Title: The theory of quantum information: channels, capacities, and all that

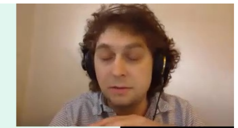
Speakers: Graeme Smith

Series: Perimeter Institute Quantum Discussions

Date: February 10, 2021 - 4:00 PM

URL: http://pirsa.org/21020023

Abstract: Information theory offers mathematically precise theory of communication and data storage that guided and fueled the information age. Initially, quantum effects were thought to be an annoying source of noise, but we have since learned that they offer new capabilities and vast opportunities. Quantum information theory seeks to identify, quantify, and ultimately harness these capabilities. A basic resource in this context is a noisy quantum communication channel, and a central goal is to figure out its capacities---what can you do with it? Iâ€™ll highlight the new and fundamentally quantum aspects that arise here, such as the role of entanglement, ways to quantify it, and bizarre new kinds of synergies between resources. These ideas elucidate the nature of communication in a quantum context, as well as revealing new facets of quantum theory itself.



The theory of quantum information: Channels, Capacities, and all that

Graeme Smith

JILA and CU Boulder

February 10, 2021

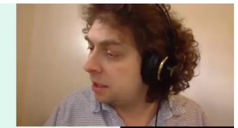
PI Quantum Information Seminar

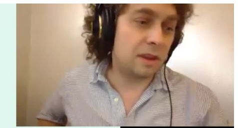
JILA CU Boulder and NIST

University of Colorado Boulder

Center for Theory of Quantum Matter CTQM

Quantum Information





Nonadditivity of Quantum Capacity

Slightly different question. Say we know

$$Q(N_1) = \lim_{n\to\infty} \frac{1}{n} Q^1(N_1^{\otimes n})$$

$$Q(N_2) = \lim_{n\to\infty} \frac{1}{n} Q^1(N_2^{\otimes n})$$

What about $Q(N_1 \otimes N_2)$?

Is there a better way to use N_1 and N_2 together?

Yes, when N_1 and N_2 are different enough, they're kind of like different ingredients (different resources).

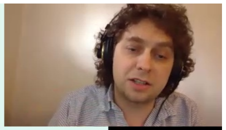
Then you get $Q(N_1 \otimes N_2)$ >> $Q(N_1) + Q(N_2)$

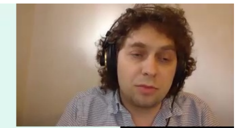
Information Theory

"The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point."

-Claude Shannon 1948

Source coding, channel coding, detection, cryptography…

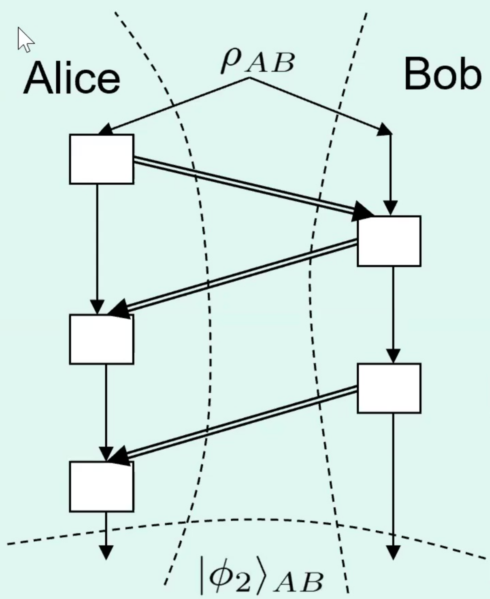


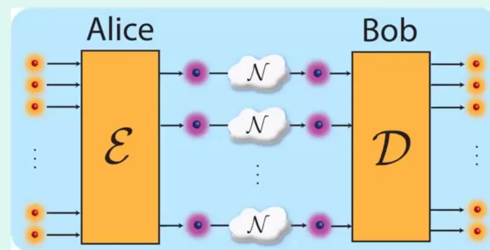


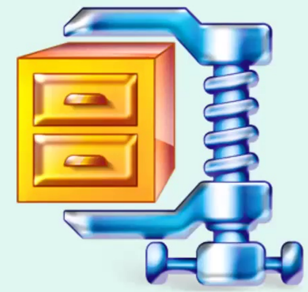
Information theory

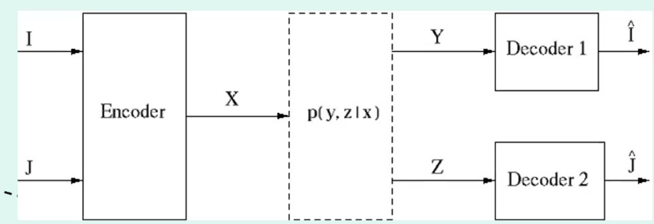
Sending, storing, processing data.

Using noisy resources to simulate noiseless resources









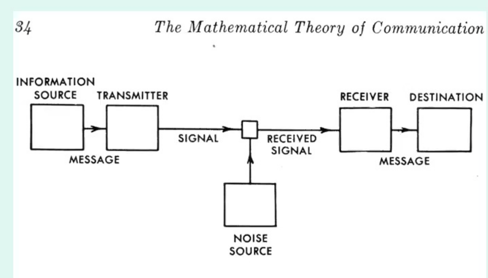
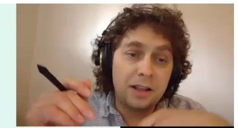


Fig. 1. — Schematic diagram of a general communication system.

a sad duk went to unavrsadee $\longrightarrow$ a sad duck went to university



Quantum Information Theory: The Philosophy

Goal 1) Abstract away as much detail as possible to find out the fundamental limits nature puts on information processing

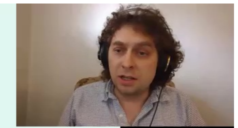
Goal 2) The details that are left give us a clearer picture of quantum mechanics itself. Can help understand traditional physics.

Goal 3) Strategies for approaching these fundamental limits may be realizable. Either today or in the future.

It’s about physics, but draws on other things too, like geometry, computer science, engineering, etc.

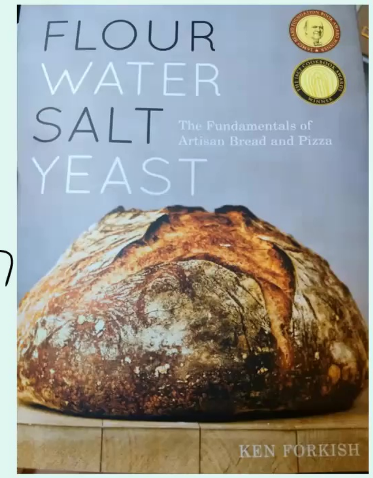
It’s certainly different from more traditional branches of physics. Maybe it’s “toy physics”.

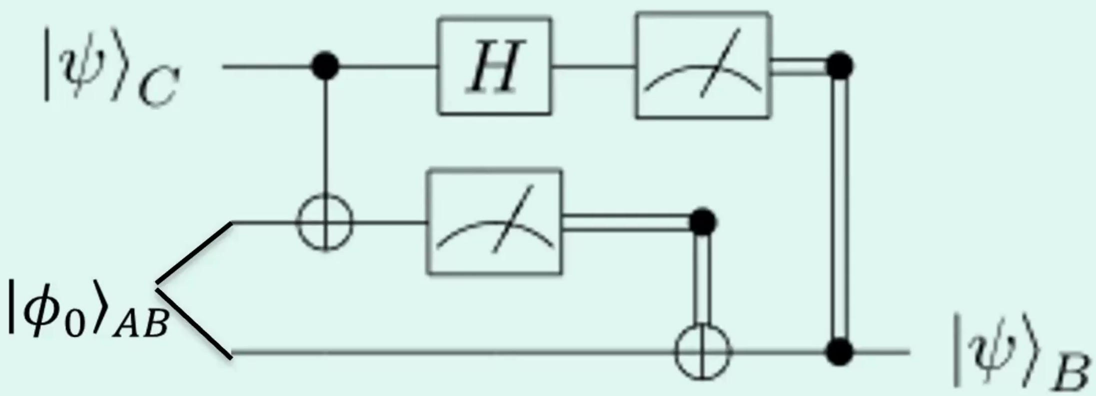
Quantumly: lots more resources, and more interesting interactions.



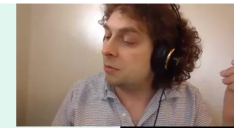
Quantum Information Theory

- What are the resources?
- How can we convert them?
- How do they interact?
- What's the recipe?



