CO781 / QIC 890:

Theory of Quantum Communication

Topics 4, part 2 ctd

Encoding classical information in quantum states and retrieving it

Scenario 1: accessible information (ctd)

# Recall 3 things from last lecture:



Definition:

Let $\Lambda = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_{x,Q}$.

$m$ measurement on Q with output space Y

The accessible information for ensemble $\mathcal{E} = \{p_x, \rho_x\}$ is

$$I_{acc}(\mathcal{E}) := \max_m I(X:Y)_{I \otimes m(\Lambda)}$$

## The example of the trine:

Define the ensemble $\mathcal{E}$ with

$p(0) = p(1) = p(2) = 1/3$, $\rho_x = |\psi_x\rangle\langle\psi_x|$ ,

$|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle$

$|\psi_2\rangle = \cos\frac{\pi}{3}|0\rangle - \sin\frac{\pi}{3}|1\rangle$

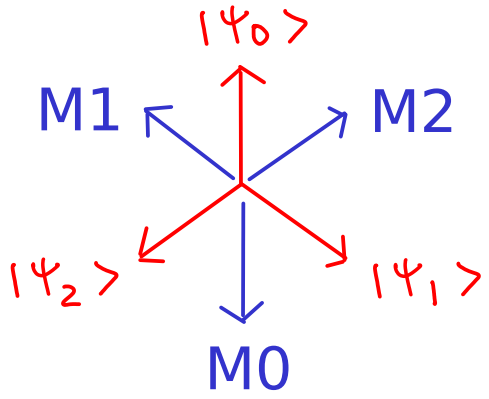
Optimal measurement

$M_1 = \{M_k\}_{k=0,1,2}$

$M_0 = |\psi_0^\perp\rangle\langle\psi_0^\perp| = |1\rangle\langle 1|$

$M_1 = |\psi_1^\perp\rangle\langle\psi_1^\perp|$ , $|\psi_1^\perp\rangle = \sin\frac{\pi}{3}|0\rangle - \cos\frac{\pi}{3}|1\rangle$

$M_2 = |\psi_2^\perp\rangle\langle\psi_2^\perp|$ , $|\psi_2^\perp\rangle = \sin\frac{\pi}{3}|0\rangle + \cos\frac{\pi}{3}|1\rangle$




Iacc = $H(X) - H(X|Y) = (\log 3) - 1 = 0.5850.$

## Additivity of accessible info on product ensembles



Let $\mathcal{F}_1 = \{ p(x_1), \rho_{x_1} \}$ , $\mathcal{F}_2 = \{ p(x_2), \sigma_{x_2} \}$

The product ensemble of $\mathcal{F}_1, \mathcal{F}_2$ is

$$\mathcal{F}_1 \otimes \mathcal{F}_2 = \{ p(x_1) p(x_2) , \rho_{x_1} \otimes \sigma_{x_2} \}$$

Thm. $I_{acc}(\mathcal{F}_1 \otimes \mathcal{F}_2) = I_{acc}(\mathcal{F}_1) + I_{acc}(\mathcal{F}_2)$

So, applying the 2 optimal measurements on the 2 ensembles separately is optimal for the product ensemble.

e.g., for 2 draws of the trine ensemble,
there are 9 equiprobable 2-qubit states:

$|\psi_0\rangle|\psi_0\rangle$ $|\psi_0\rangle|\psi_1\rangle$ $|\psi_0\rangle|\psi_2\rangle$

$|\psi_1\rangle|\psi_0\rangle$ $|\psi_1\rangle|\psi_1\rangle$ $|\psi_1\rangle|\psi_2\rangle$

$|\psi_2\rangle|\psi_0\rangle$ $|\psi_2\rangle|\psi_1\rangle$ $|\psi_2\rangle|\psi_2\rangle$

Optimal measurement can be chosen to be:

$M_0 \otimes M_0$ $M_1 \otimes M_0$ $M_2 \otimes M_0$

$M_0 \otimes M_1$ $M_1 \otimes M_1$ $M_2 \otimes M_1$

$M_0 \otimes M_2$ $M_1 \otimes M_2$ $M_2 \otimes M_2$

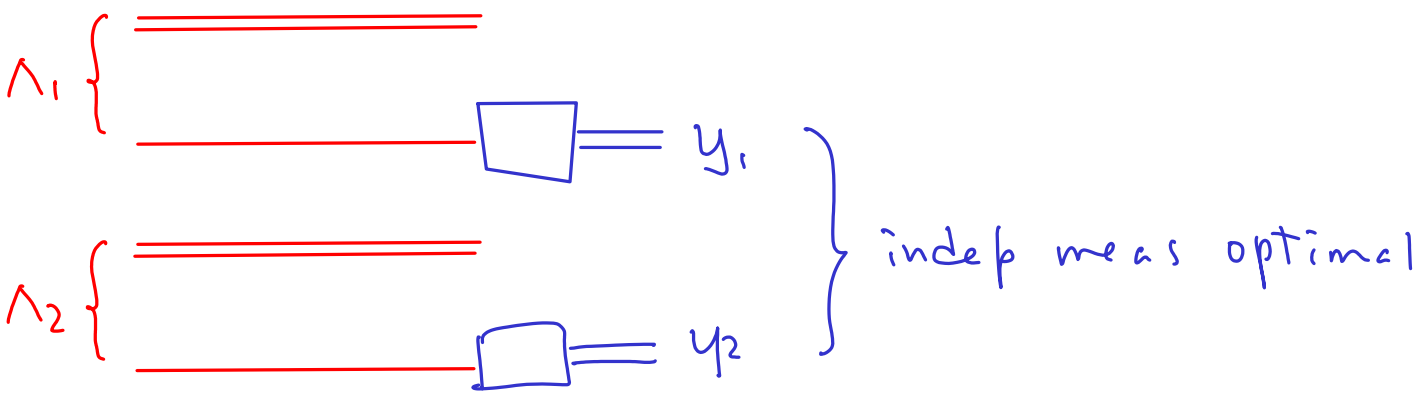
for $M_0 = |\psi_0^\perp\rangle\langle\psi_0^\perp|$

