Lec 2: CO781 / QIC890 F2016

Last time:

Communication primitives : cbit, qbit, ebit

Communication protocol	Resource inequality
•	qbit ≥ cbit
• Superdense coding (SD)	1 qbit + 1 ebit ≥ 2 cbits
• Teleportation (TP)	2 cbits + 1 ebit ≥ 1 qbit

Def :

1 qbit refers to the ability of Alice & Bob to effect the following TCP map :

$$\Phi(\rho_A) = \rho_B$$

← need to say what happens to @ entry of input

only say where basis goes.

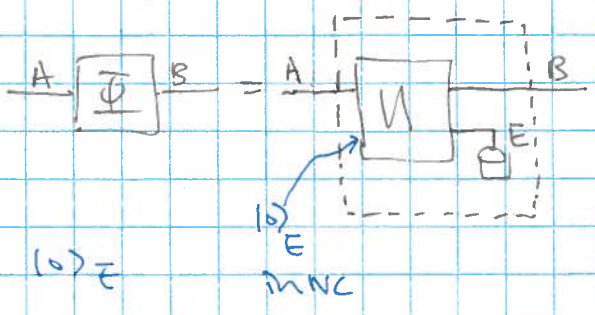
Φ can be specified by its Stinespring dilation

(aka the unitary representation in NC00, Isometric extension...)

$$|x\rangle_A \rightarrow |x\rangle_B$$

for a basis $\{|x\rangle\}$.

ie no output to E or it remains $|0\rangle_E$



Def:

1 cbit refers to the ability to implement

$$\Phi(\rho_A) = \left[\mathrm{Diag}(\rho)\right]_B$$

Φ has isometric extension

$$|x\rangle_A \longrightarrow |x\rangle_B |x\rangle_E$$

for a basis $\{|x\rangle\}$.

- When $\underline{\Phi}$ is implemented approximately, say by $\underline{\Phi}'$ we require $\| \underline{\Phi} - \underline{\Phi}' \|_\diamond$ to be small enough for what we try to achieve.

- Composability requirement:
  We say $\underline{\Phi}'$ simulates $\underline{\Phi}$ if for any protocol P consuming $\underline{\Phi}$ as a resource, modifying P to use $\underline{\Phi}'$ gives a protocol P' that behaves similarly to P.

- Note that $\| P - P' \|_\diamond \leq \| \underline{\Phi} - \underline{\Phi}' \|_\diamond$ so the diamond norm distance is a "composable measure" of accuracy.
  Operationally, no one obeying QM & possessing side info can discriminate $\underline{\Phi}$ from $\underline{\Phi}'$ with prob $\frac{1}{2} + \frac{1}{4} \| \underline{\Phi} - \underline{\Phi}' \|_\diamond$.

- Small enough: e.g.
  Say each qbit has error ϵ
  n qbits has error $\leq n\epsilon$.
  So if overall transmission is to have error $\leq p$,
  we need $\epsilon \leq p/n$.

Principles:

(P1) No signalling without communication

(P2) QM

NB (P2) ⇒ (P1).

Consequences:

from Bob to Alice

(C1) Unlimited correlation and back communication cannot result in signalling in the forward direction.

(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) Unlimited cbits cannot produce 1 qbit or 1 ebit.

* Cannot prove principles, but will derive consequences from principles.

Pf (C1): If a protocol consumes only correlations & back communication, then, Bob can finish his operations and obtain his output before Alice starts (or before the message exists).

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

↑

more precise statement for (C1).

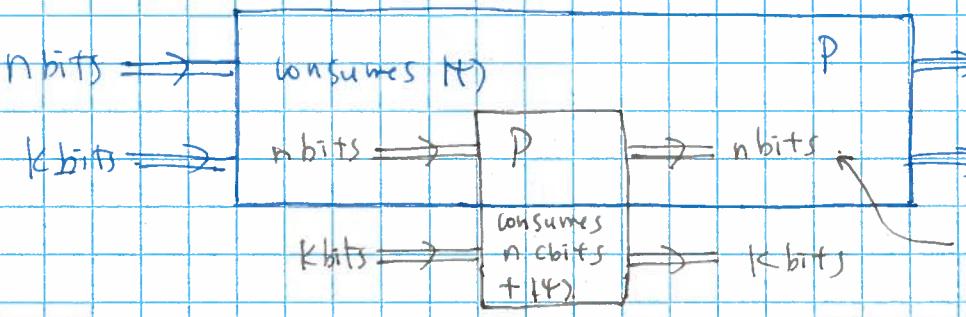
"Almost a proof" of (C2):

Idea: If something is too good to be true then, makes it better.

