CO781 / QIC 890:

Theory of Quantum Communication

Topic 1, part 5

What is communication of data?
The no-signalling principle
Optimality of superdense coding and teleportation
Cobits, duality of SD and TP,
and unitary gates as bidirectional channels
Equivalence of generalized teleportation
& generalized encryption of quantum states

Non-composable qbit: remote state preparation
& approximation encryption of pure states

References:

Private quantum channel:
- Ambainis, Mosca, Tapp, deWolf 2000
- Boykin, Roychowdhury 2000

Connecting generalized teleportation
& generalized encryption of quantum states:
- Leung, Shor 2002

Remote state preparation & approx encryption:
- Lo 1999
- Bennett, DiVincenzo, Show, Smolin, Terhal, Wootters 00
- Devetak 2001
- Leung, Shor 2002
- Bennett, Hayden, Leung, Shor, Winter 2003
- Hayden, Leung, Shor, Winter 2003

Lo 99: Remote state preparation of a re-bit

Alice comes up with some $|\Psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{R}$

Her goal: prepare a copy of $|\Psi\rangle$ in Bob's lab

using entanglement & classical communication

Solution 1: teleportation

But is there a cheaper solution ?

Lo 99: Remote state preparation of a re-bit

Alice comes up with some $|\psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{R}$

Her goal: prepare a copy of $|\psi\rangle$ in Bob's lab

using entanglement & classical communication

Solution 2:

Alice & Bob share 1 ebit $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$

$$= \frac{1}{\sqrt{2}}\left[(a|0\rangle + b|1\rangle)\otimes(a|0\rangle + b|1\rangle) + (-b|0\rangle + a|1\rangle)\otimes(-b|0\rangle + a|1\rangle)\right]$$

Alice measures A along the basis:

$|e_0\rangle = a|0\rangle + b|1\rangle,$

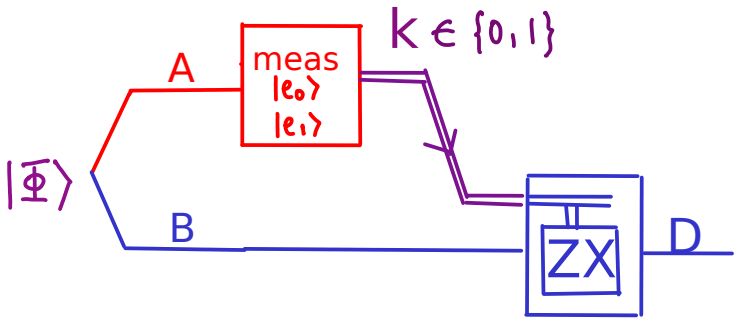
$|e_1\rangle = -b|0\rangle + a|1\rangle$

& tells Bob the outcome (1 cbit)

If outcome is $|e_0\rangle$, Bob has $|e_0\rangle$

If outcome is $|e_1\rangle$, Bob has $|e_1\rangle$

in which case he applies ZX to recover $|e_0\rangle$.



Remarks:

1. Alice's measurement depends on a, b
   Bob's decoding is independent on a, b

2. Why does RSP not contradict the optimality of TP?

   (a) Only works for some qubit states, not all

   but this limitation is not fundamental
   -- we will see a solution for large dimension

   (b) Protocol does not produce "qbits" -- it does not preserve entanglement between the transmitted system and an arbitrary reference system.

   Crucial -- optimality proof of TP does not apply.

   (c) Alice needs to know the state

   Crucial -- knowledge is power ...

We will discuss:

1. remote state preparation for arbitrary pure states in d dims
2. make connection with approximate encryption
3. open problems and known bounds
4. discuss extensions to superdense coding of quantum state (leaving most in A1)

A useful lemma:

If Alice and Bob share $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$ on AB

and Alice applies (to A) meas with POVM $\{M_k\}$,

then, prob(k) = $\frac{1}{d} \mathrm{tr}(M_k)$,

postmeas state conditioned on outcome k = $\frac{M_k^T}{\mathrm{tr}\, M_k}$

Proof: similar to self-study notes, show that

$$\mathrm{tr}_1 \left(|\Phi_d\rangle\langle\Phi_d| \; M_k \otimes I \right) = \frac{1}{d} M_k^T$$

$$\| $$

prob(k) * postmeas state

Rule of thumb: to "induce" a state ρ, choose $M_k \propto \rho^T$

Lo 99: Remote state preparation of a re-bit (revisited)

Alice comes up with some $|\psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{R}$

