Title: Quantifying Entanglement with Quantum Entropy

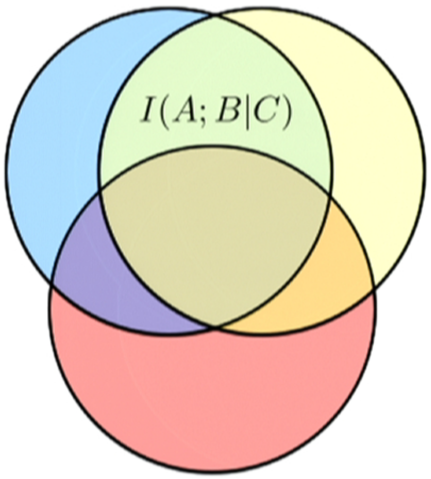
Date: Mar 07, 2012 02:00 PM

URL: http://pirsa.org/12030092

Abstract: Entropy plays a fundamental role in quantum information theory through applications ranging from communication theory to condensed matter physics. These applications include finding the best possible communication rates over noisy channels and characterizing ground state entanglement in strongly-correlated quantum systems. In the latter, localized entanglement is often characterized by an area law for entropy. Long-range entanglement, on the other hand, can give rise to topologically ordered materials whose collective excitations are robust against local noise. In this talk, I will present a property of quantum entropy for multipartite quantum systems that resolves several open questions in quantum information theory about entanglement measures, provides new algorithmic opportunities and makes nontrivial statements about the structure of states with vanishing - but nonzero - topological entropy. I will also comment how extensions of this work could help our understanding of quantum communication over certain very noisy channels.

Quantifying entanglement

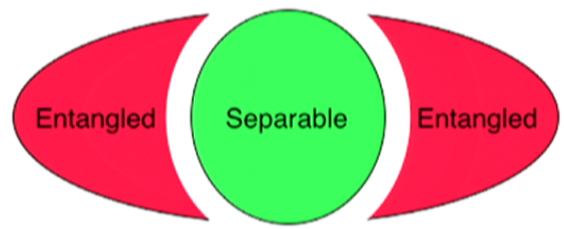
with quantum entropy



Jon Yard

Los Alamos National Laboratory

March 7, 2012
Perimeter Institute
Colloquium



based on joint work
with
Fernando Brandão and Matthias Christandl

Los Alamos
NATIONAL LABORATORY

CCS-3

Shannon's information theory

The Bell System Technical Journal

Vol. XXVII *July, 1948* *No. 3*

A Mathematical Theory of Communication

By C. E. SHANNON

$$H(X) = -\sum p(x) \log p(x)$$

Entropy arises in the answers to fundamental questions:

Data compression, channel capacity

This talk: applications of quantum entropy

$$H(\rho) = -\mathrm{Tr}\rho \log \rho$$

Quantum entanglement

Product pure states:

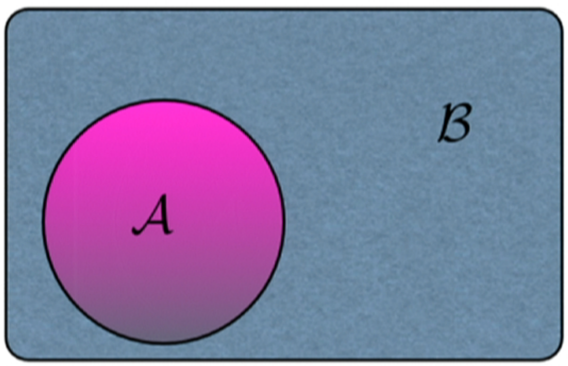
$$|\psi\rangle_{AB} = |\psi\rangle_A |\psi\rangle_B \equiv |\psi\rangle_A \otimes |\psi\rangle_B$$

Most states in $A \otimes B$ are entangled.

Example: EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Straightforward to quantify - entanglement entropy

$$E(|\psi\rangle_{AB}) = H(\rho_A) = -\mathrm{Tr}\rho_A \log \rho_A = H(\rho_B)$$



Example: Ground state of a lattice of spins $A = \bigotimes_{i \in \mathcal{A}} \mathbb{C}^2, \; B = \bigotimes_{i \in \mathcal{B}} \mathbb{C}^2$

