CO781 / QIC 890 Lec 2 Sep13.

rec1: TP: 2 cbits + 1 ebit ≥ 1 qbit
SD: 1 qbit + 1 ebit ≥ 2 cbits

When ebits are free 2cbits = 1 qbit!

rec2: Optimality & what happens when ebits are not free.

Principles.

(P1) QM

(P2) No superluminal comm.

Consequences:

(C1) Correlation and back comm cannot result in forward comm.
Unlimited

(C2) $\forall n, k \in \mathbb{Z}^+$, n cbits & unlimited entanglement cannot produce $(n+k)$ cbits.

(C3) $\forall n, k \in \mathbb{Z}^+$, n qbits & unlimited entanglement cannot produce $(n+k)$ qbits.

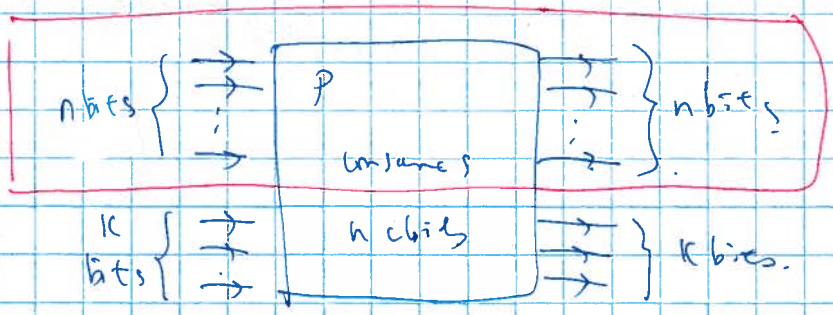
(C4) No amount of cbits can produce 1 qbit (nor an ebit).

Pf (C1) Even with a shared state $|\Psi\rangle_{AB}$ & back comm (from Bob to Alice) Bob can finish his step before Alice starts.

∴ Bob's output must be indep of Alice's message.

Almost a pf of (C2):

Suppose by contradiction, there's a protocol P' consuming entanglit & n cbits & transmits $n+k$ bits.



∴ n cbits becomes $n+k$ cbits becomes $\cdots$ $n+rk$ cbits.

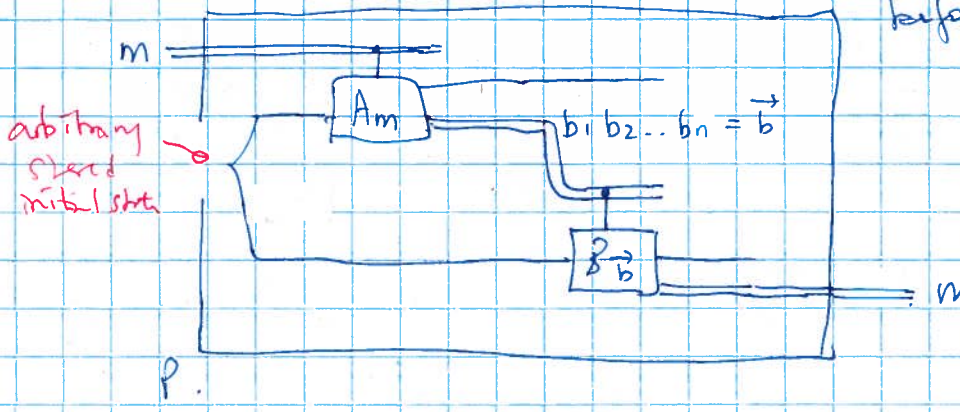
+ ent + ent

for unbounded r. Almost a contradiction.

Pf (c2):

- Suppose $\exists$ protocol (set of LO's comm etc) consuming entanglement & n cbits & transmits any $m \in \{1, 2, \ldots, 2^{n+1c}\}$ whp