Her goal: prepare a copy of $|\psi\rangle$ in Bob's lab
using entanglement & classical communication

Solution 2: Alice & Bob share 1 ebit $|\Phi\rangle$

Let $M_0 = (|\psi\rangle\langle\psi|)^T = \begin{bmatrix} a^2 & ab \\ ab & b^2 \end{bmatrix}$, $M_1 = (XZ\,|\psi\rangle\langle\psi|\,ZX)^T = \begin{bmatrix} a^2 & -ab \\ -ab & b^2 \end{bmatrix}$

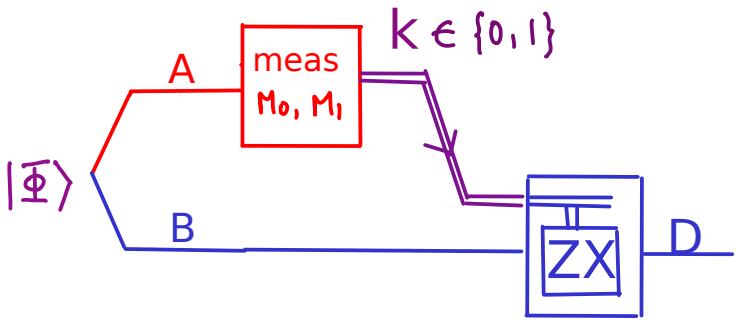
NB M_0, M_1 depend on $|\psi\rangle$, but $M_0 + M_1 = I$

Alice applies meas on A, with POVM M_0, M_1
& tells Bob the outcome (1 cbit)

If outcome = 0, Bob has $|\psi\rangle\langle\psi|$

If outcome = 1, Bob has $XZ\,|\psi\rangle\langle\psi|\,ZX$

in which case he applies ZX to
recover $|\psi\rangle\langle\psi|$



Sufficient conditions + protocol for remote state preparation

Goal: Alice prepares a copy of $|\psi\rangle \in S \subseteq \mathbb{C}^d$ in Bob's lab
using a copy of $|\Phi_d\rangle$ (on AB) & classical comm

Suppose $\exists\, U_1, U_2, \ldots U_t \in \mathcal{U}(d)$

s.t. $\forall\, |\psi\rangle \in S$, $\frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger = \frac{I}{d}$

same set of U_k for all $|\psi\rangle$

Then, each $|\psi\rangle \in S$ defines a POVM $\{M_k\}$ on A:

$$M_k = \frac{d}{t} \left(U_k |\psi\rangle\langle\psi| U_k^\dagger \right)^T \qquad \left(\because M_k \geq 0,\ \sum_{k=1}^{t} M_k = I \right)$$

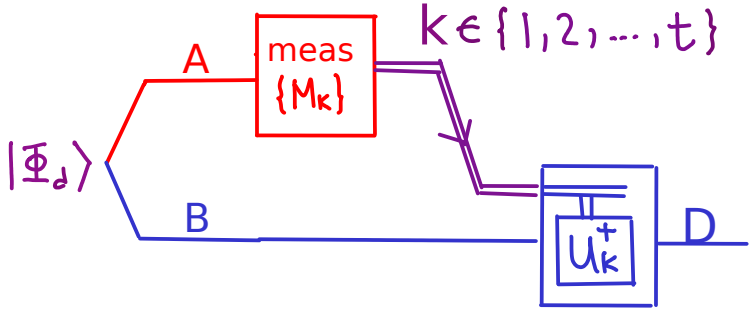
Protocol T: Alice comes up with some $|\psi\rangle \in S$

Alice applies meas on A, with POVM $\{M_k\}$

& tells Bob the outcome k (log t cbits)

If outcome = k, Bob has $U_k |\psi\rangle\langle\psi| U_k^\dagger$

he applies $U_k^\dagger$ to recover $|\psi\rangle\langle\psi|$



For protocol T :

How large does t have to be for the U_k's to exist?

In Lo 99, S = equator of Bloch sphere, and t=2 sufficient.

If S = $\mathbb{C}^d$, t = d^2 sufficient

choose U_k to be generalized Pauli's (pf ~ SS notes)

note this consumes as many resources as TP

If S = $\mathbb{C}^d$, then t = d^2 necessary.

The condition $\forall\, |\psi\rangle \in S$, $\frac{1}{t}\sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger = \frac{I}{d}$ gives an exact encryption scheme for quantum states, and the lower bound for t follows from last lecture.