$M_1 = |\psi_1^\perp\rangle\langle\psi_1^\perp|$

$M_2 = |\psi_2^\perp\rangle\langle\psi_2^\perp|$

Accessible info = 2 * 0.5850 = 1.19 bit

$$\Lambda_1 = \sum_{x_1} \frac{1}{3} |x_1\rangle\langle x_1| \otimes |\psi_{x_1}\rangle\langle\psi_{x_1}|$$




$$\Lambda_2 = \sum_{x_2} \frac{1}{3} |x_2\rangle\langle x_2| \otimes |\psi_{x_2}\rangle\langle\psi_{x_2}|$$

$$\max I(X_1X_2 : Y_1Y_2) = 2 \times 0.585$$

Today: exotic properties of Iacc, and useful bounds and consequences, including the Holevo bound.

Instead of 2 draws of the trines, next we consider the double trine.

The double trine: Define the ensemble $\mathcal{E}_2$ with

$p(0) = p(1) = p(2) = 1/3$, $\rho_x = |\psi_x\rangle\langle\psi_x|^{\otimes 2}$, $|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle$

$|\psi_2\rangle = \cos\frac{\pi}{3}|0\rangle - \sin\frac{\pi}{3}|1\rangle$

Note the difference of the double trine from 2 draws of the trine: only 3 states here, and the two qubits are in identical states

You will work out some details in A3.
We consider 2-3 measurements briefly here.

We call the first and second qubit Q1 and Q2 resp.

The double trine: Define the ensemble $\mathcal{E}_2$ with

$p(0) = p(1) = p(2) = 1/3$, $\rho_x = |\psi_x\rangle\langle\psi_x|^{\otimes 2}$, $|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle$

$|\psi_2\rangle = \cos\frac{\pi}{3}|0\rangle - \sin\frac{\pi}{3}|1\rangle$

Consider the measurement $\mathcal{M}_2$ :

(1) on 1st qubit, apply optimal meas for 1 draw of trine

$\mathcal{M}_1 = \{M_k\}_{k=0,1,2}$

$M_0 = |\psi_0^\perp\rangle\langle\psi_0^\perp| = |1\rangle\langle 1|$

$M_1 = |\psi_1^\perp\rangle\langle\psi_1^\perp|$, $|\psi_1^\perp\rangle = \sin\frac{\pi}{3}|0\rangle - \cos\frac{\pi}{3}|1\rangle$

$M_2 = |\psi_2^\perp\rangle\langle\psi_2^\perp|$, $|\psi_2^\perp\rangle = \sin\frac{\pi}{3}|0\rangle + \cos\frac{\pi}{3}|1\rangle$

by symmetry

If outcome is "a" then $\rho_a$ is ruled out. WLOG, let a=0.

Second qubit equally likely to be $|\psi_1\rangle$, $|\psi_2\rangle$.

(2) on 2nd qubit, apply optimal meas for ensemble $\{\frac{1}{2}, |\psi_i\rangle\}_{i=1,2}$

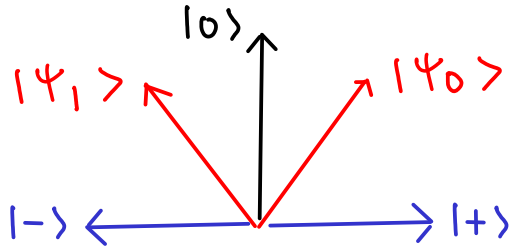
From last time:

Example 1. $x = 0, 1$, $p(0) = p(1) = 1/2$,

$\rho_x = |\psi_x\rangle\langle\psi_x|$ , $|\psi_0\rangle = a|0\rangle + b|1\rangle$

$|\psi_1\rangle = a|0\rangle - b|1\rangle$ $\quad a, b \geq 0$ , $a^2 + b^2 = 1$

Optimal measurement:
projective, along basis $\{|+\rangle, |-\rangle\}$




We found all the p(xy) ...

Iacc = I(X:Y) = $H(X) - H(X|Y) = 1 - h(1/2+ab)$

The double trine: Define the ensemble $\mathcal{E}_2$ with

$p(0) = p(1) = p(2) = 1/3$, $\rho_x = |\psi_x\rangle\langle\psi_x|^{\otimes 2}$, $|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle$

$|\psi_2\rangle = \cos\frac{\pi}{3}|0\rangle - \sin\frac{\pi}{3}|1\rangle$

The measurement $M_2$ :

(1) on 1st qubit Q1, apply optimal meas for 1 draw of trine

got outcome "a" (rv A)

(2) conditioned on the first outocme being "a", a postmeas ensemble is induced on 2nd qubit Q2:

$\widetilde{\mathcal{E}}$ : $|\psi_b\rangle$, $|\psi_c\rangle$, $b \neq a$, $c \neq a$

each with prob 1/2

apply optimal meas for $\widetilde{\mathcal{E}}$

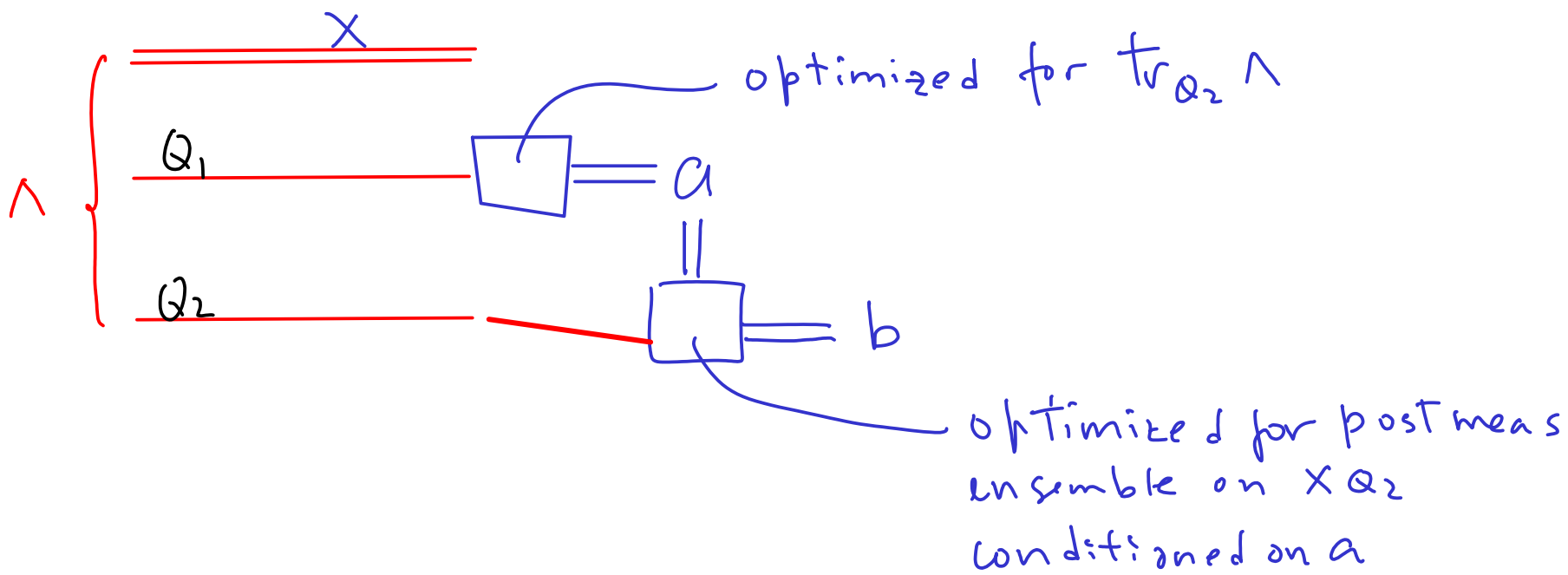
got outcome "b" (rv B|A=a)

What is the mutual info between X and AB? From A3: ~1.23038 bit

NB: this lower bounds Iacc of the double trine, and exceeds Iacc of 2 indep draws of the trine (2 * 0.5850 = 1.19 bits)

* correlation between Q1, Q2 can increase mutual info between X and meas outcome -- back to this later.

$$\Lambda = \sum_x \frac{1}{3} |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|^{\otimes 2}$$




$I(X:AB) = 1.23038$ bit.

The double trine: Define the ensemble $\mathcal{E}_2$ with

$p(0) = p(1) = p(2) = 1/3$, $\rho_x = |\psi_x\rangle\langle\psi_x|^{\otimes 2}$, $|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle$

$|\psi_2\rangle = \cos\frac{\pi}{3}|0\rangle - \sin\frac{\pi}{3}|1\rangle$

Consider the measurement $M_3$ :

Let $\Gamma = \rho_0 + \rho_1 + \rho_2$, $M_y = \Gamma^{-\frac{1}{2}} \rho_y \Gamma^{-\frac{1}{2}}$ for $y = 0, 1, 2$

$M_3 = I - M_0 - M_1 - M_2$

If $\Gamma = \sum_k \lambda_k |e_k\rangle\langle e_k|$, $\lambda_k > 0$, then $\Gamma^{-\frac{1}{2}} = \sum_k \lambda_k^{-\frac{1}{2}} |e_k\rangle\langle e_k|$.

NB: $\Gamma$ separable, but $\Gamma^{-\frac{1}{2}}$ may not be.

So, $M_3$ may not be separable.

The double trine: Define the ensemble $\mathcal{E}_2$ with

$p(0) = p(1) = p(2) = 1/3$, $\rho_x = |\psi_x\rangle\langle\psi_x|^{\otimes 2}$, $|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle$

$|\psi_2\rangle = \cos\frac{\pi}{3}|0\rangle - \sin\frac{\pi}{3}|1\rangle$

Consider the measurement $M_3$ :

Let $\Gamma = \rho_0 + \rho_1 + \rho_2$, $M_y = \Gamma^{-\frac{1}{2}} \rho_y \Gamma^{-\frac{1}{2}}$ for $y = 0, 1, 2$

$M_3 = I - M_0 - M_1 - M_2$

From A3: I(X:Y) = 1.3691 bit

NB: this exceeds the mutual info obtained by $M_2$ with first meas optimized on Q1, and use the outcome to optimize the 2nd meas on Q2 (1.23038 bit)

