QIC 890 / CO781 / CS 867, W24

Course website: https://www.math.uwaterloo.ca/~wcleung/qic890-w2024.html

Pre-requisite:

QIC 710, https://cleve.iqc.uwaterloo.ca/qic710/lecture-notes/index.html

- Primer chaps 1-4, 6, 8, 10, 11
- Quantum info theory chaps 1-7

Lecture 1: basics of quantum noise and quantum error correction

Part 1: Know your enemy

- Q state / info: $\rho \in B(\mathbb{C}^d)$

  $\rho \geq 0$, $tr \rho = 1$

  dim

  bounded operators from $\mathbb{C}^d$ to $\mathbb{C}^d$
  ie $d \times d$ matrices

- Q operations / Q channels / Admissible operations / CPTP maps / TCP maps

$$\mathcal{E}: B(\mathbb{C}^d) \longrightarrow B(\mathbb{C}^{d'})$$
$$\rho \longmapsto \mathcal{E}(\rho)$$

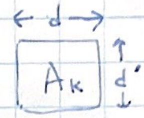
s.t

1. $\mathcal{E}$ linear
2. $\mathcal{E}$ trace preserving $(tr(\mathcal{E}(\rho)) = tr(\rho))$
3. $\mathcal{E}$ completely positive $(\forall \mu \geq 0, \; I \otimes \mathcal{E}(\mu) \geq 0)$

- Kraus representation:

Kraus operator

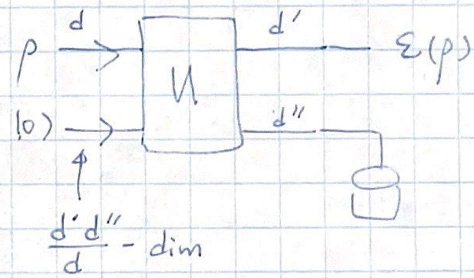
$$\mathcal{E} \text{ TCP map} \iff \mathcal{E}(\rho) = \sum_{k=1}^{\ell} A_k \rho A_k^{\dagger}, \quad \sum_{k=1}^{\ell} A_k A_k^{\dagger} = I_d$$



- Stinespring dilation:

$$\mathcal{E} \text{ TCP map} \iff \mathcal{E}(\rho) = \mathrm{tr}_E\, U \rho U^{\dagger}$$

for isometry $U : \mathbb{C}^d \to \mathbb{C}^{d'} \otimes \mathbb{C}^{d''}$



<u>Examples:</u>

(I) Unitary channels $(d = d')$ $(d'' = 1,\ \ell = 1)$

$$\mathcal{E}(\rho) = U \rho U^{\dagger}$$

eg, $d = d' = 2$, $\underbrace{U = I \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad Y = iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}}_{\text{Pauli ops}}$

no error, bit flip, phase flip, both

eg, $d = d' = 2$, $U = \begin{bmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{bmatrix} = e^{-i\theta Z} = R_Z(\theta)$

NB These are "noiseless" channels.

(II) Generalized Pauli channels:

$$\mathcal{E}(\rho) = p_X X\rho X + p_Y Y\rho Y + p_Z Z\rho Z + (1-p_X-p_Y-p_Z)\rho$$

$d = d' = 2, \quad l \leq 4.$

eg. Dephasing channel: $\mathcal{E}(\rho) = p\, Z\rho Z + (1-p)\rho \qquad (l=2)$

eg. Depolarizing channel: $\mathcal{E}(\rho) = \frac{q}{3}(X\rho X + Y\rho Y + Z\rho Z) + (1-q)\rho$

$$= \underbrace{\frac{4q}{3}\frac{I}{2}}_{\text{rubbish}} + \left(1-\frac{4q}{3}\right)\underbrace{\rho}_{\text{info.}} \qquad (l=4)$$

(III) Amplitude damping channel

$$\mathcal{E}(\rho) = A_0\rho A_0^\dagger + A_1\rho A_1^\dagger \qquad (l=2)$$

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$$

Let $U|0\rangle|0\rangle = |0\rangle|0\rangle$

$U|1\rangle|0\rangle = \sqrt{1-\gamma}\,|1 0\rangle + \underbrace{\sqrt{\gamma}\,|01\rangle}$ (second system: E)

