Part 4 lec 3 

LOCC measurements (Ch 19)

Consider discrimination of bipartite states:

Richard draws $x$ wp $p_x$, prepares $\rho_x \in D(X_A \otimes X_B)$
gives sys $X_A$ to Alice, sys $X_B$ to Bob.

Alice and Bob can apply a measurement (in LOCC, or SEP, or PPT, or jointly).

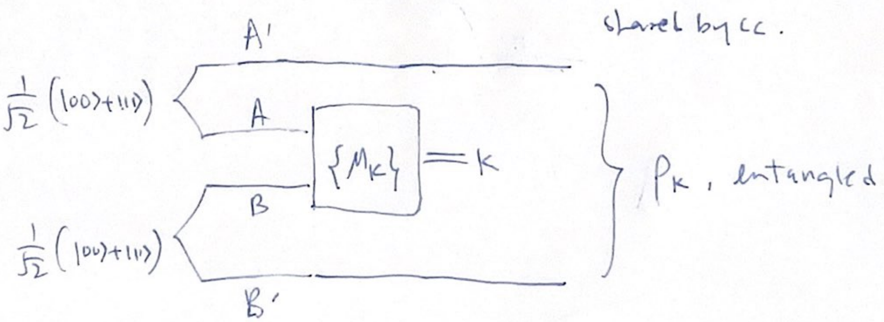
When locality restriction reduces the prob of success,
the ensemble to be discriminated is said to exhibit nonlocality.

eg 1. let $x = 0, 1, 2, 3$, $p_x = \frac{1}{4}$ for all $x$

$\rho_{0,1,2,3}$ are the 4 Bell states

- Using a joint measurement, the 4 Bell states can be perfectly discriminated.
- Using a meas in LOCC, SEP or PPT, the 4 Bell states cannot be perfectly distinguished. To see this, suppose such a Sep meas exists. This perfect measurement $\{M_k\}$ necessarily has $M_k \propto \rho_k$. With this measurement, instead of using it for state discrimination Alice & Bob instead,

(1) each prepares local $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, (2) Apply meas, (3) Obtain outcome $k$ shared by cc. (4) post meas state on $A'B'$ $\propto M_k$ which is $\rho_k$.




Then the sep meas turns a state in $Ent_1(A'A : BB')$ to $Ent_2(A' : B')$
a contradiction. Similar proof holds for PPT meas.

More detailed proof in Sec 19.2.1:

Let $|\psi_K\rangle = (U_K \otimes \mathbb{1})\tilde{\beta} \in \mathcal{X}_A \otimes \mathcal{X}_B$,

$\tilde{\beta} = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle|i\rangle$, $\beta = \sum_{i=1}^{n} |i\rangle|i\rangle$

$n = \dim(\mathcal{X}_A)$

$U_K$ unitary (so $|\psi_K\rangle$ max ent)

$K = 1, 2, \ldots, t$, $p_K = \frac{1}{t}$ $\forall K$.

Let $M_K = \sum_j P_{Kj} \otimes Q_{Kj} \in \mathrm{Sep}(\mathcal{X}_A : \mathcal{X}_B)$ be meas op corr to $|\psi_K\rangle$.

$$\text{Prob suc} = \frac{1}{t} \sum_{K=1}^{t} \mathrm{tr}\left( M_K \cdot |\psi_K\rangle\langle\psi_K| \right)$$

$$= \frac{1}{t} \sum_{K=1}^{t} \mathrm{tr}\left( \sum_j P_{Kj} \otimes Q_{Kj} \cdot \frac{1}{n} \cdot (U_K \otimes \mathbb{1}_{\mathcal{X}_B}) \beta\beta^* (U_K^* \otimes \mathbb{1}_{\mathcal{X}_B}) \right)$$

transpose trick $$= \frac{1}{t} \sum_{K=1}^{t} \mathrm{tr}\left( \sum_j P_{Kj} \otimes \mathbb{1}_{\mathcal{X}_B} \frac{1}{n} \cdot (U_K Q_K^t \otimes \mathbb{1}_{\mathcal{X}_B}) \beta\beta^* (U_K^* \otimes \mathbb{1}_{\mathcal{X}_B}) \right]$$

partial trace $$= \frac{1}{t} \sum_{K=1}^{t} \mathrm{tr}_{\mathcal{X}_A} \left[ \sum_j P_{Kj} \cdot \frac{1}{n} \cdot U_K Q_K^t \cdot \left( \mathrm{tr}_{\mathcal{X}_B} \beta\beta^* \right) \cdot U_K^* \right]$$

