Lec 3: CO781 / QIC 890 F2016

(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

Optimality of SD & TP:

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

} If ent is free, SD & TP are inverses of one another.
* useful ltr $Q_E = \frac{1}{2} C_E$.

Thm 1 (optimality of TP)

If $2n\alpha$ cbits + $n\beta$ ebits $\geq$ n qbits for some β

then $\alpha \geq 1$.

Thm 2 (optimality of SD)

If $n\alpha$ qbit + $n\beta$ ebits $\geq$ 2n cbits for some β

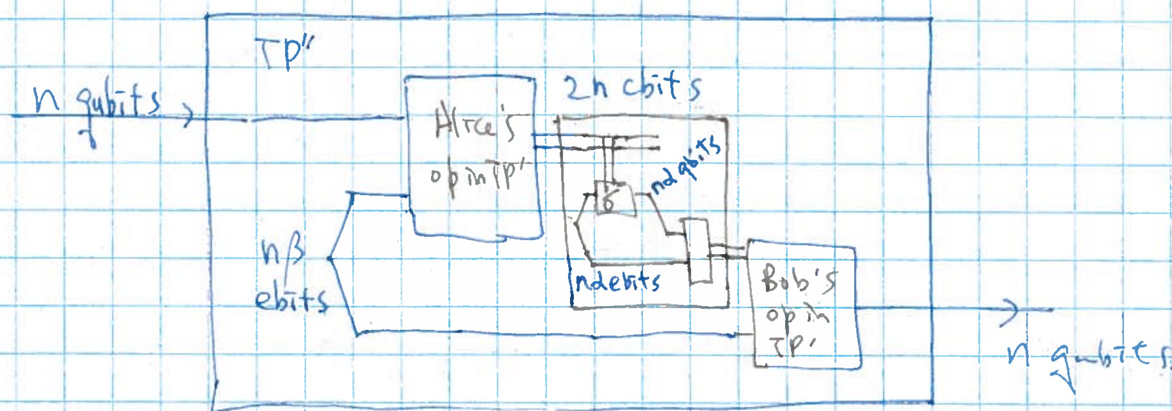
then $\alpha \geq 1$.

ie even with unlimited ebits, the communication costs of SD & TP are optimal since no protocol can achieve the same communication task with less.

Pf (Thm 1):

Suppose a protocol TP' exists that consumes $2n\alpha$ cbits and $n\beta$ ebits to transmit n qubits.

Now produce those $2n\alpha$ cbits by SD, consuming in turns $n\alpha$ qbits and $n\alpha$ ebits. Call the resulting protocol TP":



So TP" consumes $n\beta + n\alpha$ ebits and $n\alpha$ qbits to generate n qbits. By (C3), $n\alpha \geq n$ ∴ $\alpha \geq 1$.

Summary with resource inequalities (RI):

By SD: $n\alpha$ qbits + $n\alpha$ ebits $\geq$ $2n\alpha$ cbits

If $2n\alpha$ cbits + $n\beta$ ebits $\geq$ n qbits

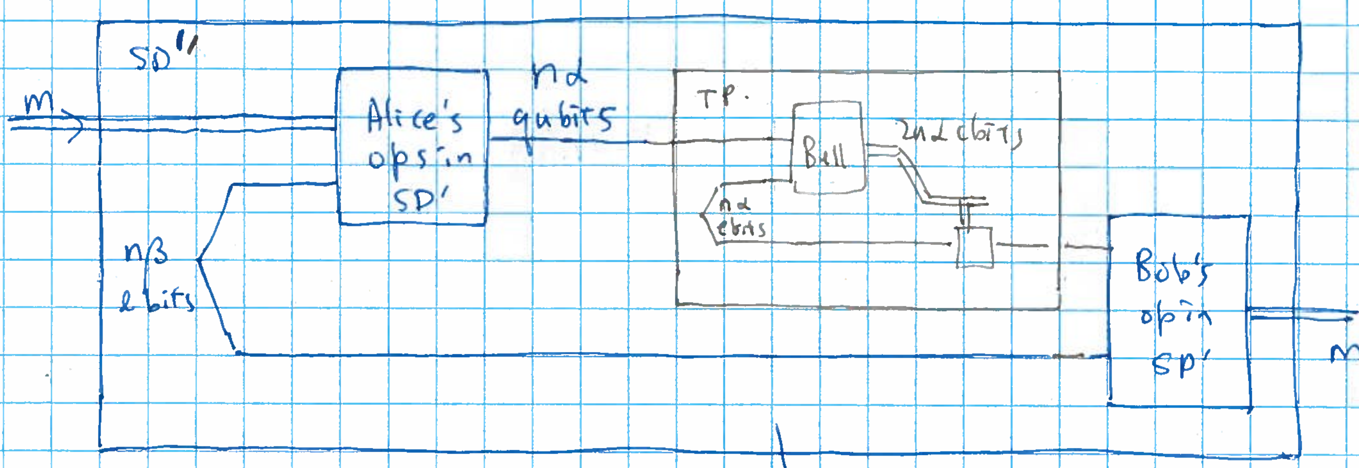
then $n\alpha$ qbits + $n\alpha$ ebits + $n\beta$ ebits $\geq$ n qbits.

