

4/6/06

Channel Capacities - II ('Shor')

$$\chi(\hat{p}_i, |v_i\rangle) = H\left(\sum_i p_i |v_i\rangle\langle v_i|\right)$$

Allowed to send  $p_1, p_2, \dots, p_k$ 

$$\text{Capacity is } \max_{\{p_i, \hat{p}_i\}} \chi = \max_{\{p_i, \hat{p}_i\}} H\left(\sum_i p_i \hat{p}_i\right) - \sum_i p_i H(\hat{p}_i)$$

block length:  $n$ capacity:  $C$ pick  $2^{n(C-\epsilon)}$  random codewordsw/ letters chosen w/ probs maximizing  $H(B) - H(B|A)$ 

- Alice sends Bob's codeword.
  - Bob gets codeword with noise
  - Finds the codeword most likely to have been the input works.
- as  $n \rightarrow \infty$ ,  $\epsilon \rightarrow 0$ .

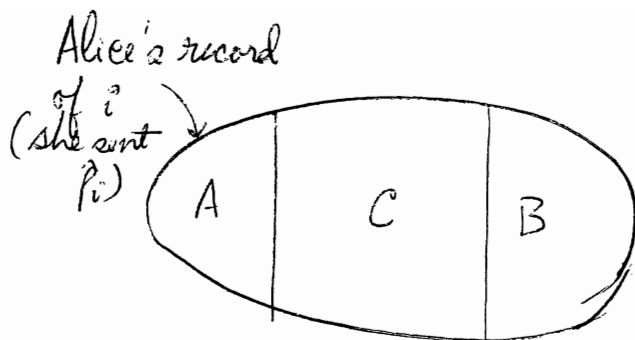
How about quantum case?

Upper bound:

Alice sends  $\hat{p}_i$  to Bob

Will show that for single-state decoding,

Shannon information provided by any measurement of Bob's  $<$  Holevo information  $\chi$



$$|i\rangle \longrightarrow \hat{p}_i \xrightarrow{\text{Bob's measurement}} |b_j\rangle$$

basis-states of measurement  
telling Bob the meas. result.

There could be a residual state  $|r_i\rangle$  after Bob's measurement.

$$I(A;B) \text{ Shannon-capacity} \\ = H(A) + H(B) - H(A,B)$$

Holevo quantity

$$H(\sum_i p_i \hat{p}_i) - \sum_i p_i H(p_i)$$

$$\uparrow \\ H(p_{BC})$$

$$\uparrow \\ H(p_{ABC}) - H(p_A)$$

We want  $H(A) + H(B) - H(A,B)$

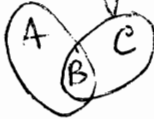
or,  $H(p_A) + H(p_B) - H(p_{AB})$

... just change of notation.

$$\leq H(p_{ABC}) + H(p_{BC}) + H(p_A)$$

$$0 \leq -H(\rho_{ABC}) + H(\rho_{AB}) + H(\rho_{BC}) - H(\rho_B)$$

Strong subadditivity of quantum entropy



Why is  $\sum_i p_i H(\hat{\rho}_i) = H(\rho_{ABC}) - H(\rho_A)$

A is classical.  $1, 2, \dots, k$

Alice has density matrix:

$$\left[ \begin{array}{ccc} p_1 \hat{\rho}_1 & & \\ & p_2 \hat{\rho}_2 & \\ & & p_3 \hat{\rho}_3 \dots \\ & & & \dots & \\ & & & & p_k \hat{\rho}_k \end{array} \right]$$

Entropy is  $\sum_{ij} -p_i \lambda_{ij} \log(p_i \lambda_{ij})$

$$= \sum_{ij} -p_i \lambda_{ij} \log p_i - \sum_i p_i \lambda_{ij} \log \lambda_{ij}$$

$$= \sum_i -p_i \log p_i - \sum_i p_i H(\hat{\rho}_i)$$

- Proof ingredients:
- random coding
  - typical subspaces
  - pretty good measurement  
(SPM: Square-root-meas.)

We have codewords  $|v_i\rangle$  which we use with associated probability  $p_i$

$$\text{Density matrix } \hat{\rho} = \sum_i p_i |v_i\rangle\langle v_i|$$

$$= \sum_i \lambda_i |\tilde{v}_i\rangle\langle \tilde{v}_i|$$

Typical subspace of  $\mathcal{H}^{\otimes n}$

↳ is spanned by typical sequences of  $|\tilde{v}_i\rangle \doteq \{ |v_i\rangle \text{ that appear } \approx \lambda_i \cdot n \text{ times} \}$