$$= \frac{1}{t} \sum_{K=1}^{t} \frac{1}{n} \cdot \sum_j \mathrm{tr}\left( P_{Kj} \; U_K Q_K^t U_K^* \right)$$

$$\leq \frac{1}{t} \sum_{K=1}^{t} \frac{1}{n} \sum_j \mathrm{tr}\, P_{Kj} \cdot \underbrace{\mathrm{tr}\, U_K Q_K^t U_K^*}_{\mathrm{Tr}\, Q_K^t \,=\, \mathrm{tr}\, Q_K}$$

$$= \frac{1}{t} \sum_{K=1}^{t} \frac{1}{n} \sum_j \mathrm{tr}\left( P_{Kj} \otimes Q_{Kj} \right)$$

$$= \frac{1}{t} \sum_{K=1}^{t} \frac{1}{n} \underbrace{\sum_j \mathrm{tr}\, M_j}_{n^2} = \frac{n}{t}.$$

if $t \geq n+1$, cannot perfectly distinguish with SEP meas.

Also if $t = n^2$, prob suc $\leq \frac{1}{n}$ (achievable).

eg2 Any 2 orthogonal bipartite pure states can be discriminated (0007098)
perfectly by LOCC.

Pf: Let the 2 states be $|\psi\rangle = |1\rangle_A|\eta_1\rangle_B + |2\rangle_A|\eta_2\rangle_B + \cdots + |n\rangle_A|\eta_n\rangle_B$

$|\phi\rangle = |1\rangle_A|\nu_1\rangle_B + |2\rangle_A|\nu_2\rangle_B + \cdots + |n\rangle_A|\nu_n\rangle_B$

Note $|\eta_i\rangle$, $|\nu_i\rangle$ not normalized, can be 0, not Schmidt decomp.

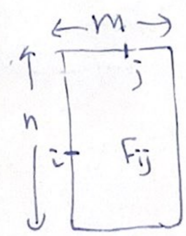
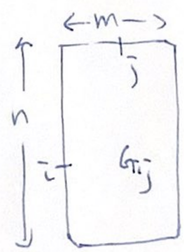
but $\{|1\rangle, |2\rangle, \ldots, |n\rangle\}$ o.n. basis for A.

Let $\{|1\rangle, \ldots, |m\rangle\}$ be o.n basis for B, $m \le n$

$$|\eta_i\rangle_B = \sum_{j=1}^{m} F_{ij}\,|j\rangle_B$$

$$|\nu_i\rangle_B = \sum_{j=1}^{m} G_{ij}\,|j\rangle_B.$$

$F = \sum_{ij} |i\rangle\langle j|\, F_{ij}$ , $G = \sum_{ij} |i\rangle\langle j|\, G_{ij}$

=  = 

$$FG^* = \sum_{ij} |i\rangle\langle j|\, F_{ij} \sum_{i'j'} |j'\rangle\langle i'|\, G^*_{i'j'}$$

$$= \sum_{ii'} |i\rangle\langle i'| \sum_j F_{ij}\, G^*_{i'j}$$

$$= \sum_{ii'} |i\rangle\langle i'|\, \langle \nu_{i'}|\eta_i\rangle = \begin{bmatrix} \langle \nu_1|\eta_1\rangle & \cdots & \langle \nu_1|\eta_n\rangle \\ \langle \nu_2|\eta_1\rangle & \cdots & \langle \nu_2|\eta_n\rangle \\ \vdots & & \\ \langle \nu_n|\eta_1\rangle & \cdots & \langle \nu_n|\eta_n\rangle \end{bmatrix}$$

Note that $\langle \phi | \psi \rangle = 0 = \sum_{i=1}^{n} \langle \nu_i | \eta_i \rangle = \mathrm{Tr}(FG^*)$

