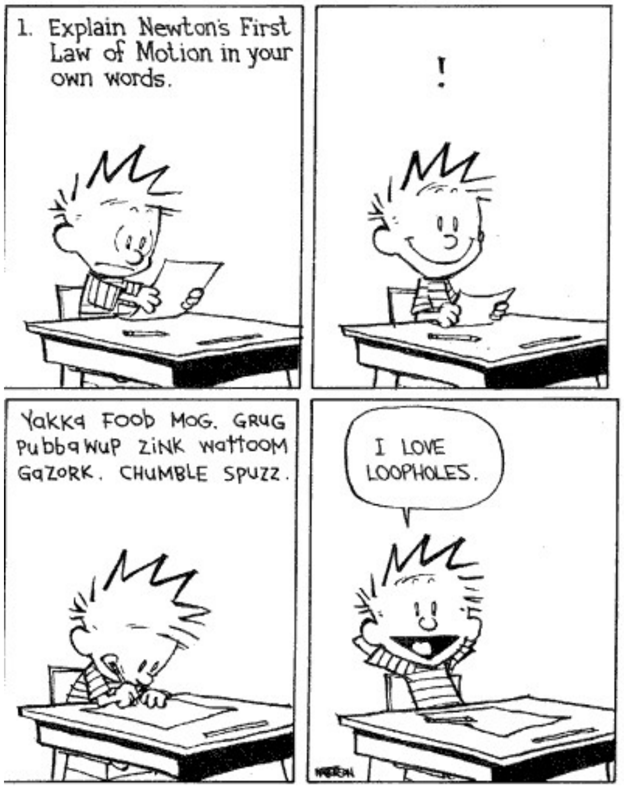
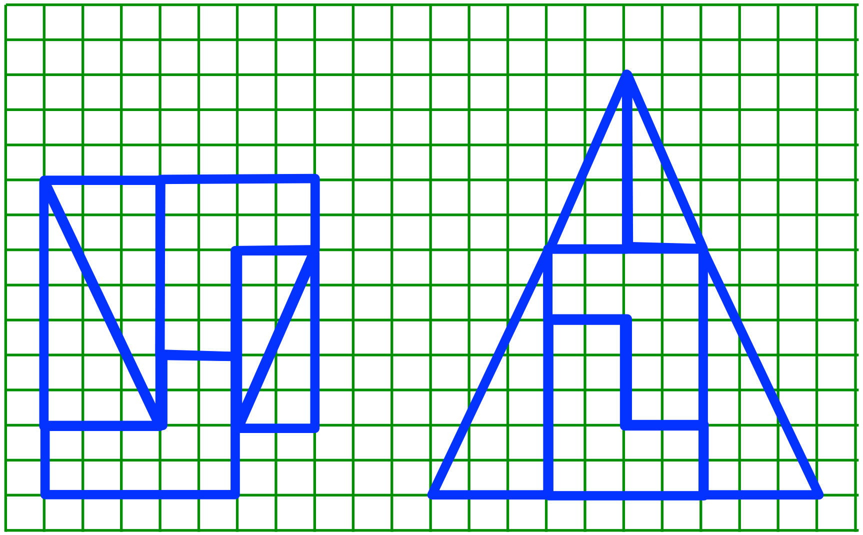
A Short Tour of the Laws of Entanglement (And How to Evade Them)





59 units

60 units

Patrick Hayden
Stanford University

Simons Institute
UC Berkeley 2014

From the *Universal Compendium of Rock Solid Physico-Informational Facts*

- §1.0.1.
  - *Entanglement cannot be created without interaction*
  - Evasion strategy: embezzlement
  - Applications
- §1.0.2.
  - *Entanglement is monogamous*
  - One mathematical formulation
  - No applications

The Great Laws: Part 1

§1.0.0. Thou shalt not create *correlation* without a commensurate investment of interaction.

