CO781 / QIC 890:

Theory of Quantum Communication

Topic 5, part 6

Consequences of the LSD theorem

- sufficient conditions for zero quantum capacity

- private capacity

- private capacity $\neq$ quantum capacity

- symmetric-side-channel-assisted quantum capacity

- superactivation

- nonconvexity of quantum capacity

- rocket & half-rocket channels (probably have to omit)

Sufficient conditions for zero quantum capacity

Recall:

1. in general, $Q^{(1)}(\mathcal{N}) = 0 \not\Rightarrow Q(\mathcal{N}) = 0$

2. if N antidegradable, then Q(N) = 0

Here:

3. if N is PPT, then Q(N) = 0

(need some background on PPT states and PPT channels for this)

(a) The partial transpose

Let T denote the transpose operation on square matrices.

$$T\left(\sum_{ij} c_{ij}\,|i\rangle\langle j|\right) = \sum_{ij} c_{ji}\,|i\rangle\langle j| = \sum_{ij} c_{ij}\,|j\rangle\langle i|$$

Consider a bipartite system AB.
The partial transpose on B is defined as $I_A \otimes T_B$

$$I_A \otimes T_B\left(\sum_{kl}\sum_{ij} c_{klij}\,|k\rangle\langle l|_A \otimes |i\rangle\langle j|_B\right) = \sum_{kl}\sum_{ij} c_{klij}\,|k\rangle\langle l|_A \otimes |j\rangle\langle i|_B$$

e.g., $I_A \otimes T_B\left(\rho_A \otimes \nu_B\right) = \rho_A \otimes \nu^T{}_B$

e.g., $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$, $\Phi_{AB} = |\Phi\rangle\langle\Phi|_{AB} = \frac{1}{2}$

$$\begin{array}{c} \begin{matrix} |0\rangle_A|0\rangle_B & |0\rangle_A|1\rangle_B & |1\rangle_A|0\rangle_B & |1\rangle_A|1\rangle_B \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{array} \begin{matrix} \\ |0\rangle_A|0\rangle_B \\ |0\rangle_A|1\rangle_B \\ |1\rangle_A|0\rangle_B \\ |1\rangle_A|1\rangle_B \end{matrix}$$

$$I_A \otimes T_B\left(\Phi_{AB}\right) = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

inner block has a negative eigenvalue

NB the transpose is not a TCP map.
It signifies time reversal (i becomes -i in density matrices).
On uncorrelated systems, or such mixtures, effect not unphysical.
But sufficiently correlated systems show the unphysical effect.

(b) PPT states (states remaining positive under partial transpose)

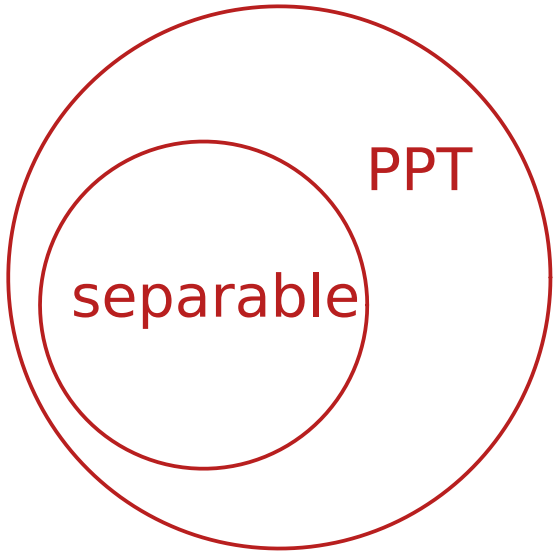
Def: A state ρ_{AB} is PPT if $I_A \otimes T_B (\rho_{AB}) \geq 0$

e.g., product states and separable states (mixtures of product states) are PPT, max entanged state (MES) is not PPT.

Intuition: PPT states are not very entangled.

Useful results: PPT state cannot be distilled (using LOCC) to MES

(Peres, (PMR)HHH ~96-97)



distillable

(c) PPT channels

MES for whole lecture

Def: A channel N is PPT if the Choi-state $I_R \otimes \mathcal{N}(\Phi)$ is PPT

e.g., entanglement-breaking channels are PPT

$\forall |\psi\rangle_{RA}$, $I \otimes \mathcal{N}(|\psi\rangle\langle\psi|)$ separable

Intuition: PPT channels can NEVER produce suff entangled states

Lemma: if N is PPT, $\forall \rho_{RA}$, $I_R \otimes \mathcal{N}(\rho)$ is PPT

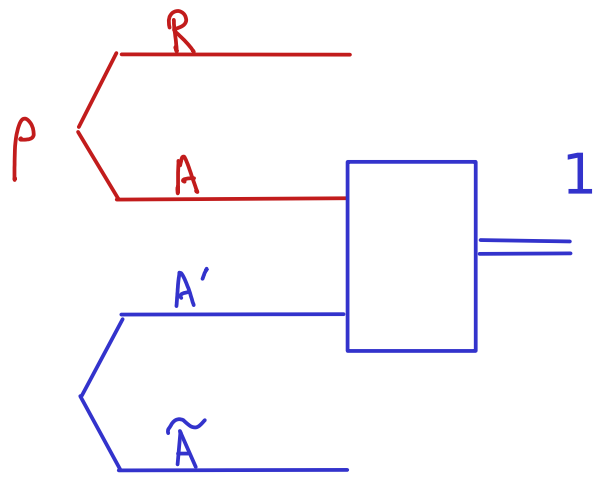
Significance: the PPT-ness of all possible input (including reference) can be verified on just 1 input (the MES).