∴ $\alpha n \geq n$ and $\alpha \geq 1$.

Substitution of RI of SD into that of TP' requires SD to be composable.

Pf (Thm 2):

If there is a protocol SD' consuming $n\alpha$ qbits and $n\beta$ ebits to transmit $2n$ cbits then we use $2n\alpha$ cbits & $n\alpha$ ebits to perform TP to supply those $n\alpha$ qbits.



consumes ent + $2n\alpha$ cbits.
transmits $2n$ cbits $\therefore \alpha \geq 1$ by (C2).

In terms of RI:

SD': $\underbrace{n\alpha \text{ qbits}}_{\geq \text{ TP}} + n\beta \text{ ebits} \geq 2n \text{ cbits}$

$2n\alpha$ cbits + $n\alpha$ ebits.

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

$\therefore \alpha \geq 1$ by (C2).

Recall 2 cbits $\underset{TP}{\overset{SD}{\rightleftarrows}}$ 1 qbit when entanglement is free.

What happens when entanglement is charged?

Recall:

- qbit = $|x\rangle_A \to |x\rangle_B$ for any basis $\{|x\rangle\}$.
- cbit = $|x\rangle_A \to |x\rangle_B |x\rangle_E$ $(|x\rangle_A)$ for the computational basis $\{|x\rangle\}$
- cobit = $|x\rangle_A \to |x\rangle_A |x\rangle_B$

(isometric extensions)

Coherent classical communication (Harrow 2003).

Bob must have a copy

qbit vs cobit vs cbit

- qbit: no one else has a copy
- cobit: Alice must retain a copy and not Eve
- cbit: Eve must have a copy

Why such a strange form of communication?

- occurs naturally if classical comm is sent via coherent methods (SD, unitary 2-way channels, ...)
- allows efficient conversions between protocols.
- completes the understanding of SD & TP.

Resource inequalities concerning cobits:

① 1 cobit ≥ 1 cbit

② 1 qbit ≥ 1 cobit

③ 1 cobit ≥ 1 ebit

④ 1 qbit + 1 ebit ≥ 2 cobits (SD)

⑤ 1 qbit + 2 ebits ≤ 2 cobits + 1 ebit (TP^{co})

inverses of one another

Cancellation: catalytic input resource

Previously:

④ 1 qbit + 1 ebit ≥ $\boxed{\text{2 cbits}}$ (SD)

⑤ 1 qbit + $\boxed{\text{2 rbits}}$ ≤ $\boxed{\text{2 cbits}}$ + 1 ebits. (TP)

relatively free resources are not spelt out explicitly before achieves 1 cbit

Pf ①: $|x\rangle_A \longrightarrow |x\rangle_A |x\rangle_B \longrightarrow |x\rangle_E |x\rangle_B$.

use 1 cobit

partial trace of A (local)

measurement of A (local) $\longrightarrow |x\rangle_A |x\rangle_E |x\rangle_B$

partial tracing of A

achieves 1 cobit

Pf ②: $|x\rangle_A \longrightarrow |x\rangle_A |0\rangle_{A_1} \longrightarrow |x\rangle_A |x\rangle_{A_1} \longrightarrow |x\rangle_A |x\rangle_B$.

attach ancilla (local)

local unitary

use 1 qbit on A_1

Pf ③: $\frac{1}{\sqrt{2}} \sum_{x=0}^{1} |x\rangle_A \longrightarrow \frac{1}{\sqrt{2}} \sum_{x=0} |x\rangle_A |x\rangle_B$

Local state preparation for Alice

uses 1 cobit

achieves 1 ebit.