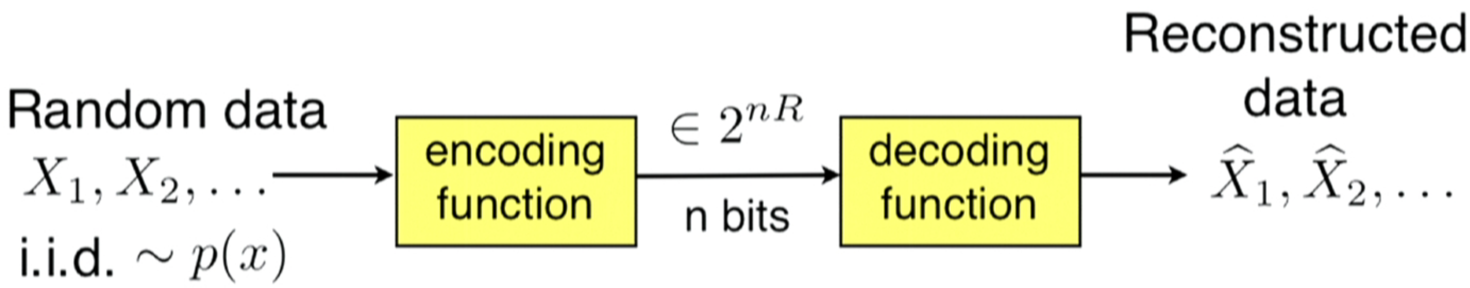
Area law: $H($  $) = \alpha L - \gamma + \cdots$

localized entanglement (αL)

long-range entanglement (γ)

How exactly does this "quantify" the entanglement?

Shannon's data compression



Goal: send as few bits as possible (i.e. minimize rate R)

while making negligible errors

$$\Pr\{(X_1, \ldots X_n) \neq (\widehat{X}_1, \ldots \widehat{X}_n)\} \to 0 \text{ as } n \to \infty$$

Shannon's theorem: The best (smallest) compression rate is $R = H(X)$.

Operational interpretation of entropy, quantifies "information content"

Philosophy of information theory

Schumacher's quantum data compression

$(\mathbb{C}^2)^{\otimes nR} = \mathbb{C}^{2^{nR}}$

Random states $|\psi_{x_1}\rangle|\psi_{x_2}\rangle\cdots$ i.i.d. $\sim p(x)$ → encoding operation → n qubits → decoding operation → Reconstructed state $\rho_{\text{out}}^{(n)}$

Goal: send as few qubits as possible (i.e. minimize rate R)

while making negligible errors

$$\sum_{x^n} p(x_1)\cdots p(x_n)\langle\psi_{x_1}|\cdots\langle\psi_{x_n}|\rho_{\text{out}}^{(n)}|\psi_{x_1}\rangle\cdots|\psi_{x_n}\rangle \to 1$$

Schumacher's theorem: The best (smallest) compression rate is $R = H(\rho)$, where $\rho = \sum_x p(x)|\psi_x\rangle\langle\psi_x|$.

Independent of particular ensemble $\{p(x), |\psi_x\rangle\}$

The church of the larger Hilbert space

Any other ensemble with the same

$$\rho = \sum_x p(x)|\psi_x\rangle\langle\psi_x|$$

can be created by measuring part of the purification

$$|\psi\rangle = \sum_x \sqrt{p(x)}|x\rangle|\psi_x\rangle$$

Interpret Schumacher compression as measuring correlations in such a purified source, simply requiring

$$\langle\psi|^{\otimes n}\rho_{\text{out}}^{(n)}|\psi\rangle^{\otimes n} \to 1$$

Compressing both sides distills the entanglement

$$|\psi\rangle^{\otimes n} \to (|00\rangle + |11\rangle)^{\otimes Hn}$$

EPR states

entropy

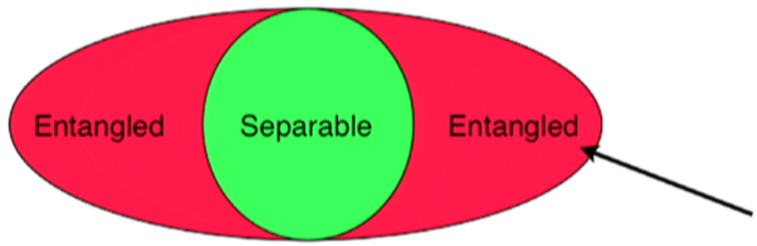
Mixed state entanglement

Not as straightforward

Definition. A bipartite state ρ^{AB} is *separable* if

$$\rho^{AB} = \sum_x p(x) |\psi_x\rangle\langle\psi_x|_A \otimes |\psi_x\rangle\langle\psi_x|_B$$

Separable states are a convex subset of the set of all states



Definition. everything else is called *entangled*.

Given a description of ρ^{AB}:

Is it entangled? (NP-hard - Gurvits 2002)

How entangled is it? (Entanglement measures)

Is it far from any separable state? (easy! - this talk)

Main tool: recently discovered properties of quantum entropy

Some famous entanglement measures

Distillable entanglement

how many pure EPR pairs can I produce from $\rho_{AB}^{\otimes n}$?

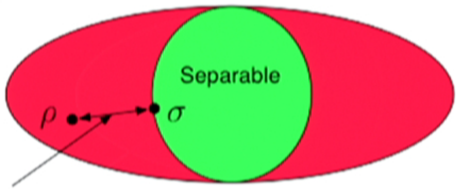
(related to quantum error-correction and channel capacity)

Entanglement cost

How much pure entanglement needed to create $\rho_{AB}^{\otimes n}$?