Operationally, suppose by contradiction, there is a protocol P consuming ent stated (4) & n cbits to transmit (n+k) bits.

Now, n of those transmitted bits, along with another copy of (4), enables another execution of P.

So a total of $\underbrace{(n+k)}_{\text{2nd}} + \underbrace{k}_{\text{1st}}$ bits are transmitted.



Recursing the construction r times,

n cbits & r copies of (4) enable $\underbrace{(n+kr)}_{\text{unbounded}}$ bits of comm,

for any $r \in \mathbb{Z}^+$.

This almost contradict (C1).

* Recursive argument works because we assume P produces composably good cbits

In terms of resource inequalities:

If n cbits + $\langle\psi\rangle \geq (n+k)$ cbits for some $\langle\psi\rangle$

then $\forall r \in \mathbb{Z}^+$, n cbits + $\langle\psi\rangle^{\otimes r}$

$\geq (n+k)$ cbits + $\langle\psi\rangle^{\otimes r-1}$

$\geq (n+2k)$ cbits + $\langle\psi\rangle^{\otimes r-2}$

$\vdots$

$\geq (n+rk)$ cbits.

NB: if $a+b \geq c$ ①, $c+d \geq e$ ②

then $a+b+d \geq e$

This assumes ① is composably good.

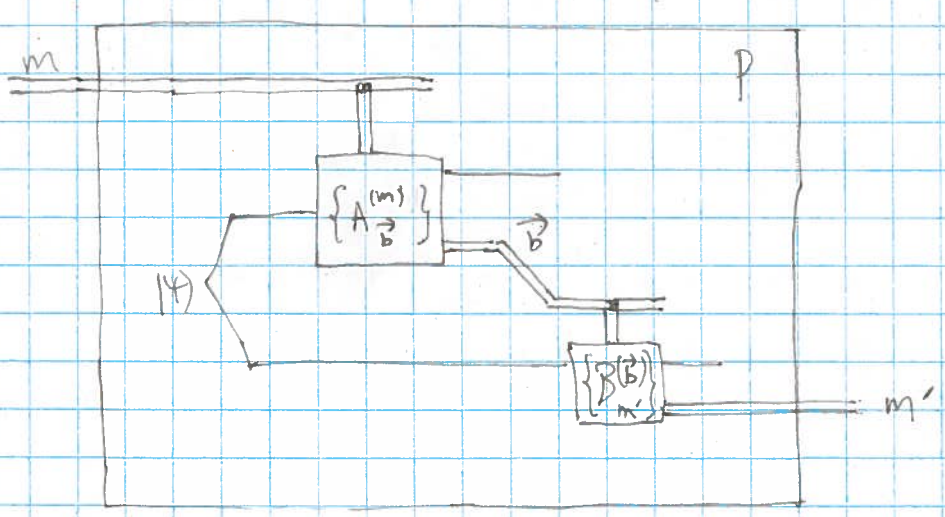
Qn: does the proof hold in the presence of back communication?

Pf (12):

Idea: we prove by contradiction. If it takes too little resource to achieve a task, then we can approx the task too well even without the resource.

- Suppose there is a protocol P consuming an entangled state $|\Psi\rangle$ and n cbits, and transmits any $m \in \{1, 2, \ldots, 2^{n+k}\}$ (whp).

In the absence of back communication, most general operation of Alice is to receive the message m, apply a measurement with POVM $\{A^{(m)}_{\vec{b}}\}_{\vec{b}}$ to her half of $|\Psi\rangle$ and the outcome $\vec{b}$ to Bob.