Recall: for exact encryption scheme $\forall \rho\ \mathcal{E}(\rho) = \sigma$

which implies $\forall\, |\psi\rangle$, $I \otimes \mathcal{E}(|\psi\rangle\langle\psi|) = (tr_2 |\psi\rangle\langle\psi|) \otimes \sigma$.

What about more general RSP protocols?

For exact RSP (arbitrary entangled state):

- if S includes a basis, needs log d cbits (due to C2)

- if $S = \mathcal{L}^d$, no further restriction, open problem ...

- if $S = \mathcal{L}^d$, "oblivious to Bob" (he receives no more info about the state beyond the prepared copy), then needs 2 log d cbits. (L, Shor 02)

  e.g., protocol in previous slide is oblivious
  -- prob(k) indep of $|\psi\rangle$

  Proof idea: from RSP protocol, construct encryption scheme, then argue similar to last lecture

- if $S = \mathcal{L}^d$, Bob's decoding restricted to Pauli's but prob(k) may depend on the state, still needs 2 log d cbits (Nayak).

Approx RSP, approx oblivious, ~log d cbits sufficient!

Approx RSP (based on protocol T & a technical lemma):

Technical lemma (HLSW03, BHLSW03):

For large d, $\varepsilon > 0$,

$$\exists\, U_1, U_2, \ldots U_t \in \mathcal{U}(d)$$

$$\text{s.t. } \forall\, |\psi\rangle \in \mathbb{C}^d, \quad \left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$$

for t = $\frac{1}{\varepsilon^2}$ 134 d log d (t = $\frac{1}{\varepsilon^2}$ 150 d log $\frac{1}{\varepsilon}$ in Aubrun 08)

where $\| \quad \|_\infty$ = operator-norm (max (abs (eigenvalue)))

When $\varepsilon = 0$, same as the sufficient condition for protocol T and requires $t \geq d^2$.

Proof ideas for technical lemma:

Want $U_1, U_2, \ldots U_t \in \mathcal{U}(d)$

$$\text{s.t. } \forall |\psi\rangle \in \mathbb{C}^d, \left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$$

Note $\forall |\psi\rangle \in \mathbb{C}^d, \int dU \; U|\psi\rangle\langle\psi|U^\dagger = \frac{I}{d}$. Fix $|\psi\rangle$.

dU: Haar measure

View $U|\psi\rangle\langle\psi|U^\dagger$ as an operator-valued RV, with average $\frac{I}{d}$.

Take iid samples according to Haar measure:

$$U_1|\psi\rangle\langle\psi|U_1^\dagger, \; U_2|\psi\rangle\langle\psi|U_2^\dagger, \; \ldots, \; U_t|\psi\rangle\langle\psi|U_t^\dagger$$

Take empirical average: $\frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger$

Analyse how quickly empirical average converges to actual average (as a function of t) ...

Can show that: fix $|\psi\rangle$. With very high prob over which $U_1, U_2, \ldots, U_t$ are drawn, $\left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$

(Prob(above doesn't hold) rapidly vanishes with t, d.)

Take union bound over a net of $|\psi\rangle$

The prob the above fail for at least one $|\psi\rangle$ is still very low.

So, there must exist some $U_1, U_2, \ldots, U_t$

$$\forall |\psi\rangle \quad \left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$$

Actual proof more technical ... possible term project.

First of many randomized arguments, with a protocol known to exist existentially (but without an explicit construction).

Consequences of technical lemma:

1. RSP of any $|\psi\rangle \in \mathbb{C}^d$ exactly with prob $\geq 1-\varepsilon$ possible

   using log d ebits & log d + loglog d + 2 log $\frac{1}{\varepsilon}$ + 8 cbits

   Proof: $\forall\, |\psi\rangle \in \mathbb{C}^d,\ \left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$

   $$\Longrightarrow \left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger \right\|_\infty \leq \frac{(1+\varepsilon)}{d}$$

   Then, each $|\psi\rangle \in S$ defines a POVM $\{M_k\}$

   $$M_k = \frac{1}{(1+\varepsilon)} \frac{d}{t} \left(U_k |\psi\rangle\langle\psi| U_k^\dagger \right)^T \quad \text{for k = 1,2,...,t}$$

   $$M_{t+1} = I - \sum_{k=1}^{t} M_k\ , \qquad \left\| \sum_{k=1}^{t} M_k \right\|_\infty \leq 1 \ \therefore\ M_{t+1} \geq 0$$

   Other $M_k \geq 0$, and $\sum_{k=1}^{t+1} M_k = I$.