(c) PPT channels

Def: A channel N is PPT if the Choi-state $I_R \otimes \mathcal{N}(\Phi)$ is PPT

Lemma: if N is PPT, $\forall \rho_{RA}$, $I_R \otimes \mathcal{N}(\rho)$ is PPT

Proof: (i) using teleportation,



1. if outcome corresponds to Φ (no correction) then state on $R\tilde{A}$ is ρ.

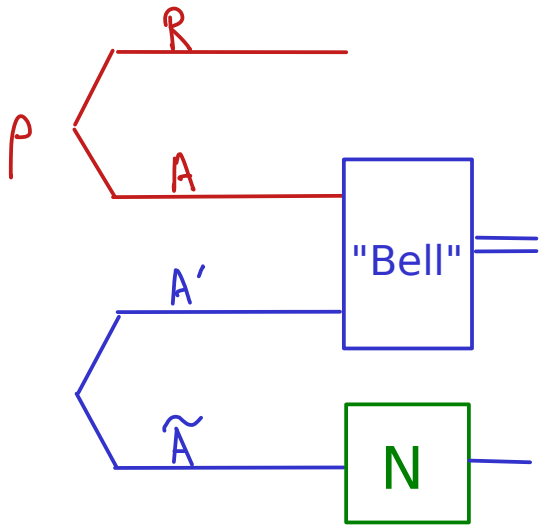
$$\mathrm{tr}_{AA'}\left(I_R \otimes \Phi_{AA'} \otimes I_{\tilde{A}}\right)\left(\rho_{RA} \otimes \Phi_{A'\tilde{A}}\right) = \rho_{R\tilde{A}}$$

(c) PPT channels

Def: A channel N is PPT if the Choi-state $\mathcal{I}_R \otimes \mathcal{N}(\Phi)$ is PPT

Lemma: if N is PPT, $\forall \rho_{RA}$, $\mathcal{I}_R \otimes \mathcal{N}(\rho)$ is PPT

Proof: (i) using teleportation,



1. if outcome corresponds to Φ (no correction) then state on $R\tilde{A}$ is ρ.

$$\mathrm{tr}_{AA'}\left(\mathcal{I}_R \otimes \Phi_{AA'} \otimes \mathcal{I}_{\tilde{A}}\right)\left(\rho_{RA} \otimes \Phi_{A'\tilde{A}}\right) = \rho_{R\tilde{A}}$$

2. apply N to $\tilde{A}$

$$\mathrm{tr}_{AA'}\left(\mathcal{I}_R \otimes \Phi_{AA'} \otimes \mathcal{I}_{\tilde{A}}\right)\left(\rho_{RA} \otimes \underbrace{\mathcal{I} \otimes \mathcal{N}(\Phi)_{A'\tilde{A}}}\right) = \mathcal{I}_R \otimes \mathcal{N}(\rho)$$

N commutes pass this

Choi-state of N

recall: want to show this is PPT

2. apply N to $\widetilde{A}$

$$\mathrm{tr}_{AA'}\left(I_R \otimes \Phi_{AA'} \otimes I_{\widetilde{A}}\right)\left(\rho_{RA} \otimes \underbrace{I \otimes N(\Phi)_{A'\widetilde{A}}}_{\text{Choi-state of N}}\right) = I_R \otimes N(\rho)$$

N commutes pass this

want to show this is PPT

3. apply partial transpose on $\widetilde{A}$

$$I_R \otimes T_{\widetilde{A}}\left[\mathrm{tr}_{AA'}\left(I_R \otimes \Phi_{AA'} \otimes I_{\widetilde{A}}\right)\left(\rho_{RA} \otimes I \otimes N(\Phi)_{A'\widetilde{A}}\right)\right] = I_R \otimes T_{\widetilde{A}}\left(I_R \otimes N(\rho)\right)$$

commute pass

see also circuit

$$\Big\Vert$$

$$\mathrm{tr}_{AA'}\underbrace{\left(I_R \otimes \Phi_{AA'} \otimes I_{\widetilde{A}}\right)}_{\text{meas operator}}\Big(\underbrace{\rho_{RA}}_{\text{state}} \otimes \underbrace{I_R \otimes T_{\widetilde{A}}\left[I \otimes N(\Phi)_{A'\widetilde{A}}\right]}_{\text{positive semidefinite (since N is PPT)}}\Big) \geq 0 \quad !!$$

