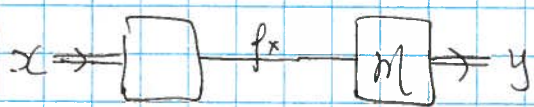
Lec 6.

How much info can we learn about a quantum state by measuring it?

Suppose Alice draws x wp $p(x)$, ← rv X
prepares ρ_x and sends it to Bob.

Bob performs meas $\mathcal{M}$ with POVM $\{M_y\}$. ← $\sum_y M_y = I$

← rv Y.



For classical rv's $X\,Y$, $p(x,y) = p(y|x)\,p(x)$.

$p(y|x) = \mathrm{tr}(M_y \rho_x)$, so $I(X:Y)$ depends only on $\mathcal{M}$.

↑ quantifies how much info about X is revealed in Y.

Def: for an ensemble $\mathcal{E} = \{p(x), \rho_x\}$

The accessible info $I_{acc}(\mathcal{E}) := \max_{\mathcal{M}} I(X:Y)$.

Why such def?

① Why store classical info in non ortho, possibly mixed states?

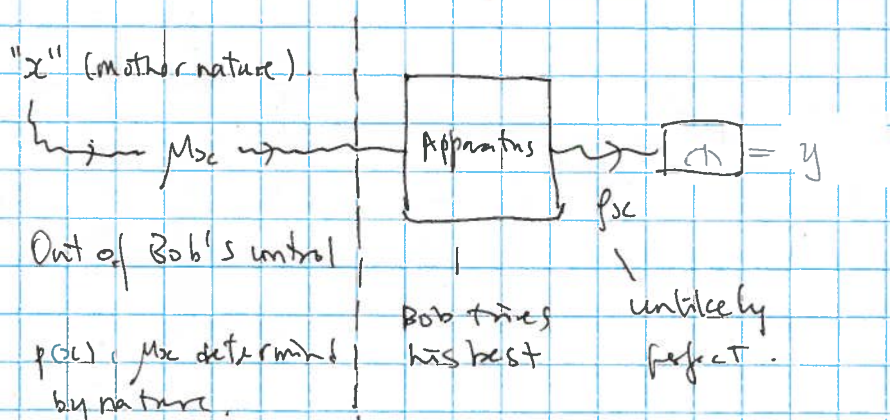
② Why $x \sim p(x)$?

③ $I(X:Y)$ suggests iid draws, why?

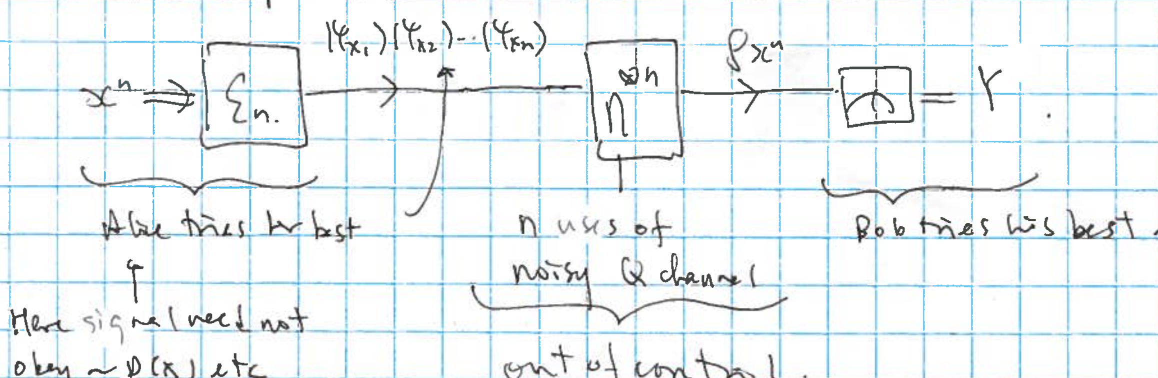
Some partial answers:

- In physics, an experimentalist (Bob) builds apparatus to measure some classical data about the world.

  e.g. gravity waves in LIGO
  frequency in atomic clocks @ NIST.