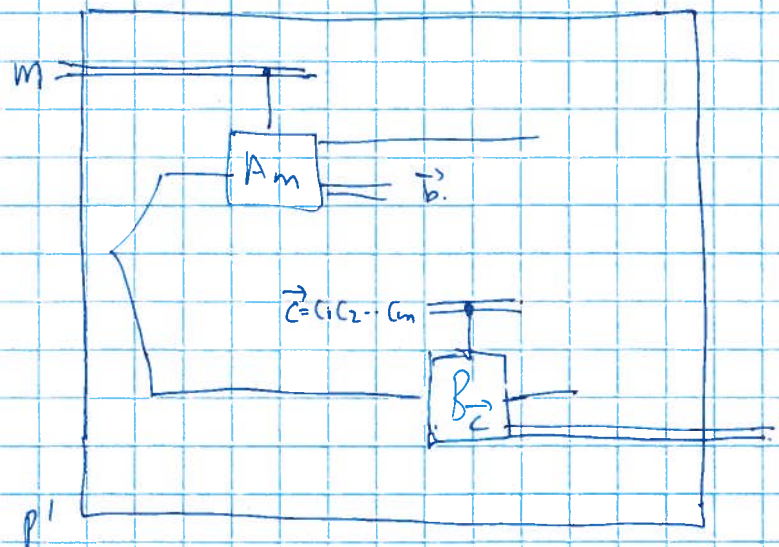
WLOG (∵ no back comm). Alice finishes all her steps before communicating to Bob.



- Modify P to get a contradiction:

Don't comm & let Bob guess.

ie replace n cbit by n coin toss of Bob.



$\hat{m}$ follows a distribution depending on m.

If $\vec{c} = \vec{b}$, then $\hat{m} = m$!

$$\Pr(\tilde{m} = m \mid m) \geq \sum_{\vec{b}} \Pr^{(m)}(\vec{b}) \Pr^{(m)}(\vec{c} = \vec{b} \mid \vec{b})$$

(or omitting $^{(m)}$)

$$= \sum_{\vec{b}} \Pr(\vec{b}) \frac{1}{2^n}$$

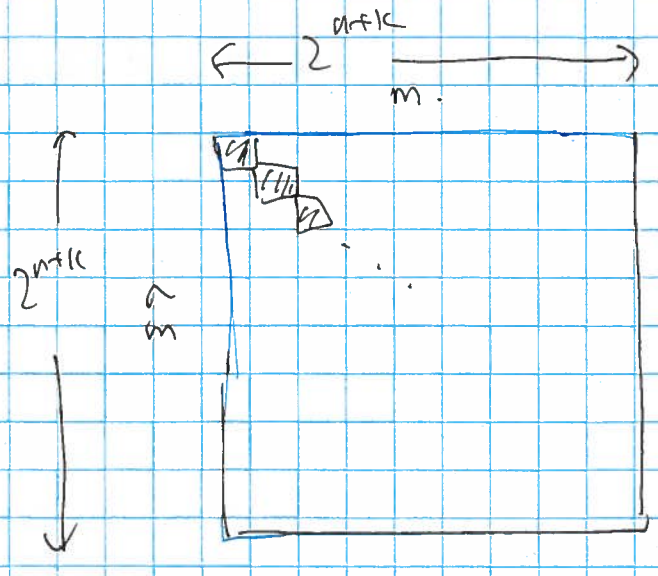
$$= \frac{1}{2^n}.$$

But m uniform over 2^{n+k} values $\Rightarrow$ $\tilde{m}$ & m not independent.

$\therefore$ P' can comm using only correlation (0 bit) violating (C1).

If you want: $\exists\, m_1 \neq m_2$ s.t. $\Pr(m_2 \mid m_1) < \frac{1}{2^{n+k}}$

Alice can send 1 bit whp. $\Pr(m_2 \mid m_1) \geq \frac{1}{2^n}$.



← table listing $Pr(\hat{m}|m)$.

① $\sum_{\hat{m}} Pr(\hat{m}|m) = 1$ ie col sum = 1.

② $\forall m \quad Pr(m|m) \geq \frac{1}{2^n}$

$\Rightarrow \exists$ off diagonal entry $< \frac{1 - 2^{-n}}{2^{n+k} - 1} < \frac{1}{2^{n+k}}$

$Pr(m_2|m_1)$ for some $m_2 \neq m_1$

off diag.

ie based on input = m_1 or m_2 Bob has $\frac{1}{2}$ prob of output m_2

Anyway $Pr[m_2|m_2] \geq \frac{1}{2^n}$!

- 2nd modification.

Alice decides $i = 1$ or 2.