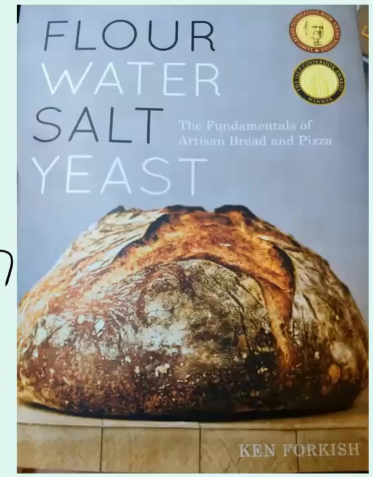


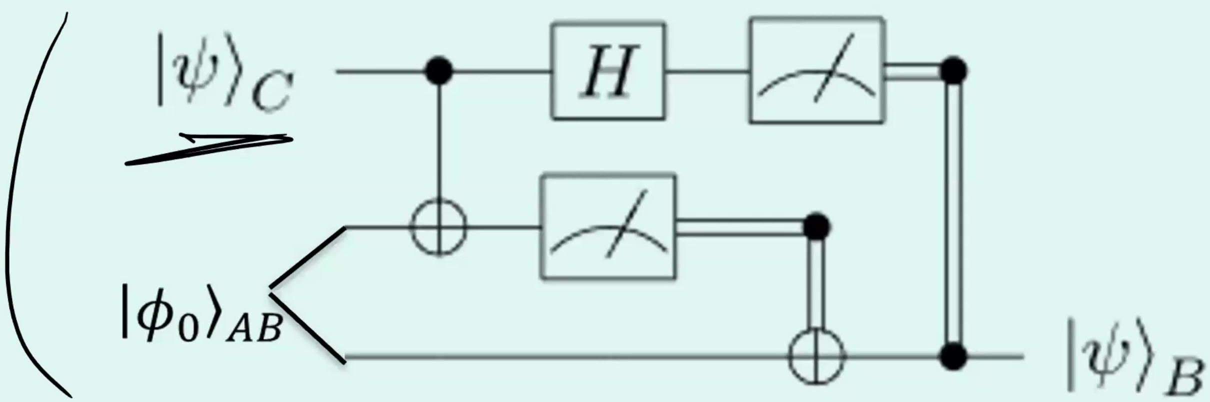
Teleportation



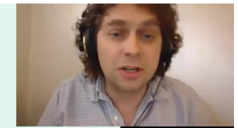
Quantum Information Theory

- What are the resources?
- How can we convert them?
- How do they interact?
- What's the recipe?



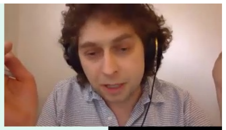


Teleportation



Outline

- Information Theory Basics
- Quantum Capacity
- Additivity and nonadditivity
- Quantum boost for classical networks
- Quantifying quantum correlations



Channel Capacity

Sender

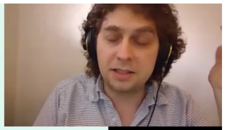
Receiver

The capacity is the amount of stuff you can send per use of the channel. For a truck, measured in tons per load. For classical channel it's bits per channel use.

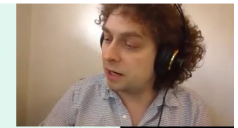
Channel Capacity

Sender

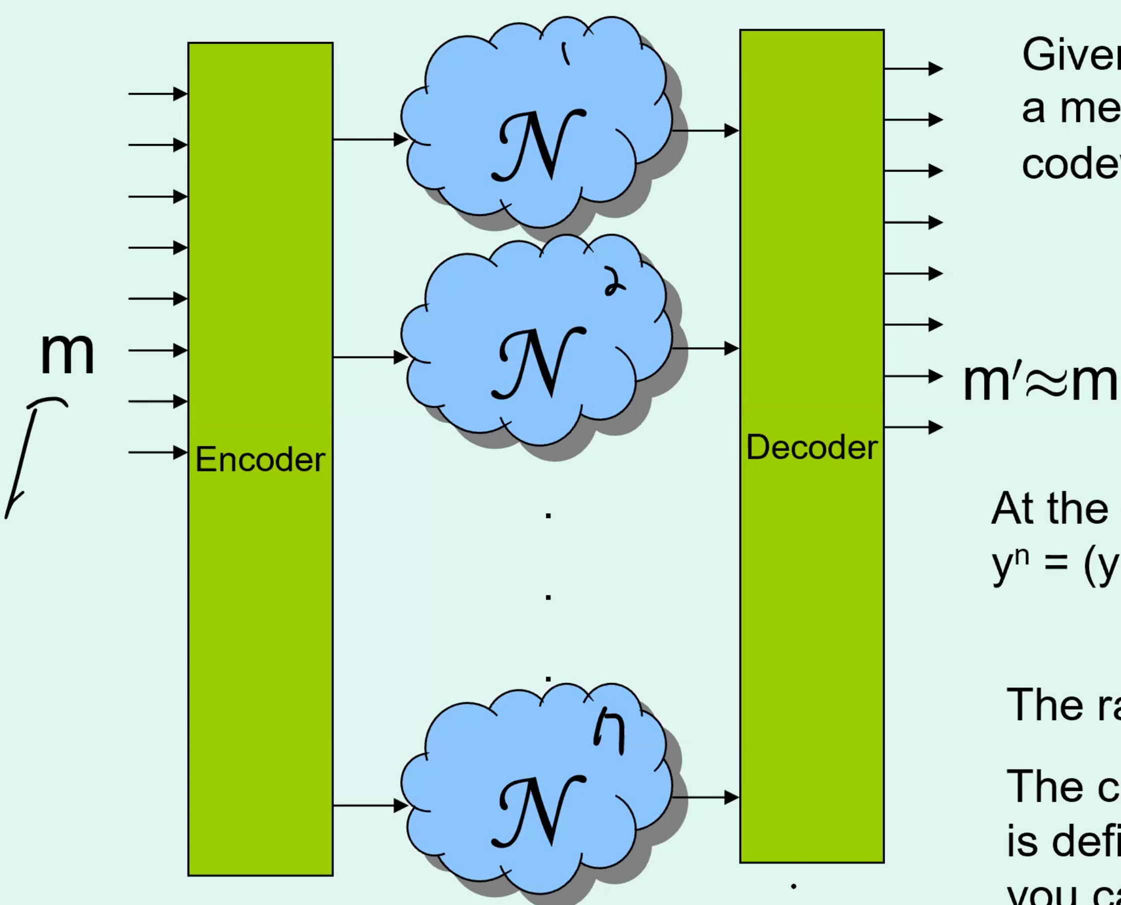
Receiver



The capacity is the amount of stuff you can send per use of the channel. For a truck, measured in tons per load. For classical channel it's bits per channel use.



Channel Capacity

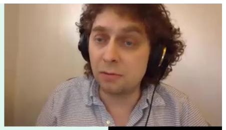


Given n uses of a channel, encode a message $m \in \{1,\ldots,M\}$ to a codeword $x^n = (x_1(m),\ldots, x_n(m))$

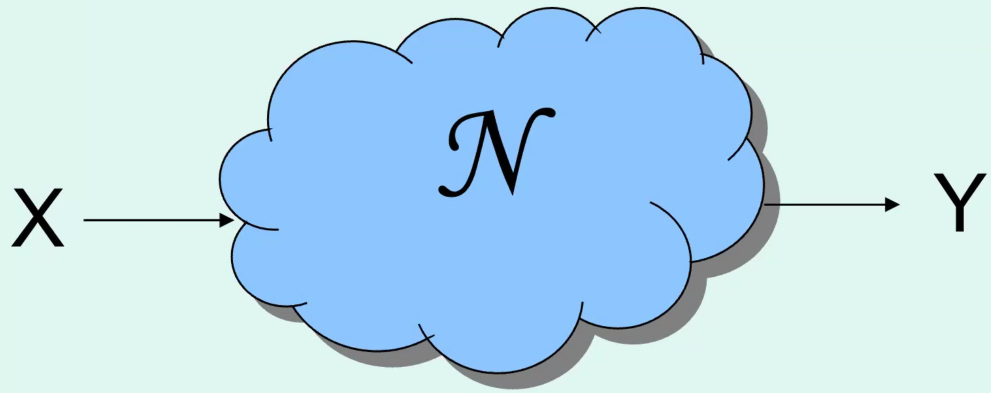
At the output of the channel, use $y^n = (y_1,\ldots,y_n)$ to make a guess, m'.

The rate of the code is $(1/n)\log M$.

