Lecture 3

17 JUN 2014

- no-cloning theorem
- entanglement distribution
- super-dense coding
- teleportation
- optimality of these.
- monogamy of entanglement

No-cloning theorem

there does not exist a universal quantum copying machine, i.e., a ~~[illegible]~~ unitary U that gives the transformation

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \forall |\psi\rangle$$

Proof: let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

~~So~~ Suppose this U exists.

then the output is

$$|\psi\rangle|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$
$$= \alpha^2|00\rangle + \beta\alpha(|10\rangle + |01\rangle) + \beta^2|11\rangle$$

However all transformations are linear so that if

$$U|0\rangle|0\rangle = |0\rangle|0\rangle$$

$$U|1\rangle|0\rangle = |1\rangle|1\rangle$$

then $U(\alpha|0\rangle + \beta|1\rangle)|0\rangle =$

$$\alpha|00\rangle + \beta|11\rangle$$

So the only way that this transformation is possible is if

$$\alpha^2 = \alpha$$

$$\alpha\beta = 0$$

$$\& \ \beta^2 = \beta \ , \text{ i.e.,}$$

$$\alpha = 1, \ \beta = 0 \quad \text{or} \quad \alpha = 0, \ \beta = 1$$

There are very important consequences of this theorem for QIP.

~~Lecture 19~~

three noiseless protocols

- entanglement distribution
- super-dense coding
- teleportation

- resource counting
- proofs of optimality

Nonlocal unit resources

1) noiseless qubit channel

$$|i\rangle^A \to |i\rangle^B$$

preserves superpositions so that

$$\alpha|0\rangle^A + \beta|1\rangle^A \to \alpha|0\rangle^B + |1\rangle^B$$

indicate this resource w/ notation

$$[q \to q]$$

2) ~~noiseless classical bit channel~~

$$\cancel{|i\rangle\langle i|^A \to |i\rangle\langle i|^B}$$

$$\cancel{\alpha\ |i\rangle\langle j| \to 0} \quad \text{~~for } i \neq j\text{~~}$$

~~resource is~~

$$\cancel{[c \to c]}$$

4

Ebit : shared nonlocal entanglement

$\frac{1}{\sqrt{2}}\left(|0\rangle^A|0\rangle^B + |1\rangle^A|1\rangle^B\right)$

Classical comm. alone cannot simulate entanglement or quantum comm.

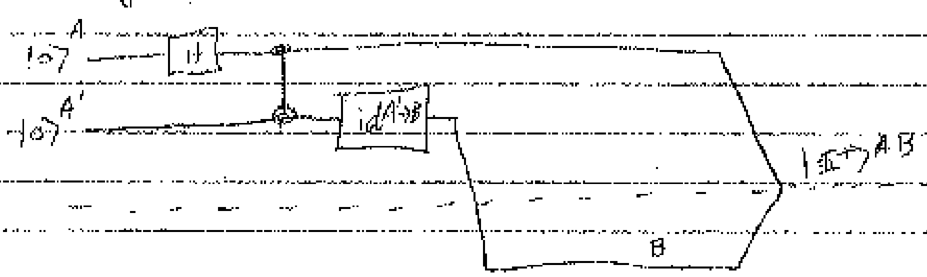
Entanglement alone cannot simulate classical or quantum comm.

1st Protocol : Entanglement Distribution

Two steps

1) Create Bell state locally
2) send half of it over a noiseless qubit channel to create ebit

Diagram



$[q \to q] \to [qq]$

1) becomes ebit
2) only count nonlocal resource
3) operations are perfect

2/3/2011

Could we have

$[qq] \geq [q \to q]$?