Relative entropy of entanglement

$$E_R(\rho^{A:B}) = \min_{\sigma \in \mathrm{SEP}} D(\rho \| \sigma)$$



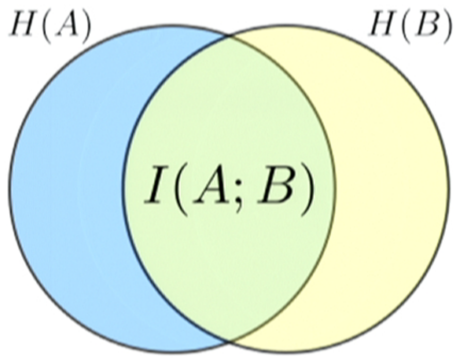
$$D(\rho\|\sigma) = \mathrm{Tr}\rho(\log\rho - \log\sigma)$$

Squashed entanglement

$$E_{\mathrm{sq}}(\rho^{AB}) = \inf\left\{\tfrac{1}{2}I(A;B|C) : \mathrm{Tr}_C\,\rho^{ABC} = \rho^{AB}\right\}$$

quantum conditional mutual information

Quantum mutual information



Function of bipartite density matrices ρ_{AB}

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

Von Neumann entropy

$$H(A) = -\mathrm{Tr}\rho_A \log_2 \rho_A$$

Operational meanings: measures correlations, channel capacities

Characterizes product states

$$I(A;B) = 0 \iff \rho_{AB} = \rho_A \otimes \rho_B$$

$I(A;B) \approx 0 \Rightarrow$ approximately a product

$$I(A;B) \geq \frac{1}{2} \|\rho_{AB} - \rho_A \otimes \rho_B\|_1$$

trace distance

$\|X\|_1 = \mathrm{Tr}\sqrt{XX^\dagger}$
$= \sum$singular values(X)

Trace distance as distinguishability measure

Suppose given one of the states ρ, σ but don't know which

ρ, σ with equal probability → measurement $\{M, I-M\}$, $0 \leq M \leq I$

$$\Pr\{\text{declare}\,\rho\,|\,\rho\} = \mathrm{Tr} M \rho$$

$$\Pr\{\text{declare}\,\sigma\,|\,\sigma\} = \mathrm{Tr}(I - M)\sigma$$

$$\Pr\{\text{correct}\} = \frac{1}{2}\Pr\{\text{declare}\,\rho\,|\,\rho\} + \frac{1}{2}\Pr\{\text{declare}\,\sigma\,|\,\sigma\}$$

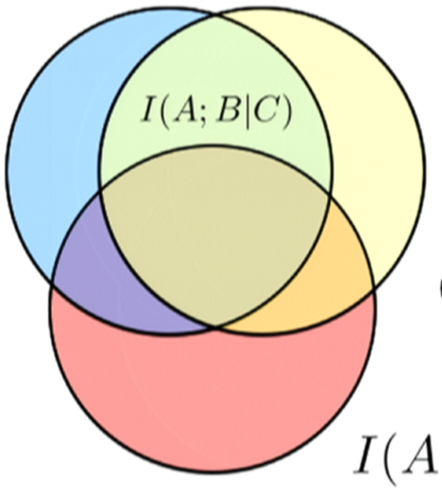
$$= \frac{1}{2} + \frac{1}{2}\underbrace{\mathrm{Tr} M(\rho - \sigma)}_{\max_{0\leq M\leq I} \;=\; \frac{1}{2}||\rho-\sigma||_1}$$

$$\boxed{\max \Pr\{\text{correct}\} = \frac{1}{2} + \frac{1}{4}||\rho - \sigma||_1}$$

Measures optimal *bias*, optimized over all measurements.

Quantum conditional mutual information

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



no interpretation as an average

$$H(A|C) + H(B|C) - H(AB|C)$$

Operational relevance only found recently
state redistribution problem (Devetak & Yard)

$I(A;B|C) \geq 0$ nontrivial to prove (Lieb & Ruskai '72)

Characterizes conditional independence

$I(A;B|C) = 0 \iff A - C - B$ (Hayden et al.)

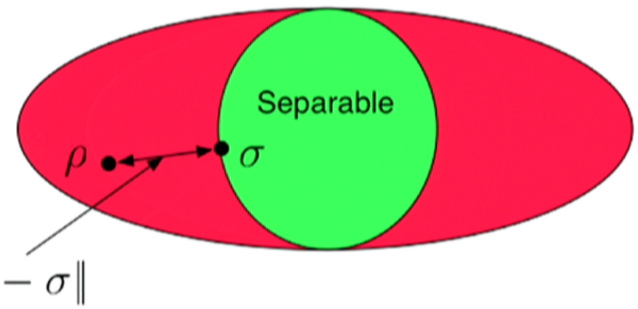
Unlike classical, approximate version unclear (Ibinson et al.)