The capacity of the channel, $C(N)$, is defined as the maximum rate you can get with vanishing error probability as $n \to \infty$



Channel Capacity



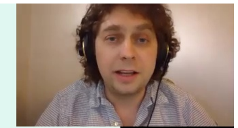
p(y|x)

Capacity: bits per channel use in the limit of many channels

$$C(N) = \max_X \underline{I(X;Y)}$$

$$H(X) = -\sum_x p_x \log p_x$$

I(X;Y) = H(X)+H(Y)-H(XY) is the mutual information

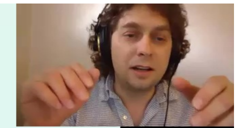


Additivity lets us calculate answers

C( × )

= C() + C()

Classical Capacity of Classical Channel



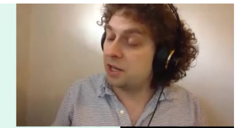
Additivity tells us that resources only interact trivially

Additive: trivial interaction

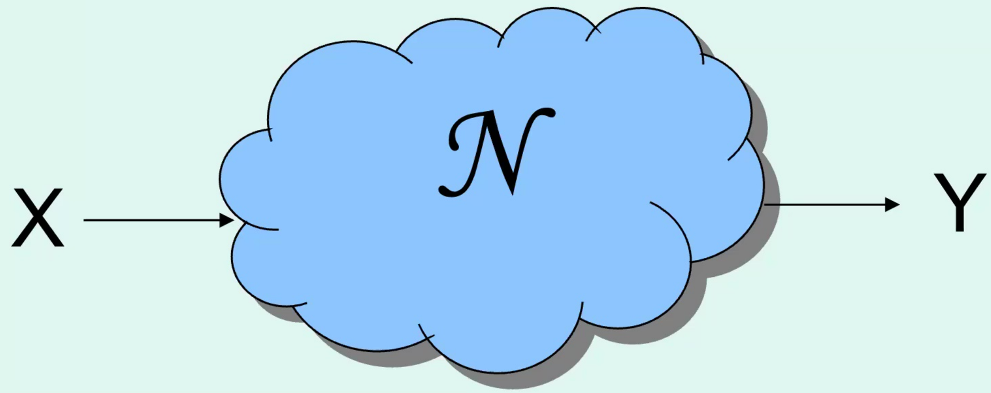
$$C(N_1 \times N_2) = C(N_1) + C(N_2)$$

Nonadditive:
nontrivial interaction

$$Q(N_1 \otimes N_2) > Q(N_1) + Q(N_2)$$



Channel Capacity



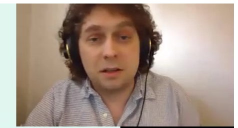
p(y|x)

Capacity: bits per channel use in the limit of many channels

$$C(N) = \lim_{n\to\infty} \frac{1}{n}\, C^{(1)}(N^{\times n})$$

where $C^{(1)}(N) = \max_X I(X;Y)$. Luckily $C^{(1)}$ is additive, so

$$C(N) = C^{(1)}(N)$$



Quantum Information theory: Making information theory consistent with physics

Quantum effects as annoying noise

Noise at Optical Frequencies; Information Theory.

J. P. Gordon

Bell Telephone Laboratories, Incorporated - Murray Hill, N. J.

1965

НЕКОТОРЫЕ ОЦЕНКИ ДЛЯ КОЛИЧЕСТВА ИНФОРМАЦИИ, ПЕРЕДАВАЕМОГО КВАНТОВЫМ КАНАЛОМ СВЯЗИ

А. С. Холево

1973

Quantum effects give new capabilities

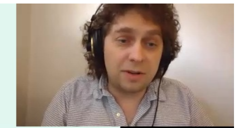
- Weisner, Bennett-Brassard: QKD
- Quantum Communication: sending quantum information over quantum links, quantum error correction, etc.

Quantum Channel Capacities

Sender

Receiver

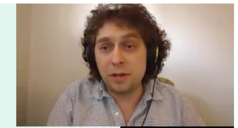
The capacity is the amount of stuff you can send per use of the channel. You want to send qubits, then it's quantum capacity. You want to send bits, it's classical capacity.



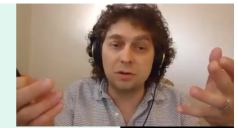
Quantum Channel Capacities

Sender

Receiver



The capacity is the amount of stuff you can send per use of the channel. You want to send qubits, then it's quantum capacity. You want to send bits, it's classical capacity.

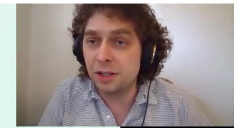


Quantum Capacities

Classical channels have only one capacity (bits per channel use), but Quantum channels have several:

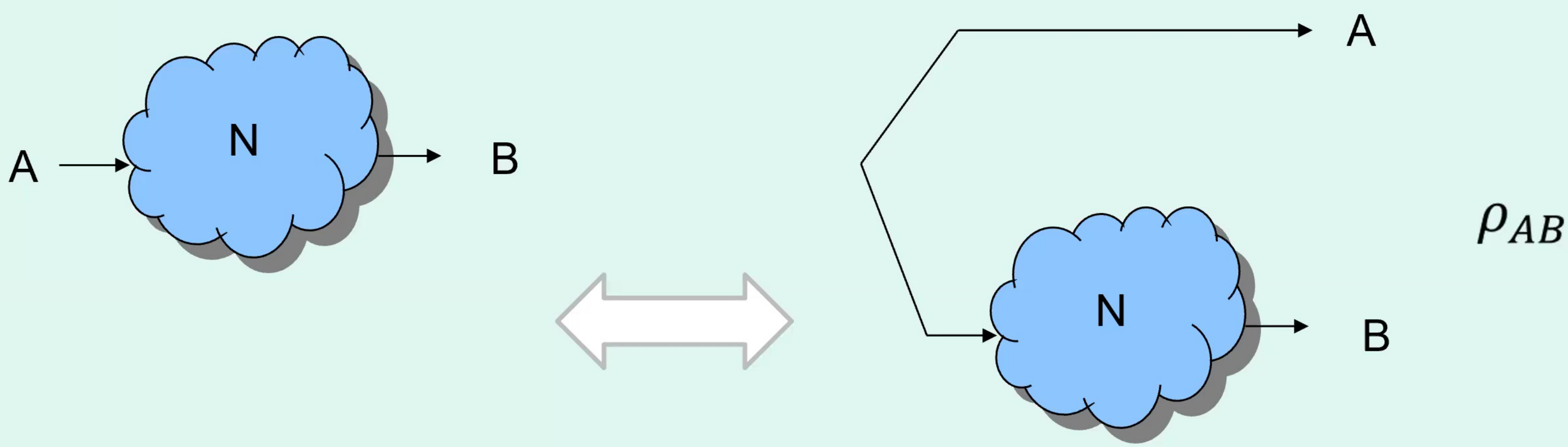
- Classical C (bits per channel use)
- Private P (private bits per channel use)
- Quantum Q (qubits per channel use)

As well as various assisted capacities: entanglement assisted capacity or quantum capacity assisted by classical feedback



Aside: Channels vs States

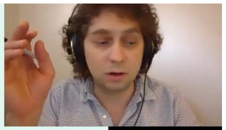
Channel | State



Quantum Capacity
Private Capacity
...

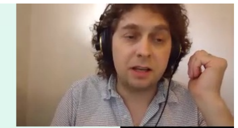
Distillable Entanglement
Distillable key
...

Basically, there's always a state version and a channel version of any problem. We'll focus on channels, but could equally well focus on states.