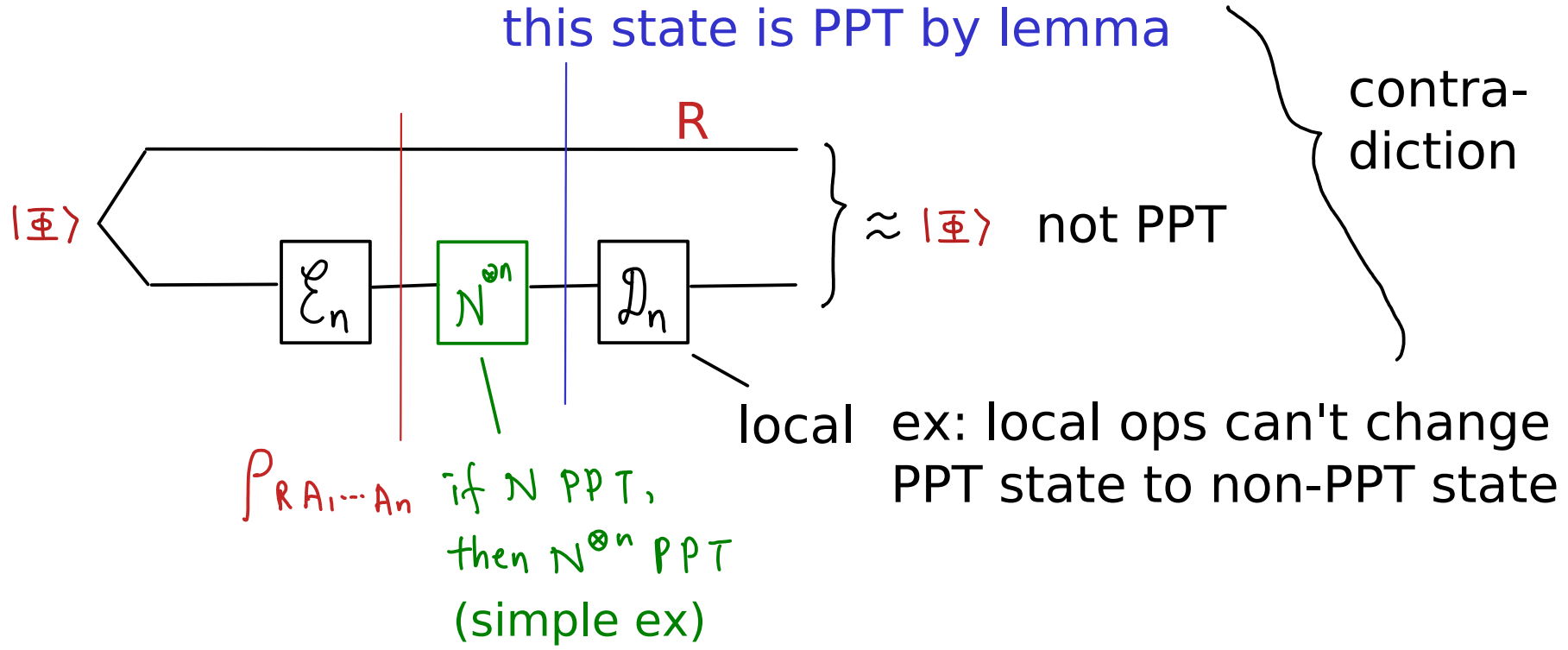
$\propto$ state

$\propto$ some post meas state

Sufficient conditions for zero quantum capacity

3. if N is PPT preserving, then Q(N) = 0 ((MPR)HHH 9904092)

Proof: suppose the opposite. There exists some PPT channel N with Q(N) > 0. There is an n-use protocol transmitting half of 1 EPR pair with high fidelity.



CO781 / QIC 890:

Theory of Quantum Communication

Topic 5, part 6

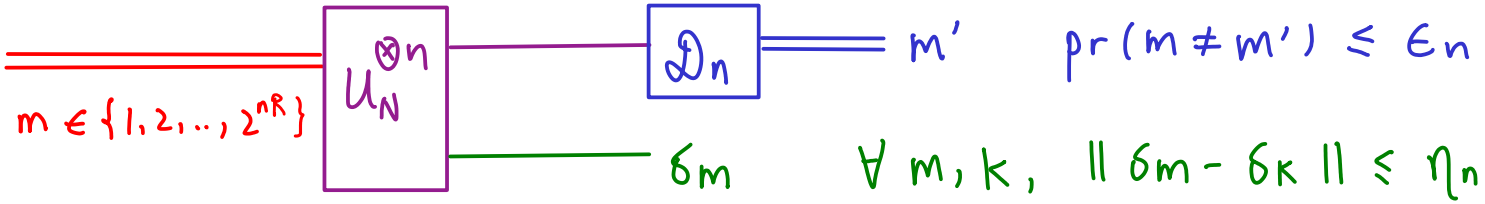
Consequences of the LSD theorem

- sufficient conditions for zero quantum capacity ✓
- private capacity
- private capacity $\neq$ quantum capacity
- symmetric-side-channel-assisted quantum capacity
- superactivation
- nonconvexity of quantum capacity
- rocket & half-rocket channels (probably have to omit)

Private capacity e.g., quantum data is private

We can use a quantum channel to transmit private classical data.

Roughly speaking, the private capacity is the best rate for comm classical data from Alice to Bob such that the complementary channel has vanishing info about the data. (passive eavesdropping)



R achievable if $\epsilon_n, \eta_n \to 0$ as $n \to \infty$. P(N) = sup achievable R's

Devetak 05: $P(N) = \sup_{r \to \infty} \underbrace{\frac{1}{r} P^{(1)}(N^{\otimes r})}$
(0304127)

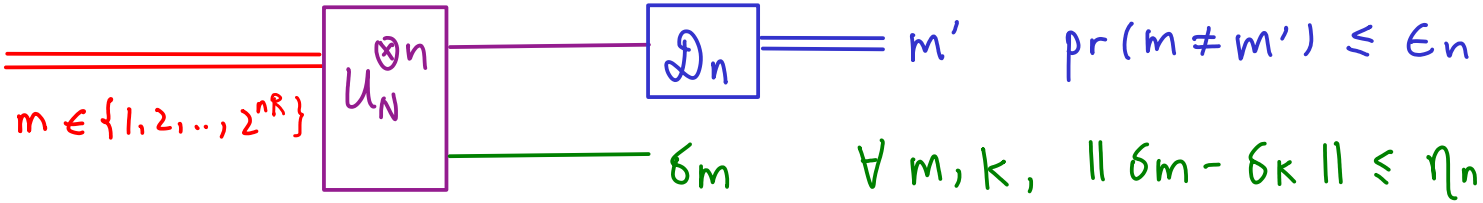
r-shot private information of N

where $P^{(1)}(N) = \max_{\psi_{XA} = \sum_x p_x |x\rangle\langle x|_X \otimes \phi_{xA}} S(X:B)_{I \otimes N(\psi)} - S(X:E)_{I \otimes N^c(\psi)}$

Private capacity

We can use a quantum channel to transmit private classical data.