Consider a unitary $U$ on $A$ relating the basis $\{|1\rangle, \dots, |n\rangle\}$ to $\{|1'\rangle, \dots, |n'\rangle\}$ as:

$$|i\rangle_A = \sum_j \bar{u}_{ij} |j'\rangle_A$$

and define $|1'\rangle_B, |2'\rangle_B, \dots, |n'\rangle_B$ as

$$|k\rangle_B = \sum_l u_{kl} |l'\rangle_B$$

Then,
$$|\psi\rangle = \sum_{i=1}^{n} |i\rangle_A |\eta_i\rangle_B = \sum_{i=1}^{n} |i\rangle_A \sum_{k=1}^{m} F_{ik} |k\rangle_B$$

$$= \sum_{i=1}^{n} \left( \sum_{j=1}^{n} \bar{u}_{ij} |j'\rangle_A \right) \sum_{k=1}^{m} F_{ik} \sum_{l=1}^{n} u_{kl} |l'\rangle_B$$

$$= \sum_{j=1}^{n} \sum_{l=1}^{n} \underbrace{\left( \sum_{i=1}^{n} \sum_{k=1}^{m} \bar{u}_{ij} F_{ik} u_{kl} \right)}_{= (U^* \tilde{F} U)_{jl} = \boxed{F|}} |j'\rangle_A |l'\rangle_B$$

$$|\phi\rangle = \sum_{j=1}^{n} \sum_{l=1}^{n} (U^* \hat{G} U)_{jl} |j'\rangle_A |l'\rangle_B .$$

$$FG^* \rightarrow (U^* \hat{F} U)(U^* \hat{G} U)^* = U^* \hat{F} \hat{G}^* U$$

$|i\rangle|k\rangle$ basis $\quad$ $|j'\rangle|l'\rangle$ basis

$$\boxed{F|0} \; \boxed{\tfrac{G^*}{0}} = FG^*$$

and vice-versa, that conjugation of $FG^*$ corr to local change of basis by Alice & Bob.

Claim: $\exists U$ s.t. $U^* F G^* U$ has equal diagonal entries.

Pf (elementary, see 0007098)

But $\operatorname{tr} U^* F G^* U = \operatorname{tr} F G^* = 0$ $\therefore$ all diagonal entries of $U^* F G^* U$ are zero!

Protocol: Alice measures along $\{|1'\rangle, |2'\rangle, \ldots, |n'\rangle_A\}$ basis, sends outcome "$j$" to Bob.

if state was $|\psi\rangle$, Bob's state is now $\sum_l (U^* \tilde{F} U)_{jl} |l'\rangle_B$

- - - $|\phi\rangle$, - - - $\sum_l (U^* \tilde{G} U)_{jl} |l'\rangle_B$

orthogonal $\therefore$ can be perfectly discriminated by a measurement on B!!

Bonus: works for any # parties, by letting B = (party 2, party 3, ... )

Since now the problem for parties in B is again to discriminate 2 ortho pure states.

It takes 1 classical message from party 1 to part 2

1 - - - 2 3

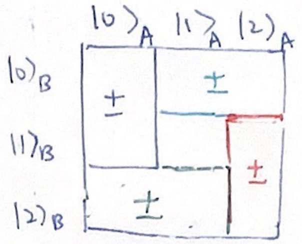
and last party finds out which of $|\phi\rangle, |\psi\rangle$ is given and announced to all other parties.

# parties + 1 rounds, 2× # parties messages needed.

eg3 LOCC ≠ SEP, $\overline{\text{LOCC}}$ ≠ SEP

↙ topological closure!

Consider the 9 states in $\mathbb{C}^3 \otimes \mathbb{C}^3$:




(call nonlocality without entanglement 9804053)

$|0\rangle_A \left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}\right)_B$ , $|2\rangle_A \left(\frac{|1\rangle \pm |2\rangle}{\sqrt{2}}\right)_B$ ,

$\left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}\right)_A |2\rangle_B$ , $\left(\frac{|1\rangle \pm |2\rangle}{\sqrt{2}}\right)_A |0\rangle_B$ , $|1\rangle_A |1\rangle_B$

① They form a basis for $\mathbb{C}^3 \otimes \mathbb{C}^3$.

② Each is a product state.

Perfect measurement for discrimination $\in$ SEP $(\mathbb{C}^3_A : \mathbb{C}^3_B)$.

Prob (failure) given LOCC meas $\geq 10^{-6}$ !

↑ a constant

∴ not only perfect meas ∉ LOCC

cannot even converge to perfect meas by LOCC!

∴ $\overline{\text{LOCC}}$ (closure) $\subsetneq$ SEP!

NB. Doesn't help to have unlimited # messages, and unlimited length of those messages.

Back to pure state transformation, but 3 parties.

eg 4 Initial state: $\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}$

Alice & Bob share $\frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)_{AB}$ Sep, no entanglt

Cannot distill a key that Charlie doesn't know!