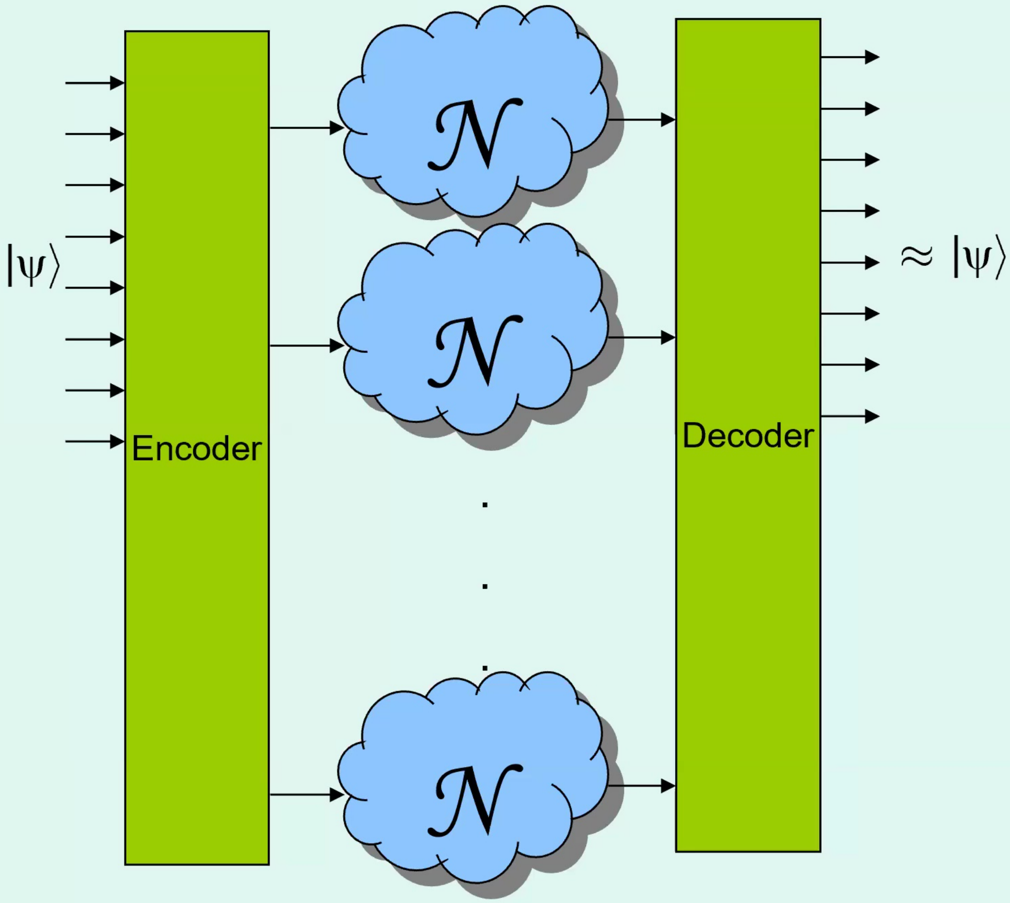


Outline

- ~~Information Theory Basics~~
- Quantum Capacity
- Additivity and nonadditivity
- Quantum boost for classical networks
- Quantifying quantum correlations

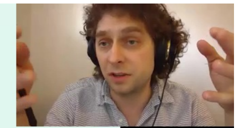


Quantum Capacity

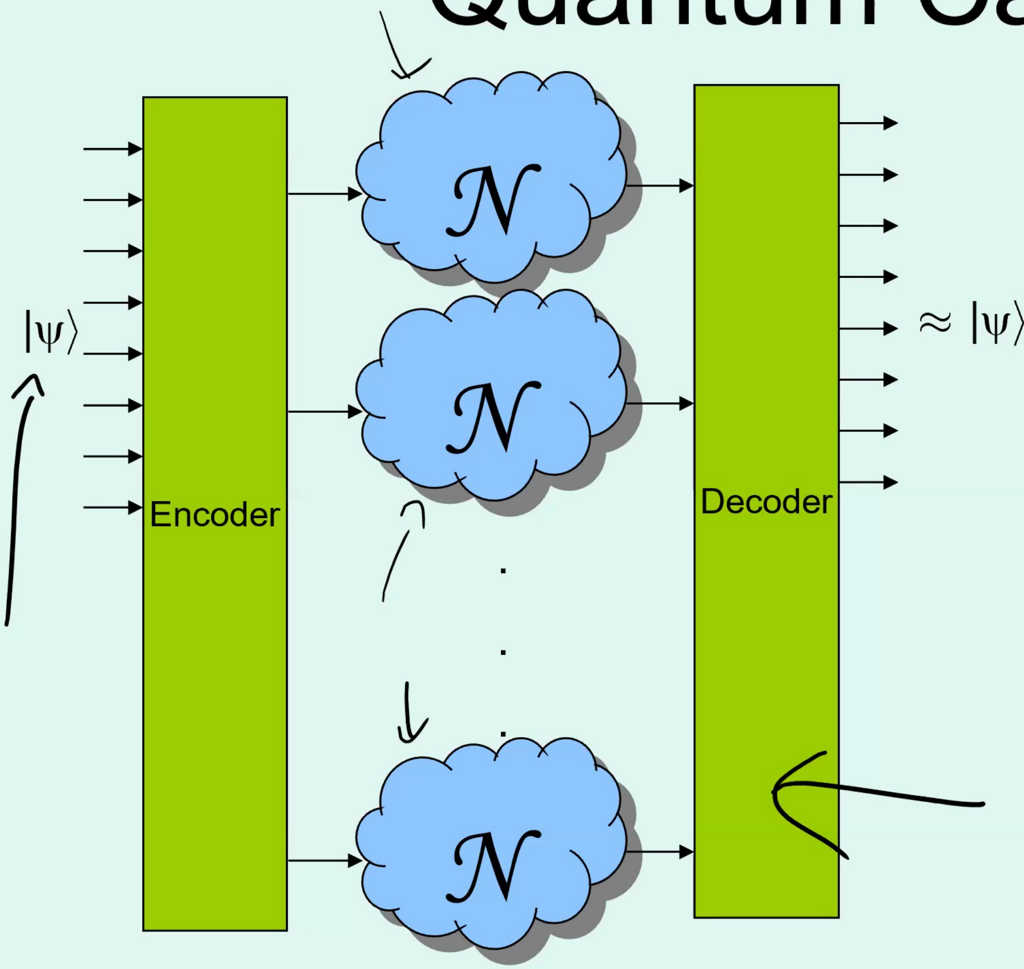


- If we try to transmit an arbitrary quantum state, we arrive at the quantum capacity, $Q(\mathcal{N})$.
- The quantum capacity, measured in qubits per channel use, gives the ultimate limit on quantum error correction.

$$Q(\mathcal{N}) = \max \frac{\#\ qubits\ sent}{\#\ channel\ uses}$$

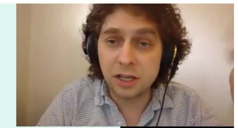


Quantum Capacity



- If we try to transmit an arbitrary quantum state, we arrive at the quantum capacity, $Q(\mathcal{N})$.
- The quantum capacity, measured in qubits per channel use, gives the ultimate limit on quantum error correction.

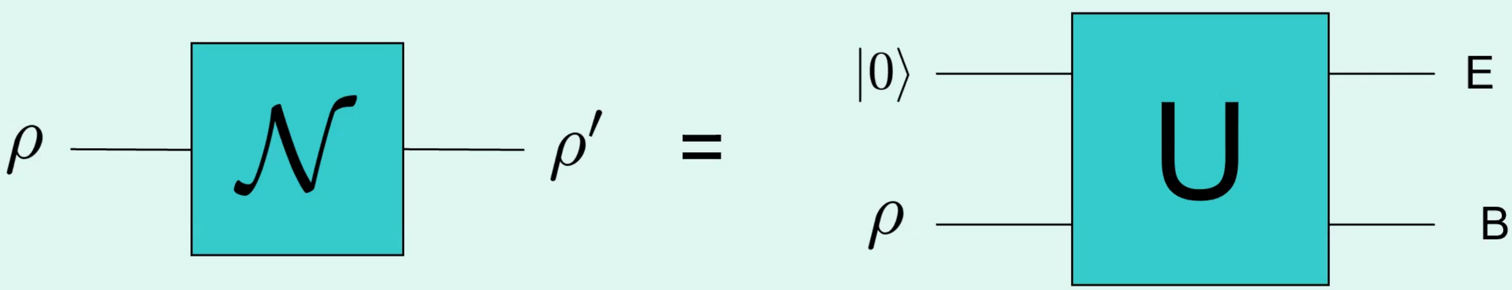
$$Q(\mathcal{N}) = \max \frac{\#\ qubits\ sent}{\#\ channel\ uses}$$