Roughly speaking, the private capacity is the best rate for comm classical data from Alice to Bob such that the complementary channel has vanishing info about the data. (passive eavesdropping)



R achievable if $\epsilon_n, \eta_n \to 0$ as $n \to \infty$. P(N) = sup achievable R's

Devetak 05: $P(N) = \sup_{r \to \infty} \frac{1}{r} P^{(1)}(N^{\otimes r})$

intractable

r-shot private information of N

where $P^{(1)}(N) = \max_{\psi_{XA} = \sum_x p_x |x\rangle\langle x|_X \otimes \phi_{xA}} S(X:B)_{I \otimes N(\psi)} - S(X:E)_{I \otimes N^c(\psi)}$

bruteforce, not easy

but any ensemble gives a lower bound

Static (distillation from noisy states)

$\rho^{\otimes n} \longrightarrow nE$ ebits

(diff E's for diff allowed distillation protocols)

$\rho^{\otimes n} \longrightarrow nK$ keybits

keybits: shared random bits that env has no info about

(diff K's for diff allowed distillation protocols)

$\rho^{\otimes n} \longrightarrow nR$ rbits

shared random bits

(diff R's for diff allowed distillation protocols)

Fact: $E \leq K \leq R$

under similar protocols

Dynamical (transmission via noisy channels)

$\mathcal{N}^{\otimes n} \longrightarrow nQ$ qbits

(diff Q's for diff allowed assistance, e.g., 2-way CC)

$\mathcal{N}^{\otimes n} \longrightarrow nP$ priv bits

priv bits: classical comm that env has no info about

(diff P's for diff allowed assistance, e.g., public CC)

$\mathcal{N}^{\otimes n} \longrightarrow nC$ cbits

Fact: $Q \leq P \leq C$

under similar assistance

e.g., Q=P=C=1 for noiseless qubit quantum channel, Q=P=0 for antidegradable channels

Long standing questions:

Is it the case that $\forall \rho, \quad E(\rho) = K(\rho)$?

$\forall N, \quad Q(N) = P(N)$?

HHHO 03:

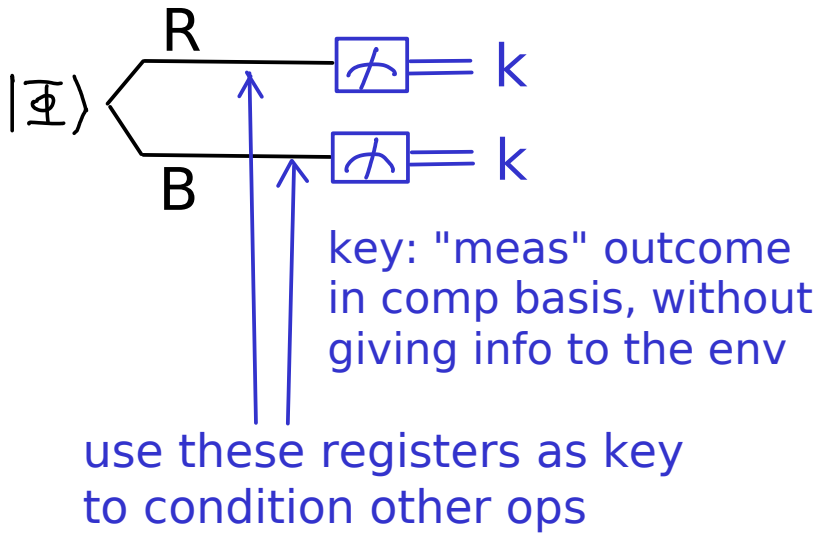
(a) for 1-way distillation $\exists \rho_{AB}$ s.t $E(\rho_{AB}) = 0$, $K(\rho_{AB}) > 0$

(b) for unassisted capacities $\exists N$ s.t $Q(N) = 0$, $P(N) > 0$

A proper explanation requires about 1-3 lectures.
Here we cover 2 crucial ideas.

Idea 1:

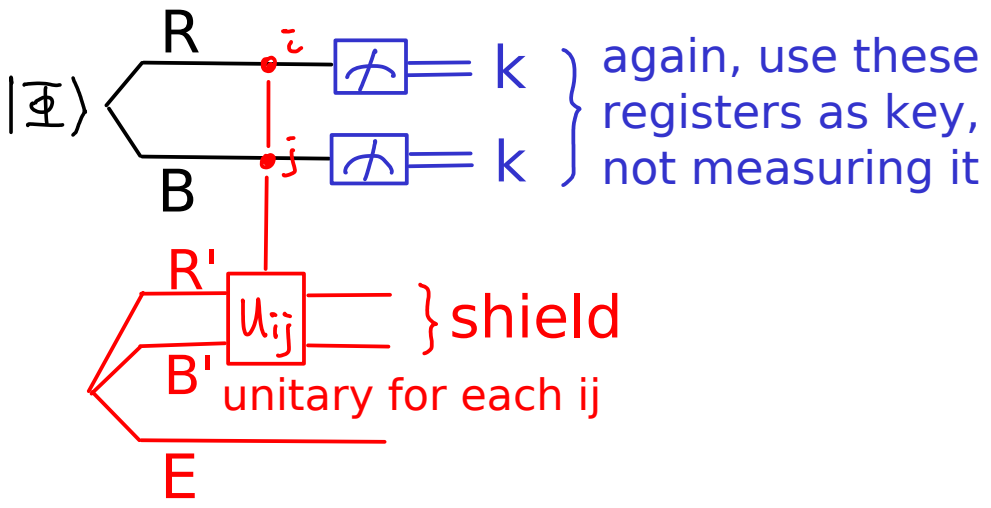
Entanglement (ebit):



key is secure because ebit is pure w/ no corr with Eve (without discarding)

but the twisting op prevents distillation of entanglement

Private state or twisted ebit (pbit)



Eve has correlation with the state but only indirectly via R'B' (shield). Controlled-Uij is called "twisting".