WLOG by absorbing "processing of outcome to the n bits sent" into the measurement

Upon receiving the n-bit message $\vec{b}$, Bob applies a measurement with POVM $\{B^{(\vec{b})}_{m'}\}_{m'}$ and output the measurement outcome m' as the message received.

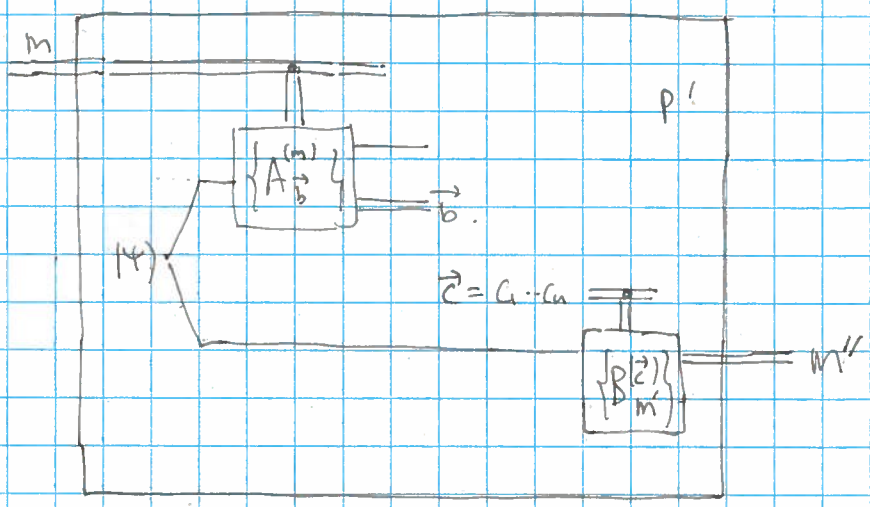
With high prob, $m = m'$.

- Modify P to P' to get a contradiction.

In P', $\vec{b}$ is not communicated and Bob guesses it.

So Bob tosses a fair coin n times to get $\vec{c} = c_1 c_2 \cdots c_n$.

He proceeds with $\vec{c}$ instead of $\vec{b}$.



Condition on these.

For each m, for each $\vec{b}$, $\text{prob}(\vec{C} = \vec{b} \mid \vec{b}\, m) = \frac{1}{2^n}$ (cond on m & $\vec{b}$)

Cond only on this.

For each m, $\text{prob}(\vec{C} = \vec{B} \mid m) = \sum_{\vec{b}} \text{prob}(\vec{b}) \times \text{prob}(\vec{C} = \vec{b} \mid \vec{b}\, m)$

$= \sum_{\vec{b}} \text{prob}(\vec{b}) \times \frac{1}{2^n} = \frac{1}{2^n}$.

When $\vec{C} = \vec{B}$, $M'' = M' \approx M$

$\therefore \text{Prob}(M'' \approx m \mid m) \geq \text{Prob}(\vec{C} = \vec{B} \mid m) = \frac{1}{2^n}$

Together, $\text{prob}(M'' \approx M) = \sum_m \text{prob}(m) \times \text{Prob}(M'' \approx m \mid m) = \frac{1}{2^n}$

So m'' & m are not independent (else $\text{prob}(m'' = m) = \frac{1}{2^{n+k}}$).

This contradicts (c).

Pf (C3):

Idea: apply the amplification as in "almost-a-proof-for-(C2)" and apply TP to contradict (C2).

Using resource inequalities:

Suppose n qbits + $|\psi\rangle \geq n+k$ qbits.

Then n qbits + $|\psi\rangle^{\otimes r} \geq n+kr$ qbits

We now supply the n qbits required by TP:

$2n$ cbits + n ebits + $|\psi\rangle^{\otimes r} \geq n+kr$ qbits.

$\geq 3n$ qbits (if $kr \geq 2n$)

$\geq 3n$ cbits.

This contradicts (C2).

Ex: expand the above resource inequality argument in terms of protocols & how to compose things to get a contradiction.

Pf (C4): Assignment, via a proof cbits cannot take SEP states to entangled states, or PPT states to NPT states.