Does $I(A;B|C) \approx 0 \implies \rho_{ACB} \approx$ Markov chain??

We'll see $I(A;B|C) \approx 0 \implies \rho_{AB} \approx$ separable

Measuring entanglement with norms

Distance to the set of separable states:



$$\left\|\rho^{AB} - \mathrm{SEP}^{AB}\right\| \equiv \min_{\sigma^{AB} \in \mathrm{SEP}^{AB}} \left\|\rho^{AB} - \sigma^{AB}\right\|$$

where SEP^{AB} is the set of separable states on AB

ρ^{AB} is separable $\Leftrightarrow \left\|\rho^{AB} - \mathrm{SEP}^{AB}\right\| = 0$

But $\|\cdot\|_1$ is too strong! Weaker norm maximizes over local measurements

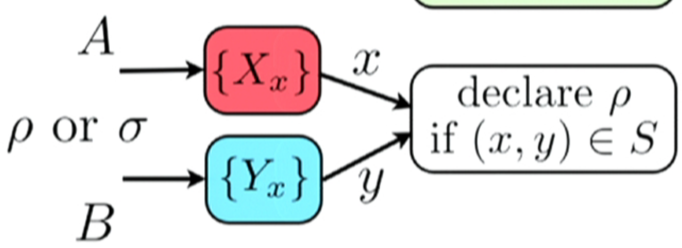
$$\|\rho - \sigma\| = 2 \max_{M} \mathrm{Tr} M(\rho - \sigma)$$

where M satisfies certain locality constraints.

Local measurements

$$\|\rho - \sigma\| = 2 \max_M \mathrm{Tr} M(\rho - \sigma)$$

$$\|\rho - \sigma\|_{\mathrm{LO}}$$

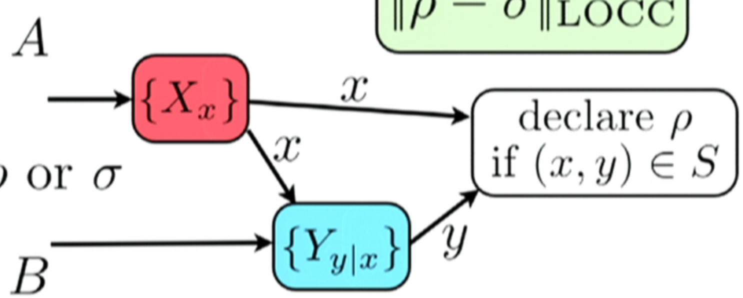


$$M = \sum_{(x,y)\in S} X_x \otimes Y_y$$

$$\sum_{x=1}^{m} X_x = I, \ \sum_{y=1}^{n} Y_y = I.$$

$$S \subset \{1, \ldots, m\} \times \{1, \ldots, n\}$$

$$\|\rho - \sigma\|_{\mathrm{LOCC}}$$



$$M = \sum_{x} X_x \otimes Y_x$$

$$\sum_x X_x \leq I, \ Y_x = \sum_y Y_{y|x} \leq I$$

$$\|\cdot\|_1 \geq \|\cdot\|_{\mathrm{LOCC}} \geq \|\cdot\|_{\mathrm{LO}} \geq \frac{1}{\sqrt{153}} \|\cdot\|_2 \geq \frac{1}{\sqrt{153 D}} \|\cdot\|_1$$

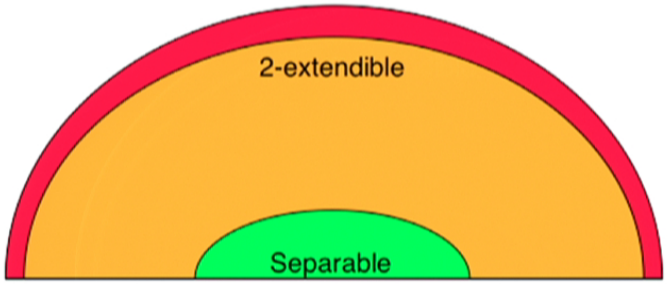
[Matthews, Wehner & Winter]

Hierarchy of separability criteria

A symmetric k-extension of ρ^{AB} is a state on $AB_1 \cdots B_k$ such that

$$\rho^{AB} = \mathrm{Tr}_{B_2 \cdots B_k} \rho^{A\underbrace{B_1 \cdots B_k}_{\text{symmetric}}}$$

Gives a hierachy of conditions satisifed by separable states:



$$\rho^{AB} = \sum_x \rho_x^A \otimes \rho_x^B = \mathrm{Tr}_{B_2 \cdots B_k} \sum_x \rho_x^A \otimes \rho_x^{B_1} \otimes \cdots \otimes \rho_x^{B_k}$$