This corr gives no info on the key. Intuition: if Ref & Bob get together they can untwist to recover ebit.

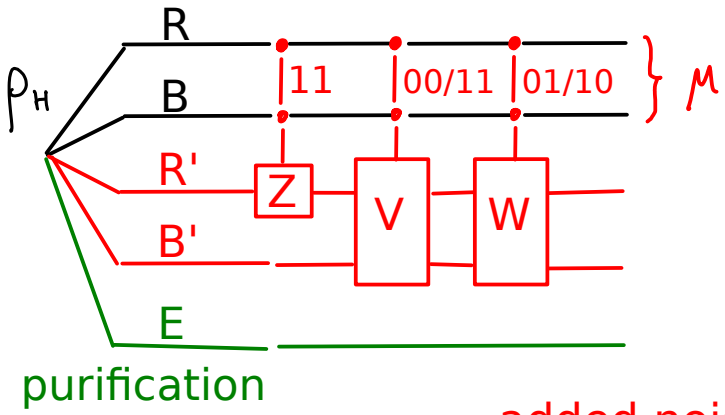
Twisting characterizes the most general noise that does not compromise security of key.

Idea 2:

e.g. (HHHO 05, 0608195)

ρ_H on RBR'B' each 1-qubit

ρ_H can be untwisted as:



added noise

$M = 0.5858\,|\Phi\rangle\langle\Phi| + 0.4142\,|\Phi_x\rangle\langle\Phi_x|$

$|\Phi\rangle$: $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ $\quad$ $|\Phi_x\rangle$: $\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$

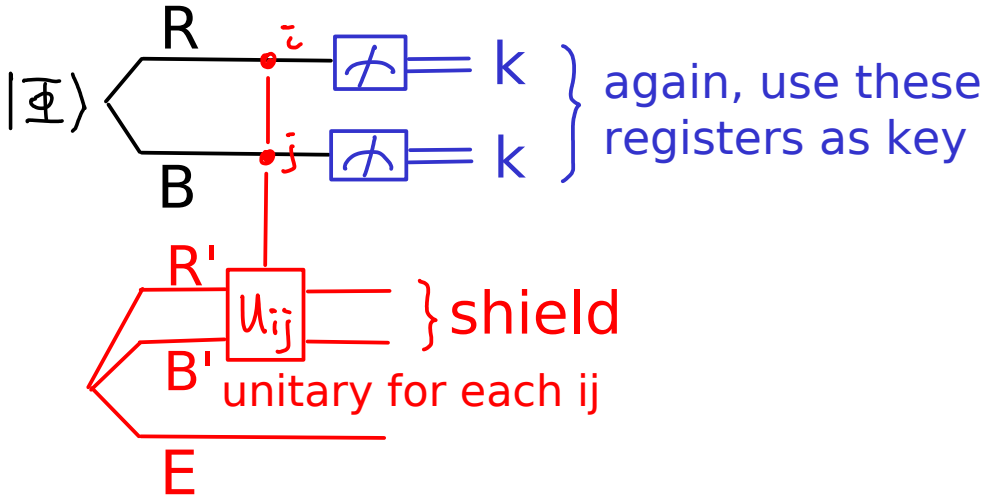
$K(\rho_H) \geq 0.0213$.

ρ_H PPT (over RR' / BB'). In fact, $PT(\rho) = \rho$.

ρ_H = Choi state of some N_H.

So, $Q(N_H) = 0$, $P(N_H) \geq 0.0213$.

Private state or twisted ebit (pbit)



A private state with perfect key has distillable entanglement.

Idea 2: choose special pbits so that a little extra noise makes the state PPT (no distillable ent), while lower bound on distillable key remains positive.

CO781 / QIC 890:

Theory of Quantum Communication

Topic 5, part 6

Consequences of the LSD theorem

- sufficient conditions for zero quantum capacity ✓
- private capacity ✓
- private capacity $\neq$ quantum capacity ✓
- symmetric-side-channel-assisted quantum capacity ←
- superactivation
- nonconvexity of quantum capacity
- rocket & half-rocket channels (probably have to omit)

Assisted quantum capacity

When defining the achievable rate for a channel, Alice and Bob can be given additional resources for the communication task.

The resulting capacity is called "assisted".

The given resources should NOT trivialized the comm task.

For quantum capacity, entanglement, or 2-way classical comm are commonly considered assistance.

Motivations:

- free resource may be easy to obtain in real life
- assisted capacities may be easier to calculate (useful bounds)
- more insight and understanding to communication problems

e.g., Q_ε, C_ε has 1-shot expression (0106052) (0106052,0912.5537)
e.g., study of C_ε lead to (q or c) reverse Shannon theorem
e.g., assistance by CC relates QECC & entanglement purification (9604024)

Symmetric-side-channel-assisted quantum capacity

In BDSW96, they found free 1-way CC from Alice to Bob does NOT increase the quantum capacity of a quantum channel.

Smith, Smolin, Winter (0607039) expanded the assistance to ANY symmetric side-channel (classical channel is a special case).