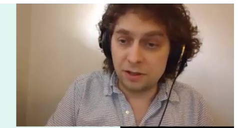
Noisy Quantum Channels

- Noiseless quantum evolution: $\rho \rightarrow U\rho U^{\dagger}$

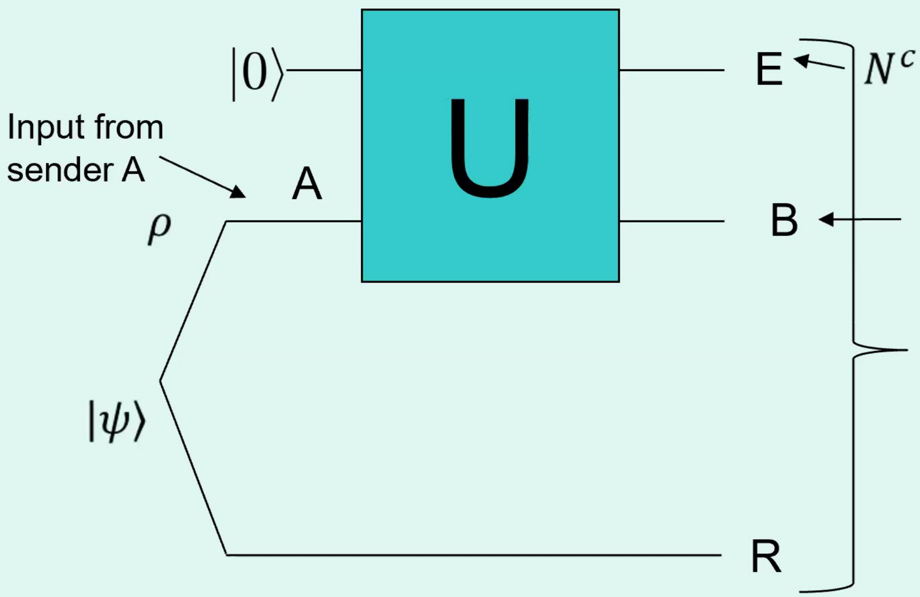
  Unitary satisfies $U^{\dagger}U = I$
- Noisy quantum evolution: unitary interaction with inaccessible environment



Think of optical fiber: E is the dof that absorb the light



Coherent Information



$N^c(\rho)$ complementary channel from A to E

$N(\rho)$ channel from A to B

$I \otimes U_N \, |\psi\rangle\langle\psi| I \otimes U_N^{\dagger}$

A ---Alice
B ---Bob
E ---Eve

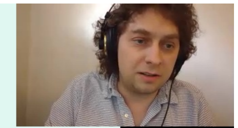
$$Q^{(1)}(N) = \frac{1}{2} \max_{|\psi\rangle} [\, I(R;B) - I(R;E)]$$

Coherent information: how much more information goes to B than E

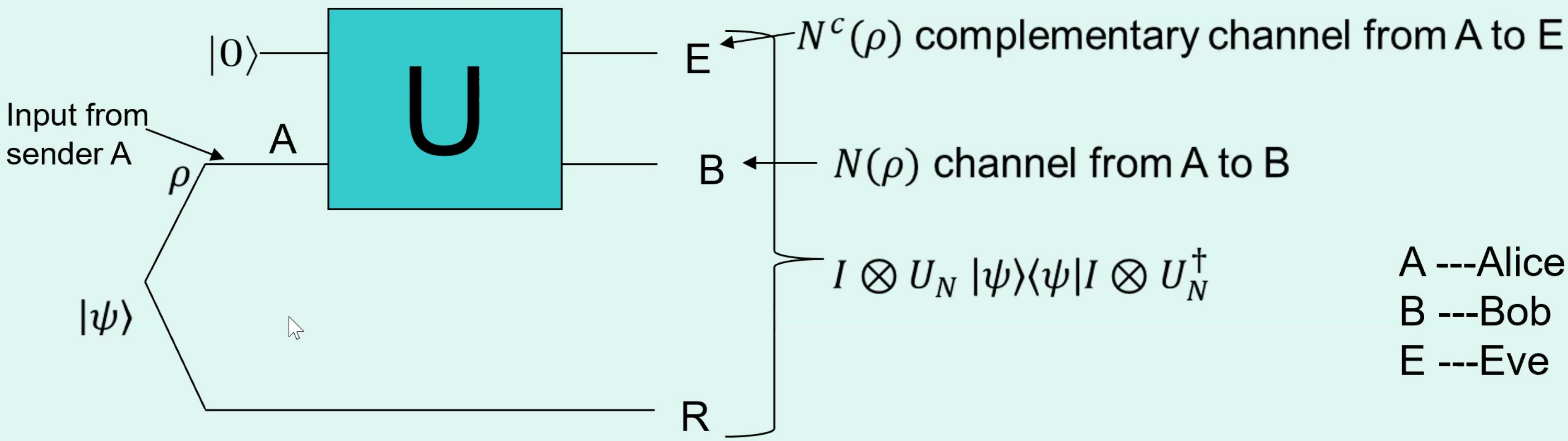
$I(R;B) = S(R) + S(B) - S(RB)$

Mutual information of R with output

Mutual information of R with environment



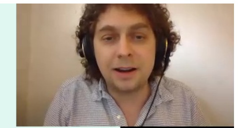
Lloyd-Shor-Devetak (LSD) Theorem



$Q(N) \geq Q^{(1)}(N)$ ⟵ Random coding

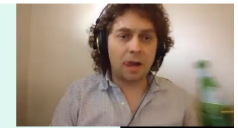
$Q(N) = \lim_{r \to \infty} \frac{1}{r} Q^{(1)}(N^{\otimes r})$ ⟵ Optimization over infinite number of variables

Lloyd 97, Shor 02, Devetak 04



Outline

- ~~Information Theory Basics~~
- ~~Quantum Capacity~~
- Additivity and nonadditivity
- Quantum boost for classical networks
- Quantifying quantum correlations



Additivity tells us that resources only interact trivially

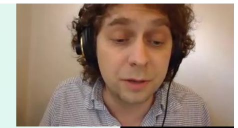
Additive: trivial interaction

$$C(N_1 \times N_2) = C(N_1) + C(N_2)$$

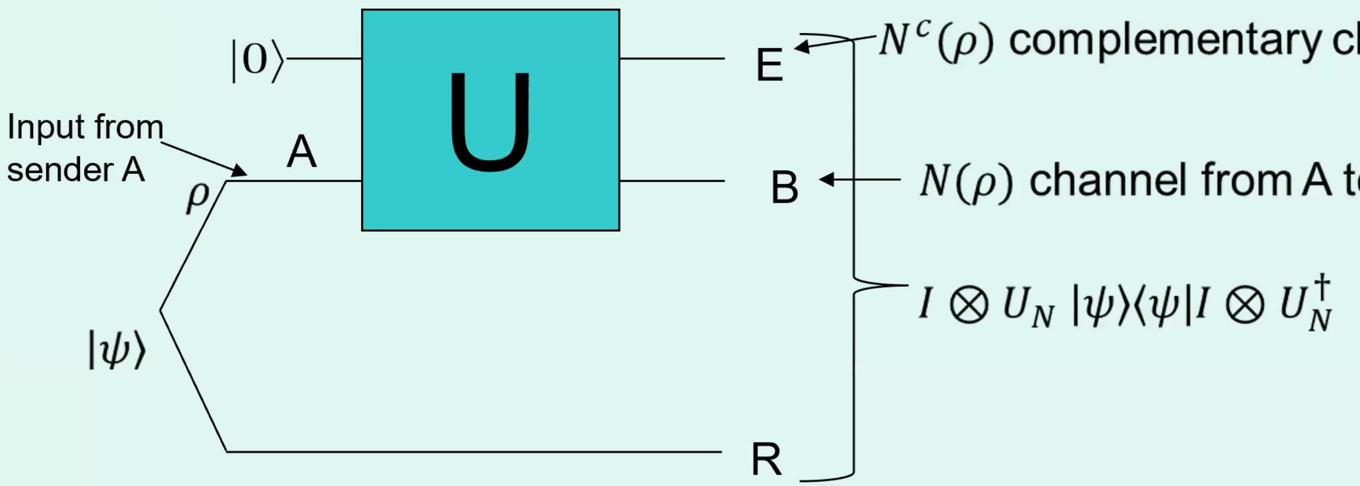
Nonadditive:
nontrivial interaction

$$Q(N_1 \otimes N_2) > Q(N_1) + Q(N_2)$$

Smoothies are quick and easy. Bread is delicious, but takes time.