$$\sigma_{AB}$$

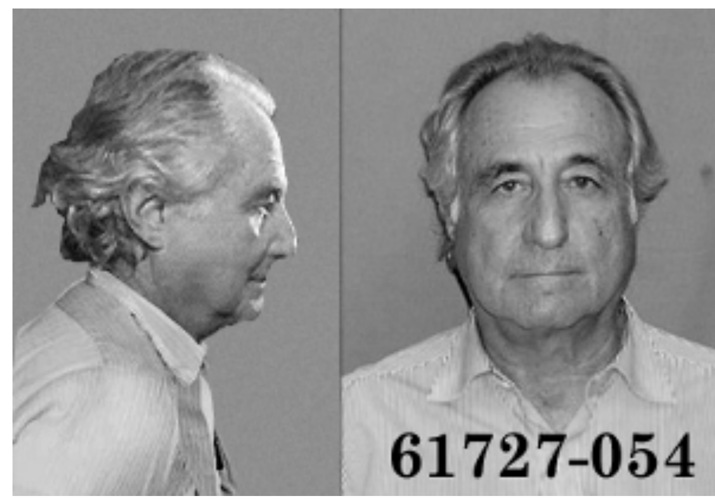
$$\uparrow \; \mathcal{N}_A \otimes \mathcal{M}_B$$

$$\rho_{AB}$$

$$I(A;B)_\sigma \leq I(A;B)_\rho$$

Embezzlement

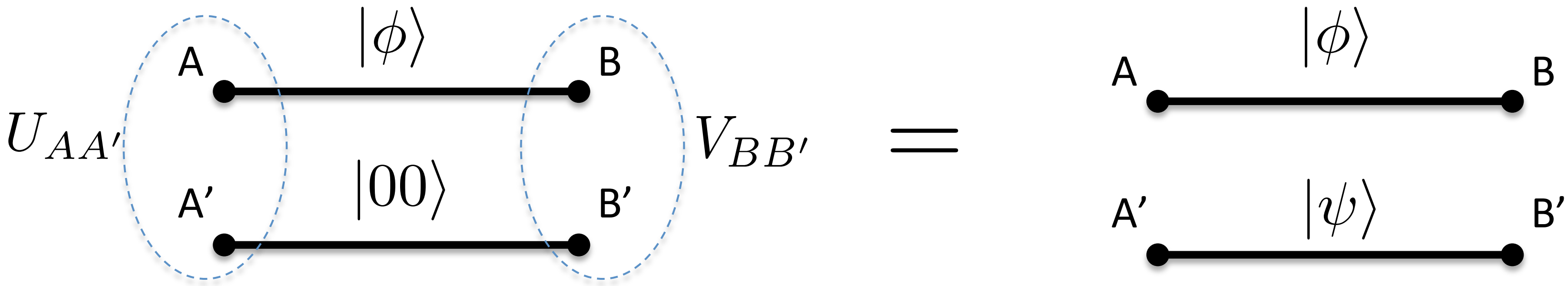
Theft from a reservoir of wealth sufficiently large that the crime is not noticed.



(Until it is.)

Embezzling entanglement

The perfect crime: $|\phi\rangle_{AB}|00\rangle_{A'B'} \xrightarrow{U_{AA'}\otimes U_{BB'}} |\phi\rangle_{AB}|\psi\rangle_{A'B'}$



Extract the entangled state ψ from the entanglement bank ϕ without leaving behind a trace in the bank.