1. Resulting capacity $Q_{ss}(\mathcal{N})$ has a 1-shot expression !

2. Theorem: $\frac{1}{2} P^{(1)}(\mathcal{N}) \leq \frac{1}{2} P(\mathcal{N}) \leq Q_{ss}(\mathcal{N}) = \sup_{S:\,\text{sym channel}} Q^{(1)}(\mathcal{N} \otimes S)$

Smith-Yard-2008: $\mathcal{N} = \mathcal{N}_H$, $S = \mathcal{E}_{\frac{1}{2}}$ 50-50 erasure channel, used to transmit the shield R' to Bob

$\frac{1}{2} P^{(1)}(\mathcal{N}_H) = 0.01067 \leq Q^{(1)}(\mathcal{N}_H \otimes \mathcal{E}_{\frac{1}{2}}) \leq Q(\mathcal{N}_H \otimes \mathcal{E}_{\frac{1}{2}})$

wp 1/2, shield is sent
coh info is weighted average of outcomes

PPT $Q(\mathcal{N}_H) = 0$

antidegradable $Q(\mathcal{E}_{\frac{1}{2}}) = 0$

Superactivation of quantum capacity Smith-Yard-2008:

$$\frac{1}{2}P^{(1)}(N_H) = 0.01067 \leq Q^{(1)}(N_H \otimes E_\Sigma) \leq Q(N_H \otimes E_\Sigma)$$

PPT: $Q(N_H) = 0$ antidegradable: $Q(E_\Sigma) = 0$

Theorem $\exists\, N_1, N_2,\ Q(N_1) = Q(N_2) = 0,\ Q(N_1 \otimes N_2) = 0$

Interpretation:
There're different ways for a quantum channel to have no capacity.
N1 is PPT and cannot generate distillation entanglement.
N2 is antidegradable and cannot generate private key.

$N_1 \otimes N_2$ is neither antidegradable or PPT.

In fact, N1 gives some "key", which breaks the symmetry for N2.
(N2 is used to try to transmit the shield for the untwisting ...)

It's fitting to call superactivation 0+0 > 0 :)

CO781 / QIC 890:

Theory of Quantum Communication

Topic 5, part 6

Consequences of the LSD theorem

- sufficient conditions for zero quantum capacity ✓
- private capacity ✓
- private capacity $\neq$ quantum capacity ✓
- symmetric-side-channel-assisted quantum capacity ✓
- superactivation ✓
- nonconvexity of quantum capacity ←
- rocket & half-rocket channels (probably have to omit)

Nonconvexity & superactivation

Consider a mixture of 2 resources R1 and R2 (with prob p1, p2). Intuitively, n units of this mixture seems no better than n*p1 units of R1 + n*p2 units of R2 (in the latter, the users can exploit the knowledge of what's the resource in each use).

But strong superadditivity of channel coherent information and superactivation breaks this intuition.

Nonconvexity of quantum capacity

Consider $\mathcal{N}(\rho) = q\, N_H(\rho) \otimes |0\rangle\langle 0|_{B'} + (1-q)\, E_{\frac{1}{2}}(\rho) \otimes |1\rangle\langle 1|_{B'}$

So, one of N_H, $E_{\frac{1}{2}}$ occurs probabilistically for each use of N.

Alice has no info / control which, Bob knows afterwards.

For 2 uses of N (inputs A1 A2, outputs B1 B1' B2 B2') state $|\psi\rangle_{RA_1A_2}$

$I_c(R\rangle B_1 B_2\, B_1' B_2')_{I_R \otimes N^{\otimes 2}(\psi)}$ (B1'B2' classical)

$= q^2\, I_c(R\rangle B_1 B_2)_{I_R \otimes N_H^{\otimes 2}(\psi)}$ ← β β can be negative

$+ q(1-q)\Big[I_c(R\rangle B_1 B_2)_{I_R \otimes N_H \otimes E_{\frac{1}{2}}(\psi)}$ ← α

$\quad + I_c(R\rangle B_1 B_2)_{I_R \otimes E_{\frac{1}{2}} \otimes N_H(\psi)} \Big]$ ← ; also α

superactivation: $\exists\, |\psi\rangle_{RA_1A_2}$ making $\alpha > 0$. Some such $|\psi\rangle$ are inv under swapping A1 A2.

$+ (1-q)^2\, I_c(R\rangle B_1 B_2)_{I_R \otimes E_{\frac{1}{2}}^{\otimes 2}(\psi)}$ 0 by symmetry of $E_{\frac{1}{2}}$

$= q^2 \beta + q(1-q)\, 2\alpha > 0$ since α, β fixed, choose q small.

Nonconvexity of quantum capacity

Consider $\mathcal{N}(\rho) = q\, \mathcal{N}_H(\rho) \otimes |0\rangle\langle 0|_{B'} + (1-q)\, \mathcal{E}_{\frac{1}{2}}(\rho) \otimes |1\rangle\langle 1|_{B'}$

For 2 uses of $\mathcal{N}$ (inputs A1 A2, outputs B1 B1' B2 B2') $\exists\, |\psi\rangle_{RA_1A_2}$

$$I_c(R\rangle B_1 B_2 B_1' B_2')_{I_R \otimes \mathcal{N}^{\otimes 2}(\psi)} > 0$$

$$\therefore\ Q(\mathcal{N}) \geq Q^{(2)}(\mathcal{N}) > 0$$

But $\mathcal{N} = q\, \mathcal{N}_H + (1-q)\, \mathcal{N}_2$, with $Q(\mathcal{N}_H) = Q(\mathcal{N}_2) = 0$.

So, Q is not convex in general.