Pf (4): We denote the conversion between the Bell basis and the computational basis by U:

$$|x\rangle \underset{U^{-1}}{\overset{U}{\rightleftarrows}} (\sigma_x \otimes I)|\Phi\rangle$$

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

for $x = 0, 1, 2, 3$. The following transformation achieves the claimed RI:

$$|x\rangle_A \underbrace{\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)_{A_1 B}}_{\text{uses 1 ebit}}$$

↓ conditioned on A being x, apply σ_x to A_1 (local unitary on AA_1)

$$|x\rangle_A (\sigma_x \otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)_{A_1 B}.$$

↓ uses 1 qbit to send A_1 from Alice to B_1 with Bob

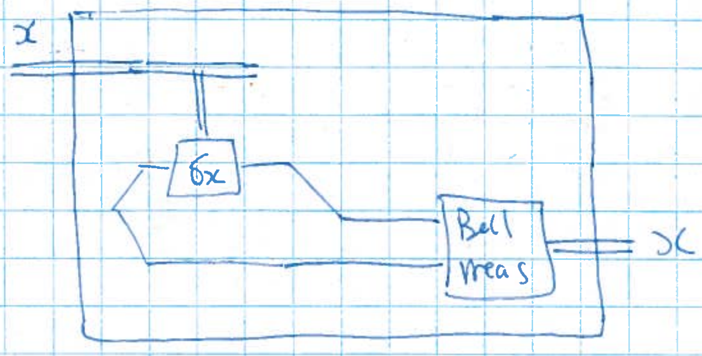
$$|x\rangle_A (\sigma_x \otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)_{B_1 B}$$

↓ apply U^{-1} to $B_1 B$. (local)

$$|x\rangle_A \, |x\rangle_{(B_1 B)}$$

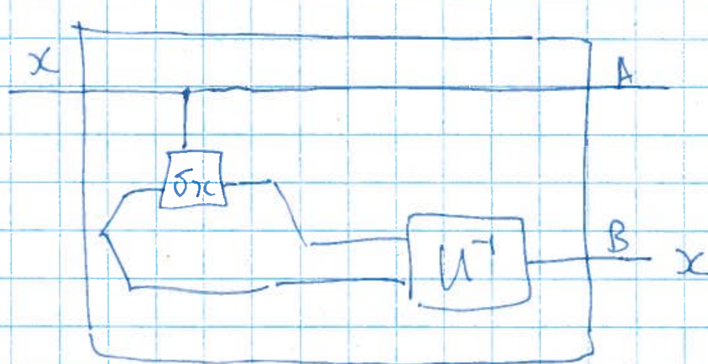
achieves 2 cobits

Original SD:



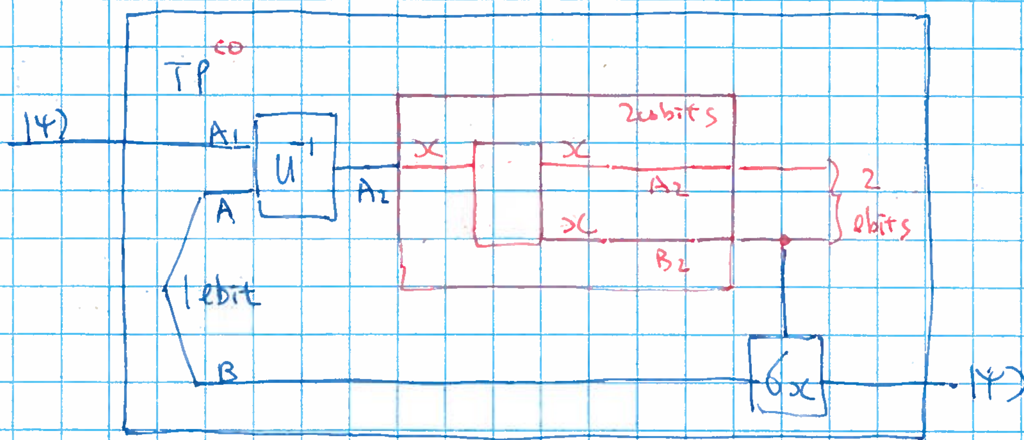
where

Keeping everything coherent.



