CO781 / QIC890 Fall 2016 Lec 07

Def [Von Neumann entropy]

Let $\rho \geq 0$, $\operatorname{tr}\rho = 1$, $\rho \in B(\mathbb{C}^d)$

Then $S(\rho) := -\operatorname{tr} \rho \log \rho = -\sum_{i=1}^{d} \lambda_i \log \lambda_i$

where $\lambda_1, \ldots, \lambda_d$ are eigenvalues of ρ.

eg. B92

$\rho_0 = |0\rangle\langle 0|$, $q(0) = \frac{1}{2}$

$\rho_1 = |+\rangle\langle +|$, $q(1) = \frac{1}{2}$

Average state $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$

$$= \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\cdot\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{bmatrix} = \lambda_1 |e_1\rangle\langle e_1| + \lambda_2 |e_2\rangle\langle e_2|$$

$$\left.\begin{array}{ll} \text{where } \lambda_1 \doteq 0.14645, & |e_1\rangle = \begin{bmatrix} \sin\frac{\pi}{8} \\ -\cos\frac{\pi}{8} \end{bmatrix} \\ \lambda_2 \doteq 0.85355, & |e_2\rangle = \begin{bmatrix} \cos\frac{\pi}{8} \\ \sin\frac{\pi}{8} \end{bmatrix} \end{array}\right\} \text{ very diff from } \rho_0, \rho_1$$

$$H(p) \doteq -0.14645 \log 0.14645 - 0.85355 \log 0.85355$$

$$\doteq 0.60088.$$

Def: Let ρ be a density matrix with spectral decomposition

$$\rho = \sum_{v=1}^{d} p(v)\, |e_v\rangle\langle e_v| .$$

Let V be a rv with sample space $\{1, 2, \ldots d\}$

and distribution $p(v)$.

Let $T_{n,\delta}$ be the typical set for n iid draws of V.

For $v^n = v_1 v_2 \ldots v_n \in T_{n,\delta}$, let

$$|e_{v^n}\rangle = |e_{v_1}\rangle |e_{v_2}\rangle \ldots |e_{v_n}\rangle .$$

The δ-typical space of $\rho^{\otimes n} = \text{span}\{ |e_{v^n}\rangle : v^n \in T_{n,\delta}\} =: S$.

Let $\Pi_S = \sum_{v^n \in T_{n,\delta}} |e_{v^n}\rangle\langle e_{v^n}|$ (projector onto S).

Quick facts:

① $\dim S = |T_{n,\delta}| \leq 2^{n(H(V)+\delta)} = 2^{n(S(\rho)+\delta)}$

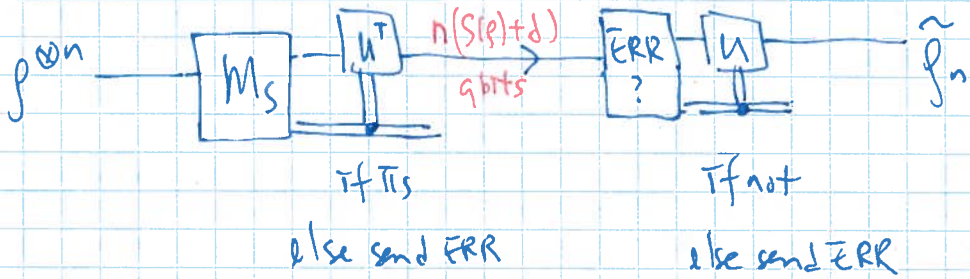
② $\mathrm{Tr}(\rho^{\otimes n}\, \Pi_S) = \sum_{v^n \in T_{n,\delta}} p(v^n) \geq 1 - \varepsilon$ if $n \geq n_0 = \ldots$

$\sum_{\text{all } v'^n} |e_{v'^n}\rangle\langle e_{v'^n}|\, p(v'^n)$ $\qquad$ $\sum_{v^n \in T_{n,\delta}} |e_{v^n}\rangle\langle e_{v^n}|$

Fact ② means, for example, $\rho^{\otimes n}$ can be transmitted with high fidelity by transmitting S alone. Let:

$$\mathbb{C}^{2^{n(S(\rho)+\delta)}} \underset{U^{+}}{\overset{U}{\rightleftarrows}} S$$

Let M_s be a measurement with POVM $\{\Pi_s, I-\Pi_s\}$.



Ex: $\| \tilde{\rho}_n - \rho^{\otimes n} \|_1 = 1 - \mathrm{prob}(\Pi_{n,\delta}) \leq \varepsilon$.