Trivial solution: the infinite reservoir

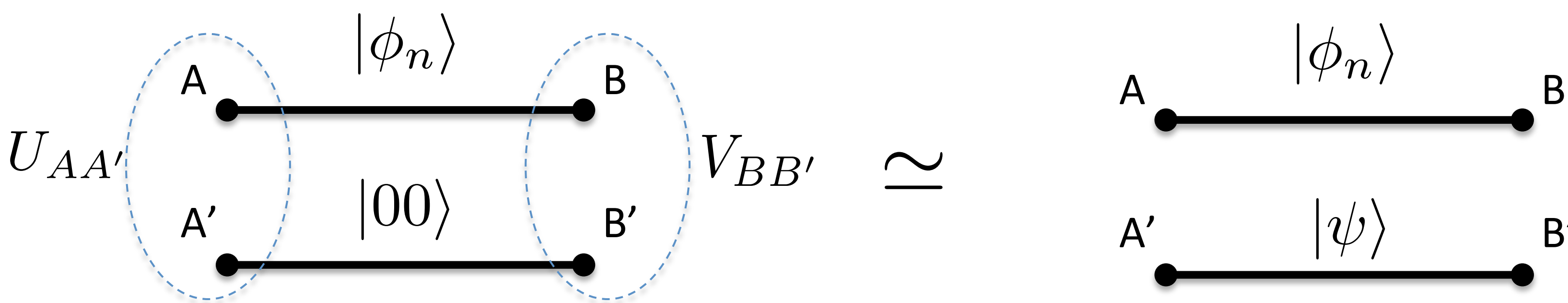
$$|\phi\rangle_{AB} = (|\psi\rangle)^{\otimes\infty}$$

Drawbacks:

* Not even the Federal Reserve has an infinite amount of entanglement
* Must keep a separate account for every possible Ψ

Embezzling states

$$|\phi_n\rangle = \frac{1}{\sqrt{C_n}} \sum_{j=1}^{n} \frac{1}{\sqrt{j}} |j\rangle_A |j\rangle_B$$



Theorem: For every pure state $|\psi\rangle_{A'B'}$ of Schmidt rank m, there exist unitary transformations $U_{AA'}$ and $V_{BB'}$ such that

$$_{AB}\langle\phi_n|_{A'B'}\langle\psi|U_{AA'} \otimes V_{BB'}|\phi_n\rangle_{AB}|00\rangle_{A'B'} \geq 1 - \frac{\log m}{\log n}$$

#qubits(ϕ_n) = O(#qubits(ψ)/ε) for inner product 1-ε

[H-van Dam 2003]

Embezzling Bell pairs

$$|\phi_n\rangle = \frac{1}{\sqrt{C_n}} \sum_{j=1}^{n} \frac{1}{\sqrt{j}} |j\rangle_A |j\rangle_B \qquad |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Schmidt coefficients:

$|\phi_n\rangle$:
$$\frac{1}{\sqrt{C_n}} \times \left\{ \frac{1}{\sqrt{1}} \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{3}} \quad \cdots \quad \frac{1}{\sqrt{n}} \right\}$$

$|\phi_n\rangle|\psi\rangle$:
$$\frac{1}{\sqrt{C_n}} \times \left\{ \begin{matrix} \frac{1}{\sqrt{1\cdot 2}} & \frac{1}{\sqrt{2\cdot 2}} & \frac{1}{\sqrt{3\cdot 2}} & \cdots & \frac{1}{\sqrt{n\cdot 2}} \\ \frac{1}{\sqrt{1\cdot 2}} & \frac{1}{\sqrt{2\cdot 2}} & \frac{1}{\sqrt{3\cdot 2}} & \cdots & \frac{1}{\sqrt{n\cdot 2}} \end{matrix} \right\}$$

Embezzling Bell pairs

$$|\phi_n\rangle = \frac{1}{\sqrt{C_n}} \sum_{j=1}^{n} \frac{1}{\sqrt{j}} |j\rangle_A |j\rangle_B \qquad |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Schmidt coefficients:

$|\phi_n\rangle$: $$\frac{1}{\sqrt{C_n}} \times \left\{ \frac{1}{\sqrt{1}} \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{3}} \quad \frac{1}{\sqrt{4}} \quad \cdots \quad \frac{1}{\sqrt{n-1}} \quad \frac{1}{\sqrt{n}} \right\}$$