Apply protocol T as before: Alice and Bob share $|\Phi_d\rangle$

Alice comes up with some $|\psi\rangle$

Alice applies meas on A, with POVM $\{M_k\}_{k=1}^{t+1}$

& tells Bob the outcome k (log (t+1) cbits)

If outcome = k < t+1, Bob has $U_k |\psi\rangle\langle\psi| U_k^\dagger$

he applies $U_k^\dagger$ to recover $|\psi\rangle\langle\psi|$

If outcome = k = t+1, Bob outputs an error symbol.

$$\text{Prob}(k=t+1) = \text{tr}\left(M_{t+1} \cdot \frac{I}{d} \right)$$

$$= \text{tr}\left[\left(I - \sum_{k=1}^{t} M_k \right) \cdot \frac{I}{d} \right]$$

$$= 1 - \frac{t}{d} \text{tr}\, M_k$$

$$= 1 - \frac{t}{d} \frac{1}{(1+\varepsilon)} \frac{d}{t}$$

$$= \frac{\varepsilon}{(1+\varepsilon)} \leq \varepsilon$$

(state on A = I/d)

$$M_k = \frac{1}{(1+\varepsilon)} \frac{d}{t} \left(U_k |\psi\rangle\langle\psi| U_k^\dagger \right)^T$$

So, the protocol succeeds with prob at least 1- ε
It uses log d ebits,
and log (t+1) cbits, for $t = \frac{1}{\varepsilon^2} 134\, d \log d$

For large d and constant ε, log (t+1) is dominated by the leading term log d.

With prob $\frac{1}{(1+\varepsilon)}$, protocol is exact and oblivious.

Bob gets one exact copy of $|\Psi\rangle$, & prob(k) is indep of $|\Psi\rangle$

With prob $\frac{\varepsilon}{(1+\varepsilon)}$, Bob gets $\frac{M_{t+1}}{\mathrm{Tr}\, M_{t+1}}$.

This breaks the lower bound from LS02 ...

$$M_k = \frac{1}{(1+\varepsilon)} \frac{d}{t} \left(U_k |\Psi\rangle\langle\Psi| U_k^\dagger \right)^T$$

$$M_{t+1} = I - \sum_{k=1}^{t} M_k$$

Consequences of technical lemma:

2. Any $|\psi\rangle \in \mathbb{C}^d$ can be encrypted and decrypted with

   $\log d + \log\log d + 2 \log \frac{1}{\varepsilon} + 8$ kbits

   such that the quantum ciphertex is ε close to $\frac{I}{d}$ in trace distance.

Proof: $\forall\, |\psi\rangle \in \mathbb{C}^d$, $\left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$

$$\left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_1 \leq \varepsilon$$

Encryption scheme: $\forall k$, $p_k = \frac{1}{t}$

Conditioned on the key k, Alice applies U_k to encrypt

Bob applies $U_k^\dagger$ to decrypt

Eve sees the state $\frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger$ which is ε close to $\frac{I}{d}$

Consequences of technical lemma:

3. Define the completely randomizing map R on d-dim state as: $\forall \rho \,.\, R(\rho) = \frac{I}{d}$

Let $\mathcal{E}(\rho) = \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger$.

So, $\forall \rho \,.\, \| R(\rho) - \mathcal{E}(\rho) \|_1 \leq \varepsilon$ but $\| R - \mathcal{E} \|_\diamond \approx 1$

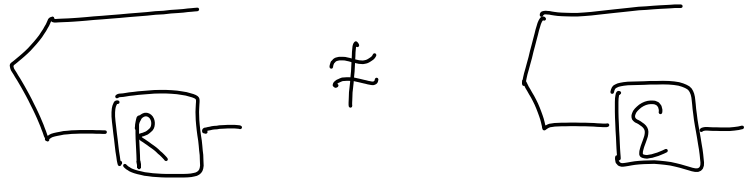
In particular, $I \otimes R(|\Phi_d\rangle\langle\Phi_d|) = \frac{I}{d} \otimes \frac{I}{d}$

But $I \otimes \mathcal{E}(|\Phi_d\rangle\langle\Phi_d|)$ only has rank t $\ll d^2$.