But this is not a task we're interested in....

Quantum source, entropy and data compression

X, Ω as before, $\Pr(X=x) = q(x)$

Consider the process:

① Sample X, obtain $x \in \Omega$ w.p. $q(x)$

② Prepare quantum state ρ_x

Resulting state:

$$\Lambda = \sum_{x\in\Omega} q(x) \underbrace{|x\rangle\langle x|_R}_{\substack{\text{a reference has a record}\\ \text{of the outcome of sampling}\\ \text{the classical source}}} \otimes \underbrace{\rho_{x\,S}}_{\substack{\text{the quantum state is often}\\ \text{given to someone without the}\\ \text{knowledge of } x.}}$$

Terminology:

- receiving a specimen ρ_x w.p. $q(x)$ is called "one draw" of the ensemble $\mathcal{E} = \{q(x), \rho_x\}$
- the "average state" of $\mathcal{E}$ is $\rho = \sum_x q(x)\,\rho_x = \mathrm{Tr}_R \Lambda$

eg. BB84: $\Omega = \{0,1,2,3\}$, $q(x) = \frac{1}{4} \quad \forall x \in \Omega$

$\rho_0 = |0\rangle\langle 0|$, $\rho_1 = |1\rangle\langle 1|$, $\rho_2 = \underbrace{|+\rangle}_{\frac{|0\rangle+|1\rangle}{\sqrt{2}}}\langle +|$, $\rho_3 = \underbrace{|-\rangle}_{\frac{|0\rangle-|1\rangle}{\sqrt{2}}}\langle -|$.

$\rho = \frac{I}{2}$

* Repeat n-times.

Alice keeps $R_1 R_2 \ldots R_n$, while $S_1 S_2 \ldots S_n$ is sent to Eve then to Bob

Take n draws from this quantum source:

① Sample X n times iid.

Obtain $x^n = x_1 \ldots x_n$ wp $q(x^n) = q(x_1) \ldots q(x_n)$.

② Prepare $\rho_{x^n} = \rho_{x_1} \otimes \rho_{x_2} \otimes \ldots \otimes \rho_{x_n}$.

Resulting state:

$$\Lambda^{\otimes n} = \sum_{x^n \in \mathcal{X}^n} q(x^n) \underbrace{|x^n\rangle\langle x^n|}_{\text{in } R^n = R_1 \ldots R_n} \otimes \underbrace{\rho_{x^n}}_{\text{in } S^n = S_1 \ldots S_n}$$

Qn: Can we "compress" this quantum source?

ie A referee draws x^n wp $q(x^n)$, ← Def (QDC)

Referee gives ρ_{x^n} to Alice who has to send it to Bob.

For each x^n, Bob should output something close to ρ_{x^n}.

(Say Bob gives output to referee who checks how good the compression is.)

Averaged over X^n, transmission should have high fidelity.

Equivalent to:

Referee prepares $\Lambda^{\otimes n}$, gives S^n to Alice who transmits it to Bob in a way that preserves the correlation with R^n.

NB: Alice is not sen[...] Verbal [...]b; this does not preserve correlat[...]lso Bob knows ρ!

NB: ρ_{x^n} is a quantu[...]. More on this later.

<u>Quantum data compression:</u>

Let $\Lambda = \sum_x q(x)\, |x\rangle\langle x| \otimes \rho_x$, $\quad \rho = \sum_x q(x)\, \rho_x$.

Consider:

s.t. $I_{R^n} \otimes (D_n \circ E_n)_{S^n} (\Lambda^{\otimes n}) =: \tilde{\Lambda}_n \approx \Lambda^{\otimes n}$

What is the min R s.t. $\forall n$ large enough, E_n, D_n exist?

- For general ρ_x's, min R is still unknown.
- Schumacher 95: when $\rho_x = |\psi_x\rangle\langle\psi_x|$
  $R \approx S(\rho)$ sufficient & necessary.

<u>Thm</u>: Let $\Lambda = \sum_x q(x)\, |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_S$, $\quad \rho = \sum_x q(x)\, |\psi_x\rangle\langle\psi_x|$.