$|\phi_n\rangle|\psi\rangle$: $$\frac{1}{\sqrt{C_n}} \times \left\{ \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{4}} \quad \frac{1}{\sqrt{4}} \quad \cdots \quad \frac{1}{\sqrt{n}} \quad \frac{1}{\sqrt{n}} \quad \cdots \right\}$$

$$\text{Dot product} \geq \frac{1}{C_n} \times \left(\frac{1}{2} + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \cdots + \frac{1}{n} + \frac{1}{n} \right)$$

$$\geq \frac{\log(n/2)}{\log(n)} = 1 - \frac{\log 2}{\log n}$$

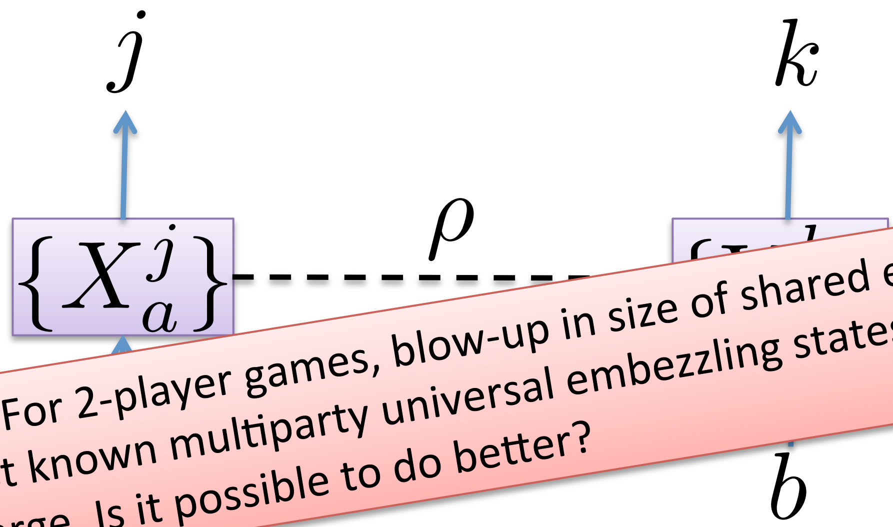
Further developments

and much earlier

- [Araki ~1967]:
  - Exploited (exact) embezzlement in the classification of von Neumann algebras
- [Leung+Toner+Watrous 2013*]:
  - Embezzlement for multiparty states
- [Dinur+Steurer+Vidick 2013]:
  - Robust embezzlement
    - Alice and Bob don't quite agree on the target state ψ
  - a.k.a. *Quantum correlated sampling lemma*
  - Key step in proving parallel repetition for projection games
- [Leung+Wang 2013]:
  - Characteristics of universal embezzling states
- [Haagerup+Scholz+Werner 2014?]:
  - Universal embezzling algebra
    - Uniquenessness of universal embezzling "eigenvalue" scaling
    - *Every* state in free quantum field theory is embezzling!

* Really 2008, but who can be bothered to submit to journals in a timely fashion these days?

Application: Multiplayer quantum games



Open question: For 2-player games, blow-up in size of shared entangled state is polynomial. Best known multiparty universal embezzling states are doubly exponentially large. Is it possible to do better?

$$\omega^* = \sup_{\dim =: n} \sup_{X,Y,\rho} \mathbb{E}_{a,b} \sum_{a,b,j,k} V(j,k|a,b)\, \mathrm{tr}[\rho X_a^j \otimes Y_b^k]$$