Alice & Bob repeat P' l times, @ w/ input m_i

Bob applies Chernoff bdd (or any other technique) to infer i.

Pf (C3): Using the "cheat" pf for (C2).

If n qbits $+|\varepsilon\rangle \geq n+k$ qbits.

then

$$n \text{ qbits} + |\varepsilon\rangle^{\otimes \ell} \geq n+\ell k \text{ qbits} \qquad \forall \ell \in \mathbb{Z}^+$$

Take $\ell k = 2n$

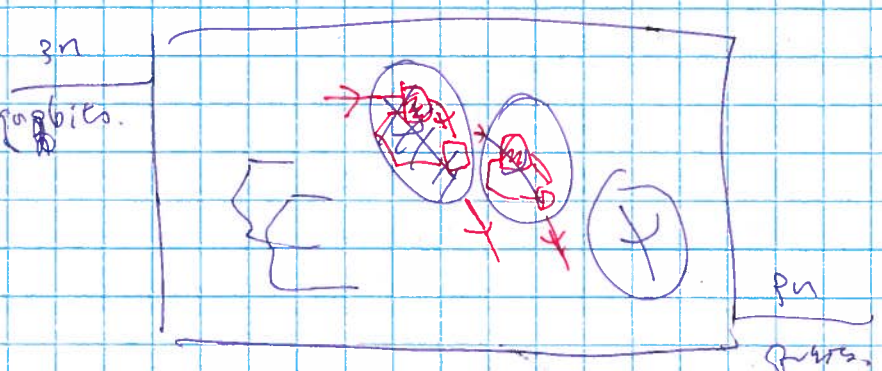
Now n cbits $+$ $2n$ cbits $+ |\varepsilon\rangle^{\otimes \ell}$

$\geq^{??}$ n qbits $+ |\varepsilon\rangle^{\otimes \ell} \geq n+\ell k$ qbits

$\geq$ $3n$ qbits.

$\geq$ $3n$ cbits.

Violates (C2)



Pf (C4) Assignment.

Optimality of SD & TP:

Known: SD: 1 qbit + 1 ebit ≥ 2 cbits.

TP: 2 cbits + 1 ebit ≥ 1 qbit.

① Is TP optimal?

because of some protocol TP'

Statement: if $2n\alpha$ cbits + $n\beta$ ebits ≥ n qbits for some β

then $\alpha \geq 1$.

even w/ unlimited ent, still requires 2 cbits per qbit sent

Note asymptotics allowed.

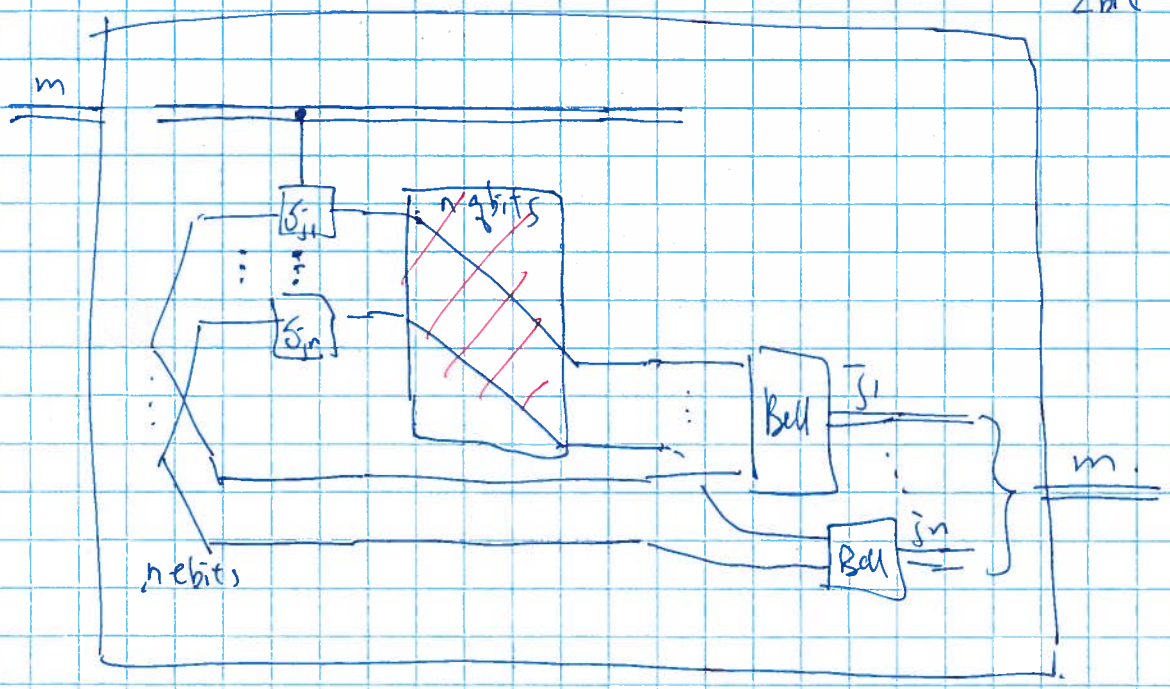
② SD optimal:

If $n\alpha$ qbit + $n\beta$ ebit ≥ $2n$ cbits for some β

then $\alpha \geq 1$.

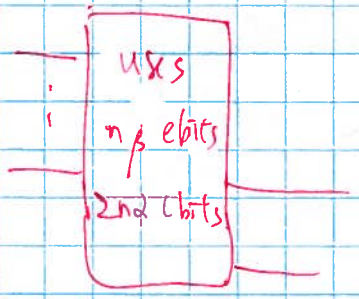
Pf ① If TP' exists, compose w/ SP.

In particular, use SP to send a 2n-bit message $m = j_1 \ldots j_n$ (2 bit, 2 bit)



Above works thanks to SP.

Replace n q bits by TP'.



Composition uses $n + \beta n$ ebits & transmits $2n$ cbits

$2n\alpha$ cbits

By $(2, 2n\alpha)$, $2n$

$\alpha \geq 1$.

Summary:

(2) TP' : $2n\alpha$ cbits + $n\beta$ ebits $\geq$ n qbits + a ebit $\geq 2n$ cbits + n ebits.

(1) SD

$\therefore \alpha \geq 1$.

NB $\beta \geq 1$ also by (4) (Pf: Ex).

Pf (2) Similar. (Ex?!)

If SD' exists, replace @ qbit in SD' by TP.

$2n\alpha$ cbits + $n(\alpha+\beta)$ ebits $\geq$ (TP) $n\alpha$ qbits + $n\beta$ ebits $\geq 2n$ cbits (SD')

$\therefore \alpha \geq 1$.

Alt: TP of n qubits, use SD' to transmit the $2n$ bits. Then apply (3) instead.

NB: $\beta \geq 1$ but requires Holevo's bd. (will do in 2-3 weeks!)

- Connection w/ SD & TP when ebits aren't free:

Recall qbit: $|x\rangle_A \to |x\rangle_B$ for any basis $\{|x\rangle\}$

cbit: $|x\rangle_A \to (x)_B\ |x\rangle \in (|x\rangle_A)$ for a special basis $\{|x\rangle\}$

Def: cobit $\overset{\text{coherent classical comm.}}{=}$ $|x\rangle_A \to |x\rangle_A |x\rangle_B$.

qbit	vs	cobit	vs	ebit
Bob must have a copy throughout		Alice must have a copy and not Env.		Env must have a copy.
No one else.				

- Simple RIFs:

① 1 cobit $\geq$ 1 cbit.

Alice & Bob performs cobit
Then Alice discards A (i.e. A goes to Env).

sending this to 0.

② 1 qbit $\geq$ 1 cobit

Given 1 qbit, here's a way to create a cobit:

$x \in \{0,1\}$ $\quad |x\rangle_A \longrightarrow |x\rangle_A |0\rangle_{A_1} \longrightarrow (x)_A |x\rangle_{A_1} \to |x\rangle_A |x\rangle_B$.

- Alice attaches ancilla $|0\rangle_{A_1}$
- local unitary by Alice
- use qbit on A_1 (becomes B)

Extends to $x \in \{0,1,\ldots,d-1\}$.

③ 1 cobit ≥ 1 ebit.

Pf: $\frac{1}{\sqrt{2}} \sum_x |x\rangle_A$ (LO for Alice.) $\xrightarrow{\text{uses 1 cobit}}$ $\frac{1}{\sqrt{2}} \sum_x |x\rangle_A |x\rangle_B$.