$\forall \varepsilon > 0$, $\forall R > S(R)$

$\exists n_0$ s.t $\forall n \geq n_0$ $\exists E_n, D_n$

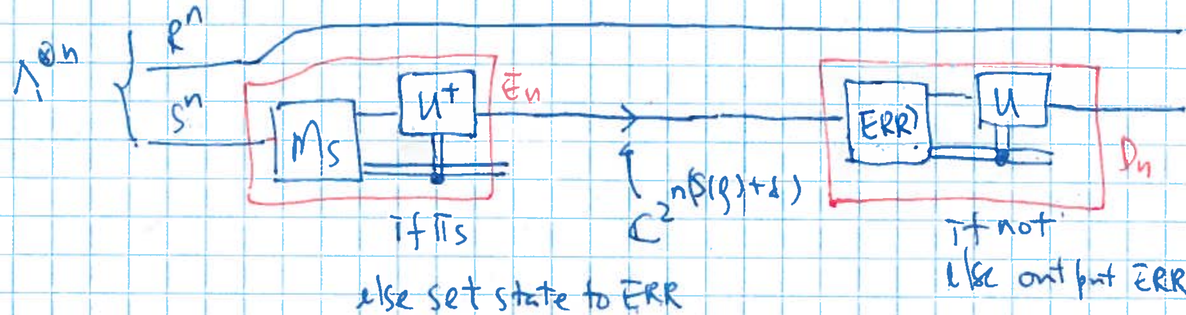
s.t. output dim of $E_n = 2^{nR}$

and $\| I_{R^n} \otimes (D_n \circ E_n)_{S^n} (\Lambda^{\otimes n}) - \Lambda^{\otimes n} \|_1 \leq 2\sqrt{2}\sqrt{\varepsilon} + \varepsilon$.

Pf: claim: transmitting only the δ-typical space of $\rho^{\otimes n}$ works!

NB we have a much harder job than sending $\rho^{\otimes n}$ here!!

It is a very nice surprise!!



Weaker analysis:

$$\text{Average fidelity} = \sum_{x^n} p(x^n) \; |\langle \underset{\text{input}}{\psi_{x^n}} | \underbrace{\Pi_s |\psi_{x^n}\rangle}_{\text{output}} |$$

unlike classical case there is additional distortion even if M_s yields outcome "Π_s".

!! all x^n

$$= \sum_{x^n} p(x^n) \; \langle \psi_{x^n} | \Pi_s | \psi_{x^n} \rangle$$

$$= \mathrm{tr}\left[\left(\sum_{x^n} p(x^n) \; |\psi_{x^n}\rangle\langle\psi_{x^n}| \right) \Pi_s \right]$$

not what's transmitted but $\rho^{\otimes n}$ appears in this choice of meas of success.

$$= \mathrm{tr}\left[\rho^{\otimes n} \; \Pi_s \right] \geq 1-\varepsilon .$$

Harder analysis:

$$\tilde{\Lambda}_n = I_{R^n} \otimes (D_n \circ E_n)_{S^n} (\Lambda^{\otimes n})$$

$$\text{all } x^n \longrightarrow = \sum_{x^n} f(x^n) \, |x^n\rangle\langle x^n|_R \otimes \Pi_S |\psi_{x^n}\rangle\langle\psi_{x^n}| \Pi_S$$

$$+ \sum_{x^n} f(x^n) \, |x^n\rangle\langle x^n|_R \otimes \text{ERR} \left[\operatorname{tr} (I - \Pi_S) |\psi_{x^n}\rangle\langle\psi_{x^n}| \right]$$

$(*)$ $\operatorname{tr}(\text{2nd term}) \leq \varepsilon$

$$\| \tilde{\Lambda}_n - \Lambda^{\otimes n} \|_1$$

$$\overset{\Delta\text{ Ineq}}{\leq} \| \text{1st term of } \tilde{\Lambda}_n - \Lambda^{\otimes n} \|_1 + \| \text{2nd term of } \tilde{\Lambda}_n \|_1$$

$$\overset{\Delta I, (*)}{\leq} \sum_{x^n} f(x^n) \, \| \Pi_S |\psi_{x^n}\rangle\langle\psi_{x^n}| \Pi_S - |\psi_{x^n}\rangle\langle\psi_{x^n}| \|_1 + \varepsilon$$

$$\overset{\text{see notes}}{\leq} \sum_{x^n} f(x^n) \, 2 \sqrt{1 - \langle\psi_{x^n}| \Pi_S |\psi_{x^n}\rangle^2} + \varepsilon$$

$$\leq \sum_{x^n} f(x^n) \, 2\sqrt{2} \sqrt{1 - \langle\psi_{x^n}| \Pi_S |\psi_{x^n}\rangle} + \varepsilon$$

$$\leq 2\sqrt{2} \sqrt{\sum_{x^n} f(x^n) \left(1 - \langle\psi_{x^n}| \Pi_S |\psi_{x^n}\rangle\right)} + \varepsilon$$

Concavity of $\sqrt{\ }$

$$\leq 2\sqrt{2} \sqrt{1 - \operatorname{tr}(\rho^{\otimes n} \Pi_S)} + \varepsilon$$

$$\leq 2\sqrt{2} \sqrt{\varepsilon} + \varepsilon .$$

Converse: that $R > S(\rho)$ is necessary
is implied by Holevo's bound we will prove later.