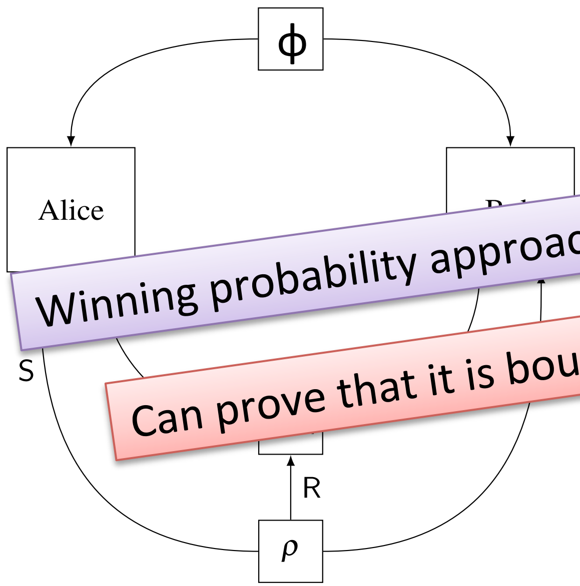
$$= \sup_{\dim =: n} \sup_{X,Y} \mathbb{E}_{a,b} \sum_{a,b,j,k} V(j,k|a,b)\, \mathrm{tr}[\rho_n X_a^j \otimes Y_b^k]$$

Schmidt rank n embezzling state

[Oliveira 2010]

Application:
Games can require unbounded entanglement

2-player cooperative quantum game



Winning probability approaches 1 as dimension of embezzling state goes to infinity.

Can prove that it is bounded away from 1 for all finite dimensional |ϕ>.

Generalizes usual model: *quantum messages*

Referee performs a projection to determine win/loss.

Let's play…

$$|\rho\rangle_{RST} = \frac{1}{\sqrt{2}}(|0\rangle_R|00\rangle_{ST} + |1\rangle_R|\psi\rangle \ldots |\phi_{ebz}\rangle$$

$$\ldots \frac{1}{\sqrt{2}}(|11\rangle_{ST} + |22\rangle_{ST})$$

Goal:

$$|\text{win}\rangle_{RAB} = \frac{1}{\sqrt{2}}(|000\rangle_{RAB} + |111\rangle_{RAB}).$$

Easy if Alice and Bob could apply unitaries to all of ST since |00> and |ψ> are orthogonal.

They can't because they are separated…

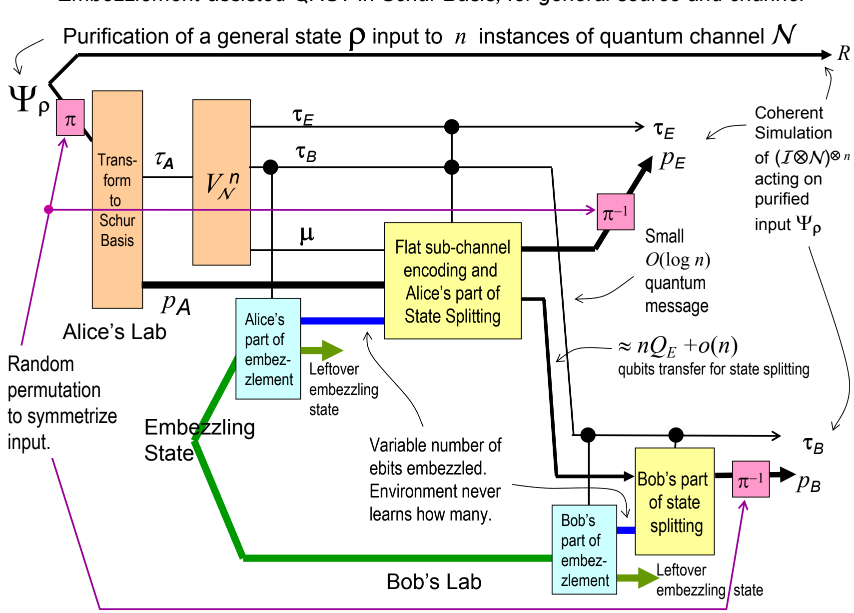
But since they can coherently embezzle |ψ> from $|\phi_{ebz}\rangle$ they can also coherently unembezzle it!

