Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 20 (2017)

Jon Yard

QNC 3126

jyard@uwaterloo.ca

http://math.uwaterloo.ca/~jyard/qic710

Entanglement

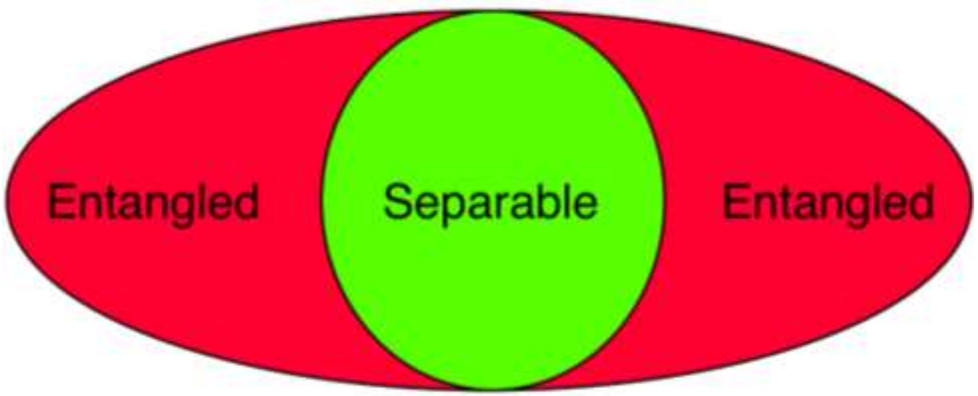
Separable states

A density matrix ρ^{AB} is **separable** if there exist probabilities $p(x)$ and density matrices ρ_x^A, ρ_x^B such that

$$\rho^{AB} = \sum_x p(x) \rho_x^A \otimes \rho_x^B \, .$$

If ρ^{AB} is not separable, then it is called **entangled**.

Note: if ρ^{AB} is separable, exists a decomposition with $\rho_x^A = |\psi_x\rangle\langle\psi_x|^A$, $\rho_x^B = |\psi_x\rangle\langle\psi_x|^B$.



Operational meaning: separable states can be prepared starting with only classical correlations.

Separable?

Theorem [Horodeckis '96]: ρ^{AB} is entangled iff there exists a positive (but not completely positive) linear map $\mathcal{A}$ on $\mathbb{C}^{d\times d}$ such that $(\mathcal{A} \otimes id)(\rho^{AB})$ is not positive semidefinite.

We have already seen examples of positive-but-not-completely positive maps, such as…

Proof (Easy direction – only if): Let $\mathcal{A}$ be any positive map. If

$$\rho^{AB} = \sum_x p(x)\rho_x^A \otimes \rho_x^B$$

is a separable density matrix, then

$$\sum_x p(x)\mathcal{A}(\rho_x^A) \otimes \rho_x^B$$

is still positive semidefinite. Interpretation: every entangled state is broken by some non-physical positive map.

Separable?

Example: The **Werner state**

$$\rho^{AB} = (1-p)\frac{(|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+|)}{3} + p|\psi^-\rangle\langle\psi^-|$$

has a Positive Partial Transpose (PPT) $(T \otimes id)(\rho^{AB}) \geq 0$ iff $p \leq \frac{1}{2}$, where T is the transpose map $T(M) = M^T$.

It turns out that the PPT test is sufficient to decide entanglement, i.e. the Werner state is entangled iff $p > 1/2$.

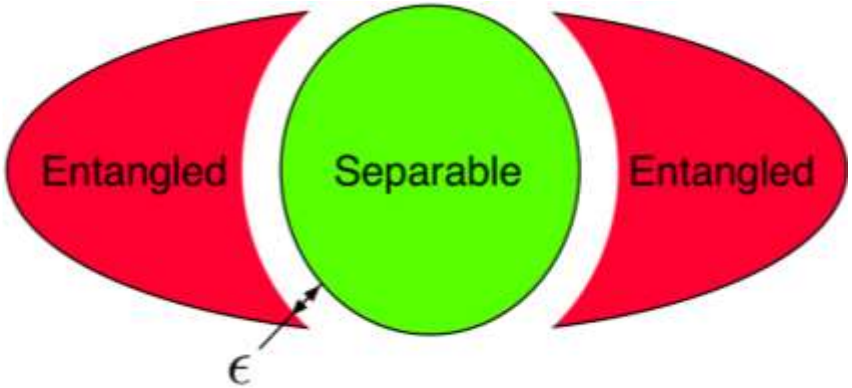
In fact, the PPT test is sufficient to decide whether an arbitrary 2×2 or 2×3 density matrix is entangled.