Explain if there is time

Direct proof for special case can be found in Preskill
10.2.2 (the Ky Fan dominance principle)
10.3.2 Round (10.151) until pass (10.155).

Further remarks:

- For mixed state ensemble $\mathcal{E} = \{ q(x), \rho_x \}$
  where $\rho_x = \sum_j \mu_j^x \, |a_j^x\rangle\langle a_j^x|$

  One can compress $\mathcal{E}' = \{ q(x)\, \mu_j^x , \; |a_j^x\rangle \}$
  with rate $\approx S(\rho)$, preserving info on j.

  But conjectured to be unnecessary, that
  $$S(\rho) - \sum_x q(x)\, S(\rho_x)$$
  is an achievable rate! Open.

- Var length codes, universal compression possible.

A minor detail:

From NC 9.2.3, Eq (9.97) – (9.99):

$$\frac{1}{2} \| \, |a\rangle\langle a| - |b\rangle\langle b| \, \|_1 = \sqrt{1 - |\langle a|b\rangle|^2}$$

Here we have

$\frac{1}{2} \| \, \Pi|b\rangle\langle b|\Pi - |b\rangle\langle b| \, \|_1$ and $\Pi|b\rangle$ is not a unit vector.

But it still holds that

$$\frac{1}{2} \| \, |a\rangle\langle a| - |b\rangle\langle b| \, \|_1 = \sqrt{\left(\frac{1+\langle a|a\rangle}{2}\right)^2 - |\langle a|b\rangle|^2}$$

$$\leq \sqrt{1 - |\langle a|b\rangle|^2}$$

Pf: WLOG, $|a\rangle = \gamma |0\rangle$

$|b\rangle = c|0\rangle + s|1\rangle$, $c = \cos\theta$, $s = \sin\theta$ for some θ.

$$m = |a\rangle\langle a| - |b\rangle\langle b| = \begin{bmatrix} \gamma^2 - c^2 & -cs \\ -cs & -s^2 \end{bmatrix}$$

$$= -\frac{(1-\gamma^2)}{2} I + \left(\frac{\gamma^2 - c^2 + s^2}{2}\right) Z - cs \, X$$

$$= -\frac{(1-\gamma^2)}{2} I + \frac{\gamma^2 - c_2}{2} Z - \frac{s_2}{2} X, \quad c_2 = \cos 2\theta, \; s_2 = \sin 2\theta.$$

Eigenvalues of $\alpha Z + \beta X = \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}$

are $\pm\sqrt{\alpha^2+\beta^2}$, by solving $\det\left(\lambda I - \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}\right) = 0$.

$$\therefore \mathrm{Eval}(m) = -\frac{(1-\gamma^2)}{2} \pm \sqrt{\left(\frac{\gamma^2-c_2}{2}\right)^2 + \left(\frac{s_2}{2}\right)^2}$$

$$= -\frac{(1-\gamma^2)}{2} \pm \frac{1}{2}\sqrt{(\gamma^2-c_2)^2 + s_2^2}$$

$$= -\frac{(1-\gamma^2)}{2} \pm \frac{1}{2}\sqrt{1+\gamma^4-2\gamma^2 c_2}\,, \quad c_2 = 2c^2-1$$

$$= -\frac{(1-\gamma^2)}{2} \pm \frac{1}{2}\sqrt{1+2\gamma^2+\gamma^4-4\gamma^2c^2}$$

$$= -\frac{(1-\gamma^2)}{2} \pm \frac{1}{2}\sqrt{\underbrace{(1+\gamma^2)^2}_{\langle a|a\rangle} - \underbrace{4\gamma^2c^2}_{|\langle a|b\rangle|^2}}$$

For $\gamma \approx 1$, $\|m\|_1 = \sqrt{(1+\gamma^2)^2-4\gamma^2c^2} \leq 2\sqrt{1-\gamma^2c^2}$

Sum of abs vals $= 2K$ still.