Complete: turns out every entangled state fails some test

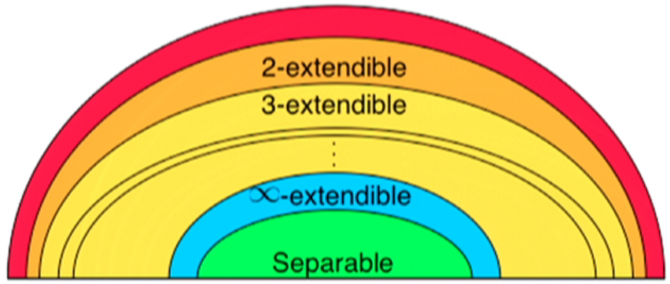
$$\rho^{AB} \text{ entangled} \Rightarrow \rho^{AB} \text{ not } k\text{-extendible } \exists k$$

Hierarchy of separability criteria

A symmetric k-extension of ρ^{AB} is a state on $AB_1 \cdots B_k$ such that

$$\rho^{AB} = \mathrm{Tr}_{B_2 \cdots B_k} \rho^{A \underbrace{B_1 \cdots B_k}_{\text{symmetric}}}$$

Gives a hierachy of conditions satisifed by separable states:



$$\rho^{AB} = \sum_x \rho_x^A \otimes \rho_x^B = \mathrm{Tr}_{B_2 \cdots B_k} \sum_x \rho_x^A \otimes \rho_x^{B_1} \otimes \cdots \otimes$$

Complete: turns out every entangled state fails som

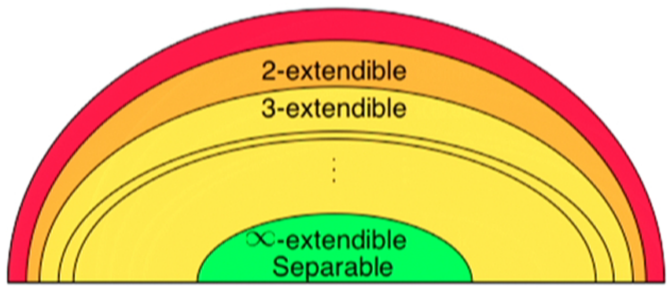
$$\rho^{AB} \text{ entangled} \Rightarrow \rho^{AB} \text{ not } k\text{-extendible } \exists k$$

Hierarchy of separability criteria

A symmetric k-extension of ρ^{AB} is a state on $AB_1\cdots B_k$ such that

$$\rho^{AB} = \mathrm{Tr}_{B_2\cdots B_k}\,\rho^{A\underbrace{B_1\cdots B_k}_{\text{symmetric}}}$$

Gives a hierachy of conditions satisifed by separable states:



$$\rho^{AB} = \sum_x \rho_x^A \otimes \rho_x^B = \mathrm{Tr}_{B_2\cdots B_k} \sum_x \rho_x^A \otimes \rho_x^{B_1} \otimes \cdots \otimes$$

Complete: turns out every entangled state fails som

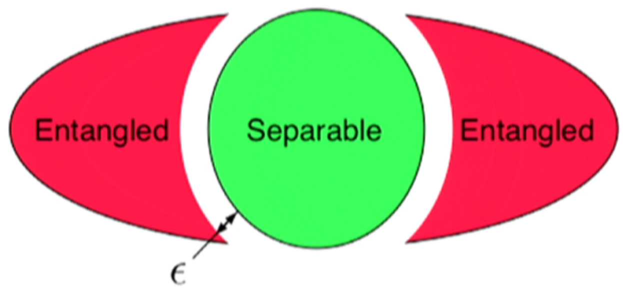
ρ^{AB} entangled $\Rightarrow \rho^{AB}$ not k-extendible $\exists k$

Algorithm for separability?

To show that

- ρ^{AB} is separable, find a k-extension for some k
- ρ^{AB} is entangled, show some k-extension doesn't exist

Problem: Might have to check infinitely many k

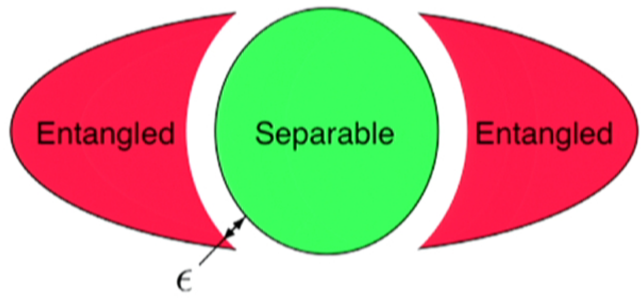


Weak membership problem: given ρ^{AB} and $\epsilon > 0$, decide if

- ρ^{AB} is separable
- $\left\|\rho^{AB} - \mathrm{SEP}^{AB}\right\| \geq \epsilon$

with the promise that only one can happen.

Didn't you say this was NP-hard?