Separable?

Fundamental problem: Given a description of ρ^{AB}, (i.e. as a $d^2 \times d^2$ matrix), determine whether it is separable or entangled.

Bad news: This problem is NP-hard [Gurvits ’02].

Good news: There exists [BCY’12] an efficient (quasipolynomial-time $\exp(\epsilon^{-2} O(\log(d)^2))$ algorithm for deciding this given a promise that ρ^{AB} is either separable or a constant distance (in $\| \ \|_2$-norm) from separable.



$$\|\rho - \sigma\|_2 = \sqrt{\mathrm{Tr}(\rho - \sigma)^2}$$

How entangled?

(brief)

Entanglement measures

An **entanglement measure** is a function $E(\rho^{AB})$ on bipartite density matrices ρ^{AB} that quantifies, in one way or another, the *amount* of bipartite entanglement in ρ^{AB}.

Last time, we saw two examples for pure states:
- Schmidt rank
- Entanglement entropy

Some nice properties for such a measure to satisfy:
1) Invariant under local unitaries
2) Non-increasing under Local Operations and Classical Communication (LOCC)
3) Monogamous
4) Additive
5) Faithful

Monogamy of entanglement

Many nice entanglement measures are **monogamous**:
The more A is entangled with B, the less it can be entangled with C.

$$E(\rho^{AB_1}) + E(\rho^{AB_2}) \leq E(\rho^{AB_1B_2}).$$

Implies that quantum correlations cannot be shared.
Application of this idea: Quantum Key Distribution.

Extreme example: $\rho^{AB_1B_2} = |\phi\rangle\langle\phi|^{AB_1} \otimes \rho^{B_2}$,
where $|\phi\rangle = |00\rangle + |11\rangle$ is a Bell state

$$1 + 0 \leq 1$$

Entanglement of formation

How much entanglement does it take to make ρ^{AB} using LOCC?

Entanglement of formation: How much entanglement does it take, on average, to create a single copy of ρ^{AB}?

$$E_F(\rho^{AB}) = \min_{p(x),|\psi_x\rangle^{AB}} \left\{ \sum_x p(x) S(\psi_x^A) : \sum_x p(x) |\psi_x\rangle\langle\psi_x|^{AB} = \rho^{AB} \right\}$$

Faithful, not monogamous, not additive…

Entanglement cost: how much entanglement does it take, per copy, to create many copies of ρ^{AB}?

$$E_C(\rho^{AB}) = \lim_{n\to\infty} \frac{1}{n} E_F\left(\rho_{AB}^{\otimes n}\right) \leq E_F(\rho^{AB})$$

Shor '01, Hastings '08: Can have $E_C < E_F$ (explicit example?).

Faithful, not monogamous. Additive?

Distillable entanglement

How much entanglement can be extracted from ρ^{AB}, in the limit of many copies?does it take, on average, to create a single copy of ρ^{AB}?

$E_D(\rho^{AB})$ = the largest rate R such that, by local operations and classical communication, Alice and Bob can produce nR Bell states (ebits)

$$(|0\rangle|0\rangle + |1\rangle|1\rangle)^{nR} = \sum_{x\in\{0,1\}^{nR}} |x\rangle|x\rangle$$

from $\rho_{AB}^{\otimes n}$, with vanishing errors in the limit as $n \to \infty$.