Random code

codeword  $|\phi_i\rangle$  is  $|v_{i_1}\rangle \otimes |v_{i_2}\rangle \otimes \dots \otimes |v_{i_n}\rangle$

prob( $v_i$ ) =  $p_i$

Choose  $N = 2^{n(H(p) - \epsilon)}$  codewords

Codewords  $|\phi_1\rangle, \dots, |\phi_N\rangle$

$$\Phi = \sum_{k=1}^N |\phi_k\rangle\langle\phi_k|$$

$$|\mu_k\rangle = \Phi^{-1/2} |\phi_k\rangle$$

$$\sum_{k=1}^N |\mu_k\rangle\langle\mu_k| = \Phi^{-1/2} \left( \sum_{k=1}^N |\phi_k\rangle\langle\phi_k| \right) \Phi^{1/2} = \mathbb{1}$$

(POVM elements)

$$S_{jk} \text{ matrix} = \langle\phi_j|\phi_k\rangle$$

$$\begin{aligned} (\sqrt{S})_{j,k} &= \langle\mu_j|\phi_k\rangle \\ &= \langle\phi_j|\Phi^{-1/2}|\phi_k\rangle \quad \dots \text{It's Hermitian.} \end{aligned}$$

$$\begin{aligned} (\sqrt{S})_{j\ell}^2 &= \sum_k \langle\phi_j|\mu_k\rangle \langle\mu_k|\phi_\ell\rangle \\ &= \langle\phi_j|\phi_\ell\rangle \end{aligned}$$

Protocol of encoding/decoding:

- Alice sends  $|0\rangle$
- Bob projects onto typical subspace.
- Bob applies SRM  $(\sqrt{S})$  measurement.

- $P_E$  if Alice sent  $|\phi_j\rangle$ , is  $1 - |\langle \mu_j | \Pi_A |\phi_j\rangle|^2$
- Use  $S_i = \Pi_A |\phi_i\rangle$   
 $\uparrow$  projects onto typical subspace.

$$\downarrow$$

$$1 - |\langle \mu_j | S_j \rangle|^2$$

- Average error

$$P_E = 1 - \sum_i \frac{1}{N} |\langle \mu_i | S_i \rangle|^2$$

$$= \frac{1}{N} \sum_i (1 - \langle \mu_i | S_i \rangle^2)$$

$$= \frac{1}{N} \sum_i (1 - \langle \mu_i | S_i \rangle)(1 + \langle \mu_i | S_i \rangle)$$

$$\leq \frac{2}{N} (1 - \langle \mu_i | S_i \rangle)$$

$$\leq \frac{2}{N} (1 - \sqrt{S_{ii}})$$

$$\sqrt{S} \geq \frac{3}{2} S - \frac{1}{2} S^2$$

$$\leq \frac{2}{N} \sum_i \left( \frac{3}{2} S_{ii} - \frac{1}{2} S_{ii}^2 \right) = \frac{2}{N} \sum_i \left( 1 - \left( \frac{3S}{2} - \frac{1}{2} S^2 \right) \right)_{ii}$$

$$\leq \frac{2}{N} \sum_i 1 - \frac{3}{2} S_{ii} + \frac{1}{2} \sum_j S_{ij} S_{ji}$$

$$\leq \frac{2}{N} \sum (1 - \frac{3}{2} n_i + \frac{1}{2} n_i^2) + \frac{1}{N} \sum_{j \neq i} S_{ij} S_{ji}$$

$$|S_k\rangle = \Pi_\Lambda |\Phi_k\rangle$$

$$\langle S_k | S_k \rangle = \langle \Phi_k | \Pi_\Lambda | \Phi_k \rangle$$

$$E \langle S_k | S_k \rangle = 1 - \epsilon$$

$$\begin{aligned} S_{ij} S_{ji} &= \langle S_i | S_j \rangle \langle S_j | S_i \rangle \\ &= E \langle \Phi_i | \Pi_\Lambda | \Phi_j \rangle \langle \Phi_j | \Pi_\Lambda | \Phi_i \rangle \\ &= \text{Tr}(\Pi_\Lambda |\Phi_j\rangle \langle \Phi_j| \Pi_\Lambda |\Phi_i\rangle \langle \Phi_i|) \\ &= \text{Tr}(\Pi_\Lambda \rho^{\otimes n} \Pi_\Lambda \rho^{\otimes n}) \\ &= \text{Tr}(\Pi_\Lambda (\rho^{\otimes n})^2 \Pi_\Lambda) \end{aligned}$$

$\Pi_\Lambda \rho^{\otimes n} \Pi_\Lambda$  has  $\approx 2^{nH(\hat{\rho})}$  eigenvectors  $\neq 0$

$|\Phi_i\rangle = |v_{i_1}\rangle \otimes |v_{i_2}\rangle \otimes \dots \otimes |v_{i_n}\rangle$   
 each of them has eigenvalue  $\approx 2^{-n(H(\hat{\rho}) + \epsilon)}$

Square it: get  $2^{nH(\hat{\rho})}$  vectors w/ e.v.  $2^{-nH(\hat{\rho})}$   
 add  $N = 2^{nH(\hat{\rho}) - \epsilon n}$  of these up