- In channel capacities:



How to optimize m?

MAJOR OPEN PROBLEM, EVEN FOR SIMPLE ENSEMBLES.

Some partial results:

① E B Davies IEEE TIT 24, p596, 1978

Let $\mathcal{E} = \{p(x), \rho_x\}$, $\rho_x \in \mathcal{L}(\mathbb{C}^d)$.

Optimal measurement $\{M_i\}_{i=1}^n$ can be chosen s.t.

(a) $\operatorname{rank}(M_i) = 1$
(b) $d \le n \le d^2$

$\left.\begin{matrix} \text{(a)} \\ \text{(b)} \end{matrix}\right\}$ simultaneous.

Intuition:

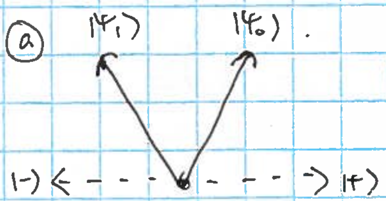
(a) ~~M_i with rank ≥ 2 is a positive sum of $M_{i,k}$'s each with rank 1.~~

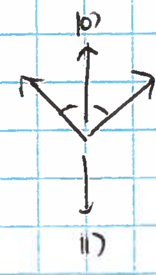
~~That we use~~ $M_i = \sum_k M_{i,k}$ corresponds to "coarse graining" all outcomes (i, k) into a single (i), which cannot increase mutual info by monotonicity.

(b) Use convexity of and Caratheodory's thm.

② Special ensembles.

ⓐ





If $|\psi_0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$

$|\psi_1\rangle = \cos\theta\,|0\rangle - \sin\theta\,|1\rangle$.

each drawn wp $\frac{1}{2}$

Then optimal measurement is along $|+\rangle, |-\rangle$.

Due to Chris Fuchs thesis P81, using a result by Levitin

ⓑ If $\mathcal{E}$ group covariant,

ie $\exists$ finite group G s.t.

(i) can index ρ_x as ρ_g, $g \in G$.

(ii) $p(x) = \frac{1}{|G|}$ $\forall x$

(iii) $\exists$ irrep $\left[\begin{array}{l} \{U_g\} \subseteq U(d), \quad d = \dim(\rho_x), \\ U_g \cdot U_h = U_{g \cdot h}, \quad \text{"}U_g K U_g^\dagger = K \;\forall g \Rightarrow K \propto I\text{"} \end{array} \right]$

group op

s.t. $U_g \rho_h U_g^\dagger = \rho_{g \cdot h}$

Then $\exists\, |\psi\rangle \in \mathbb{C}^d$ s.t.

$\left\{ M_g = \frac{d}{|G|} U_g^\dagger |\psi\rangle\langle\psi| U_g \right\}_{g \in G}$ is an optimal POVM.

[Davies 78].

(c) 9812062:

Remove condition (b) (iii)

Impose: U_g real

$$\left[U_{g_1} \cdot U_{g_2} = e^{i\phi(g_1, g_2)} U_{g_1 \cdot g_2}\right]$$

$\{U_g\}$ acts irreducibly on $\mathbb{R}^d$

then: $\exists\ |\psi\rangle \in \mathbb{R}^d$ s.t.

$$\left\{ \frac{d}{|G|} U_g |\psi\rangle\langle\psi| U_g^+ \right\}_{g \in G}.$$

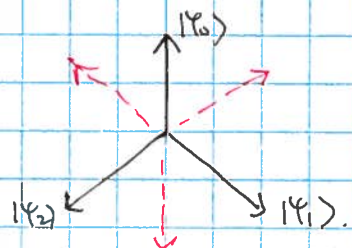
is optimal POVM.