Bound entanglement

There exist “bound entangled states” with $E_D < E_F$
[Horodeckis ’97]
Analogous to bound energy in thermodynamics.

$$\frac{1}{8a+1}\begin{bmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{bmatrix} \qquad 0 < a < 1$$

Has $E_D = 0$ since it is PPT. But it is entangled.
So E_D not faithful.
Big open question: do there exist NPT bound entangled states?
Would imply E_D not additive.

Squashed entanglement

$$E_{sq}(\rho^{AB}) = \inf_{\rho^{ABC}} I(A;B|C)$$

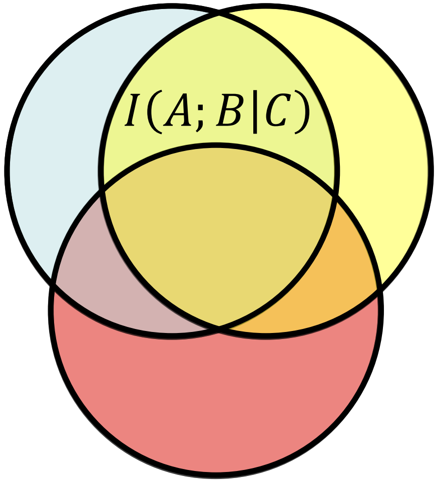
Conditional mutual information

$$I(A;B|C) = H(AC) + H(BC) - H(C) - H(ABC)$$

Satisfies strong subadditivity $I(A;B|C) \geq 0$ (not easy proof)

Generalizes mutual information

$$I(A;B) = S(A) + S(B) - S(AB)$$

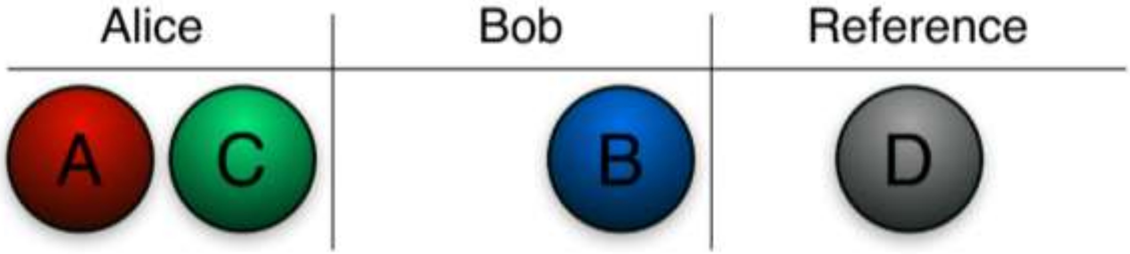


It is monogamous, additive and faithful!

Easy to show that $E_{sq} = 0$ on separable states.

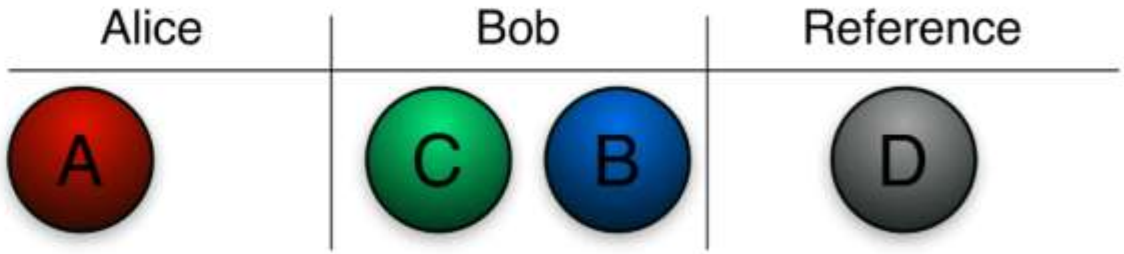
We don't know how to compute it…

State redistribution problem



- Multi-part pure state $|\psi\rangle^{ABCD}$
- Alice wants to give *C* to Bob
- Many independent copies
- Satisfied with approximate transfer
- Alice may send Bob qubits
- Alice and Bob can use preexisting ebits: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- How much does this cost?