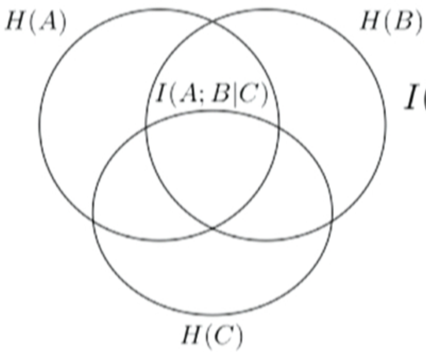
- Gurvits '02: NP-hard if $1/\epsilon = \exp(a, b)$
- Gharibean '08: NP-hard if $1/\epsilon = \text{poly}(a, b)$
- What if $1/\epsilon = \text{poly}\log(a, b)$ (where it takes quasipoly time)?

This would give quasipolynomial-time algorithm for SAT which is believed to require exponential time (Impagliazzo & Paturi '99)

But how do we prove the de Finetti bound? (lots of information theory)

Squashed entanglement

$$E_{\rm sq}(\rho^{AB}) = \inf \left\{ \tfrac{1}{2} I(A;B|C) : {\rm Tr}_C\, \rho^{ABC} = \rho^{AB} \right\}$$



$$\begin{aligned} I(A;B|C) &= H(AC) + H(BC) - H(C) - H(ABC) \\ &= H(A|C) + H(B|C) - H(AB|C) \\ &= I(A;BC) - I(A;C) \end{aligned}$$

Seems hard to compute in general (no known bound on c)

Yet it has nice properties: *normalized* & *monogamous*

$$E_{\rm sq}(\rho^{A:B}) \leq \log a, \quad E_{\rm sq}(\rho^{A:B_1B_2}) \geq E_{\rm sq}(\rho^{A:B_1}) + E_{\rm sq}(\rho^{A:B_2})$$

Only recently, we showed that it is *faithful*

$E_{\rm sq}$(separable) $= 0$ easy, but $E_{\rm sq}$(entangled) > 0 hard!

(so in fact it is NP-hard to compute!)

New lower bound on I(A;B|C)

Proof that $E_{\mathrm{sq}}(\text{separable}) = 0$:

If ρ^{AB} separable, then choose extension with $c \leq a^2 b^2$

$$\rho^{ABC} = \sum_x p(x) \rho_x^A \otimes \rho_x^B \otimes |x\rangle\langle x|^C.$$

Then $E_{\mathrm{sq}} = I(A;B|C) = \sum_x p(x) I(\rho_x^A \otimes \rho_x^B) = 0.$

$E_{\mathrm{sq}}(\text{entangled}) > 0$ hard since unclear if achieved for finite c.

Follows from new bound [Brandao, Christandl, Yard (2010)]

$$I(A;B|C) \geq \text{const} \times \left\| \rho^{AB} - \mathrm{SEP}^{AB} \right\|^2$$

Independent of extension and of dimension! Further implies

$$E_{\mathrm{sq}}(\rho^{AB}) \geq \text{const} \times \left\| \rho^{AB} - \mathrm{SEP}^{AB} \right\|^2$$

which immediately gives $E_{\mathrm{sq}}(\text{entangled}) > 0$

Some consequences

stronger subadditivity

strong additivity $I(A;B|C) \geq 0$ [Lieb & Ruskai '73]

$I(A;B|C) = 0$ implies ρ^{AB} separable [Hayden, Josza, Petz & Winter '03]

It was an open question whether this held approximately

We now know $I(A;B|C) \approx 0$ implies $\|\rho^{AB} - \mathrm{SEP}^{AB}\| \approx 0$

So far only negative results [Ibinson, Linden,Winter]

one-line proof of de Finetti theorem for n-extendible ρ^{AB}

$$\log|A| \geq E_{\mathrm{sq}}(\rho^{AB^n}) \geq nE_{\mathrm{sq}}(\rho^{AB}) \geq \mathrm{const} \times n\|\rho^{AB} - \mathrm{SEP}^{AB}\|^2$$

Proof of $I(A;B|C) \geq \text{const} \times \left\|\rho^{AB} - \text{SEP}^{AB}\right\|^2$

Follows from chain of new inequalities

$$I(A;B|C) \geq D_{\text{global}}(\rho^{A:BC}) - D_{\text{global}}(\rho^{A:C}) \geq D_{\text{local}}(\rho^{A:B}) \geq \frac{1}{8}\|\rho^{AB} - \text{SEP}\|^2$$

$D_{\text{global,local}}$ = optimal error rate for distinguishing $\rho_{AB}^{\otimes n}$ from SEP with one-sided error using global or local measurements:

$$\Pr\{\text{declare } \rho_{AB}^{\otimes n} \mid \text{some separable state}\} \leq 2^{-Dn}$$

$$\Pr\{\text{declare } \rho_{AB}^{\otimes n} \mid \rho_{AB}^{\otimes n}\} \to 1$$