Degradable Channels have additive coherent information

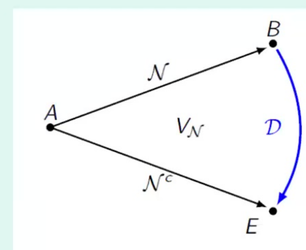


A ---Alice
B ---Bob
E ---Eve

A channel is degradable if there is a way to degrade the output B to get the environment E:

There's a channel M such that

$$N^c(\rho) = (M \circ N)(\rho)$$

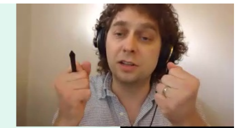


For degradable channels, we have $Q^{(1)}\left(N^{\otimes r}\right) = r\, Q^{(1)}(N)$, so

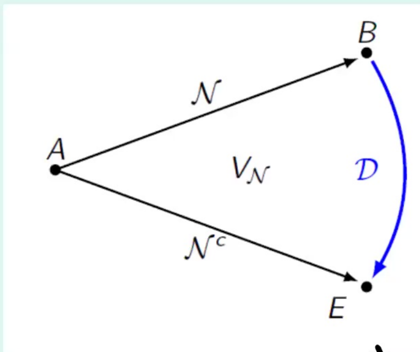
$$Q(N) = \lim_{r\to\infty} \frac{1}{r} Q^{(1)}\left(N^{\otimes r}\right) = Q^{(1)}(N) = \frac{1}{2}\max_{|\psi\rangle}[\, I(R;B) - I(R;E)].$$

Devetak-Shor CMP 2005

I can actually do this Optimization over $|\psi\rangle$



Additivity of Coherent Information



Degradable:
additive Q^1

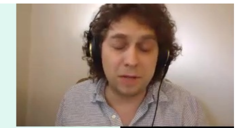
More general:

If private classical capacity to environment $P(N_E) = 0$, then

$$Q(N) = Q^1(N)$$

Watanabe '12

- Lesson 1) for some channels $Q^1(N)$ is right
- Lesson 2) nonadditivity of $Q^1(N)$ intimately connected to information sent to the environment.
- Lesson 3) $Q(N) \leq Q^1(N) + P(N)$ (Hirche '20)
- Lesson 4) Most channels aren't degradable.

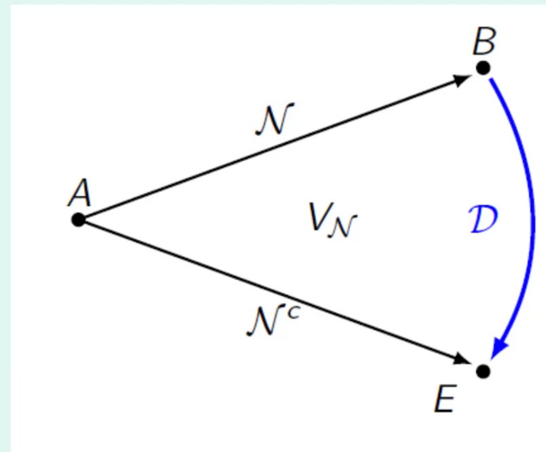


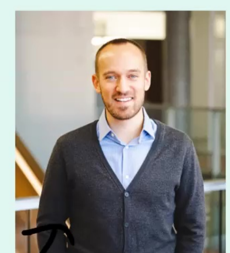
Approximate Additivity

Suppose we have a channel that has very low noise $N \approx I$.

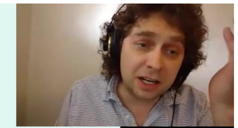
Then, very little information gets leaked to the environment.

Since a lot of information goes to the channel output, and not much to the environment, the ouput can do a pretty good job mimicking the environment.





Leditzky-Leung-Smith. PRL '18



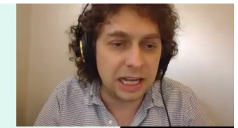
Nonadditivity of Coherent Information

$$Q^{(1)}\ (N) = \frac{1}{2}\max_{|\psi\rangle_{RA}}\ [I(R;B) - I(R;E)]$$

$Q^{(1)}$ is the rate achieved by random code that looks like $\rho_A = Tr_R|\psi\rangle\langle\psi|$

You can do better by picking structured codes.
Basically random codes that look like some $\rho_{A_1 \ldots A_n}$. Structure within a block of length n. $Q^{(1)}\left(N^{\otimes n}\right) > nQ^{(1)}(N)$. The channel is interacting nontrivially with itself.

Goal: we want to know, given N, what kind of structure good codes should have. Ideally, a compact prescription for generating such capacity achieving codes in terms of typical spaces and entropies



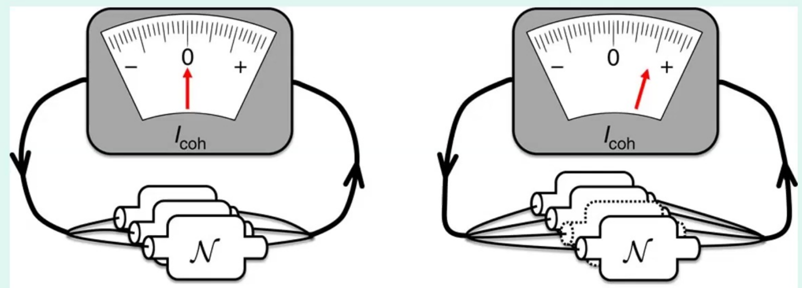
Nonadditivity of Coherent Information

There are several examples of channels with nonadditive coherent information

Depolarizing:

$$N_p(\rho) = (1-p) + p\frac{I}{2}$$

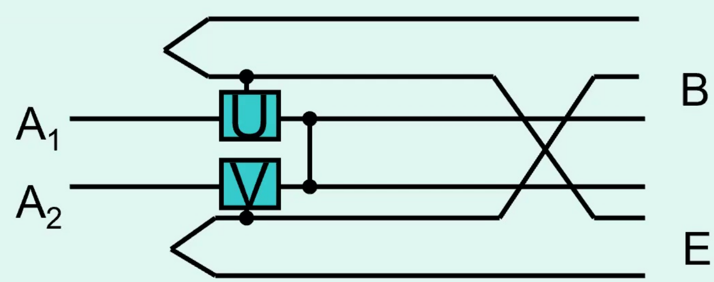
Divincenzo-Shor-Smolin ‘98
Smith-Smolin, ’07
Bausch-Leditzky, ’20…



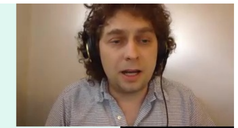
Cubitt et al, ‘15

Dephrasure:
Let $D_p(\rho) = (1-p)\rho + pZ\rho Z$ and
$E_q(\rho) = (1-q)\rho + q|e\rangle\langle e|$
$N_{p,q}(\rho) = E_q(D_p(\rho))$

Leditzky-Leung-Smith. PRL ‘18



Smith-Smolin ‘09



Nonadditivity of Coherent Information

$$V_s|0\rangle = \sqrt{s}|00\rangle + \sqrt{1-s}|11\rangle$$

$$V_s|1\rangle = |21\rangle$$

$$V_s|2\rangle = |20\rangle$$

Properties:

- Q1 nonadditive even away from Q1=0
- C = 1, P=1 for channel
- C=1, P=1 for complement
- Optimizing state not usual

Victor Kiam

Vikesh Siddhu

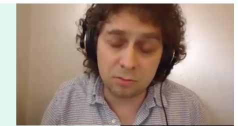
Nonadditivity: quantum resources interact nontrivially

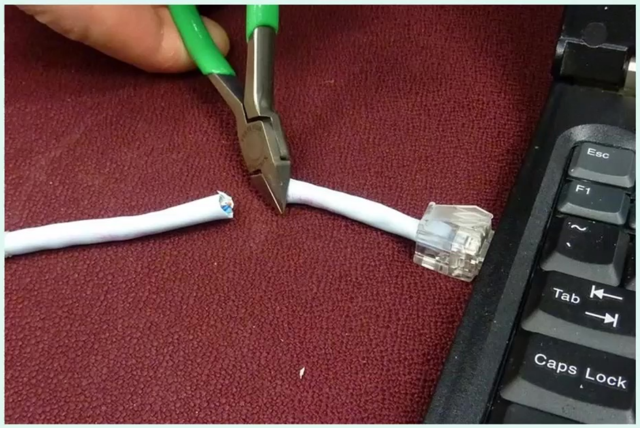
Clean examples can help us work towards general coding strategies.