State redistribution problem

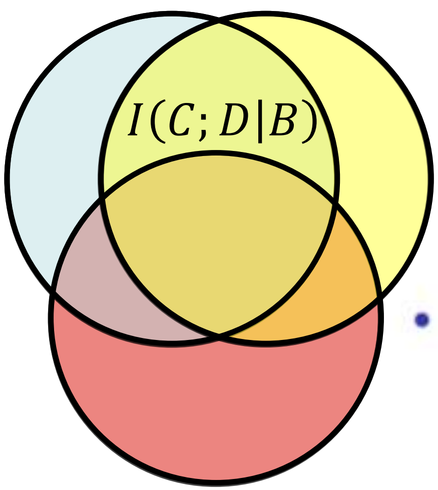


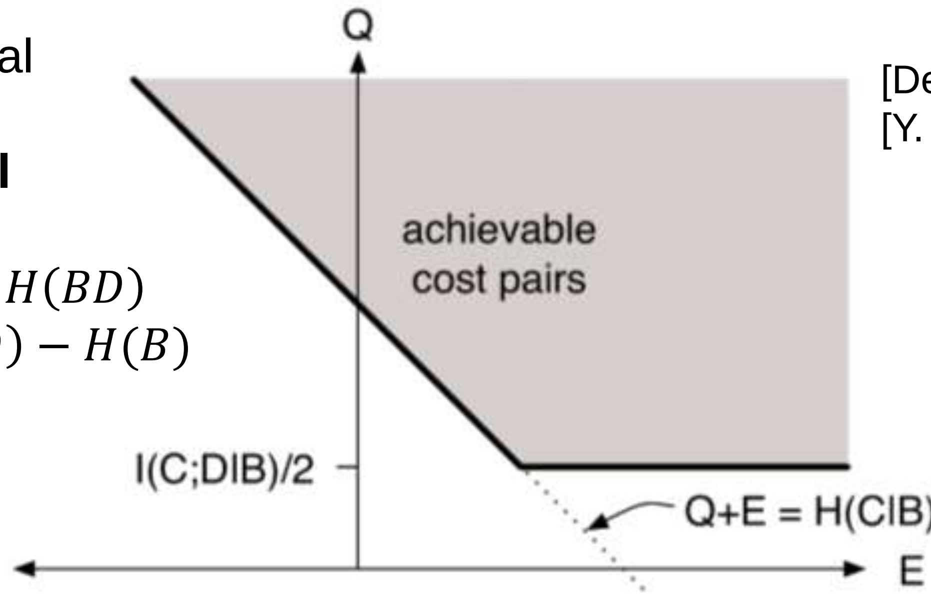
- Multi-part pure state $|\psi\rangle^{ABCD}$
- Alice wants to give C to Bob
- Many independent copies
- Satisfied with approximate transfer
- Alice may send Bob qubits
- Alice and Bob can use preexisting ebits: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- How much does this cost?

Cost of state redistribution

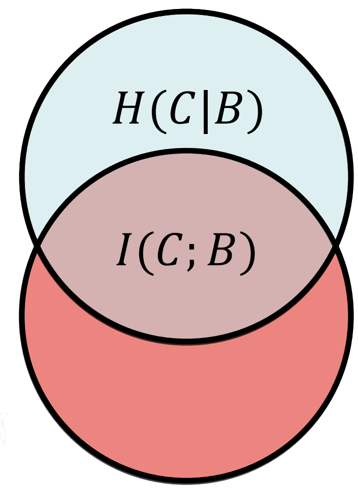
First known operational interpretation of **quantum conditional mutual information**

$$I(C;D|B) = H(BC) + H(BD) - H(BCD) - H(B)$$





[Devetak & Y. – PRL'08]
[Y. & Devetak – IEEE TIT '09]