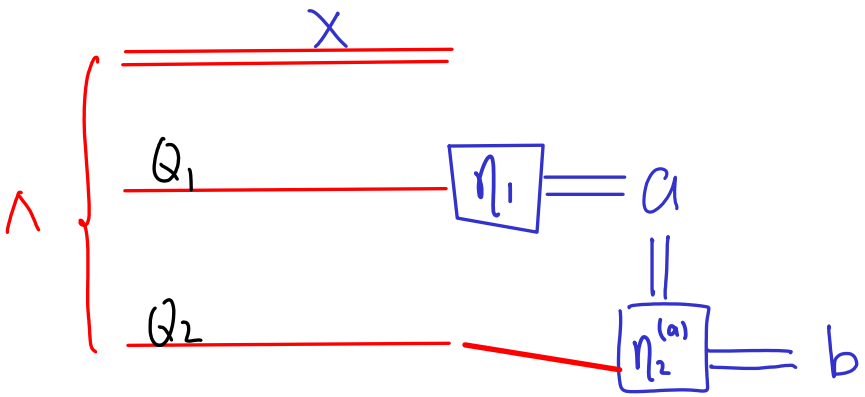
* a "joint measurement" on Q1 Q2 can exceed the mutual info obtained from classically adapting 2nd meas on the 1st outcome

$M_3$ believed to be optimal for the double trine.

Final step in Decker's analysis in 0509122 is numerical.

Wootters in 0506149 found a separable meas with the same I(X:Y).

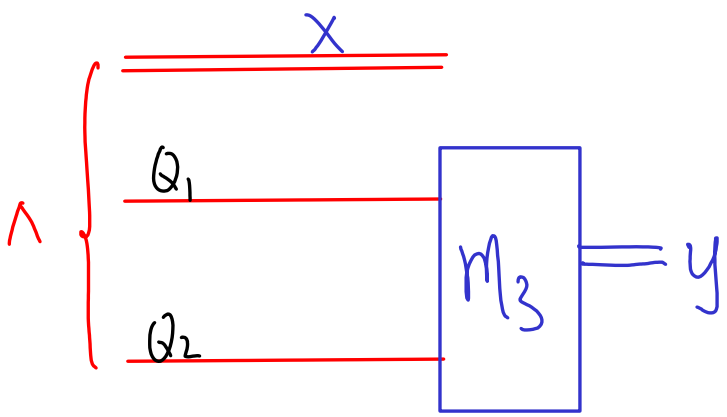
$$\Lambda = \sum_x \frac{1}{3} |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|^{\otimes 2}$$




$$I(X:AB) = 1.23038 \text{ bit.}$$

with $\eta_1, \eta_2^a$ optimized

$$\Lambda = \sum_x \frac{1}{3} |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|^{\otimes 2}$$




$$I(X:Y) = 1.3691 \text{ bit.}$$

will return to optimizing the correlation and measurement for creating cbits ...

# Example 4. (Un)Locking of accessible information

Consider an n-dim quantum system, and the 2n states forming the computational basis and a conjugate basis:

$|0\rangle, |1\rangle, |2\rangle, \ldots, |n-1\rangle$

$U|0\rangle, U|1\rangle, U|2\rangle, \ldots, U|n-1\rangle$

where $U|v\rangle = \frac{1}{\sqrt{n}} \sum_l \omega^{vl} |l\rangle$, $\omega^n = 1$, $\omega$ primitive n-th root of unity

e.g., n=3 ,

$|0\rangle, |1\rangle, |2\rangle$

$U|0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$

$U|1\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega|1\rangle + \omega^2|2\rangle)$

$U|2\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2|1\rangle + \omega|2\rangle)$

Example 4. (Un)Locking of accessible information

Consider an n-dim quantum system, and the 2n states forming the computational basis and a conjugate basis:

$|0\rangle, |1\rangle, |2\rangle, \ldots, |n-1\rangle$

$U|0\rangle, U|1\rangle, U|2\rangle, \ldots, U|n-1\rangle$

where $U|v\rangle = \frac{1}{\sqrt{n}} \sum_l \omega^{vl} |l\rangle$, $\omega^n = 1$, $\omega$ primitive n-th root of unity

Let $\sigma_x = U^k |v\rangle\langle v| U^{k\dagger}_C$ $\qquad x = vk$, $v \in \{0, 1, \ldots, n-1\}$, $k \in \{0, 1\}$.

Consider 2n states on 2n-dims:

$\rho_x = U^k |v\rangle\langle v| U^{k\dagger}_C \otimes |k\rangle\langle k|_B$, $\qquad x = vk$, $v \in \{0, 1, \ldots, n-1\}$, $k \in \{0, 1\}$.

encode n possible messages — basis info

either in the computational or conjugate basis

Define 2 ensembles: $\mathcal{E}_1 = \{p_x, \rho_x\}$, $\mathcal{E}_2 = \{p_x, \sigma_x\}$, $p_x = \frac{1}{2n}$.

i.e., each state in $\mathcal{E}_2$ is obtained from $\mathcal{E}_1$ by removing B.