Furthermore, the above gives an example for $Q^{(1)}(\mathcal{N}) = 0$, $Q^{(2)}(\mathcal{N}) > 0$. (exercise)

CO781 / QIC 890:

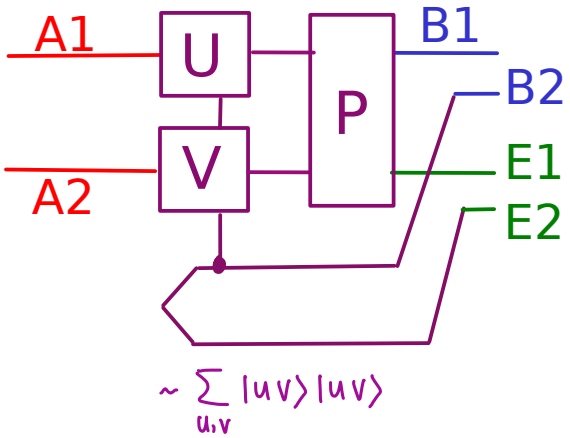
Theory of Quantum Communication

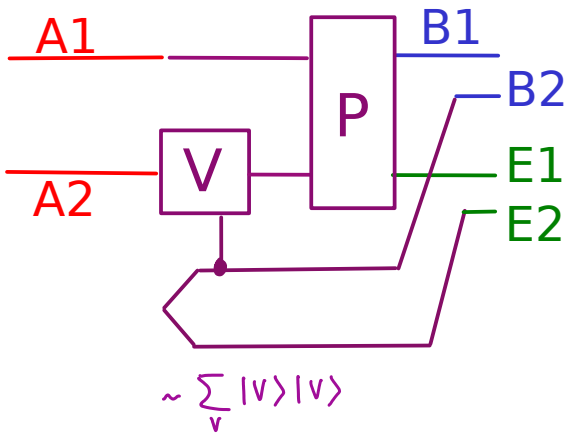
Topic 5, part 6

Consequences of the LSD theorem

- sufficient conditions for zero quantum capacity ✓
- private capacity ✓
- private capacity $\neq$ quantum capacity ✓
- symmetric-side-channel-assisted quantum capacity ✓
- superactivation ✓
- nonconvexity of quantum capacity ✓
- rocket & half-rocket channels (probably have to omit) ←

Rocket channel $\mathcal{R}_d$ (0904.4050) Half-rocket channel $\mathcal{H}_d$ (1312.4989)





A1, A2, B1, E1: d-dim, d large

$P|a\rangle|b\rangle = \omega^{ab}|a\rangle|b\rangle$, primitive dth root of unity

Uniform distribution over {U}: a 2-design on d-dim (e.g., Clifford)
same for {V}. B2, E2: classical info to Bob, Eve which U,V occur.

$2 \geq C(\mathcal{R}_d) \geq P(\mathcal{R}_d) \geq Q(\mathcal{R}_d)$ $\qquad$ $C(\mathcal{H}_d) \geq P(\mathcal{H}_d) = \log d$

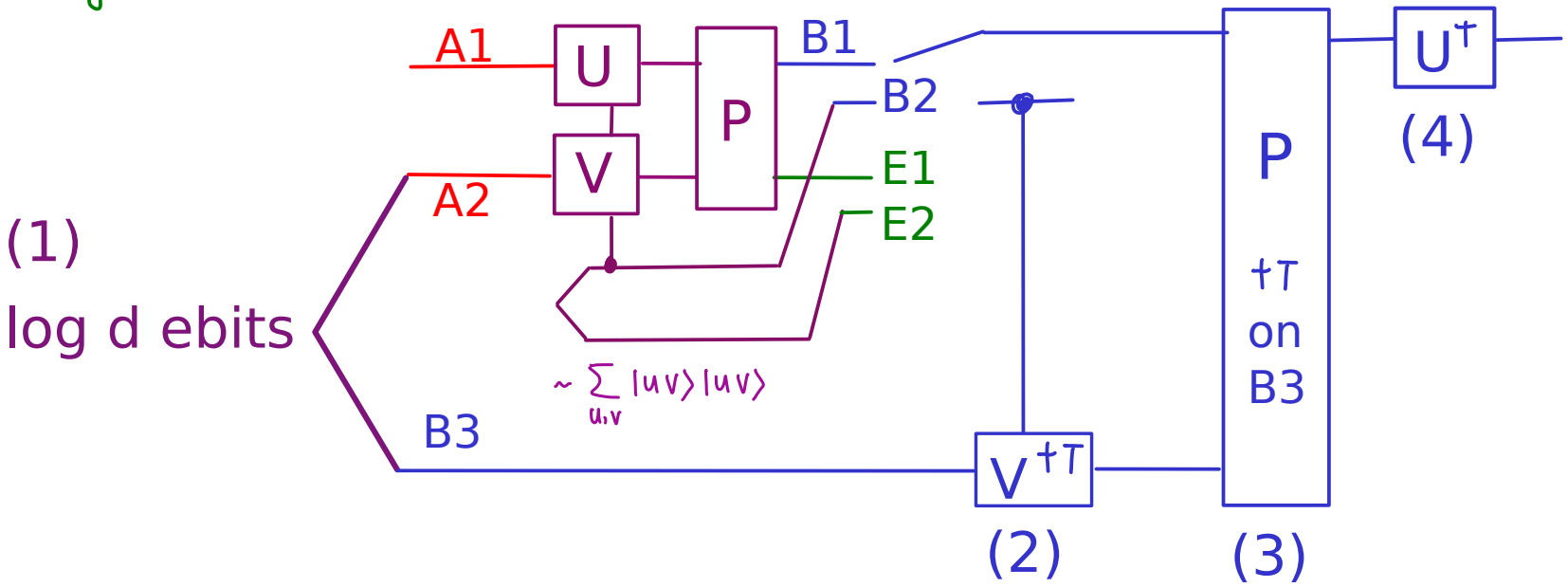
$Q^{(1)}(\mathcal{R}_d \otimes \mathcal{E}_{\frac{1}{2}}^d) \geq \frac{1}{2}\log d$ $\qquad$ $Q(\mathcal{H}_d) \leq 1$

$Q_E, Q_B, Q_{\leftrightarrow} \approx c \cdot \log d$

So, nonadditivity and P-Q can be quantitatively large.