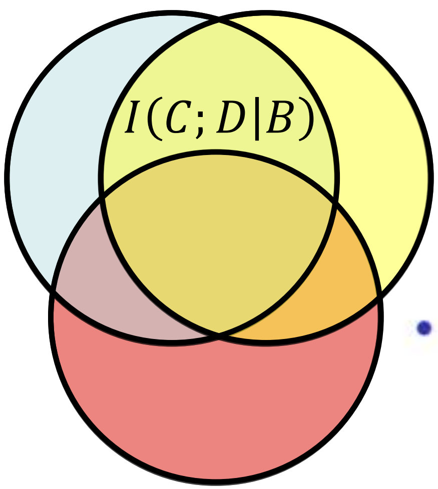
- (Q, E) achievable iff $Q \geq \frac{1}{2}I(C;D|B)$ and $Q + E \geq H(C|B)$

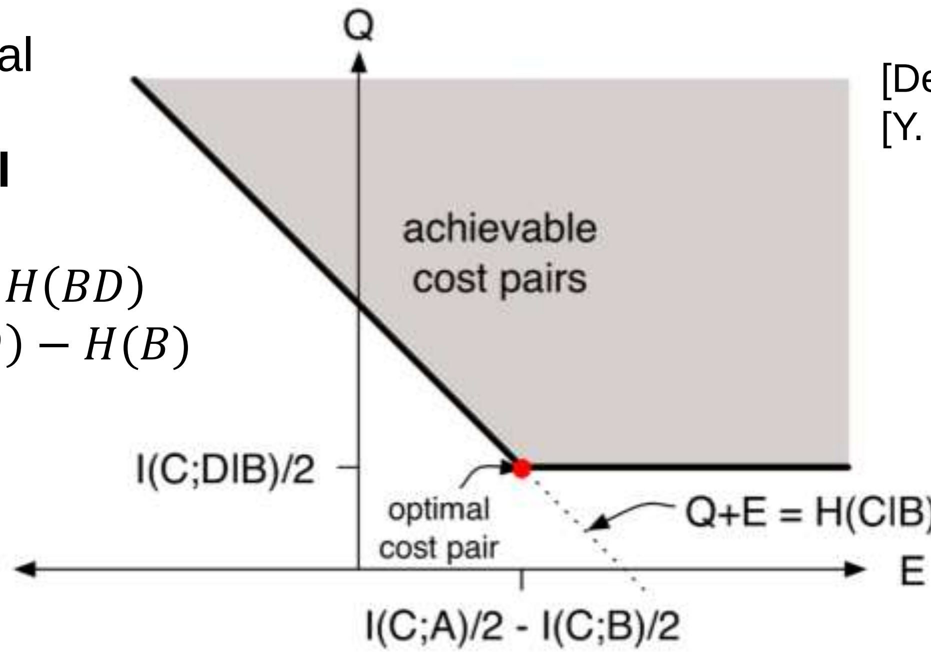
$Q^* = \frac{1}{2}I(C;D|B)$ and $E^* = \frac{1}{2}I(C;A) - \frac{1}{2}I(C;B)$

Cost of state redistribution

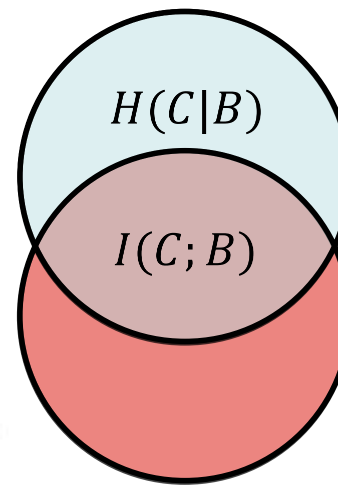
First known operational interpretation of **quantum conditional mutual information**

$$I(C;D|B) = H(BC) + H(BD) - H(BCD) - H(B)$$





[Devetak & Y. – PRL'08]
[Y. & Devetak – IEEE TIT '09]