no, violates no-signaling (story of Nick Herbert)

i.e. quantum comm. is a stronger comm. resource than entanglement

2nd protocol: Super-dense coding

But first, elementary coding

1) Alice prepares $|0\rangle$ or $|1\rangle$

2) transmits over noiseless qubit channel

3) Bob measures Z

i.e. $[q \to q] \geq [c \to c]$

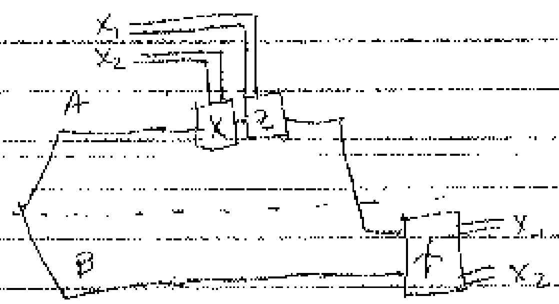
cannot do better than this (homework exercise, or more generally Holevo bound) dense coding

1) Alice & Bob share an ebit $|\Phi^+\rangle^{AB}$.
Alice applies a Pauli operator to her half of the ebit (one of $\{I, X, Z, XZ\}$). state becomes one of

$$|\Phi^+\rangle^{AB}, |\Phi^-\rangle^{AB}, |\Psi^+\rangle^{AB}, |\Psi^-\rangle^{AB}$$

2) transmits A over noiseless qubit channel

3) Bob performs Bell measurement to distinguish these states



resource inequality is

$$[qq] + [q \to q] \geq 2[c \to c]$$

Also: protocol is private

Note: could have done

$$2[q \to q] \geq 2[c \to c]$$

but dense coding only requires weaker resource of entanglement

3rd protocol : teleportation

Alice + Bob "swap their equipment"

Alice + Bob share ebit $|\Phi^+\rangle^{AB}$

Alice wants to transmit qubit

$$|\psi\rangle^{A'} \equiv \alpha|0\rangle^{A'} + \beta|1\rangle^{A'}$$

overall state is

$$|\psi\rangle^{A'}|\Phi^+\rangle^{AB}$$

$$= \left(\alpha|0\rangle^{A'} + \beta|1\rangle^{A'}\right)\left(\frac{|00\rangle^{AB} + |11\rangle^{AB}}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2}}\Big(\alpha|000\rangle^{A'AB} + \alpha|011\rangle^{A'AB} + \beta|100\rangle^{A'AB} + \beta|111\rangle^{A'AB}\Big)$$

use results from homework to write as

$$= \frac{1}{2}\Big[\alpha\left(|\Phi^+\rangle^{A'A} + |\Phi^-\rangle^{A'A}\right)|0\rangle^B + \beta\left(|\Psi^+\rangle^{A'A} - |\Psi^-\rangle^{A'A}\right)|0\rangle^B + \alpha\left(|\Psi^+\rangle^{A'A} + |\Psi^-\rangle^{A'A}\right)|1\rangle^B + \beta\left(|\Phi^+\rangle^{A'A} - |\Phi^-\rangle^{A'A}\right)|1\rangle^B\Big]$$

2/3/2011

$$= \frac{1}{2}\Big\{ |\Phi^+\rangle^{A'A}\left(\alpha|0\rangle^B + \beta|1\rangle^B\right) +$$
$$|\Phi^-\rangle^{A'A}\left(\alpha|0\rangle^B - \beta|1\rangle^B\right) +$$
$$|\Psi^+\rangle^{A'A}\left(\alpha|1\rangle^B + \beta|0\rangle^B\right) +$$
$$|\Psi^-\rangle^{A'A}\left(\alpha|1\rangle^B - \beta|0\rangle^B\right) \Big\}$$

$$= \frac{1}{2}\Big\{ |\Phi^+\rangle^{A'A}|\psi\rangle^B + |\Phi^-\rangle^{A'A} Z|\psi\rangle^B +$$
$$|\Psi^+\rangle^{A'A} X|\psi\rangle^B + |\Psi^-\rangle^{A'A} XZ|\psi\rangle^B \Big\}$$

Now can outline protocol

1) Alice performs Bell measurement on her systems $A'A$. State collapses to

$|\Phi^+\rangle^{A'A}\ |\psi\rangle^B$,
$|\Phi^-\rangle^{A'A}\ Z|\psi\rangle^B$,
$|\Psi^+\rangle^{A'A}\ X|\psi\rangle^B$,
$|\Psi^-\rangle^{A'A}\ XZ|\psi\rangle^B$

