otimes A_\alpha |\tilde{\Psi}\rangle\langle\tilde{\Psi}| I_R \otimes A_\alpha^\dagger$$

Reversing an operation

Code subspace $\mathcal{C}$, projector P_C

<u>T-p</u> reversal op $\mathcal{R}$

$\mathcal{A}$ is reversible on $\mathcal{C}$ if $\exists$ t-p $\mathcal{R}$ such that

$$\underbrace{\mathcal{R}\left(\frac{\mathcal{A}(\rho)}{\mathrm{tr}(\mathcal{A}(\rho))}\right) = \rho}\quad \forall\ \rho \text{ such that } P_C \rho P_C = \rho$$

$$\mathcal{R}\circ\mathcal{A}(\rho) = \rho\, \mathrm{tr}(\mathcal{A}(\rho)) \longrightarrow$$

Linearity of $\mathcal{R}\circ\mathcal{A}$ $\Rightarrow \mathrm{tr}(\mathcal{A}(\rho)) = \mu^2 = \text{const}$ $\forall\ \rho = P_C \rho P_C$.

Assume $\mu^2 \neq 0$

Define $\mathcal{A}_C = \mathcal{A}\circ P_C \odot P_C$

$\rightarrow \mathcal{R}\circ\mathcal{A}_C = \mu^2 P_C \odot P_C$ is a <u>pure</u> operation. (not t-p if $\mu^2 < 1$ or $\mathcal{C}$ is not entire space)

<u>Theorem:</u> $\mathcal{A} = \sum_\alpha A_\alpha \odot A_\alpha^\dagger$ is reversible on $\mathcal{C}$ iff

$$P_C A_\beta^\dagger A_\alpha P_C = \mu^2 m_{\alpha\beta} P_C,$$

Notice that $\boxed{P_C\left(\sum_\alpha A_\alpha^\dagger A_\alpha\right)P_C = \mu^2 P_C}$

where m is a unit-trace, positive matrix and $\mu^2 \le 1$.

Discussion: Let $|e_j\rangle$ be an orthonormal basis on C. Then the condition is

$$\langle e_j | A_\beta^\dagger A_\alpha | e_k \rangle = \mu^2 m_{\alpha\beta} \delta_{jk} .$$

The Kraus "error operators" A_α act like multiples of a unitary on C, but they don't have to map to $\perp$ subspaces. A unitary remixing transforms m unitarily, i.e., $B_\alpha = \sum_\beta V_{\alpha\beta} A_\beta \Longrightarrow \langle e_j | B_\beta^\dagger B_\alpha | e_k \rangle = \mu^2 \delta_{jk} \sum_{\gamma,\delta} V_{\alpha\gamma} m_{\gamma\delta} V_{\beta\delta}^*$.

Proof:

$\Longrightarrow$ Necessity: $\mathcal{R} \circ \mathcal{A}_C$ is a pure operation with Kraus operators μP_C or $R_\beta A_\alpha P_C$, so

$$R_\beta A_\alpha P_C = c_{\alpha\beta} \mu P_C , \quad \text{where} \sum_{\alpha,\beta} |c_{\alpha\beta}|^2 = 1$$

But then

$$P_C A_\beta^\dagger A_\alpha P_C = \sum_\gamma P_C A_\beta^\dagger R_\gamma^\dagger R_\gamma A_\alpha P_C = \mu^2 P_C \underbrace{\sum_\gamma c_{\alpha\gamma} c_{\beta\gamma}^*}_{(cc^\dagger)_{\alpha\beta}}$$

$$m = cc^\dagger \ge 0 \quad \text{and} \quad \mathrm{tr}(m) = \sum_{\alpha,\beta} |c_{\alpha\beta}|^2 = 1 .$$