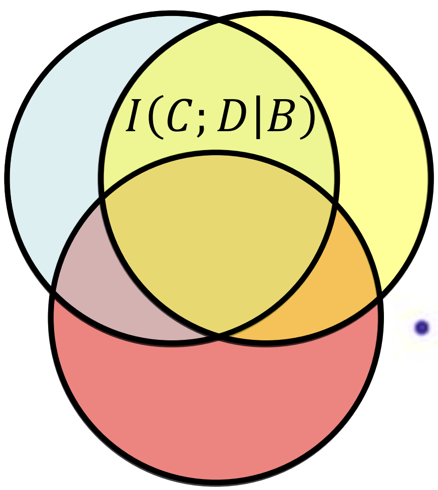
- (Q, E) achievable iff $Q \geq \frac{1}{2} I(C;D|B)$ and $Q + E \geq H(C|B)$

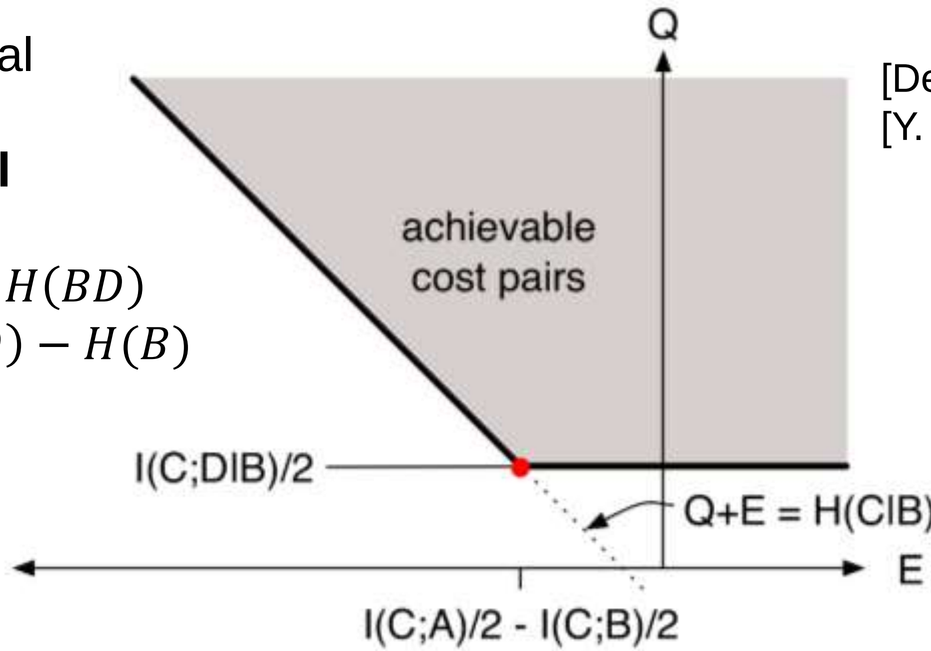
$$Q^* = \frac{1}{2} I(C;D|B) \text{ and } E^* = \frac{1}{2} I(C;A) - \frac{1}{2} I(C;B)$$

Cost of state redistribution

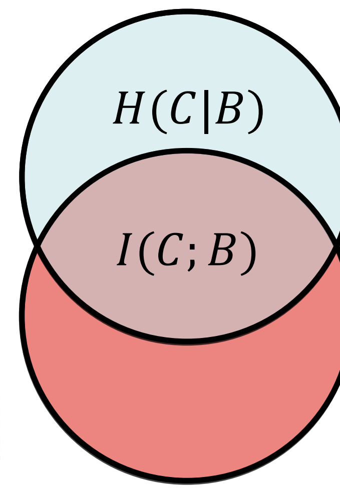
First known operational interpretation of **quantum conditional mutual information**

$$I(C;D|B) = H(BC) + H(BD) - H(BCD) - H(B)$$





[Devetak & Y. – PRL'08]
[Y. & Devetak – IEEE TIT '09]



- (Q, E) achievable iff $Q \geq \frac{1}{2} I(C;D|B)$ and $Q + E \geq H(C|B)$

$$Q^* = \frac{1}{2} I(C;D|B) \text{ and } E^* = \frac{1}{2} I(C;A) - \frac{1}{2} I(C;B)$$