$\mathcal{E}(\rho) = \mathrm{tr}_E(U\rho U^\dagger)$ $\qquad$ γ: prob leaking "$|1\rangle$" (excitation, photon) to the environment

(IV) Erasure channel

$\mathcal{E}(\rho) = (1-p)\rho + p\,|e\rangle\langle e|$

$\quad$ ↳ erasure symbol, orthogonal to input space

ie one can tell when there is an error.

$(d' = d+1)$

Ex: what is min l in the Kraus rep for the erasure channel?

Note the above exp NOT Kraus rep.

- Combining errors / channels :

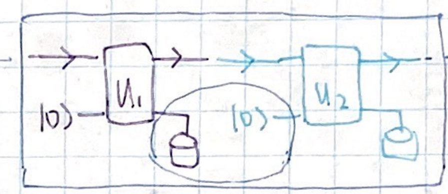
Let $\mathcal{E}_1(\rho) = \sum_k A_k \rho A_k^\dagger$, $\mathcal{E}_2(\sigma) = \sum_m B_m \sigma B_m^\dagger$

$d_1 \to d_1'$-dim $\qquad\qquad d_2 \to d_2'$-dim

(I) If $d_1' = d_2$, then $\mathcal{E}_2 \circ \mathcal{E}_1(\rho) := \mathcal{E}_2(\mathcal{E}_1(\rho)) = \sum_{k,m} B_m A_k \rho A_k^\dagger B_m^\dagger$

$$\rho \to \boxed{\mathcal{E}_1} \to \boxed{\mathcal{E}_2} \to \mathcal{E}_2 \circ \mathcal{E}_1(\rho)$$

$= \rho \to$



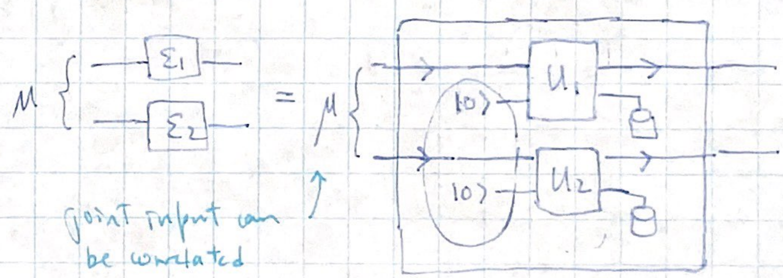
$\to \mathcal{E}_2 \circ \mathcal{E}_1(\rho)$

concatenation

memoryless

(II) Arbitrary dims, $\mathcal{E}_1 \otimes \mathcal{E}_2(\mu) = \sum_{k,m} \underbrace{(A_k \otimes B_m)\, \mu\, (A_k^\dagger \otimes B_m^\dagger)}_{d_1' d_2'\text{-dim}}$

μ: $d_1 d_2$-dim



joint input can be correlated

independent errors.

Origin of the magic behind error correction:

Approx of independent channels by low weight errors:

Consider n qubits. Def t-qubit error channel as follows:

Def 1: For a tensor product operator $A = A_1 \otimes A_2 \otimes \cdots \otimes A_n$ the weight of A, $wt(A)$, is the number of non-identity tensor components.

Def 2: For $B \in \mathcal{B}((\mathbb{C}^2)^{\otimes n})$, B is a t-qubit error if $B = \sum_i B_i$, $wt(B_i) \le t$ for all i.

Def 3: N is a t-qubit error channel if it has a Kraus rep with all Kraus operators being t-qubit errors.

eg $n=3$, $t=2$, $ZZ1$ & $1XX$ have weight 2 ($\otimes$ omitted)

$B = \frac{1}{\sqrt{2}}(ZZ1 + 1XX)$ is a 2-qubit error (but not wt 2)

$N(\rho) = (1-p)\rho + p B\rho B^\dagger$ is a 2-qubit error channel.