(d) 0509122 (Decker)

Reducible reps $\{U_g\}$, but complicated.

eg 1

$$\left.\begin{aligned} &\rho_x = |\psi_x\rangle\langle\psi_x| . \\ &|\psi_0\rangle = |0\rangle \\ &|\psi_1\rangle = \cos\tfrac{\pi}{3}|0\rangle + \sin\tfrac{\pi}{3}|1\rangle \\ &|\psi_2\rangle = \qquad\qquad\quad - \\ &\text{equiprobable.} \end{aligned}\right\} \mathcal{E}_1$$



Consider $G = \mathbb{Z}_3$,

$$U_g = e^{i\sigma_y 2\pi/3 \cdot g}, \quad g = 0,1,2.$$

Then conditions for 98 12062 hold.

In fact $|\psi\rangle = |\psi_0^\perp\rangle$, optimal meas:

$$M_i = \frac{2}{3}|\psi_i^\perp\rangle\langle\psi_i^\perp| \quad \leftarrow ☆☆$$

Here: $H(X) = \log 3$.

$H(X|y=0) = 1$ ← equiprobable $|\psi_1\rangle, |\psi_2\rangle$.

Similarly for $y = 1, 2$.

$\therefore H(X|Y) = 1$.

$$I(X:X) = \underbrace{H(X) - H(X|Y)}_{\text{Fll from eg 1.}} = \log 3 - 1 \approx 0.5850.$$

$I_{acc} = \log 3 - 1$.

Upper bound to accessible info:

Recall: Given $\mathcal{E} = \{p(x), \rho_x\}$

$$\Lambda_{XQ} = \sum_x p(x)\, |x\rangle\langle x|_X \otimes \rho_{x\,Q}$$

$$S(X:Q) = \chi(\mathcal{E})$$

where $\chi(\mathcal{E}) = S\left(\sum_x p(x)\, \rho_x\right) - \sum_x p(x)\, S(\rho_x)$.

↑ Holevo info for $\mathcal{E}$.

Thm: $I_{acc}(\mathcal{E}) \leq \chi(\mathcal{E})$.

Pf: Let $\{M_y\}$ be the optimal POVM.

Apply meas to Q, keep only classical outcome:

$$\Lambda_{XQ} \to \Lambda'_{XY} = \sum_x p(x)\, |x\rangle\langle x|_X \otimes \sum_y \mathrm{tr}(M_y \rho_x)\, |y\rangle\langle y|.$$

$$\chi(\mathcal{E}) = S(X:Q)_\Lambda \underset{\text{mono of QMI}}{\geq} S(X:Y)_{\Lambda'} = I(X:Y) \underset{\text{by assumption POVM optimal.}}{=} I_{acc}(\mathcal{E})$$

eg. 1: $\rho = \frac{I}{2}$, $\chi(\mathcal{E}_1) = S(\rho) - 0 = 1$

but $I_{acc}(\mathcal{E}_1) \approx 0.5850$

Lower bound of I_{acc}: [Jozsa, Robb, Wootters 94]

Def: for a density matrix ρ in d-dims with eigvals $\{\lambda_k\}$, subentropy

$$Q(\rho) := -\sum_{k=1}^{d} \left(\prod_{l \neq k} \frac{\lambda_k}{\lambda_k - \lambda_l} \right) \lambda_k \log \lambda_k$$

Thm: $\mathcal{E} = \{p(x), \rho_x\}$.

$$I_{acc}(\mathcal{E}) \geq Q\left(\sum_x p(x) \rho_x \right) - \sum_x p(x) Q(\rho_x).$$

$\uparrow$ achieved by meas in random basis.

$\leftarrow$ like $\chi(\mathcal{E})$ with Q in place of S.

eg. If ρ_x pure, $\rho = \frac{I}{d}$,

then $I_{acc} \geq \log d - (\log e)\left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{d}\right)$

$d=2$, $I_{acc} \geq 0.2787$

$d \to \infty$, $I_{acc} \geq 0.60995$.