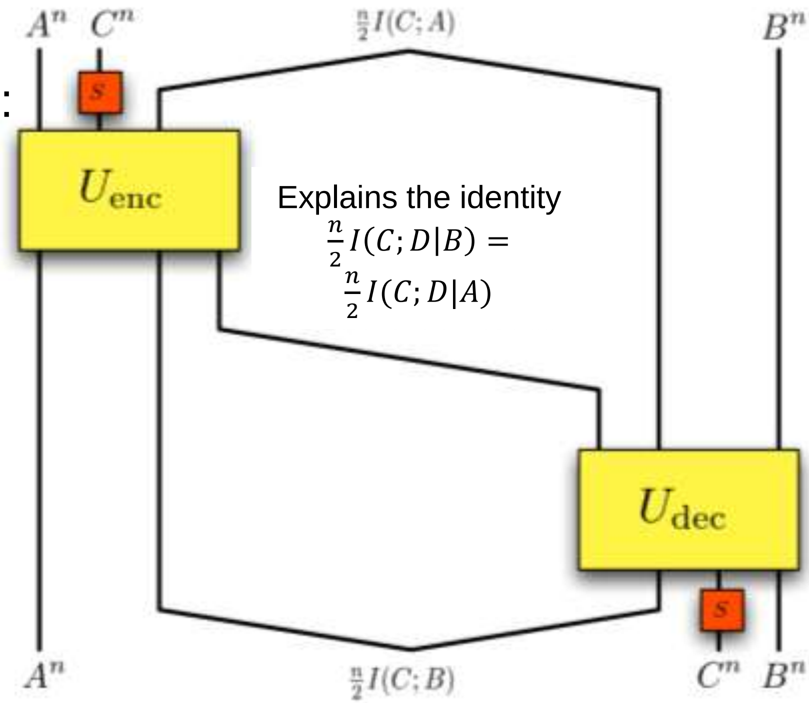
Optimal protocol for state redistribution

Simple proof: decoupling via random unitaries:
[Oppenheim – arXiv:0805.1065]
achieves different 1-shot quantities.

Applications:
- Proof that E_{sq} is faithful.
- Proof of existence of quasipolynomial-time algorithm for deciding separability.
- Communication complexity

Let's see how to prove a special case:

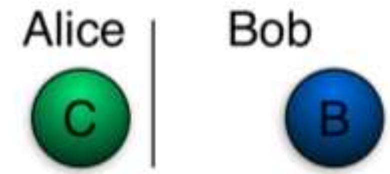
To emphasize the role of D as a reference system, relabel $D \rightarrow R$



Explains the identity
$\frac{n}{2} I(C;D|B) =$
$\frac{n}{2} I(C;D|A)$

State merging

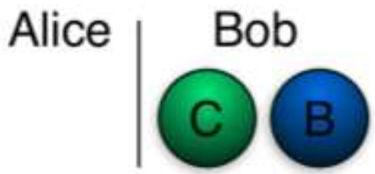
- If only Bob has side information



$$Q^* = \frac{1}{2} I(C; R), \quad E^* = -\frac{1}{2} I(C; B)$$

- Alice projects C onto typical subspace
- then does random unitary $U^{C \to C_1 C_2}$
- C_1 maximally mixed, decoupled from R
- C_1 therefore maximally entangled with $C_2 B$
- notation: $C_1 \perp R$, $C_1 == C_2 B$
- Unitarity $\Rightarrow$ Bob can extract entanglement and reconstruct CB
- Original motivation: distilling entanglement

State merging

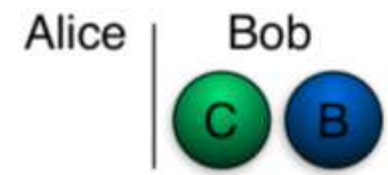


- If only Bob has side information

$$Q^* = \tfrac{1}{2} I(C;R), \quad E^* = -\tfrac{1}{2} I(C;B)$$

- Alice projects C onto typical subspace
- then does random unitary $U^{C \to C_1 C_2}$
- C_1 maximally mixed, decoupled from R
- C_1 therefore maximally entangled with $C_2 B$
- notation: $C_1 \perp R$, $C_1 == C_2 B$
- Unitarity $\Rightarrow$ Bob can extract entanglement and reconstruct CB
- Original motivation: distilling entanglement