[Leung-Toner-Watrous 2008/13]

Same thing twice, just as nice

This idea was originally used as part of the proof of the *Quantum Reverse Shannon Theorem*:

Asymptotically, every quantum channel can simulate every other using a rate of forward noiseless communication given by the ratio of their entanglement-assisted capacities plus shared entanglement.



[Bennett-Devetak-Harrow-Shor-Winter 2009*]

The Great Laws: Part 2

§1.0.1. Thou shalt not create *entanglement* without a commensurate investment of *quantum* interaction.

σ_{AB}

$\uparrow \mathcal{N}_{LOCC}$

ρ_{AB}

$$E(A;B)_\sigma \leq E(A;B)_\rho$$

LOCC = Local Operations and Classical Communication

$$\implies \mathcal{N}_{LOCC}(\rho_{AB}) = \sum_j X_j \otimes Y_j \rho_{AB} X_j^\dagger \otimes Y_j^\dagger$$

The Great Laws: Part 2

§1.0.2. Every person, human, physical or cryptographic shall be maximally entangled with at most one other person.

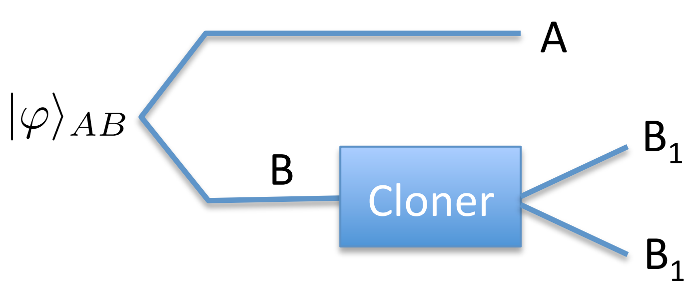
Monogamy: The more entangled Alice is with Bob, the less entangled she can be with Charlie.

In particular, if AB state is pure, then C must factorize:

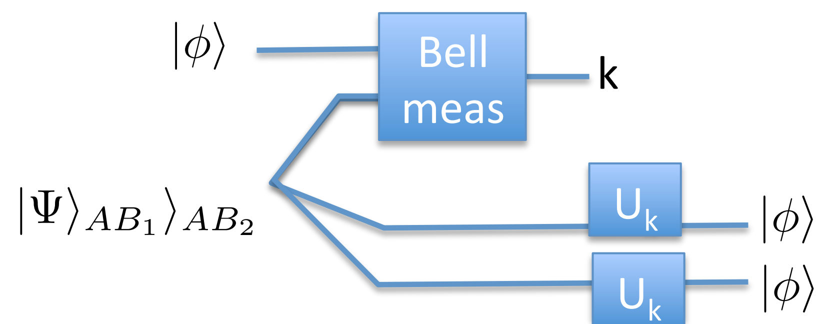
$$|\varphi\rangle_{AB} \Rightarrow |\varphi\rangle\langle\varphi|_{AB} \otimes \rho_C$$

Static version of the no-cloning theorem:

Cloning implies polygamy:



Polygamy implies cloning:



Entanglement measures

Entanglement measures extend the entanglement entropy to mixed states. For mixed state on AB measures cannot exceed $S(A)_\rho$.

$E_C(A;B)_\rho$: Entanglement of cost of the state ρ_{AB}.

What is the minimal rate of Bell pairs required to make many copies of ρ_{AB} using only LOCC operations?

$$E_C(A;B)_\rho + E_C(A;C)_\rho \leq^? S(A)_\rho$$

Random pure state on ABC has both $E_C(A;B)$ and $E_C(A;C)$ almost maximal

$E_D(A;B)_\rho$: Entanglement of distillation of the state ρ_{AB}.