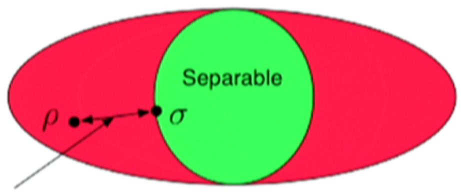
Proof uses several recent results in quantum information theory:

Operational interpretations:
of I(A;B|C) as optimal communication rate (Devetak & Yard), and

$$R_{\text{global}}(\rho^{A:B}) = \lim_{n\to\infty} \frac{1}{n} \min_{\sigma\in\text{SEP}} D(\rho^{\otimes n}||\sigma)$$

(Brandão & Plenio)

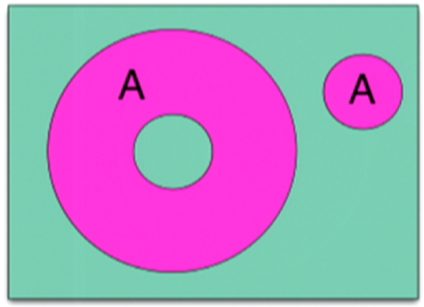
Regularized relative entropy of entanglement



$$D(\rho\|\sigma) = \text{Tr}\rho(\log\rho - \log\sigma)$$

Topological entanglement entropy

[Kitaev & Preskill, Levin & Wen]



- Gapped 2D system in ground state
- Region A large w.r.t. correlation length $\xi \sim 1/\text{gap}$

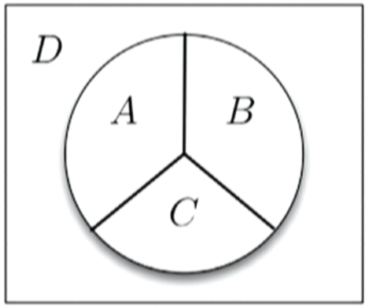
$$H(A) = \underbrace{\alpha L}_{\text{boundary term}} - \underbrace{b \log \mathcal{D}}_{\text{topological term}} + \cdots$$

- 'total quantum dimension': $\mathcal{D} = \sqrt{\sum d_i^2}$ ← quantum dimension of quasiparticle, or anyon, of type i
- b = # boundary components
- $\log \mathcal{D}$ = 'topological entanglement entropy'
- $\log \mathcal{D} > 0$ signature of topological order

Topological entanglement entropy

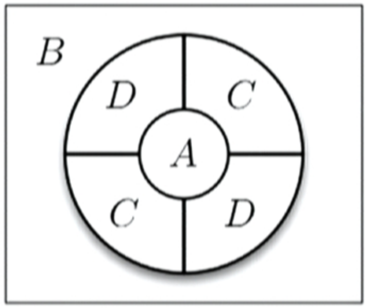
$$J = -H(A) - H(B) - H(C) - H(ABC) + H(AB) + H(BC) + H(AC)$$

Kitaev & Preskill



$\gamma = J(A, B, C)$

Levin & Wen



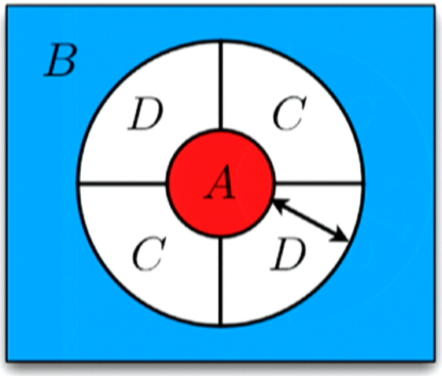
$2\gamma = J(A, B, C) = I(A; B|C)$

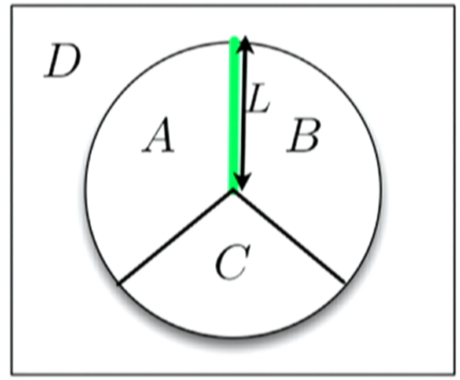
Assume general form $H(A) = \alpha L - b\gamma$

Cancel boundary terms: (integer) $\times\gamma = J(A, B, C)$

K&P: TQFT calculation gives $\gamma = \log \mathcal{D}$

What can we say about topological entropy?