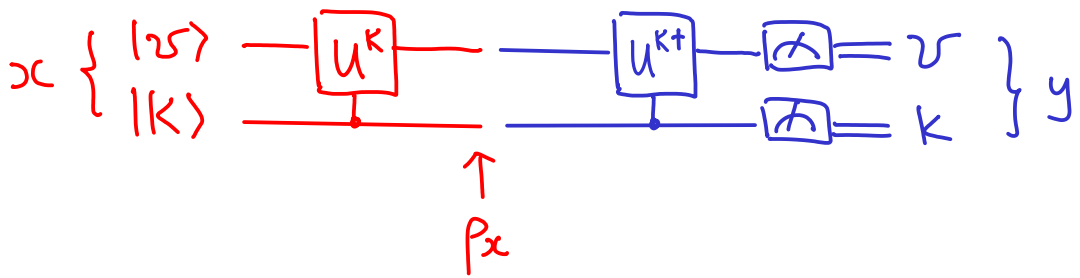
Example 4. (Un)Locking of accessible information

$\mathcal{E}_1 = \{p_x, \rho_x\}$, $\mathcal{E}_2 = \{p_x, \sigma_x\}$, $p_x = \frac{1}{2n}$.

$\rho_x = U^k |v\rangle\langle v| U^{k\dagger}_C \otimes |k\rangle\langle k|_B$, $x = vk$, $v \in \{0, 1, \ldots, n-1\}$, $k \in \{0, 1\}$.

$\sigma_x = U^k |v\rangle\langle v| U^{k\dagger}_C$

attained by the meas:




① $I_{acc}(\mathcal{E}_1) = \log(2n)$

② $I_{acc}(\mathcal{E}_2) = \frac{1}{2}\log n$ (A3, 0303088)

Removing 1 qubit (B) from $\mathcal{E}_1$ reduces the accessible info by

$I_{acc}(\mathcal{E}_1) - I_{acc}(\mathcal{E}_2) = \log(2n) - 1/2 \log(n) = 1 + 1/2 \log(n) \gg S(B)$

System B is like a "key" which locks the 1/2 log n bits of acc info in system C.

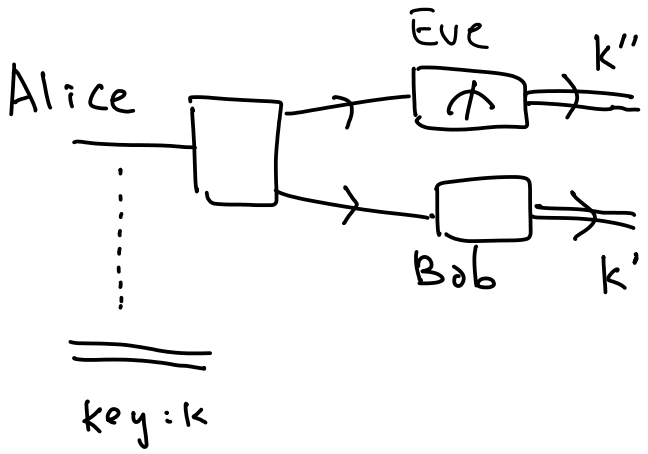
In 0307104, $(\log n)^3$ random bases (almost conjugate, easier to analyse) suppresses the acc info to $3 + \frac{\epsilon}{2} \log n$.

Key size: O(log log n), amount locked: ~ log n (max on C).

* Accessible info assumes a measurement is applied.

* But the optimal choice of measurement is sensitive to additional side info (or sensitive to small changes in the ensemble), which, in the example, is the basis info.

Before 2004, most QKD papers used accessible info to measure the security of QKD.




Want: I(K:K") small, K=K' with high prob.

But Eve need not meas her state immediate -- she can wait for Alice and Bob to use the key, and jointly attack the key and the application.

In 0409078, "composable" security measures are introdcued to resolve these kind of problems.

# Accessible information and Holevo information

Recall $\mathcal{E} = \{p_x, \rho_x\}$, $\Lambda = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_x$

The Holevo information for the ensemble

$$S(X:Q) = \chi(\mathcal{E}) = S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x)$$

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

Proof: $I_{acc}(\mathcal{E}) := \max_{\mathcal{M}} I(X:Y)_{I\otimes\mathcal{M}(\Lambda)} \leq S(X:Q)_{\Lambda}$

↑ quantum data processing ineq
(or mono of QMI under TCP maps)

e.g., $\mathcal{E}_2$ in locking example, $I_{acc}(\mathcal{E}_2) = \frac{1}{2}\log n$

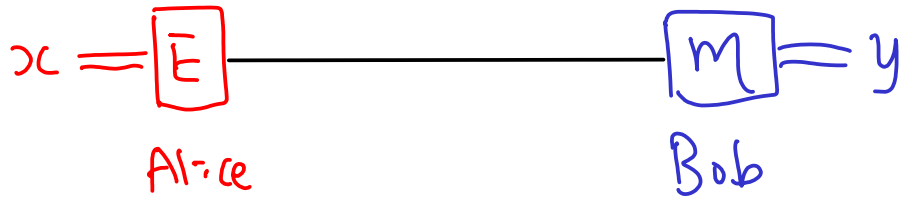
$\chi(\mathcal{E}_2) = \log n$

Holevo bound: if a d-dim system is transmitted from Alice to Bob, then, they can create at most log d cbits.

Proof: suppose there is a protocol consuming log d qbits that allows Alice to comm one out of t messages to Bob

If her message is x, Bob receives the state $\rho_x$.

Bob measures $\rho_x$ and outputs y as his decoded message.