Simply put: SD is coherent, so if Alice keeps a coherent copy without "looking" (measuring, giving info to Eve) and similarly for Bob, the 2 cbits become 2 cobits.

⑤ Let TP^{co} be the protocol obtained from replacing the 2cbits by 2 cobits in TP.



Verifying the math:

$a|0\rangle + b|1\rangle$ $\quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ $\quad$ the x^{th} Bell basis state

$$|\psi\rangle_{A_1} \, |\Phi\rangle_{AB} = \frac{1}{2} \sum_{x=0}^{3} |b_x\rangle_{A_1 A} \otimes (\sigma_x |\psi\rangle)_B$$ (proved in lec1)

1ebit

$\downarrow$ U^{-1} on $A_1 A$, output A_2 has 4 dim, local

$$\frac{1}{2} \sum_{x=0}^{3} |x\rangle_{A_2} \otimes (\sigma_x |\psi\rangle)_B$$

$\downarrow$ 2 cobits taking A_2 to $A_2 B_2$

$$\frac{1}{2} \sum_{x=0}^{3} |x\rangle_{A_2} |x\rangle_{B_2} \otimes (\sigma_x |\psi\rangle)_B$$

$\downarrow$ conditioned on B_2 being x, apply σ_x^{-1} to B
Local unitary on $B_2 B$

$$\frac{1}{2} \sum_{x=0}^{3} |x\rangle_{A_2} |x\rangle_{B_2} \otimes |\psi\rangle_B .$$

decoupled from B
2 ebits.

no more dependence on x

also achieves 1 qbit.

Together:

TP^{co}: 1 ebit + 2 cobits $\geq$ 2 ebits + 1 qbit

If 1 ebit can be borrowed and returned, net effect:

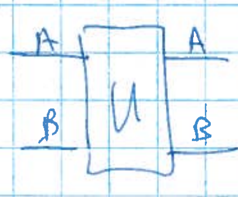
$$2 \text{ cobits} \geq 1 \text{ ebit} + 1 \text{ qbit}$$

the reverse of SD.

NB: Asymptotically, 2 cobits = 1 ebit + 1 qbit.

Extension of RI to bipartite quantum gates:

Consider



Such a gate can be nonlocal, transmitting quantum or classical data in either direction (forward from Alice to Bob or backwards from Bob to Alice) and generate entanglement.

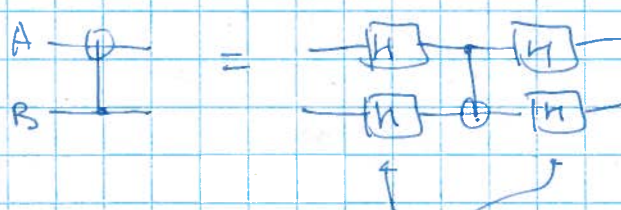
eg: $U = CNOT_{AB} = |0\rangle\langle 0|_A \otimes I_B + |1\rangle\langle 1|_A \otimes \sigma_{1\,B}$

• If Bob prepares $|0\rangle_B$,

then $CNOT_{AB} \, |x\rangle_A \, |0\rangle_B = |x\rangle_A \, |x\rangle_B$

$\therefore$ $CNOT_{AB} \geq 1$ cbit$_{(\rightarrow)}$ (from Alice to Bob)

• Since



free local operations

$CNOT_{AB}$ $\boxed{\geq}$ $CNOT_{BA} \geq 1$ cobit$_{(\leftarrow)}$ (from Bob to Alice)

$=$

• ~~cobit $\geq$ ebit $\therefore$ $CNOT_{AB} \geq 1$ ebit.~~

Thm (Harrow 03):

1 CNOT + 1 ebit = 1 cobit$_{(\rightarrow)}$ + 1 cobit$_{(\leftarrow)}$

1 SWAP = 1 qbit$_{(\rightarrow)}$ + 1 qbit$_{(\leftarrow)}$

Cor: 1 CNOT $\not\geq$ 1 qbit.

Cor: 2 CNOT = 1 SWAP !

See Harrow 03 and/or Assignment ?