Def 4: N is an independent channel on n-qubits if $N = \bigotimes_{i=1}^{n} N_i$, $N_i : \mathcal{B}(\mathbb{C}^2) \to \mathcal{B}(\mathbb{C}^2)$

eg $N = \mathcal{E}^{\otimes n}$, $\mathcal{E}(\rho) = (1-p)\rho + p Z\rho Z$

$$
\begin{aligned}
N(\rho) = \; & II \cdots I \rho I \cdots I \; (1-p)^n \\
& \left.\begin{aligned} + \; & ZI \cdots I \rho Z \cdots I \; (1-p)^{n-1} p \\ & \vdots \\ + \; & II \cdots Z \rho I \cdots Z \; (1-p)^{n-1} p \end{aligned}\right\} \binom{n}{1} \text{ wt-1 errors} \\
& \left.\begin{aligned} + \; & ZZI \cdots I \rho ZZI \cdots I \; (1-p)^{n-2} p^2 \\ & \vdots \\ + \; & II \cdots ZZ \rho II \cdots ZZ \; (1-p)^{n-2} p^2 \end{aligned}\right\} \binom{n}{2} \text{ wt-2 errors} \\
& \vdots
\end{aligned}
$$

NB: $N(\rho)$ well approximated by keeping only Kraus operators with $wt \gg np$

This phenomenon holds generally for independent channels with low noise.

Thm: Let $\mathcal{I}$ be the qubit identity channel,

$$N_i = (1-p)\,\mathcal{I} + p\,\mathcal{E}_i \,, \quad \mathcal{E}_i \text{ arbitrary qubit channel}$$

$$N = \bigotimes_i N_i$$

Then, $\exists$ t-qubit error channel $\tilde{N}$ s.t. $\| N - \tilde{N} \|_\diamond \le \binom{n}{t+1} p^{t+1} \cdot 2$

Remarks:

① Diamond norm distance between N_1 and N_2:

$$\| N_1 - N_2 \|_\diamond = \max_{|\psi\rangle_{RA}} \| I_R \otimes N_{1A} (|\psi\rangle\langle\psi|) - I_R \otimes N_{2A} (|\psi\rangle\langle\psi|) \|_1$$

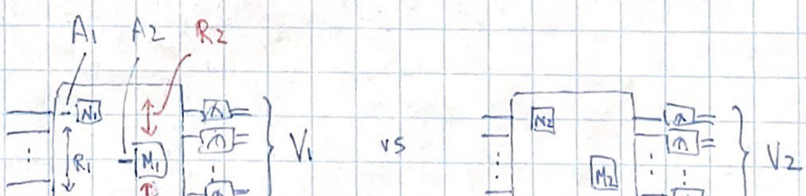
reference system, input to N_1, N_2

Schatten-1 norm = sum(abs(evals))

ⓐ Physically, if one of N_1, N_2 is applied to A uniformly, best probability to determine which N_i has been applied

$$= \frac{1}{2} + \frac{1}{4} \| N_1 - N_2 \|_\diamond$$

ⓑ Replacing N_1 by N_2 affects subsequent measurement statistics (in variation distance) by no more than $\| N_1 - N_2 \|_\diamond$. Furthermore, composing replacements → adding distance (approx is composable).



$$\| V_1 - V_2 \|_1 \le \| N_1 - N_2 \|_\diamond + \| M_1 - M_2 \|_\diamond$$

ⓒ System R crucial.

See Watrous book Sec 3.3.2 or corresponding lecture.

② If $\binom{n}{t+1} p^{t+1} \ll 1$, it suffices to correct t-qubit errors in $\tilde{N}$.

So, when is $\binom{n}{t+1} p^{t+1} \ll 1$?