Let x be uniformally distributed.
If x=y with high prob, log t ~ I(X:Y) (Fanos inequality)

$$\lesssim I_{acc}\left(\left\{\tfrac{1}{t}, \rho_x\right\}\right)$$

$$\lesssim \chi\left(\left\{\tfrac{1}{t}, \rho_x\right\}\right)$$

$$\lesssim S\left(\sum_x \tfrac{1}{t}\rho_x\right) \leq \log d$$

## Holevo information is unlockable

Recall the Araki-Lieb inequality and how much S and QMI change when adding and discard systems:

$$|\, S(AB) - S(A) \,| \leq S(B)$$

$$|\, S(AB:C) - S(A:C) \,| \leq 2\, S(B)$$

} entropy and QMI are unloackable

Let $\sigma_x = \mathrm{tr}_B \rho_x$ , $\mathcal{E}_1 = \{\rho_x, \rho_x\}$, $\mathcal{E}_2 = \{\rho_x, \sigma_x\}$

$$\Lambda_1 = \sum_x \rho_x |x\rangle\langle x|_A \otimes \rho_{x\,BC}$$

$$\Lambda_2 = \sum_x \rho_x |x\rangle\langle x|_A \otimes \sigma_{x\,C} = \mathrm{tr}_B(\Lambda_1)$$

$$\chi(\mathcal{E}_1) = S(AB:C)_{\Lambda_1}, \quad \chi(\mathcal{E}_2) = S(A:C)_{\Lambda_2}$$

By the Araki-Lieb ineq for QMI, $|\chi(\mathcal{E}_1) - \chi(\mathcal{E}_2)| \leq 2S(B)$

## Holevo bound in interactive protocol:

(Cleve, van Dam, Nielsen, Tapp 9708019)

Suppose Alice is allowed to send $n_A$ qubits to Bob

Bob is allowed to send $n_B$ qubits to Alice

in any order in an interactive protocol with any # of rounds.

Then, Alice can communicate at most $n = n_A + n_B$ bits to Bob.

Proof: let Alice's message x occur with prob p(x).

After the j-th qubit of comm (Alice's and Bob's combined), let Bob's state be $\rho_{xj}$.

i.e., Bob has the quantum state of the ensemble $\mathcal{E}_j = \{p(x), \rho_{xj}\}$.

Let Bob's final decoded message be y.

$$I(X:Y) \leq I_{acc}(\mathcal{E}_n) \leq \chi(\mathcal{E}_n) \leq S\left(\sum_x p_x \rho_{xn}\right)$$

$n = n_A + n_B$ ↑ unweldy

nice

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

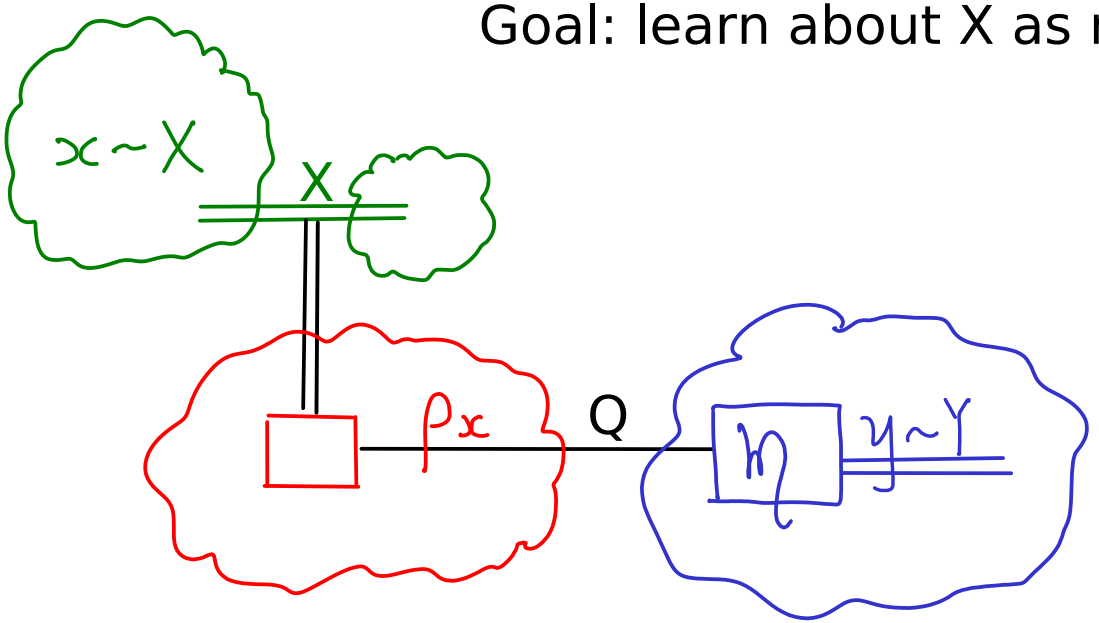
$$\vdots$$

$$\leq n_A + n_B = n$$

diff by 1 qubit AL on S

# Scenarios of encoding classical data into quantum states & retrieving it

Goal: learn about X as much as possible via rv Y.




joint distribution p(xy)