$\Longleftarrow$ Sufficiency: We'll construct a reversal operation. To do that, let

u diagonalize m, i.e.,

$$\sum_{\gamma,\delta} u_{\alpha\gamma} m_{\gamma\delta} u^*_{\beta\delta} = \underset{\substack{\uparrow \\ \text{eigenvalues of } m}}{d_\alpha} \delta_{\alpha\beta} \qquad \sum_\alpha d_\alpha = 1, \quad d_\alpha \geq 0$$

$\langle e_j | \tilde{A}^\dagger_\beta \tilde{A}_\alpha | e_k \rangle = \mu^2 d_\alpha \delta_{\alpha\beta} \delta_{jk}$

Canonical error operators with $d_\alpha \neq 0$ map unitarily to orthogonal subspaces

Define new, <u>canonical</u> error operators

$$\tilde{A}_\alpha = \sum_\beta u_{\alpha\beta} A_\beta \implies \mathcal{R} = \sum_\alpha \tilde{A}_\alpha \odot \tilde{A}^\dagger_\alpha$$

$$P_C \tilde{A}^\dagger_\beta \tilde{A}_\alpha P_C = \sum_{\gamma,\delta} u_{\alpha\gamma} u^*_{\beta\delta} \underbrace{P_C A^\dagger_\delta A_\gamma P_C}_{\mu^2 m_{\gamma\delta} P_C} = \mu^2 d_\alpha \delta_{\alpha\beta} P_C$$

The operators with $d_\alpha = 0$ are irrelevant on C. The other operators map unitarily to orthogonal subspaces. We construct $\mathcal{R}$ from these unitaries, obtained formally from the polar decomposition.

$\alpha = \beta$: $P_C \tilde{A}^\dagger_\alpha \tilde{A}_\alpha P_C = \mu^2 d_\alpha P_C$

$$\xRightarrow{\text{polar decomp}} \tilde{A}_\alpha P_C = U_\alpha \sqrt{P_C \tilde{A}^\dagger_\alpha \tilde{A}_\alpha P_C} = \mu \sqrt{d_\alpha}\, U_\alpha P_C$$

$d_\alpha \neq 0$: U_α maps C to $\underset{\substack{\uparrow \\ \text{orthogonal subspaces}}}{C_\alpha}$ with projector $P_\alpha = U_\alpha P_C U^\dagger_\alpha$.

$$\mu^2 \sqrt{d_\alpha d_\beta}\, P_C U^\dagger_\beta U_\alpha P_C = \mu^2 d_\alpha \delta_{\alpha\beta} P_C$$

$$P_C U^\dagger_\beta U_\alpha P_C = \delta_{\alpha\beta} P_C$$

$$\implies P_\beta P_\alpha = U_\beta P_C U^\dagger_\beta U_\alpha P_C U^\dagger_\alpha = \delta_{\alpha\beta} P_\alpha$$

$$Q_c = \sum_\alpha \tilde{A}_\alpha P_c \odot P_c \tilde{A}_\alpha^\dagger = \mu^2 \sum_\alpha d_\alpha U_\alpha P_c \odot P_c U_\alpha^\dagger$$

convex combination

Let $D = \bigoplus_{\{\alpha | d_\alpha \neq 0\}} C_\alpha$ and $\bar{D}$ be the orthocomplement of D.

The projector onto $\bar{D}$ is

$$P_{\bar{D}} = I - P_D = I - \sum_{\{\alpha | d_\alpha \neq 0\}} P_\alpha$$

Define

$$R = \sum_{\{\alpha | d_\alpha \neq 0\}} \overbrace{U_\alpha^\dagger P_\alpha}^{P_c U_\alpha^\dagger} \odot \overbrace{P_\alpha U_\alpha}^{U_\alpha P_c} + P_{\bar{D}} \odot P_{\bar{D}}$$

Is it t-p? $\sum_{\{\alpha | d_\alpha \neq 0\}} P_\alpha U_\alpha U_\alpha^\dagger P_\alpha + P_{\bar{D}} P_{\bar{D}} = \sum_{\{\alpha | d_\alpha \neq 0\}} P_\alpha + P_{\bar{D}} = I$ ✓