What is the maximal rate at which Bell pairs can be extracted from many copies of ρ_{AB} using only LOCC operations?

$$E_C(A;B)_\rho + E_D^{\rightarrow}(A;C)_\rho \leq^? S(A)_\rho$$ ✓

Look before you leap

Measure	E_{sq} [6]	E_D [18, 19]	K_D [20, 21]	E_C [18, 22]	E_F [18]	E_R [23]	E_R^∞ [24]	E_N[25]
normalisation	y	y	y	y	y	y	y	y
faithfulness	y Cor. 1	n [14]	?	y [26]	y	y	y [27]	n
LOCC monotonicity[a]	y	y	y	y	y	y	y	y [28]
asymptotic continuity	y [29]	?	?	?	y	y [30]	y [9]	n[9]
convexity	y	?	?	?	y	y	y [31]	n
strong superadditivity	y	y	y	?	n [32, 33]	n [34]	?	?
subadditivity	y	?	?	y	y	y	y	y
monogamy	y [11]	?	?	n [10]	n [10]	n [10]	n [10]	?

$$\sum_{j=1}^{k} E_{sq}(A;B_j) \leq E_{sq}(A;B_1B_2\cdots B_k)$$
$$\leq \log \dim A$$

$$\frac{1}{k}\sum_{j=1}^{k} E_{sq}(A;B_j)_\sigma \leq \frac{1}{k}\log \dim A$$

Monogamy: The more entangled Alice is with Bob, the less entangled she can be with Charlie.

[Brandao, Christandl, Yard 1010.1750]

Squashed entanglement

Measure	E_{sq} [6]
normalisation	y
faithfulness	y Cor. 1
LOCC monotonicity[a]	y
asymptotic continuity	y [29]
convexity	y
strong superadditivity	y
subadditivity	y
monogamy	y [11]

ρ_{AB} unentangled (*separable*): $\rho_{AB} = \sum_j p_j \phi_{j,A} \otimes \psi_{j,B}$

Consider extension: $\rho_{ABC} = \sum_j p_j \phi_{j,A} \otimes \psi_{j,B} \otimes |j\rangle\langle j|_C$

A and B are conditionally independent given C: $I(A;B|C)_\rho = 0$.

$$E_{sq}(A;B)_\rho = \frac{1}{2} \inf\{ I(A;B|C)_\sigma \, ; \, \mathrm{tr}_C \, \sigma_{ABC} = \rho_{AB} \}$$

[Christandl-Winter 2004]

Squashed entanglement

Measure	E_{sq} [6]
normalisation	y
faithfulness	y Cor. 1
LOCC monotonicity[a]	y
asymptotic continuity	y [29]
convexity	y
strong superadditivity	y
subadditivity	y
monogamy	y [11]

Proof of monogamy:

$$E_{sq}(A;B_1B_2)_\rho = \frac{1}{2}\inf_C I(A;B_1B_2|C)_\sigma$$

$$= \frac{1}{2}\inf_C \left[I(A;B_1|C)_\sigma + I(A;B_2|B_1C)_\sigma\right]$$

$$\geq \frac{1}{2}\inf_C I(A;B_1|C)_\sigma + \frac{1}{2}\inf_C I(A;B_2|C)_\sigma$$

$$E_{sq}(A;B)_\rho = \frac{1}{2}\inf\{I(A;B|C)_\sigma : \mathrm{tr}_C\,\sigma_{ABC} = \rho_{AB}\}$$

$$= E_{sq}(A;B_1)_\rho + E_{sq}(A;B_2)_\rho$$

[Christandl-Winter 2004]

Conclusions

- If your result looks like a sneaky but useless trick, just wait ten years. You might be surprised.
- For applications of the monogamy of entanglement, consult a workshop talk at random:
  - Brandao: Limitations on quantum PCP
  - Miller: Untrusted device cryptography
  - Yuen: Infinite randomness expansion with constant number of devices
  - Parrilo: Testing entanglement using symmetric extensions
  - Reichardt: Delegated quantum computation
    - (super-monogamy?)
  - …