Getting complicated:

eg 2. $\rho_x = |\psi_x\rangle\langle\psi_x|^{\otimes 2}_{Q_1 Q_2}$

$|\psi_x\rangle$ as before, $p(x)$ as before. $\Big\}\ \mathcal{E}_2$

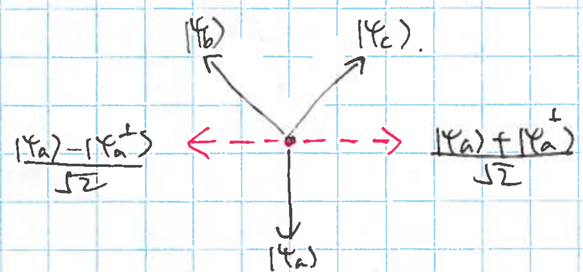
$\boxed{\text{I}}$ Consider the following measurement M_2:

① Apply the meas in eg 1 on Q_1. If outcome is "a", one of the three states, $|\psi_a\rangle^{\otimes 2}$ is eliminated.

② Now state in Q_2 is $|\psi_b\rangle$ wp $\frac{1}{2}$

$|\psi_c\rangle$ wp $\frac{1}{2}$

$b, c \in \{0,1,2\} \setminus \{a\}$, $b \neq c$.



③ Apply meas along the $\frac{|\psi_a\rangle \pm |\psi_a^\perp\rangle}{\sqrt{2}}$ basis on Q_2.

Claim: $I(X:Y)$ due to M_2 is ≈ 1.23038 bits

$> 0.5850 \times 2$ bits $= 2\, I_{acc}(\mathcal{E}_1)$.

Pf: Assignment 3

Note: meas on Q_2 conditioned on meas outcome on Q_1.

Most general: joint meas on $Q_1 Q_2$.

$\boxed{\text{II}}$ Instead, consider the following measurement M_3

$$\Lambda = |\psi_0\rangle\langle\psi_0|^{\otimes 2} + |\psi_1\rangle\langle\psi_1|^{\otimes 2} + |\psi_2\rangle\langle\psi_2|^{\otimes 2}.$$

$$M_i = \Lambda^{-\frac{1}{2}} |\psi_i\rangle\langle\psi_i| \Lambda^{-\frac{1}{2}} \quad \text{for } i = 0, 1, 2.$$

$$M_3 = I - M_0 - M_1 - M_2.$$

$$I(X:Y) \approx 1.3691. \quad \text{(Assignment 3)}.$$

Conjecture :

$\underbrace{\text{LOCC meas}}_{}$ never achieves $I_{acc}(\mathcal{E}_2)$.

meas $Q_1, Q_2, Q_1, Q_2 \ldots$
allow subsequent
meas to depend on previous outcomes

Will be great if you can prove it, but this is NOT in A3 :)

Remark 1:

- Consider an ensemble $\mathcal{E}$ of 1-qubit pure states.

  In general, there can be many many diff states.

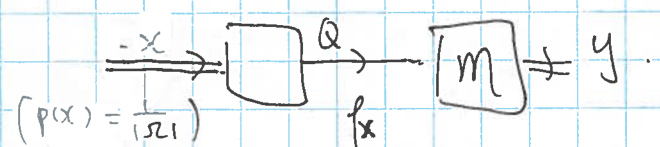
  But $I_{acc}(\mathcal{E}) \leq \chi(\mathcal{E}) \leq \log 2 = 1$.

  Preparing a state and forgetting the label is highly irreversible

[* makes it more amazing teleportation works.]

[Without entanglement, Alice can at best meas the input state and transmit 1 bit to Bob.]

- Holevo's bdd says we cannot use 1 qbit to transmit more that 1 bit of data.



if $Y = X$ whp, $I(X:Y) \approx \log |\Omega|$.

$$\leq \chi(\{p(x), \rho_x\})$$

$$\leq \log \dim Q$$

- Likewise Q Data compression requires at least $n \cdot \chi(\mathcal{E})$ qubits for n draws from $\mathcal{E}$.

Back to how much correlation can change when adding/discarding systems:

- We saw $|S(AB) - S(A)| \leq S(B)$ Cor 1 (S9)

  $|S(A:BC) - S(A:C)| \leq 2S(B)$.   Cor 2 (S9)

- We can extend such results to Holevo info:

  Let $\mathcal{E} = \{p(x), \underbrace{\rho_x}_{\text{lives in sys } BC}\}$

  $\mathcal{F} = \{p(x), \underbrace{\tau_x}_{\text{lives in sys } C}\}$

  $\tau_x := \mathrm{tr}_B\, \rho_x \quad \forall x$.