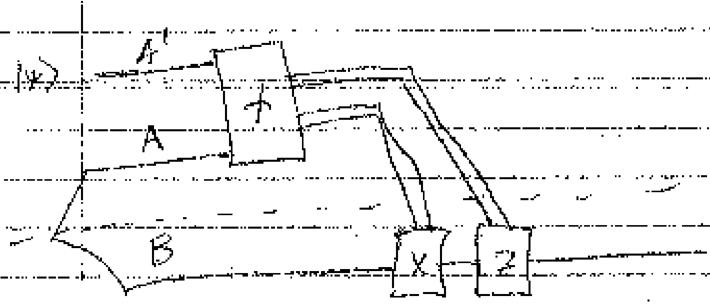
w/ uniform probability $1/4$

Alice knows which state Bob has.
Bob knows nothing: ~~his state~~ ~~[illegible]~~ is π^B.

3/3/2011

2) Alice transmits two classical bits to Bob. Bob then knows exactly which state he has

3) Bob performs a restoration operation



Note: 1) teleportation process works for any input state (universal)

2) does not violate no-cloning theorem (state is teleported, not copied)

3) not instantaneous

resource inequality is

$\{qq\} + 2\{c \to c\} \geq \{q \to q\}$

Entanglement is said to be "monogamous" in the sense that Alice cannot be maximally entangled w/ both Bob & Charlie. there are other ways of quantifying this trade-off, but we will consider the simplest case.

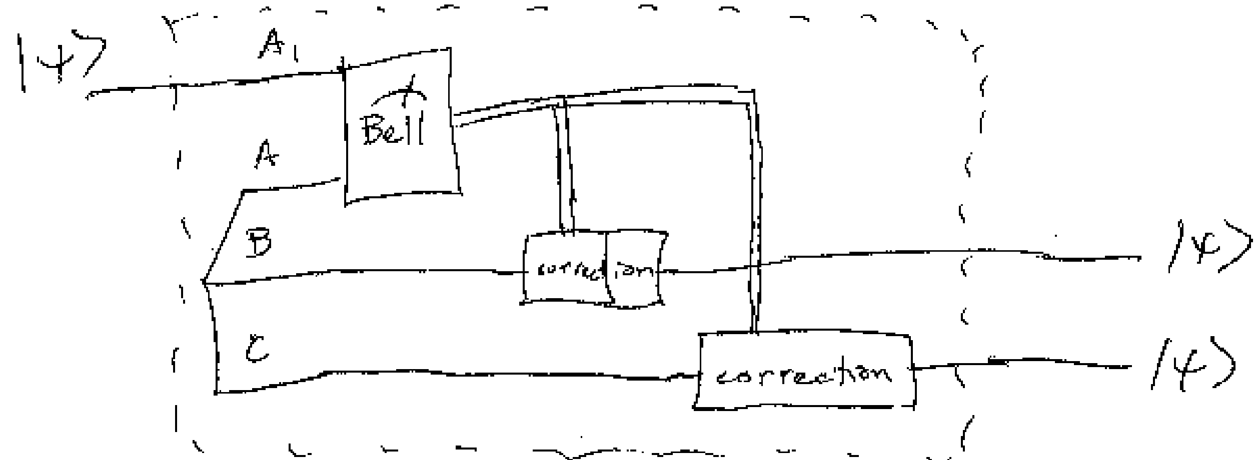
Suppose that there exists a three-party quantum state, call it ρ_{ABC}, such that the local state for AB is $|\Phi\rangle_{AB}$ & the local state for AC is $|\Phi\rangle_{AC}$. We will make this more precise later. then w/ such a state, we could violate the no-cloning theorem.

So such a state cannot exist.

(12)

Why can it not exist?

Consider the following protocol:



Alice would be able to teleport to both Bob & Charlie

if we put a box around this

device, it could serve as a

quantum copying machine,

which we proved cannot exist.