Does it reverse?

$$R \circ Q_c = \mu^2 \sum_{\substack{\{\alpha | d_\alpha \neq 0\} \\ \beta}} d_\beta \overbrace{P_c U_\alpha^\dagger U_\beta P_c}^{\delta_{\alpha\beta} P_c} \odot P_c U_\beta^\dagger U_\alpha P_c$$

$$+ \cancelto{0}{\mu^2 \sum_\beta d_\beta P_{\bar{D}} \underbrace{U_\beta P_c}_{P_\beta U_\beta^\dagger} \odot P_c U_\beta^\dagger P_{\bar{D}}}$$

$$= \mu^2 P_c \odot P_c \underbrace{\sum_\beta d_\beta}_{1}$$

$$= \mu^2 P_c \odot P_c \quad ✓$$

Discussion

① Measurement-based vs. coherent error correction. Can measure canonical error α and correct classically, or can run the whole thing coherently using ancillae.

② Canonical error basis:

$$P_c \tilde{A}_\beta^\dagger \tilde{A}_\alpha P_c = \mu^2 d_\alpha \delta_{\alpha\beta} P_c \Rightarrow \mathrm{tr}(\tilde{A}_\alpha P_c \tilde{A}_\beta^\dagger) = \mu^2 d_\alpha \delta_{\alpha\beta} \mathrm{tr}(P_c)$$

Let $\rho_c = P_c/\mathrm{tr}(P_c)$ be the unit density operator on the code subspace. Then we have

$$\mu^2 d_\alpha \delta_{\alpha\beta} = \mathrm{tr}(\tilde{A}_\alpha \rho_c \tilde{A}_\beta^\dagger) = (\tilde{A}_\beta \sqrt{\rho_c} | \tilde{A}_\alpha \sqrt{\rho_c})$$

The operators $\tilde{A}_\alpha \sqrt{\rho_c} = \mu \sqrt{d_\alpha}\, U_\alpha \sqrt{\rho_c}$ with $d_\alpha \neq 0$ make up an orthogonal set of Kraus operators for the operation $\mathcal{Q}_{\rho_c} = \mathcal{Q} \circ \sqrt{\rho_c} \otimes \sqrt{\rho_c} = \sum_\alpha \tilde{A}_\alpha \sqrt{\rho_c} \odot \sqrt{\rho_c} \tilde{A}_\alpha^\dagger$. They are the eigenoperators in the left-right sense of $\mathcal{Q}_{\rho_c}$, with eigenvalues $\mu^2 d_\alpha$.

Notice that any $\rho = P_c \rho P_c$ could be used in place of ρ_c, i.e.,

$$\mathcal{Q}_\rho = \mathcal{Q} \circ \sqrt{\rho} \otimes \sqrt{\rho} = \sum_\alpha \tilde{A}_\alpha \sqrt{\rho} \odot \sqrt{\rho} \tilde{A}_\alpha^\dagger \qquad \mathcal{Q}_\rho(I) = \mathcal{Q}(\rho)$$

$$(\tilde{A}_\beta \sqrt{\rho} | \tilde{A}_\alpha \sqrt{\rho}) = \mathrm{tr}(\sqrt{\rho} \tilde{A}_\beta^\dagger \tilde{A}_\alpha \sqrt{\rho}) = \mathrm{tr}(\tilde{A}_\alpha \rho \tilde{A}_\beta^\dagger)$$

$$= \mathrm{tr}(\rho \underbrace{P_c \tilde{A}_\beta^\dagger \tilde{A}_\alpha P_c}_{\mu^2 d_\alpha \delta_{\alpha\beta} P_c})$$

