QIC 890 / CO781 / CS 867, W22

Lec 1 : Know your enemy

References :

QIC 710, F2019, http://cleve.iqc.uwaterloo.ca/styled-26/index.html
Lectures 10-11, 12, 15

F2021, http://cleve.iqc.uwaterloo.ca/qic710/styled-7/index.html
Part 3, Quantum information theory I, II

QIC 820, F2011, https://cs.uwaterloo.ca/~watrous/TQI-notes/
Lecture 5. Naimark's theorem; char of channels

- Q state / info : $\rho \in B(\mathbb{C}^d)$
  - $\rho \geq 0, \operatorname{tr}\rho = 1$
  - $B(\mathbb{C}^d)$: bounded operators from $\mathbb{C}^d$ to $\mathbb{C}^d$, ie $d \times d$ matrices; d = dim

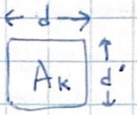
- Q operations / Q channels / Admissible operations / CPTP maps / TCP maps :

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

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

- Kraus representation:

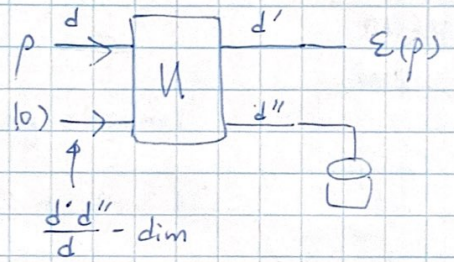
$\mathcal{E}$ TCP map $\Leftrightarrow$ $\mathcal{E}(\rho) = \sum_{k=1}^{l} A_k \rho A_k^+$, $\sum_{k=1}^{l} A_k A_k^+ = I_d$



- Stinespring dilation:

$\mathcal{E}$ TCP map $\Leftrightarrow$ $\mathcal{E}(\rho) = tr_E\, U\rho U^+$

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



Examples:

(I) Unitary channels ($d''=1$, $l=1$)

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

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

no error, bit flip, phase flip, both

Pauli ops

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

(II) Generalized Pauli channels:

$$\mathcal{E}(\rho) = p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z + (1-p_x-p_y-p_z)\rho$$

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

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

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

$$= \frac{4q}{3}\cdot\frac{I}{2} + \left(1 - \frac{4q}{3}\right)\rho$$

$\frac{I}{2}$: rubbish; ρ: info.

(III) Amplitude damping channel

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

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

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

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

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

γ: prob leaking "$|1\rangle$" (excitation, photon) to the environment

(IV) Erasure channel

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

$|e\rangle$: erasure symbol, orthogonal to input space

ie one can tell when there is an error.

($d' = d+1$) Ex: what is minimum l in Kraus rep?

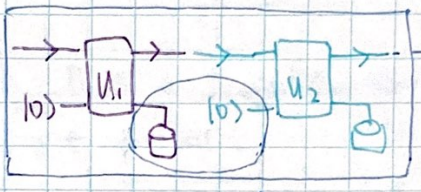
- Combining errors / channels :

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

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

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

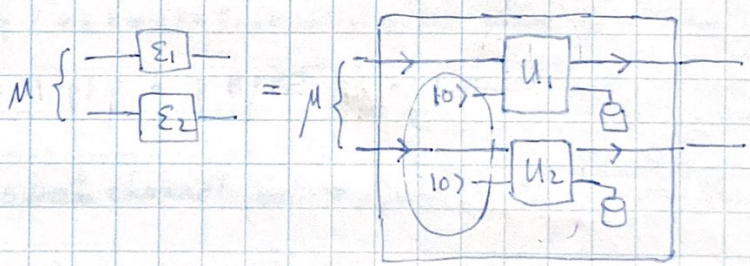
$= \rho \to$ 

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

memoryless

(II) Arbitrary dims, $\mathcal{E}_1 \otimes \mathcal{E}_2(\mu) = \sum_{k,m} (A_k \otimes B_m)\, \mu\, (A_k^\dagger \otimes B_m^\dagger)$

μ : $d_1 d_2$-dim $\qquad$ $d_1' d_2'$-dim



independent errors.

Origin of the magic behind error correction:

Approx of <u>independent</u> channels by <u>low weight</u> errors:

Consider n qubits.

Def 1: For a tensor product operator $A = A_1 \otimes A_2 \otimes \cdots \otimes A_n$ <u>the weight</u> 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 <u>t-qubit error</u> if $B = \sum_i B_i$, $wt(B_i) \le t$ for all i.

Def 3: N is a <u>t-qubit error channel</u> 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 <u>independent</u> channel on n qubits if $N = \bigotimes_{i=1}^{n} \mathcal{E}_i$

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

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

NB: $N(\rho)$ well approximated by keeping terms up to $(1+\beta)np$ errors.

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

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

$$N = \bigotimes_i N_i$$

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

Remarks:

① Diamond norm distance between N_1 and N_2:

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

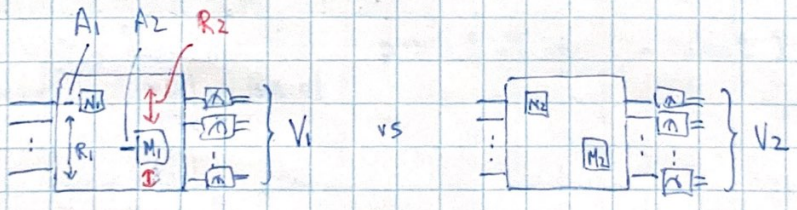
R: reference system; A: input to N_1, N_2

$\|\cdot\|_1$: Schatten-1 norm = sum(abs(evals))

ⓐ Physically, if one of N_1, N_2 occurs to A uniformly, best probability to determine which N_i:

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

ⓑ 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).



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

ⓒ 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 $\tilde{N}$.

When is $\binom{n}{t+1} p^{t+1} \ll 1$?

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

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

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

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

$$\approx 2^{n[-p\alpha \log \alpha - (1-p\alpha)\left(\frac{-p\alpha}{\ln 2}\right)]} \quad \text{(if } p\alpha \ll 1\text{)}$$

$$\approx 2^{np\alpha\left(-\log\alpha + \frac{1}{\ln 2}\right)}$$

$-\log\alpha + \frac{1}{\ln 2}$: −ve for $\alpha \gtrsim 1.7$

- 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)

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

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

• Proof of theorem:

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

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

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.

$$\| N - \tilde{N} \|_\diamond \le (1-p)^{n-t-1} p^{t+1} \| \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \cdots \otimes \mathcal{E}_{t+1} \otimes I^{\otimes n-t-1} - I^{\otimes n} \|_\diamond$$
$$+ (1-p)^{n-t-1} p^{t+1} \| \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \cdots \otimes \mathcal{E}_t \otimes I \otimes \mathcal{E}_{t+1} \otimes I^{\otimes n-t-2} - I^{\otimes n} \|_\diamond$$
$$+ \vdots$$
$$+ p^n \| \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \cdots \otimes \mathcal{E}_n - I^{\otimes n} \|_\diamond$$
$$\le 2 \sum_{j=t+1}^{n} \binom{n}{j} (1-p)^{n-j} p^j \le 2 \cdot \binom{n}{t+1} p^{t+1}.$$

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

Thm' 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 map (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 $A_0^i \approx I \cdot \alpha$, α large

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

(b) Expand each $A_0^i = I \cdot \alpha + \cdots$

(c) Truncate to wt t again.