Scenario 1: accessible information / states discrimination

$\rho_x$ , $\rho_x$ predetermined

Richard draws x with prob p(x), prepares $\rho_x$ , gives state to Bob

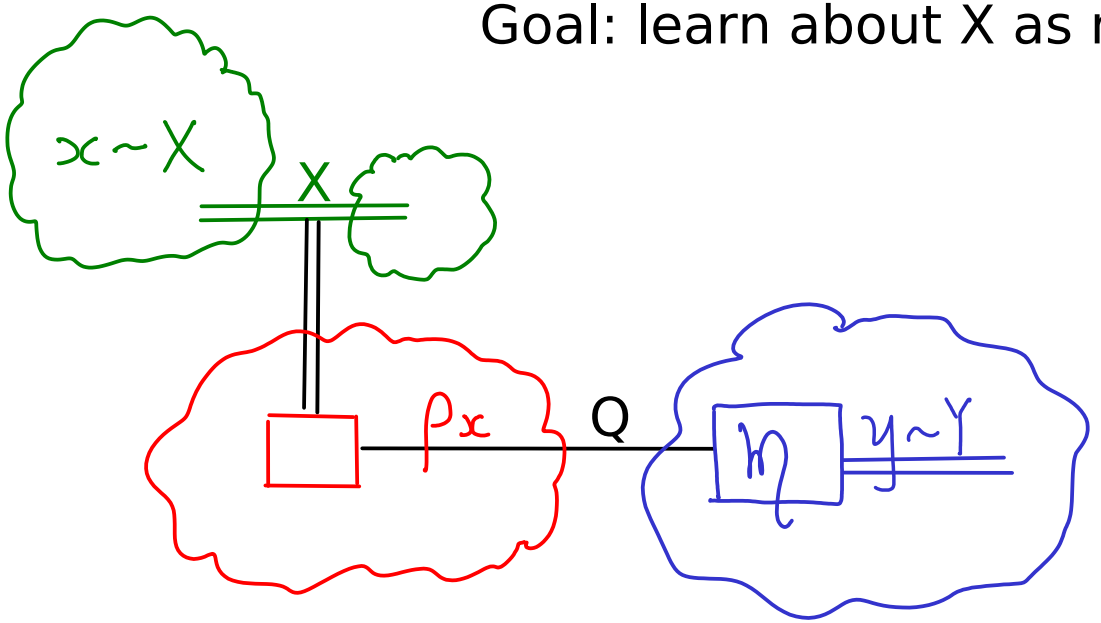
Bob picks measurement

(a) max prob(X=Y): state discrimination

(b) max I(X:Y): accessible information

# Scenarios of encoding classical data into quantum states & retrieving it

Goal: learn about X as much as possible via rv Y.




joint distribution p(xy)

Scenario 2: classical channel

$\rho_x$, $\mathcal{M}$ predetermined POVM $\{M_y\}$, $M_y \geq 0$, $\sum_y M_y = I$

Alice chooses x,

corresponding state $\rho_x$ generated, and measured (with fixed meas),

outcome is given to Bob.

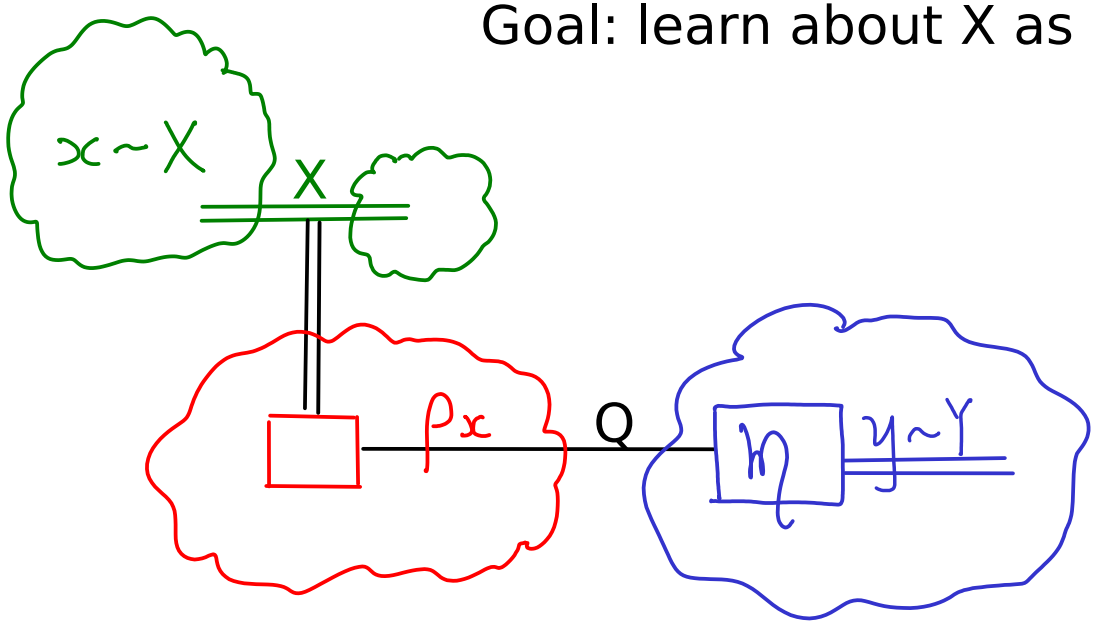
For each x, Bob receives y with prob p(y|x) = $\mathrm{tr}\, M_y \rho_x$

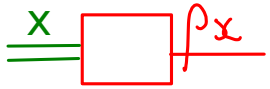
Last week: for large number of uses,

can create max_p(x) I(X:Y) cbits per use

# Scenarios of encoding classical data into quantum states & retrieving it

Goal: learn about X as much as possible via rv Y.