$$= \mu^2 d_\alpha \delta_{\alpha\beta}$$

(3) $\mathcal{Q}_c$ as an isometry

$$\mathcal{Q}_c = \sum_\alpha A_\alpha P_c \odot P_c A_\alpha^\dagger = \mu^2 \sum_\alpha d_\alpha U_\alpha P_c \odot P_c U_\alpha^\dagger$$

$$= \mu^2 \sum_\alpha d_\alpha P_\alpha U_\alpha \odot U_\alpha^\dagger P_\alpha$$

$$\mathcal{Q}_c^* = \sum_\alpha P_c A_\alpha^\dagger \odot A_\alpha P_c = \mu^2 \sum_\alpha d_\alpha P_c U_\alpha^\dagger \odot U_\alpha P_c$$

$$= \mu^2 \sum_\alpha d_\alpha U_\alpha^\dagger P_\alpha \odot P_\alpha U_\alpha$$

cf. $\mathcal{R}_D = \mathcal{R}_0 \circ P_D \odot P_D$

$$= \sum_{\{\alpha | d_\alpha \neq 0\}} U_\alpha^\dagger P_\alpha \odot P_\alpha U_\alpha$$

$$= \sum_{\{\alpha | d_\alpha \neq 0\}} P_c U_\alpha^\dagger \odot U_\alpha P_\alpha$$

$$\mathcal{Q}_c^* \circ \mathcal{Q}_c = \mu^4 \sum_{\alpha,\beta} d_\alpha d_\beta \underbrace{U_\alpha^\dagger \underbrace{P_\alpha P_\beta}_{\delta_{\alpha\beta} P_\alpha} U_\beta}_{\delta_{\alpha\beta} P_c U_\alpha^\dagger U_\alpha = \delta_{\alpha\beta} P_c} \odot U_\beta^\dagger P_\beta P_\alpha U_\alpha$$

$$= \mu^4 \sum_{\alpha,\beta} d_\alpha^2 \; P_c \odot P_c \longleftarrow \text{This is iff for reversibility}$$

(4) Uniqueness of reversal operation restricted to D

Let $\mathcal{S} = \sum_\beta S_\beta \odot S_\beta^\dagger$ be an arbitrary reversal operation, i.e.,

$$\mathcal{S} \circ \mathcal{A}_C = \mu^2 P_C \odot P_C \implies \mu \tilde{c}_{\alpha\beta} P_C = S_\beta \tilde{A}_\alpha P_C = \mu \sqrt{d_\alpha}\, S_\beta U_\alpha P_C$$

use the canonical error operators

$\tilde{A}_\alpha P_C = \mu \sqrt{d_\alpha}\, U_\alpha P_C$

$$(\tilde{C}\tilde{C}^\dagger)_{\alpha\beta} = d_\alpha \delta_{\alpha\beta}$$

$$1 = \sum_\alpha d_\alpha = \sum_{\alpha,\beta} |\tilde{c}_{\alpha\beta}|^2$$

$$S_\beta U_\alpha P_C = \frac{\tilde{c}_{\alpha\beta}}{\sqrt{d_\alpha}} P_C$$

If $d_\alpha = 0$, that row of $\tilde{c}_{\alpha\beta}$ has all zeroes. Discard it.

$$S_\beta U_\alpha P_C = S_\beta P_\alpha U_\alpha = V_{\beta\alpha} P_C , \quad V_{\beta\alpha} = \tilde{c}_{\alpha\beta}/\sqrt{d_\alpha}$$

$$\sum_\gamma V^*_{\gamma\alpha} V_{\gamma\beta} = \frac{1}{\sqrt{d_\alpha d_\beta}} \sum_\gamma \tilde{c}^*_{\alpha\gamma} \tilde{c}_{\beta\gamma}$$

$$= \frac{1}{\sqrt{d_\alpha d_\beta}} (\tilde{C}\tilde{C}^\dagger)_{\beta\alpha}$$

$$= \delta_{\alpha\beta}$$

V has orthonormal columns. Extend to a unitary by adding columns.