But Charlie is not evil....

He is willing to assist Alice & Bob in distillation.

He meas C along the $\{|+\rangle, |-\rangle\}$ basis.

$$\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle) = \frac{1}{\sqrt{2}}\left[\frac{(|00\rangle+|11\rangle)}{\sqrt{2}}\underbrace{\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}}_{①} + \frac{(|00\rangle-|11\rangle)}{\sqrt{2}}\underbrace{\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}}_{②}\right]$$

① If Charlie gets "$|+\rangle$", Alice & Bob share $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

② "$|-\rangle$" - -

So if Charlie tells Bob, he applies $\mathbb{1}$ / $\sigma_z$ if Charlie says +/−.

∴ Alice & Bob always share $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ !

(eg 5) Fortescue - Lo Random distillation 0709.4059

If initial state is $|W\rangle = \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right)_{ABC}$

then Charlie cannot help Alice & Bob distill one ebit.

But.... If they only want 2 out of 3 parties to share an ebit, they can approx the task arbitrarily well !!

In 1106.1208, Chitambar, Cui, Lo proved that

$|W\rangle \longrightarrow \begin{cases} \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle\right)_{AB} \\ \text{or} \\ \quad \cdots \quad BC \\ \quad \cdots \quad AC \end{cases}$ is in $\overline{\text{LOCC}}$ but not in "LOCC"

includes all LOCC with finite # messages and a restricted class of LOCC ops with infinitely many messages.

Alas LOCC is <u>NOT</u> a closed set !!

Semi-formal definition of LOCC (1210.4583):

- Consider discrete quantum instruments, with common input space each defined as a family of completely positive maps $\mathcal{E} = (\mathcal{E}_j : j \in \Theta)$, for an index set $\Theta$ that may be finite or countably infinite, and $\sum_j \mathcal{E}_j$ is TP.

- Discrete quantum instruments form a convex set.

- $\mathcal{E}(\rho) = \sum_{j\in\Theta} \mathcal{E}_j(\rho) \otimes |j\rangle\langle j|$

- Distance between $\mathcal{E}$ and $\mathcal{F}$ with common input space & index sets:

$$\| \mathcal{E} - \mathcal{F} \|_\diamond = \max_{0\le\rho\le 1} \sum_{j\in\Theta} \| (I\otimes \mathcal{E}_j - I\otimes \mathcal{F}_j)(\rho) \|_1$$

- Sequence of instruments $\mathcal{F}_1, \mathcal{F}_2, \ldots$ converges to $\mathcal{E}$ if

$$\lim_{n\to\infty} \| \mathcal{E} - \mathcal{F}_n \|_\diamond \to 0$$

- When input is m-partite, instrument $\mathcal{F} = (\mathcal{F}_j : j \in \Theta)$ is 1-local with respect to the party K,

$$\text{if } \forall j,\ \mathcal{F}_j = \bigotimes_{a\in\{1,2,\ldots,K-1,K+1,\ldots m\}} \Phi_{aj} \otimes \mathcal{E}_{Kj}$$

$\mathcal{E}_{Kj}$ in $CP(\mathcal{X}_K : \mathcal{Y}_K)$ s.t $\sum_j \mathcal{E}_{Kj}$ is TP

$\Phi_{aj} \in C(\mathcal{X}_a, \mathcal{Y}_a)$.

Some Channel with Input $\mathcal{X}_a$, output $\mathcal{Y}_a$ held by the a-th party

ie operationally, party K applies instrument $(\mathcal{E}_{Kj} : j \in \Theta)$ and broadcast j to all other parties.

