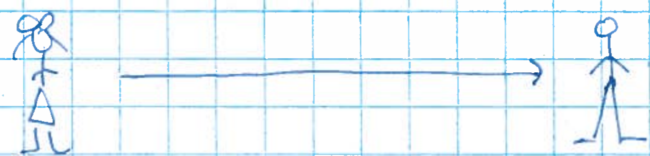
Lec 1: CO781 / QIC 890 F2016

Simple communication scenario:

One sender Alice   One receiver Bob



Goal: transmit data from Alice to Bob

- Example 1:

Data: classical message $m \in \{0,1\}$. (1 bit message).

Given: noiseless channel N with input symbol $X = \{0,1\}$
output " $Y = \{0,1\}$

$$\text{s.t. } \Pr(Y=y \mid X=x) = \delta_{yx} = \begin{cases} 0 & \text{if } x \neq y \\ 1 & \text{if } x = y \end{cases}$$

Method: Alice set the input $x = m$, so Bob's output is m.

The ability to transmit 1 classical bit : 1 cbit ← can be given or achieved
(forward, from A to B) $(\rightarrow)$

- NB: If $m \in \{0,1,2,\ldots,n-1\}$,

it can be expressed in binary form

and be transmitted to Bob using $\lceil \log_2 n \rceil$ cbits

- Example 2:

Data: classical message $m \in \{0,1\}$

Given: noiseless quantum channel N — qbit

transmitting any "q. state on 2-dim sys" — a q-bit

from Alice to Bob perfectly.

Method: Alice set the input $|\psi_m\rangle = |m\rangle$

where $\{|0\rangle, |1\rangle\}$ basis for $\mathbb{C}^2$.

Bob measures his output along the basis $\{|0\rangle, |1\rangle\}$

and the outcome is "m".

Call the ability to transmit 1 qubit : qbit

We say $\underbrace{1 \text{ qbit}}_{\text{What you are given}} \geq \underbrace{1 \text{ cbit}}_{\text{What you achieve.}}$

there is a method to convert the LHS to the RHS

- If m has n values, it can be transmitted to Bob using $\lceil \log_2 n \rceil$ qbits.

Qn: Can we send k bits using n cbits for $k > n$?

Qn: - - - - - - - - - - - n qbits - - - - ?

Ans: No & Yes. Need to spell out assumptions - - .

- Example 3: Superdense coding SD.

Data: $m \in \{0,1,2,3\}$ (2 bits of data)

Given: 1 qbit

Also Alice & Bob share "1 ebit":

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

Method: ① Alice applies σ_m to system A.

$$\underbrace{\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},}_{} \quad \underbrace{\sigma_0 \otimes I\,|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}.}_{}$$

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_1 \otimes I\,|\Phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)_{AB}$$

$$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_3 \otimes I\,|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}$$

$$\sigma_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 \otimes I\,|\Phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)_{AB}.$$

all unitary so can be applied.

Mutually orthogonal. Form the "Bell basis".

② Alice sends A to Bob using 1 qbit.

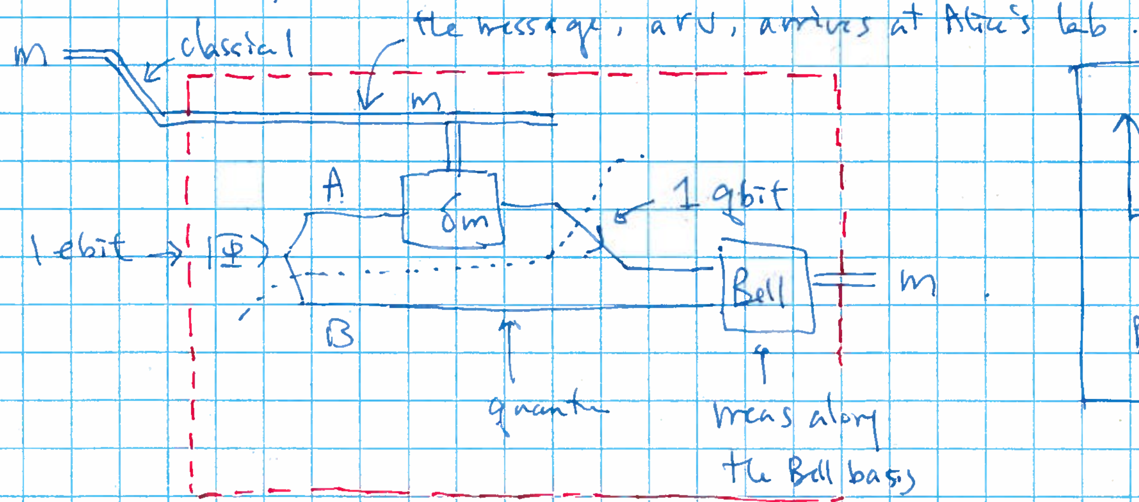
③ Bob now has both A & B, makes a Bell measurement to find out m.