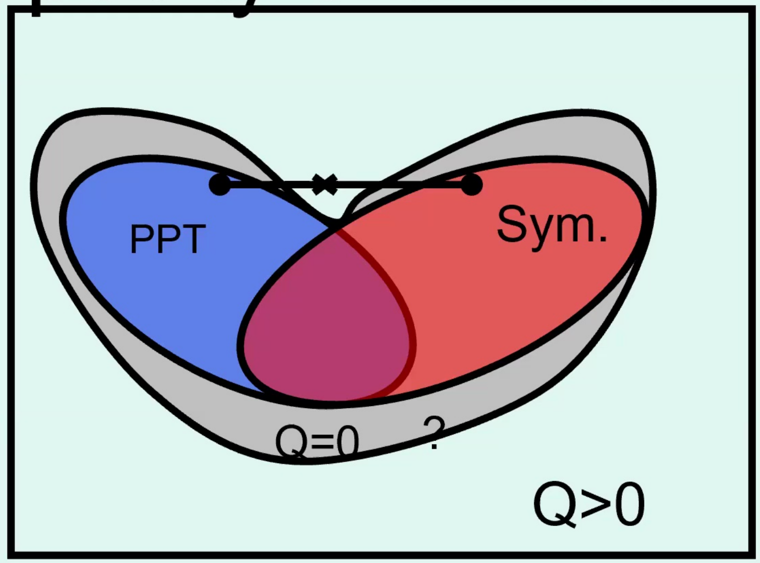
New features VS pointing towards different, more environment-focused approach to quantum capacity.

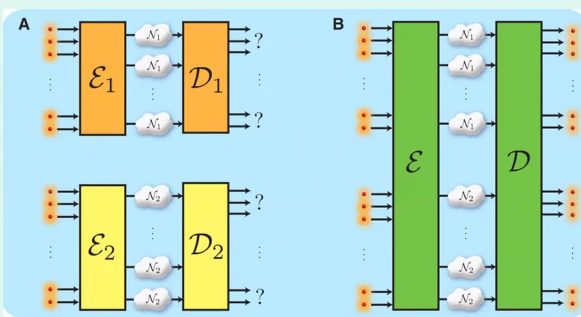
It’s about learning the recipe for good error correcting codes for a channel.

Superactivation: using zero capacity channels





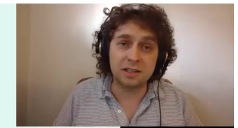




Smith-Yard ‘08

Not only can you get
$Q(N_1 \otimes N_2) \gg Q(N_1) + Q(N_2)$
You can also get
$Q(N_1 \otimes N_2) > 0$ when $\underline{Q(N_1) = 0}$, $Q(N_2) = 0$

These are two seriously different resources

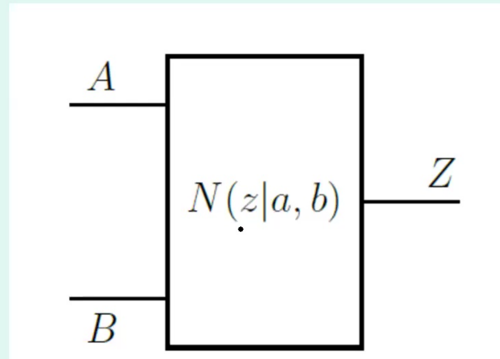


Additivity and Nonadditivity

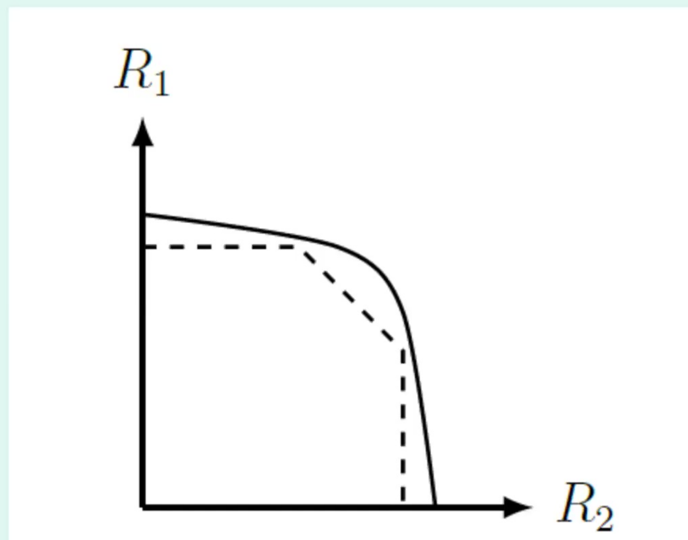
- Additivity tells us we are on the right track with random coding
- Nonadditivity tells us we are missing some key ideas about generating good structured codes.
- Complicated examples (to analyze and/or construct) obscure what's happening.
- Increasingly simple examples point towards new strategies (with more explicit role of environment info?)
- I focused on coherent information and quantum capacity, but similar stories for classical capacity, private capacity…

Simplest classical network: Classical Multiple Access Channel (MAC)

2 senders one receiver

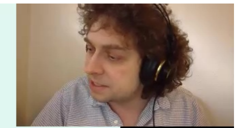


Conditional probability distribution

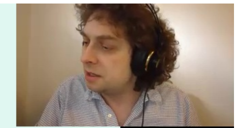


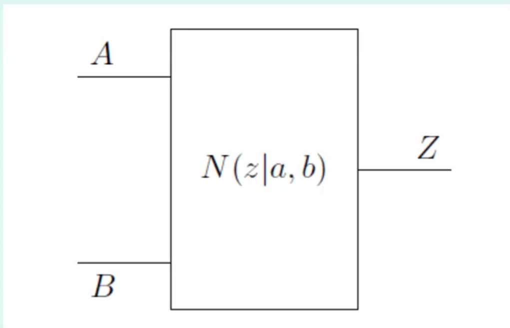
Goal: capacity region

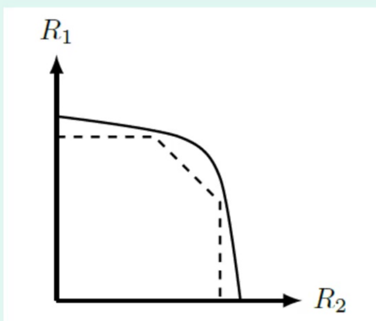
Leditzky-Alhejji-Levin-Smith,
Nature Comm. 2020



Capacity of MAC







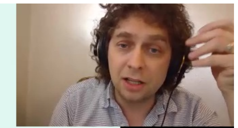
If A and B are Independent.
Can achieve:

$$R_1 \leq I(A;Z|B)$$
$$R_2 \leq I(B;Z|A)$$
$$R_1 + R_2 \leq I(A,B;Z).$$

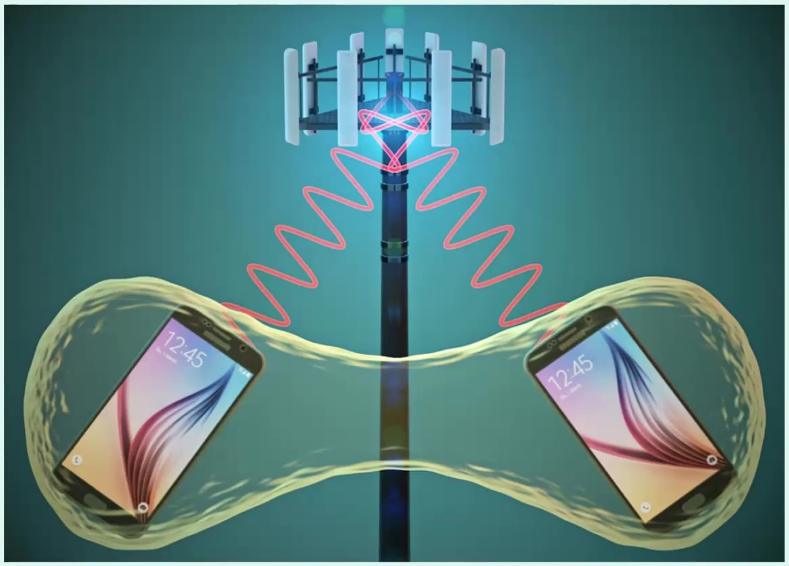
I(A;Z|B) = H(AB)+H(ZB)-H(ABZ)-H(B)
“conditional mutual information”

Take the convex hull,
that’s the capacity region.