  Then $|\chi(\mathcal{E}) - \chi(\mathcal{F})| \leq 2S(B)$. $\leftarrow$ Cor 3 (S9).

  Pf: Let $\rho = \sum_x p(x)\, |x\rangle\langle x|_A \otimes \rho_{x\,BC}$

  $\tau = \sum_x \cdots \cdots \otimes \tau_{xB}$

  Then $|\chi(\mathcal{E}) - \chi(\mathcal{F})|$

  $= |S(A:BC) - S(A:C)| \leq 2S(B)$

- So Holevo info can increase by at most $2S(B)$ if B is communicated, even in the presence of shared entanglement.

App

Thm Suppose Alice is allowed to send n_A qubits to Bob, Bob can send n_B qubits back, in any order. Then Alice can communicate at most $n_A + n_B$ bits to Bob.

ie n_A qbit$\rightarrow$ + n_B qbit$\leftarrow$ $\geq \beta$ cbit

$\Rightarrow \quad n_A + n_B \geq \beta$.

Pf. Let Alice's message be x

Suppose after the jth qubit of comm.

Bob's state is ρ_{xj} on sys B_j. Let $\mathcal{E}_j = \{ p(x), \rho_{xj} \}$

Let Bob final output be y.

$$I(X:Y) \leq \chi(\mathcal{E}_n) \leq S\left(\sum_x p(x)\, \rho_{xn}\right)$$

$I \leq I_{acc} \leq \chi$

$$\leq S\left(\sum_x p(x)\, \rho_{x\,n-1}\right) + 1$$

$$\vdots$$

$$\leq n_A + n_B$$

Locking of accessible Info:

Let $\mathcal{F} = \{ p(xt),\ \rho_{xt} \}$.

where $\rho_{xt} = U^t\ |x\rangle\langle x|\ U^{t\,\dagger}$

$t \in \{0,1\}$, $x \in \{0,1,\ldots,n-1\}$.

$p(xt) = \frac{1}{2n}$,

$U|x\rangle = \sum_l \omega^{xl} |l\rangle$, $\omega^n = 1$.

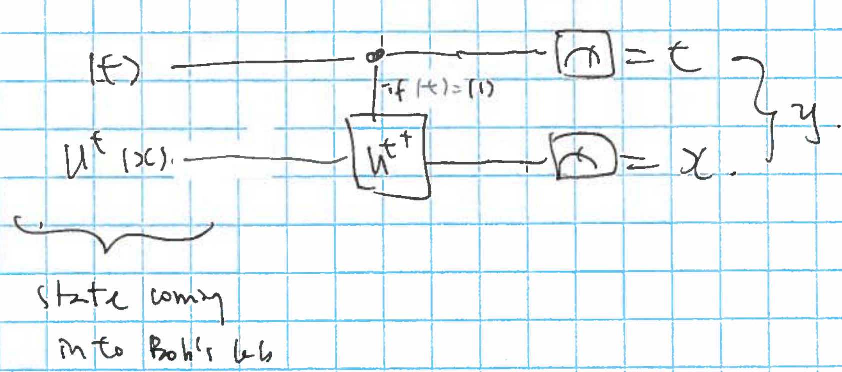
FT.

In 0303088, $I_{acc}(\mathcal{F}) = \frac{1}{2}\log n$.

Now consider:

$\mathcal{E} = \{ p(xt),\ \rho_{xt} \otimes |t\rangle\langle t| \}$.

A particular measurement is:



$\therefore\ I(TX:Y) = \log(2n) = 1 + \log n$

$\chi(\mathcal{E}) = 1 + \log n$ $\therefore$ $I_{acc}(\mathcal{E}) = 1 + \log n$.

But $\mathcal{F}$ is obtained from $\mathcal{E}$ by removing 1 qubit, yet $\chi(\mathcal{E}) - \chi(\mathcal{F}) = 1 + \frac{1}{2}\log n \gg 1$ or 2 !!