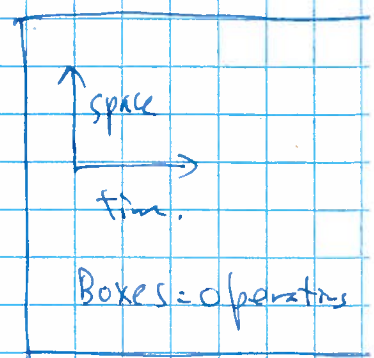
Resource inequality: 1 qbit + 1 ebit $\geq$ 2 cbits.

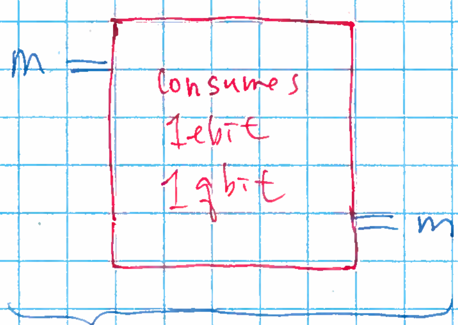
Do we cheat, since Alice may have to send B to Bob to create $|\Phi\rangle$?

No. $|\Phi\rangle$ can be created by Bob sending A to Alice. Or be given to them by a 3rd Party. It's there BEFORE m.

Circuit diagram:







achieves 2 cbits

Example 4: teleportation TP

Data: 1 qubit state $|\psi\rangle_{A_1} = a|0\rangle + b|1\rangle$

Given: 1 ebit & 2 cbits

(So Alice & Bob share $|\Phi\rangle_{AB}$
and Alice can transmit one of 4 messages to Bob).

Idea: $|\psi\rangle_{A_1} |\Phi\rangle_{AB} = (a|0\rangle + b|1\rangle)_{A_1} \overset{\otimes}{} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{AB}$

$$= \frac{1}{2} \times \left[\begin{array}{l} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{A_1A} (a|0\rangle + b|1\rangle)_B \\ + \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)_{A_1A} (a|0\rangle - b|1\rangle)_B \\ + \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)_{A_1A} (a|1\rangle + b|0\rangle)_B \\ + \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)_{A_1A} (a|1\rangle - b|0\rangle)_B \end{array} \right]$$

First two lines: $a|000\rangle + b|111\rangle$

Last two lines: $a|011\rangle + b|100\rangle$

e.g. $a|011\rangle$

Method: ① Alice applies Bell meas on $A_1 A$.
collapsing the state to one of the 4 lines.
outcome $m = 0, 3, 1, 2$ respectively.

② Alice sends m to Bob using 2 cbits

③ Bob now knows he has $\sigma_m |\psi\rangle$.
So he applies $\sigma_m^{-1} = \sigma_m$ to B to recover $|\psi\rangle$.

Note:

1. a, b take ∞ many bits to describe and given 1 specimen of $|\psi\rangle$, Alice cannot extract much of that info (topic 4).

   She doesn't need to know a, b and only needs to send 2 bits to Bob given entanglement.

2. What does Bob have BEFORE receiving m?
   Each m occurs with prob 1/4 (the norm square of each line corresponding are equal).