Q box 


as if Alice presses a button "x" and Q box spits out $\rho_x$ to Bob

Scenario 3: Q box

$\rho_x$ predetermined

Alice chooses x,

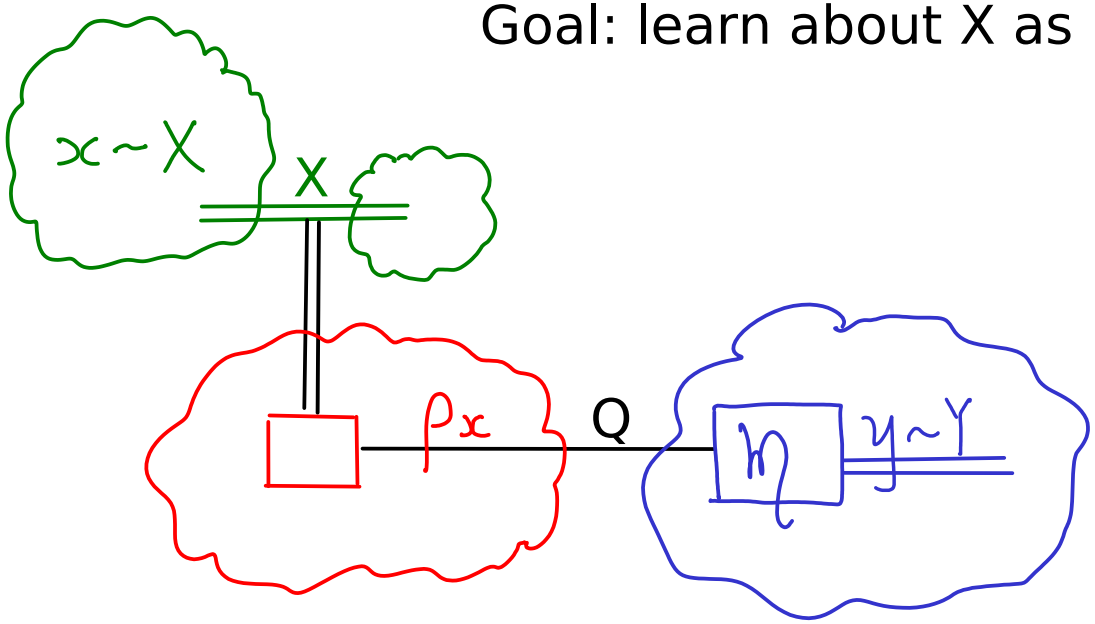
corresponding state $\rho_x$ generated and available to Bob.

Bob picks measurement and obtains y.

If Bob sticks to optimal meas for I(X:Y) for each system,
this reduces to scenario 2.

# Scenarios of encoding classical data into quantum states & retrieving it

Goal: learn about X as much as possible via rv Y.




Q box 


as if Alice presses a button "x" and Q box spits out $\rho_x$ to Bob

Scenario 3: Q box

$\rho_x$ predetermined

Alice chooses x,

corresponding state $\rho_x$ generated and available to Bob.

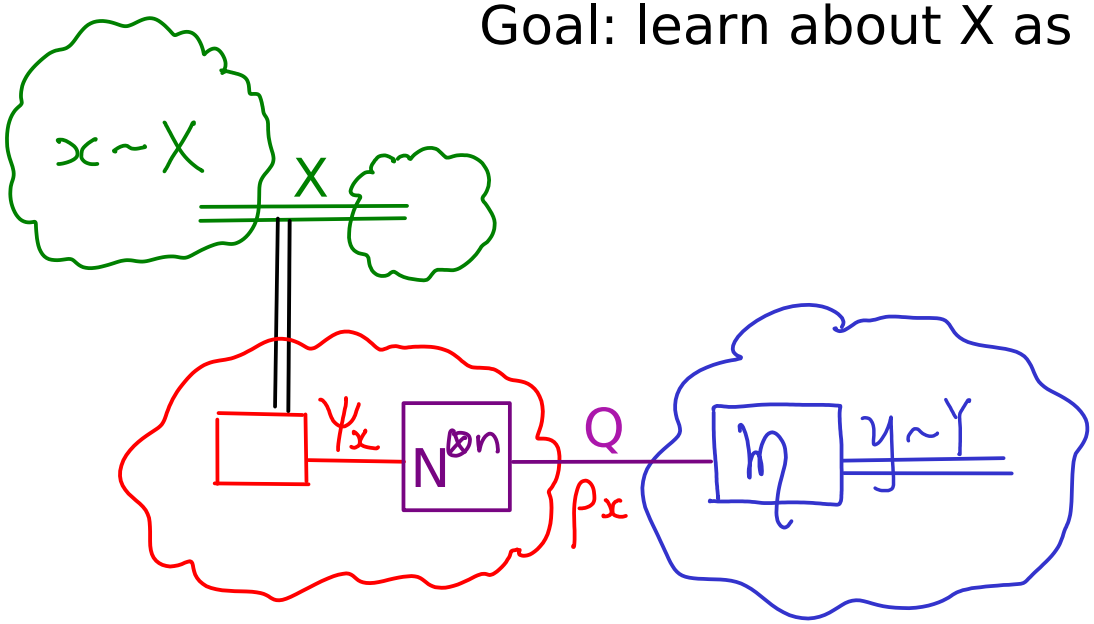
Bob picks measurement and obtains y.

Scenario 3: for multiple uses, Bob can choose JOINT measurement.

Next lecture: for large number of uses of Q boxes, can create S(X:Q) cbits per use, for $\Lambda = \sum_x p_x \, |x\rangle\langle x|_X \otimes \rho_{xQ}$.

# Scenarios of encoding classical data into quantum states & retrieving it

Goal: learn about X as much as possible via rv Y.




Scenario 4: classical capacity of quantum channel given N

Alice chooses x, and $\psi_x$ (the input to n uses of N)

$\rho_x$ is the channel output available to Bob.

Bob picks measurement and obtains y.

Scenario 4: for multiple uses, Bob can choose JOINT measurement.

Optimized: C(N) classical capacity of quantum channel N (next Thur).