↑ very very different from $\frac{I}{d} \otimes \frac{I}{d}$

Two TCP maps can thus be nearly indistinguishable on the input system alone, but very different if a reference system is included.

but



vanishing function of ε

NB. Luckily, for $R = I$,

$$\text{if } \forall \rho,\ \|\mathcal{E}(\rho) - R(\rho)\|_1 \leq \varepsilon \text{ then } \|\mathcal{E} - R\|_\diamond \leq f(\varepsilon)$$

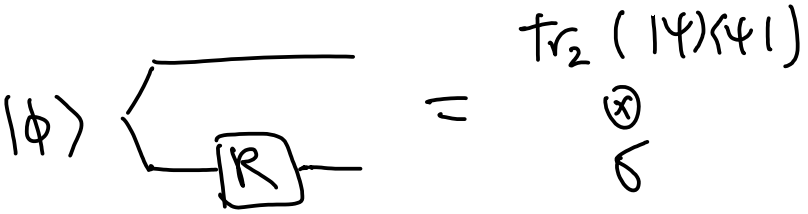
NB $\forall \rho, \|\mathcal{E}(\rho) - R(\rho)\|_1 \leq \varepsilon \iff \forall |\psi\rangle, \|\mathcal{E}(|\psi\rangle\langle\psi|) - R(|\psi\rangle\langle\psi|)\|_1 \leq \varepsilon$

Open problem: what TCP maps can be accurately characterized by pure state inputs?

Further remarks:

$\forall \rho, \ R(\rho) = \frac{I}{d}$

$\mathcal{E}(\rho) = \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger .$



entanglement (+all correlations) between the 2 sys are broken

does not break correlations

But $\forall |\psi\rangle \in \mathbb{C}^d, \ \mathcal{E}(|\psi\rangle\langle\psi|) \approx \frac{I}{d}$ with key cost similar

to classical setting. So, the factor of 2 for quantum encryption comes from having to break correlations.

Also, the approx RSP scheme breaks the 2 log d comm lower bound for TP because of the following.

From the RSP measurement, we cannot make a generalized TP scheme in which Alice operates independent of the input. The construction last lecture gives a proper measurement because

$$I \otimes \sum_k p_k \mathcal{E}_k \left(|\Phi\rangle\langle\Phi| \right) = \frac{I}{d} \otimes \frac{I}{d},$$

which does not hold for $\mathcal{E}$.

Superdense coding of quantum states:

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

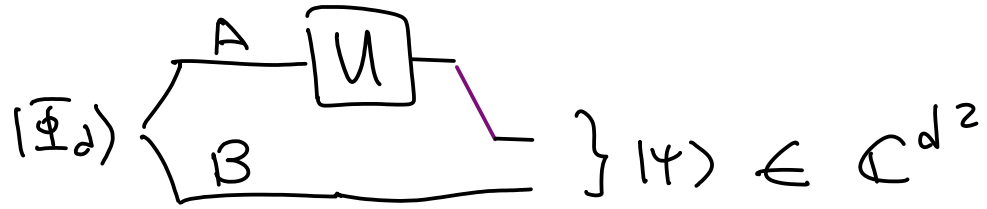
Alice applies one of 4 unitaries turning her shared state with Bob to one of 4 orthogonal states, thereby "doubling" the rate of communication.

If she instead wants to prepare a d^2-dim pure state $|\Psi\rangle$ in Bob's lab, and she knows the state to be prepared.

This is analogous to RSP, in that the sender knows the state to be prepared, but here we allow entanglement and quantum comm to be used.

Can she do so by consuming only log d qbits?

1. if the state is "maximally entangled" , $|\psi\rangle = U \otimes I \, |\Phi_d\rangle$ for some U, then she applies U to her half of $|\Phi_d\rangle$ and sends it to Bob.



2. So, the d^2 states used in SD is a special case -- Alice knows which of the d^2 orthogonal max entangled state is to be prepared in Bob's lab.

3. For large d, states in $\mathbb{C}^{d^2}$ with nearly max entanglement form a high prob set. So, if $|\psi\rangle \in \mathbb{C}^{d^2}$ is drawn at random, is there a way to super-dense-code $|\psi\rangle$ with good approximation?

4. What if someone tells Alice which $|\psi\rangle$ has to be prepared and adversarially choose $|\psi\rangle$?

Spoiler: there is still a way to super-dense-code $|\psi\rangle$

in that log d ebits and slightly larger than log d qbits are needed, but no other resources (like shared randomness) is needed.

How? there is a large subspace in a bipartite system containing only high entangled states. In A1, you will use this fact to perform SD of quantum states !!

Quantum states known to the sender seems to behave a little like classical data (in the presence of shared entanglement between Alice and Bob and in terms of the necessary communication cost of transmission).