Extends to $x \in \{0, 1, \ldots, d-1\}$.

④ 1 qbit + 1 ebit ≥ 2 cobits !

↑ SD.

$|x\rangle_A \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)_{A,B} \longrightarrow |x\rangle_A \left(\sigma_x \otimes I\right) \left|\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right\rangle_{A,B}$

$x \in \{0,1,2,3\}$

local unitary by Alice

↓ qbit. $(A_1 \to B_1)$

$|x\rangle_A \quad \sigma_x \otimes I \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)_{B_1 B}$

↓ LU by Bob.

$|x\rangle_A \quad |x\rangle_{(B,B)}$.

Qn: Is there an inverse?

Want: 1 qbit + 1 ebit ≤ 2 cobits + 1 ebit.

& recycles 2 ebits.

Suggest TP using 2 cobits instead of 2 ebits.

TP w/ cobits = TP^{co}

$a|0\rangle + b|1\rangle$ $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

The j-th Bell basis state

$$|\psi\rangle_{A_1} \, |\Phi\rangle_{AB} = \frac{1}{2} \sum_{j=0}^{3} |b_j\rangle_{A_1 A} \otimes (\sigma_j |\psi\rangle)_B$$

(derived last lec).

↓ Local unitary by Alice. (change of basis) (instead of Bell meas).

$$\frac{1}{2} \sum_{j=0}^{3} |j\rangle_{A_1 A \to \tilde{A}} \otimes (\sigma_j |\psi\rangle)_B.$$

↓ 2 cobits

$$\frac{1}{2} \sum_{j=0}^{3} |j\rangle_{\tilde{A}} \, |j\rangle_{\tilde{B}} \, (\sigma_j |\psi\rangle)_B.$$

↓ Conditioned on $\tilde{B}$ being j, apply σ_j to B.

$$\left[\frac{1}{2} \sum_{j=0}^{3} |j\rangle_{\tilde{A}} |j\rangle_{\tilde{B}}\right] \otimes (|\psi\rangle)_B$$

2 ebits recycled.

∴ 1 qbit + 2 ebits $\underset{TP^{co}}{\leq}$ 1 ebit + 2 cobits

Allowing borrowing & returning ebits:

1 qbit + 1 ebit ≤ 2 cobits.

SD ≥

∴ =

In AI, Honor code: if you use Aram's, say so.

Originates from RSP, gate capacities

Aram Harrow 2003.

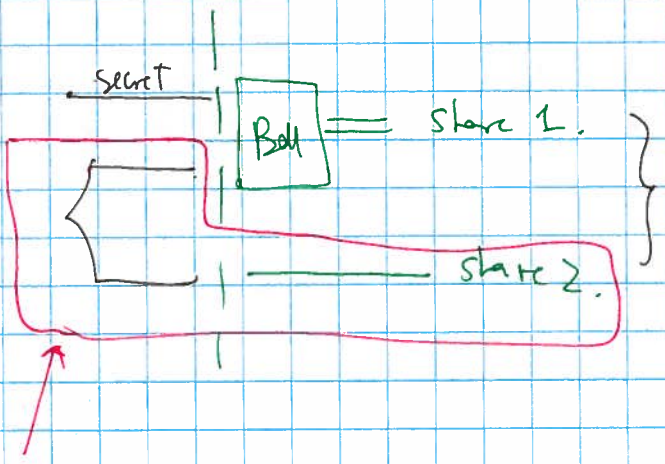
Other remarks:

TP: 1 qbit + 2 rbits $\leq$ 1 ebit + 2 cbits.

SD: 1 qbit + 1 ebit $\geq$ 2 cbits.

TP & SD are both secret sharing schemes:

For TP:



neither has info on the secret.

Needs both to reconstruct the secret.

Allows secret to be transmitted in 2 steps.

1st step = create ebit - AND verify. (requires back cc.)

Once done correctly, the rest (secure) (Composably secure.)

encrypted & authenticated.

- From this, one can derive ~~Secret~~ security of encryption & auth of Q data w/o. interact & that of key expiry.

[• Similarly for SD.]

- One can also broadcast means control w/o knowing when Bob goes!