• $\tilde{F}'$ is <u>LOCC-linked</u> to $\tilde{F} = (F_j : j \in \Theta)$

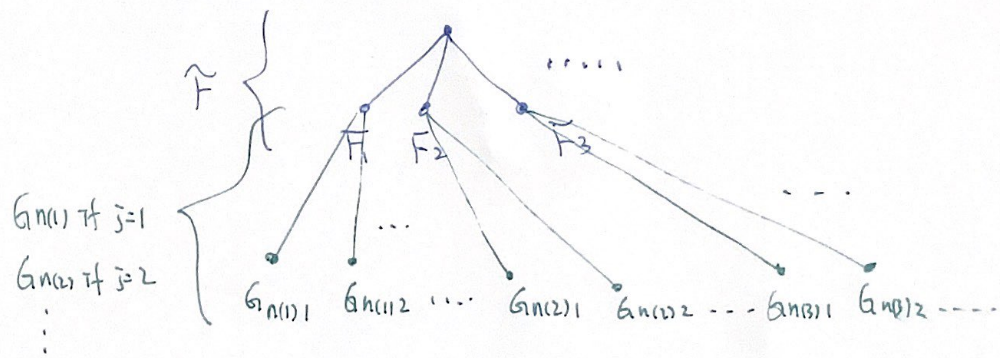
if $\exists\, G_1, G_2, \dots, G_m$,

and $\forall K$, $G_K$ 1-way local wrt to party $k$, $G_K = (G_{K\ell} : \ell \in \Theta_K)$

$\exists$ function $n : \Theta \to \{1, 2, \dots, m\}$ (who is next)

s.t. $\tilde{F}' = (G_{n(j)\ell} \circ F_j : \Theta \times \Theta_{n(j)})$

ie $\tilde{F}'$ is obtained from adding one round of LO's and CC from party $n(\ell)$ for each outcome $\ell$ from $\tilde{F}$.




• Def of LOCC:

① $LO = LOCC_0$

② $\tilde{F} \in LOCC_1$ if $\tilde{F}$ 1-way local wrt to some party $k$

③ $\tilde{F}' \in LOCC_r$ $(r \geq 2)$ if $\tilde{F}'$ LOCC-linked to some $\tilde{F} \in LOCC_{r-1}$

④ $\tilde{F} \in LOCC_{\mathbb{N}}$ if $\tilde{F} \in LOCC_r$ for some $r \in \mathbb{N} = \{1, 2, \dots\}$

⑤ $\tilde{F} \in LOCC$ if $\exists (\tilde{F}_1, \tilde{F}_2, \dots)$ s.t. each $\tilde{F}_r \in LOCC_{\mathbb{N}}$,

$\tilde{F}_r$ LOCC-linked to $\tilde{F}_{r-1}$ $\forall r \geq 2$

$\lim_{r \to \infty} \tilde{F}_r = \tilde{F}$

⑥ $\tilde{F} \in \overline{LOCC_{\mathbb{N}}}$ if $\exists (\tilde{F}_1, \tilde{F}_2, \dots)$ s.t. $\forall r$ $\tilde{F}_r \in LOCC_{\mathbb{N}}$, $\lim_{r \to \infty} \tilde{F}_r = \tilde{F}$.

Operationally, $LOCC_r$ can be implemented by $r$ rounds of classical communication (without limit to the size of the messages), $LOCC_{\mathbb{N}}$ : implemented by some finite-round LOCC, but can't say how many rounds.

LOCC : all protocols either finite-round, or approx arbitrarily well by adding more and more rounds (until reaching a desirable accuracy)

$\overline{LOCC_{\mathbb{N}}}$ : topological closure, improving the accuracy can require completely difference 1st, 2nd, .... rounds.

NB : We allow "coarse-graining" of indices as the LOCC instrument progresses through the rounds.

eg. can require infinite intermediate measurement outcomes but finally decide on one of the 9-outcomes for discrimination of  .

$$LOCC_r \subsetneq LOCC_{r+1} \subsetneq LOCC_{\mathbb{N}} \subsetneq LOCC \subsetneq \overline{LOCC_{\mathbb{N}}} \subsetneq SEP$$

$\vdots$

$LOCC_1$

UH

LO

Chitambar 1105.3451

Fortescue-Lo

Chitambar-Cui-Lo

random distillation

- Improving the accuracy requires changing even the first step!

nonlocality without entanglement

- even with approx preparing the ensemble (no entanglement needed) is irreversible

$\because$ distinguishing is not in $\overline{LOCC_{\mathbb{N}}}$

$\therefore$ cannot distinguish w/o entanglement, despite in SEP.

<u>Some good news:</u>

- LOCC is convex
- If $F = (\mathcal{E}_1, \ldots, \mathcal{E}_n)$ (finite final # of indices)

  m-partite, in $LOCC_r$, finite total dimensional input / outputs ($\leq d$)

  then a finite # of intermediate outcomes suffices

  so finite CC suffices. $n \cdot d^{4r}$ (Carathéodory)

- Subset of $LOCC_r$ with m final coarse-grained outcomes is compact.
- Much better bound on # outcomes for even LOCC

  If the goal is NOT to approx an LOCC instrument

  but to optimize an LOCC task (eg state discrimination)