Let $t+1 = np\alpha$. Use the fact $\binom{n}{np\alpha} \leq 2^{n\,h(p\alpha)}$, where

$h(x) = -x \log_2 x - (1-x)\log_2(1-x)$ = binary entropy function.

default base

Then $\binom{n}{t+1} p^{t+1} = \binom{n}{np\alpha} p^{np\alpha}$

$$\leq 2^{n[-p\alpha \log p\alpha - (1-p\alpha)\log(1-p\alpha)]}\, 2^{np\alpha \log p}$$

$$\leq 2^{n[-p\alpha \log\alpha + \frac{\sqrt{1-p\alpha}}{\ln 2}\cdot p\alpha]} \qquad \left(\text{use } \ln(1-x) \geq \frac{-x}{\sqrt{1-x}}\right)$$

$$= 2^{np\alpha\underbrace{(-\log\alpha + \sqrt{1-p\alpha}/\ln 2)}_{-\text{ve for } \alpha \geq e \doteq 2.7183}}$$

Pf of theorem uses the following:

- Lemma: If $t < n$, $0 \leq p \leq 1$, then $\sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j} \leq \binom{n}{t+1} p^{t+1}$

Pf: Toss a coin n times, prob(head) $= p$.

LHS = prob($t+1$ heads or more)

$$\underset{\text{union bound}}{\leq} \sum_{\substack{\text{subset of } \{1,\dots,n\} \\ \text{of size } t+1}} \text{prob(all heads in subset)}$$

$$= \binom{n}{t+1} \times p^{t+1}.$$

- Proof of theorem:

$$N = \bigotimes_i \left[(1-p)\, I \otimes p\, \mathcal{E}_i \right]$$

$$= (1-p)^n I^{\otimes n} + (1-p)^{n-1} p \left[\mathcal{E}_1 \otimes I^{\otimes(n-1)} + I \otimes \mathcal{E}_2 \otimes I^{\otimes(n-2)} + \dots + I^{\otimes(n-1)} \otimes \mathcal{E}_n \right]$$

$$+ (1-p)^{n-2} p^2 \left[\mathcal{E}_1 \otimes \mathcal{E}_2 \otimes I^{\otimes(n-2)} + \dots + I^{\otimes n-2} \otimes \mathcal{E}_{n-1} \otimes \mathcal{E}_n \right]$$

$$+ \dots + p^n \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \dots \otimes \mathcal{E}_n$$

To obtain $\tilde{N}$, if a term above has $t+1$ or more $\mathcal{E}_i$'s, replace all $\mathcal{E}_i$'s by I.

$$\| N - \tilde{N} \|_\diamond \le (1-p)^{n-t-1} p^{t+1} \| \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \dots \otimes \mathcal{E}_{t+1} \otimes I^{\otimes n-t-1} - I^{\otimes n} \|_\diamond$$

$$+ (1-p)^{n-t-1} p^{t+1} \| \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \dots \otimes \mathcal{E}_t \otimes I \otimes \mathcal{E}_{t+1} \otimes I^{\otimes n-t-2} - I^{\otimes n} \|_\diamond$$

$$+ \vdots$$

$$+ p^n \| \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \dots \otimes \mathcal{E}_n - I^{\otimes n} \|_\diamond$$

$$\le 2 \sum_{j=t+1}^{n} \binom{n}{j} (1-p)^{n-j} p^j \underset{\text{Lemma}}{\le} 2 \cdot \binom{n}{t+1} p^{t+1}.$$

NB: N_i very special in theorem. An extension holds in general:

<u>Thm'</u> If $\forall i$ $\| N_i - I \|_\diamond < \epsilon \le \frac{t+1}{n-t-1}$ and $\epsilon \le \frac{1}{3}$, $N = \bigotimes_{i=1}^n N_i$

then $\exists \tilde{N}$ t-qubit error <u>map</u> (not-necessarily trace preserving)

s.t. $\| N - \tilde{N} \|_\diamond \le 5 \binom{n}{t+1} \left[(4e+2)\epsilon \right]^{t+1}$

Similar to Thm up to constants.

Pf: omitted. Idea: each N_i has a Kraus operator $A_0^i \approx I \cdot \beta$, β large

ⓐ Keep only Kraus operators in N with at most t Kraus ops NOT A_0^i

ⓑ Expand each $A_0^i = I \cdot \beta + \dots$

ⓒ Truncate to wt t again.