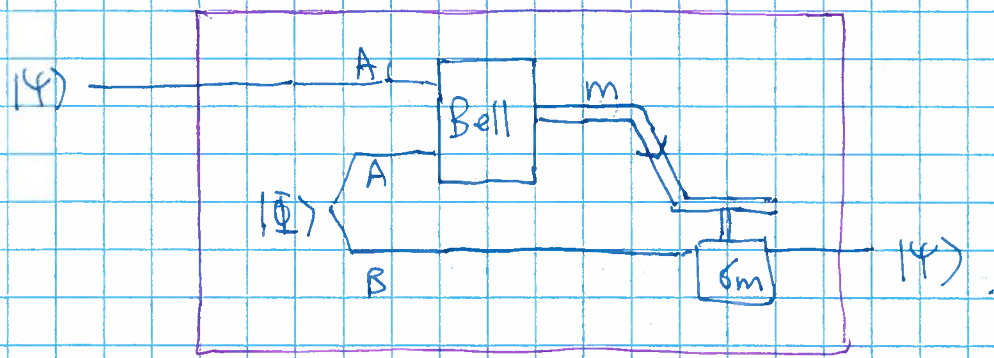
   Bob's state is
   $$\frac{1}{4}\sigma_0|\psi\rangle\langle\psi|\sigma_0 + \frac{1}{4}\sigma_1|\psi\rangle\langle\psi|\sigma_1 + \underset{\text{prob}}{\frac{1}{4}}\underbrace{\sigma_2|\psi\rangle\langle\psi|\sigma_2}_{\text{density matrix}} + \frac{1}{4}\sigma_3|\psi\rangle\langle\psi|\sigma_3 .$$

   But it is also half of $|\Phi\rangle$: $\operatorname{tr}_A |\Phi\rangle\langle\Phi| = \frac{I}{2}$.

   basis $\rightarrow$ 00 01 10 11

   $$\Phi = |\Phi\rangle\langle\Phi| = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \xrightarrow{\operatorname{tr}_A} \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{I}{2}.$$

   So no signalling to B.6 until "m" received.



The purple box simulates or achieves the transmission of $|\psi\rangle$ from A_1 to B, and consumes 1 ebits & 2 cbits.

$\therefore$ TP : 2 cbits + 1 ebit $\geq$ 1 qbit

$\exists$ protocol converting the LHS to the RHS.

Ex : What happens if Alice wants to transmit $|\psi\rangle \in \mathbb{C}^n$?
What about a reference preparing $|\eta\rangle_{RA_1}$
and the goal is to have $|\eta\rangle_{RB}$ in the end?

ie how to teleport part of an entangled state when Alice & Bob have no access to R?

Density matrix of B before "m" is received is well defined

i.e. $\forall |\psi\rangle, \quad \underbrace{\frac{1}{4}\sum_{i=0}^{3} \sigma_i |\psi\rangle\langle\psi| \sigma_i = \frac{I}{2}.}_{\text{this gives an encryption scheme}}$

NB: $|\psi\rangle$ disappeared after Bell meas & before m arrives @ Bob

It is a secret sharing scheme splitting

$|\psi\rangle$ into m & $\sigma_m |\psi\rangle\langle\psi| \sigma_m$. w/ equal prob.

- Peres the method to perform QECC by entanglement purification.

- It's the soul not the body being teleported – Asher Peres.

basis indep't.

Quantum information : $|\psi\rangle_S \in \mathbb{C}^d$, or $\rho_S \in B(\mathbb{C}^d)$

Basis. dep't

Classical information : rv $pr(x) = p_x$

Church of larger Hilbert space : $\rho_S = \mathrm{Tr}_E\, |\xi\rangle\langle\xi|$

where $|\xi\rangle_{SE} = \sum_x \sqrt{p_x}\, |x\rangle_S |x\rangle_E$

Someone already has a copy and you can never get it back.

$\rho_S = \sum_x p_x |x\rangle\langle x|$ Diagonal density matrix in the basis describing the classical information

$\Leftrightarrow \forall\, |\eta\rangle_{RA} \in \mathbb{C}^d \otimes \mathbb{C}^d$, $|\psi\rangle_{RA} \to |\psi\rangle_{RB}$.

qbit : $\forall\, |\psi\rangle \in \mathbb{C}^d$, $|\psi\rangle_A \to |\psi\rangle_B$. isometry

$\Leftrightarrow \forall\, |x\rangle$, $x = 0, 1, \ldots, d-1$, $|x\rangle_A \to |x\rangle_B$ by linearity.

basis

cbit : $\forall\, |x\rangle$, $x = 0, 1, \ldots, d-1$, $|x\rangle_A \to |x\rangle_E |x\rangle_B$

leaves the environment w/ a copy of the information.