$2\gamma = J(A, B, C) = I(A; B|C)$

Assuming gap, $\max_{0 \le X, Y \le I} \mathrm{Tr}(X \otimes Y)(\rho_{AB} - \rho_A \otimes \rho_B) \to 0$ (Hastings)

Assuming only $I(A; B|C) \approx 0$, can say $\|\rho_{AB} - \mathrm{SEP}\| \simeq 0$

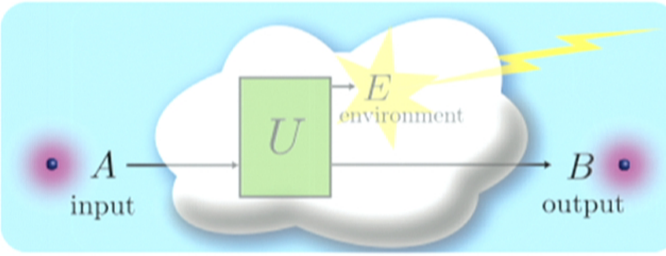
Falls short when $A \cap B \neq \emptyset$: $I(A; B|C) = 2\alpha L + \gamma + \cdots$

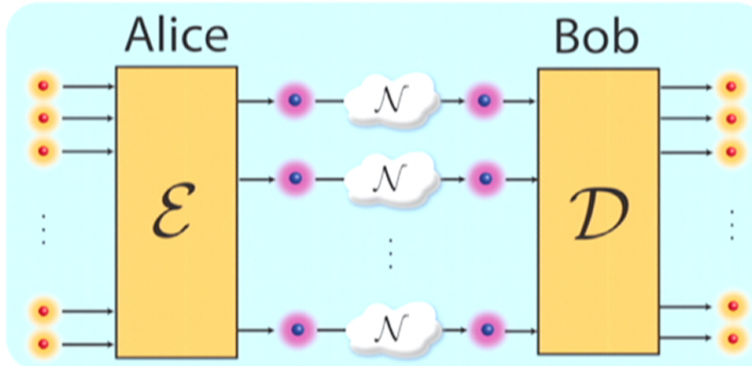
Possible interpretation for boundary or CFT states?

- $H(A) \sim \mathrm{area}(A)$ although $I(A; B|C)$ finite [Casini & Huerta]

- lack of conformally-invariant tensor product structure makes this hard

Quantum channels





Reversible interaction with inaccessible environment

Quantum capacity $Q = \max \frac{\#\text{encoded qubits}}{\#\text{transmissions}}$ is the fundamental bound on the possibility to perform quantum error correction.

Open question: find formula for Q.
Only have bounds in general.

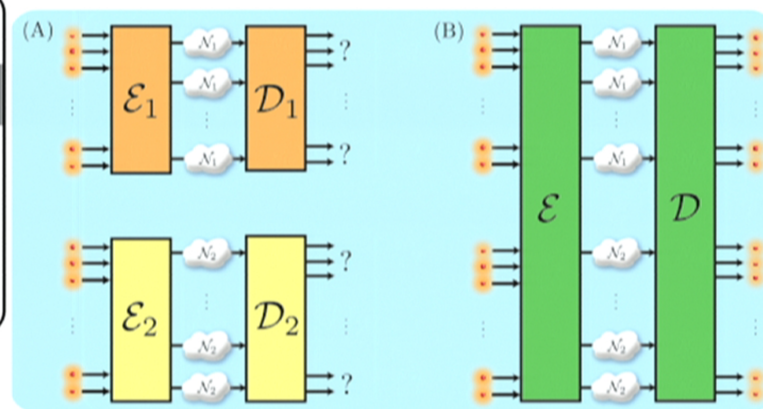
Superactivation of Q

26 SEPTEMBER 2008 VOL 321 SCIENCE www.sciencemag.org

REPORTS

Quantum Communication with Zero-Capacity Channels

Graeme Smith[1*] and Jon Yard[2]



There are pairs $\mathcal{N}_1, \mathcal{N}_2$ of quantum channels with

$$Q(\mathcal{N}_1) = Q(\mathcal{N}_2) = 0, \; Q(\mathcal{N}_1 \times \mathcal{N}_2) > 0$$

nature photonics

Quantum communication with Gaussian channels of zero quantum capacity

Graeme Smith[1*], John A. Smolin[1] and Jon Yard[2]

Formula for capacity when assisted by zero-capacity symmetric channels

$$Q_{\text{assisted}} = \max_{\rho_{AC}} I(A;B|C) - I(A;E|C)$$

also involves optimizing over arbitrarily large C

Thanks for listening

Questions:

Dimension bound for squashed entanglement?

Can we study entanglement without obvious $\otimes$ structure?

(e.g. product states make sense for nonabelian anyons, despite this)

(e.g. relative entropy exists for boundary states, despite lack of well-defined entropies [Casini & Huerta])

Max-version of squashed entanglement [Oppenheim]?

($I(A;B)$ small but $I(A;B|C)$ *large* might be more relevant for studying γ information-theoretically)

Structure of the global state?

Negative result: $\min_{\sigma_{A-C-B}} D(\rho_{ACB}||\sigma) \geq I(A;B|C)_\rho$ [Ibinson, Linden & Winter]

Regularized version? Suitable norm?

Insights for understanding channel capacity?