Rocket channel $\mathcal{R}_d$ (0904.4050)

$Q_E \geq \log d$:



(1) Alice uses her half of the ebits as input to A2

(2) Bob undoes V (learnt from B2) by operating on B3 (transpose trick)
"retrocorrection"

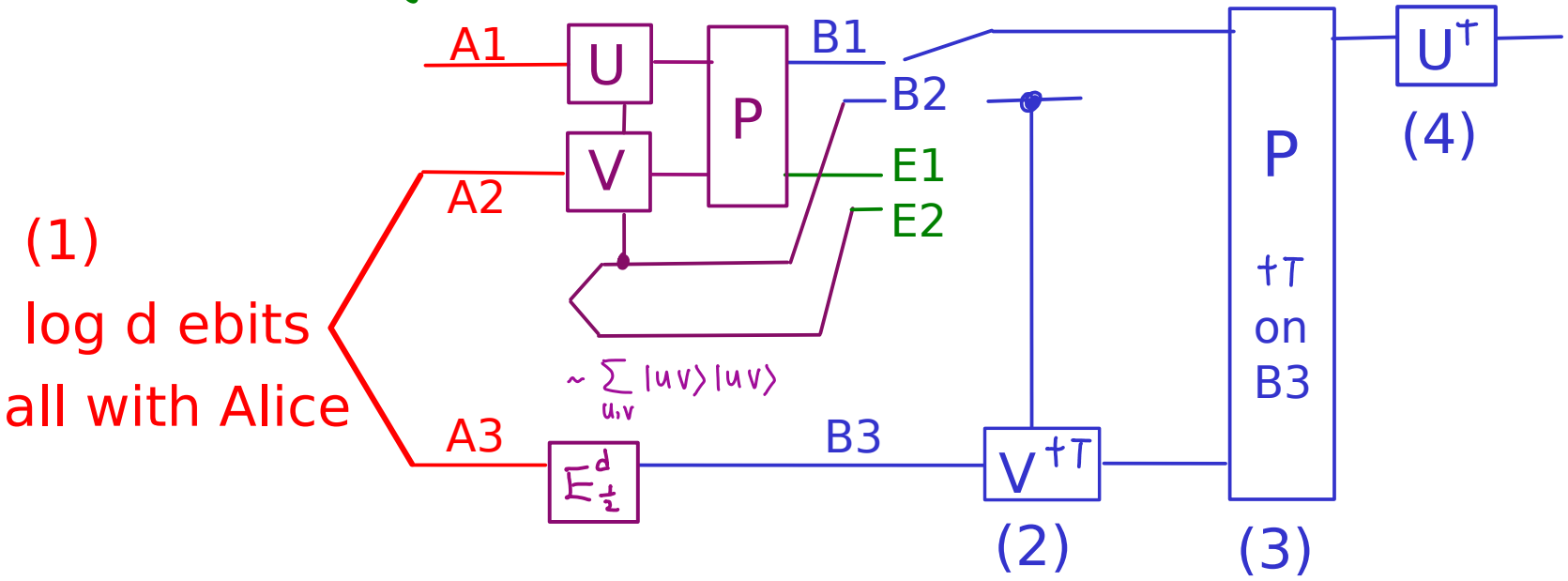
(3) Bob undoes P by operating on B1 B3 (transpose trick)

(4) Bob undoes U directly on B1

Overall: A1 to B1 noiseless transmission, so, $Q_E \geq \log d$

Rocket channel $\mathcal{R}_d$ (0904.4050)

$Q^{(1)}(\mathcal{R}_d \otimes \mathcal{E}_{\frac{1}{2}}^d) \geq \frac{1}{2}\log d$



(1) Alice locally prepares ebits on A2 A3

She sends A3 to Bob using $\mathcal{E}_{\frac{1}{2}}^d$.

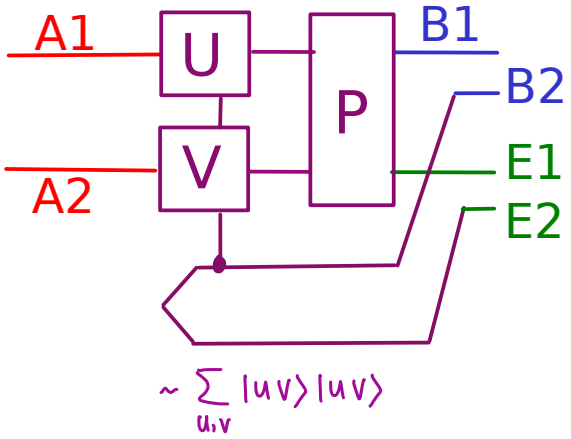
If B3 erased, Bob does nothing.

Else, Bob proceeds as in ent assisted protocol steps (2)-(4).

Overall: wp 1/2, A1 to B1 noiseless transmission, wp 1/2, sym

$\therefore\ Q^{(1)}(\mathcal{R}_d \otimes \mathcal{E}_{\frac{1}{2}}^d) \geq \frac{1}{2}\log d$

Rocket channel $\mathcal{R}_d$ (0904.4050)



$2 \geq C(\mathcal{R}_d) \geq P(\mathcal{R}_d) \geq Q(\mathcal{R}_d)$

Intuition: P heavily entangling, unless inputs to P are special.
But U, V randomize enough so hardly anything special reaches P.

Proof is not too hard, an integral with $\int du \; u \otimes u \cdots u^\dagger \otimes u^\dagger \cdots$.
Similarly with V.

For detail, and other claims concerning both channels, see refs.