$$S_\beta P_\alpha = V_{\beta\alpha} P_C U_\alpha^\dagger = V_{\beta\alpha} U_\alpha^\dagger P_\alpha = V_{\beta\alpha} R_\alpha$$

$$\implies S_\beta P_D = \sum_\alpha S_\beta P_\alpha = \sum_\alpha V_{\beta\alpha} R_\alpha \implies \mathcal{J}_D = \mathcal{R}_D$$

8 Correcting all errors in operator subspace spanned by original errors A_α.

$$\mathcal{B} = \sum_\alpha B_\alpha \odot B_\alpha^\dagger \qquad B_\alpha = \sum_\beta b_{\alpha\beta} A_\beta$$

not unitary

Let $\rho = P_C \rho P_C$ be in code subspace. Then

$$\begin{aligned}
\mathcal{B}(\rho) &= \sum_\alpha B_\alpha \rho B_\alpha^\dagger \\
&= \sum_\alpha B_\alpha P_C \rho P_C B_\alpha^\dagger \\
&= \sum_{\alpha,\gamma,\delta} b_{\alpha\gamma} b^*_{\alpha\delta} A_\gamma P_C \rho P_C A_\delta^\dagger
\end{aligned}$$

$$\begin{aligned}
\mathcal{R} \circ \mathcal{Q}(\rho) &= \sum_{\alpha,\beta,\gamma,\delta} b_{\alpha\gamma} b^*_{\alpha\delta} \underbrace{R_\beta A_\gamma P_C}_{\mu c_{\gamma\beta} P_C} \rho \underbrace{P_C A_\delta^\dagger R_\beta}_{\mu c^*_{\delta\beta} P_C} \\
&= \mu^2 \left(\sum_{\alpha,\gamma,\delta} b_{\alpha\gamma} b^*_{\alpha\delta} (cc^\dagger)_{\gamma\delta} \right) P_C \rho P_C \\
&= \boxed{\mu^2 \rho \underbrace{\mathrm{tr}(bmb^\dagger)}_{\nu^2}}
\end{aligned}$$

Here we use the linear structure of an error-operator subspace, whereas when we construct codes, we use the multiplicative structure to generate, for example, a single-qubit Y error as $Y = iXZ$.

6 Degenerate vs. nondegenerate codes

A degenerate code and set of error operators is one such that the error operators $A_\alpha P_C$ are not l.i., i.e., m is not invertible. One can always make the code nondegenerate by discarding error operators. Notice that even for a nondegenerate code, the error operators $A_\alpha P_C$ need not be orthogonal, i.e., m need not be diagonal.

Nondegenerate is often used loosely to refer to the situation where orthogonal error operators A_α remain orthogonal when projected into C, i.e., $A_\alpha P_C$, which is a stronger requirement than the definition above.

7 Error analysis.

The general theory shows that $\mathcal{R}$ reverses any error that is a linear combination of the error operators A_α; this does not mean that any such error is a stochastic combination of the A_α. Specifically, for single-qubit errors, if one can correct I, X, Y, and Z errors, then one can correct any single-qubit error, but this does not mean that any single-qubit error is a stochastic combination of $I\otimes I$, $X\otimes X$, $Y\otimes Y$, and $Z\otimes Z$. This complicates general analyses of error probabilities.

⑧ Quantum Hamming bound.

Nd code encodes k logical qubits in N physical qubits.

$$\begin{pmatrix}\text{total \# of errors} \\ \text{on } t \text{ or fewer} \\ \text{qubits}\end{pmatrix} = \sum_{j=0}^{t} \binom{n}{j} 3^j$$

$$\sum_{j=0}^{t} \binom{n}{j} 3^j \times \underset{\substack{\uparrow \\ \text{k-qubit subspace} \\ \text{for each error}}}{2^k} \leq 2^N$$

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

$k=1$, $t=1$

$(1+3n) \leq 2^{N-1}$