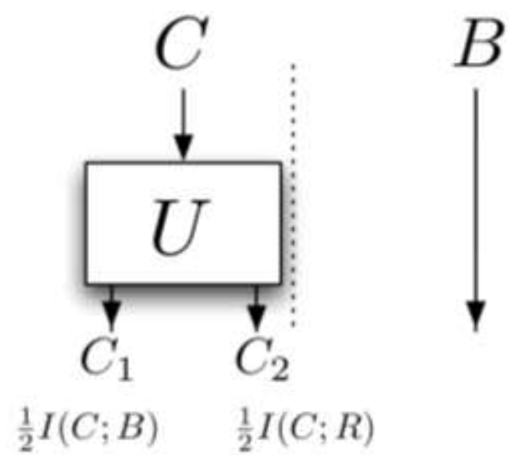
State merging



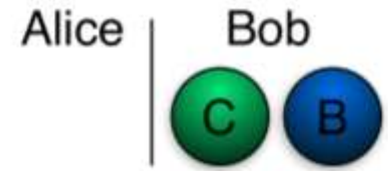
- If only Bob has side information

$$Q^* = \frac{1}{2} I(C;R), \quad E^* = -\frac{1}{2} I(C;B)$$

- Alice projects C onto typical subspace
- then does random unitary $U^{C \to C_1 C_2}$
- C_1 maximally mixed, decoupled from R
- C_1 therefore maximally entangled with $C_2 B$
- notation: $C_1 \perp R$, $C_1 == C_2 B$
- Unitarity $\Rightarrow$ Bob can extract entanglement and reconstruct CB
- Original motivation: distilling entanglement

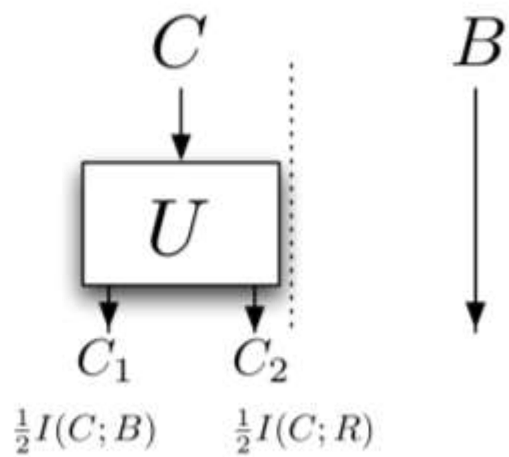


State merging



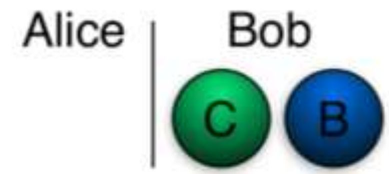
- If only Bob has side information

$$Q^* = \frac{1}{2} I(C;R), \quad E^* = -\frac{1}{2} I(C;B)$$



- Alice projects C onto typical subspace
- then does random unitary $U^{C \to C_1 C_2}$
- C_1 maximally mixed, decoupled from R
- C_1 therefore maximally entangled with $C_2 B$
- notation: $C_1 \perp R$, $C_1 == C_2 B$
- Unitarity $\Rightarrow$ Bob can extract entanglement and reconstruct CB
- Original motivation: distilling entanglement

State merging



- If only Bob has side information

$$Q^* = \frac{1}{2} I(C;R), \quad E^* = -\frac{1}{2} I(C;B)$$

- Alice projects C onto typical subspace
- then does random unitary $U^{C \to C_1 C_2}$
- C_1 maximally mixed, decoupled from R
- C_1 therefore maximally entangled with $C_2 B$
- notation: $C_1 \perp R$, $C_1 == C_2 B$
- Unitarity $\Rightarrow$ Bob can extract entanglement and reconstruct CB
- Original motivation: distilling entanglement