Ahlswede and Liao ’72
See also, Cover & Thomas textbook



MAC + entanglement:
Two very different resources that work well together



1) Entanglement boosts capacity region of classical MAC
(contrast to 1→ 1 classical channel)

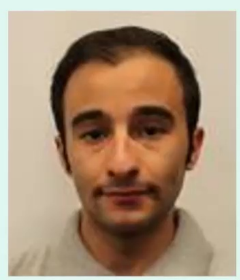
2) Fixed size classical channel may require infinite entanglement to reach capacity

3) Classical MAC has single-letter formula, but it's NP-hard to evaluate

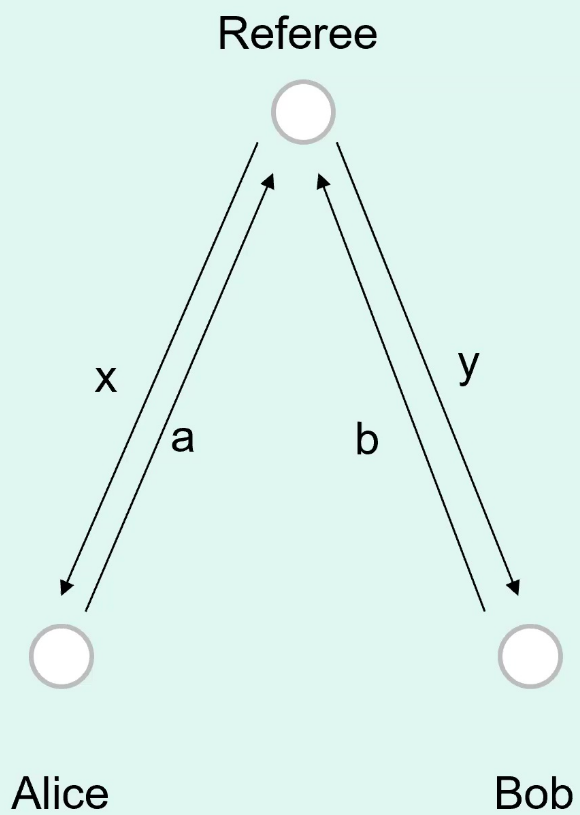
Basic idea: Force two senders to win a nonlocal game (aka violate a bell inequality): if they win, message sent faithfully, if they lose, randomize it.

(related: Quek-Shor '17,
Noetzel-Winter '20)

Note: entanglement assistance
Doesn't help regular classical channel



Nonlocal Game



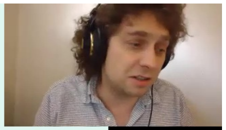
Alice and Bob are separated.

A referee sends question x to Alice and question y to Bob according to known distributions.

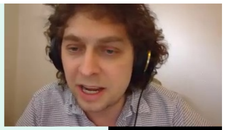
Alice replies with a, Bob replies with b.

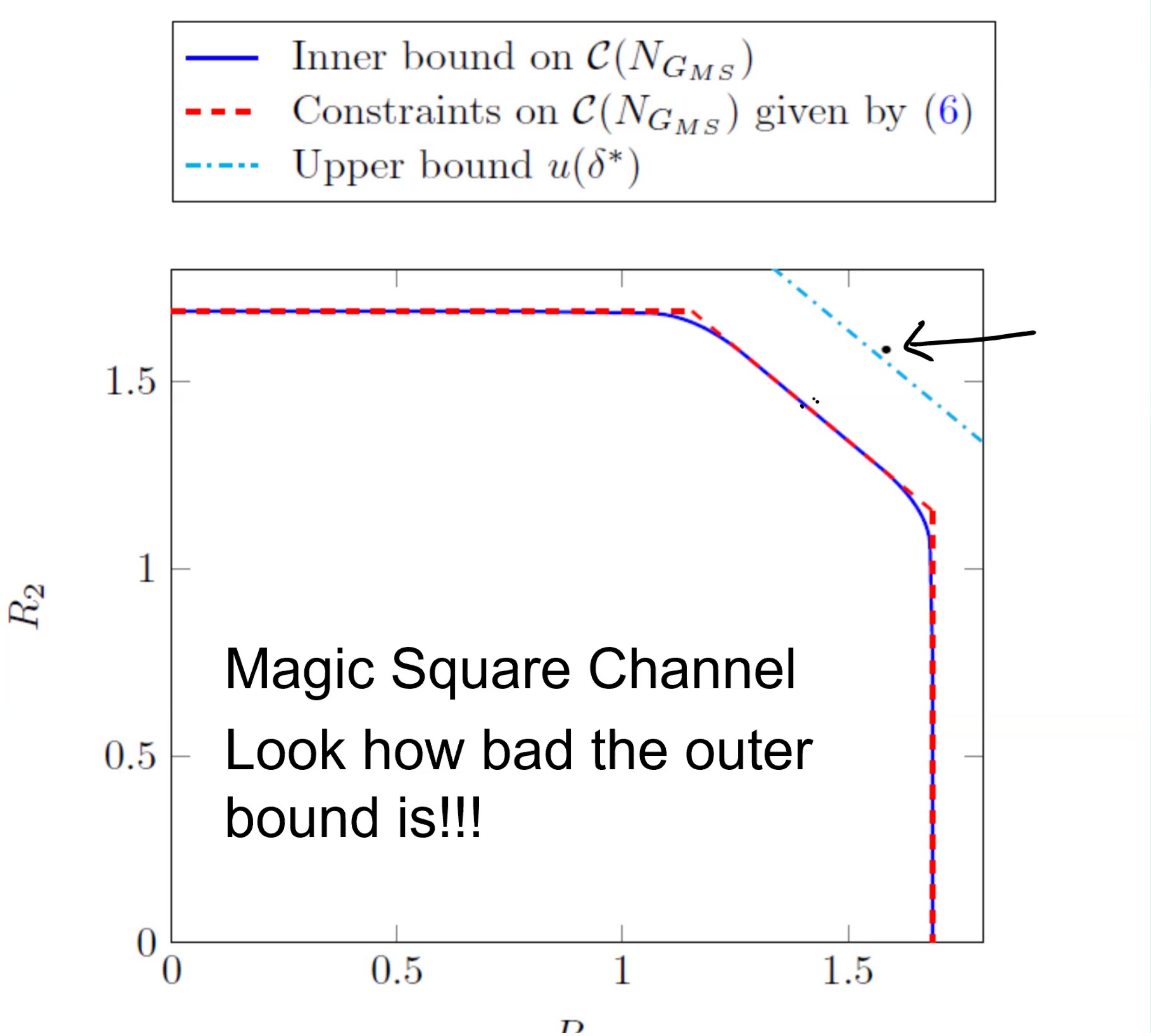
Rules of game say which question-answer pairs are allowed.

Can do better with entanglement.



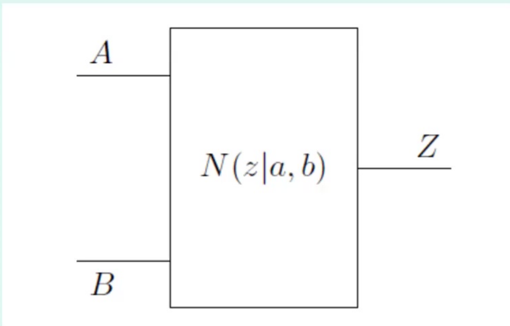
Achievable Regions with and without entanglement





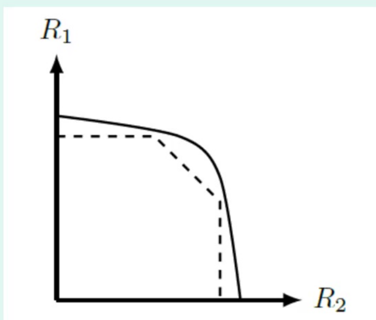
Mermin magic Square game

Outer bound for MAC: Relaxed Ahlswede-Liao region



If A and B are Independent.
Can achieve:

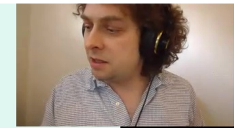
$$R_1 \leq I(A;Z|B)$$
$$R_2 \leq I(B;Z|A)$$
$$R_1 + R_2 \leq I(A,B;Z).$$

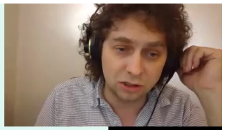


$I(A;Z|B) = H(AB)+H(ZB)-H(ABZ)-H(B)$
“conditional mutual information”

Take the convex hull,
that’s the capacity region.

Ahlswede and Liao ’72
See also, Cover & Thomas textbook





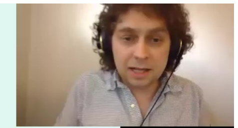
MACs summary and outlook

- Entanglement doesn't help point-to-point classical channel.
- MAC: simplest classical network. 2 senders 1 receiver.
- Capacity region boosted by entanglement between senders. Force senders to play a nonlocal game.
- Construction shows NP-hard to evaluate MAC region.

Does entanglement help more natural channels?

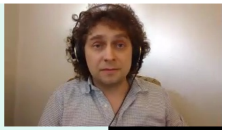
Efficient outer bound that's tighter than relaxed A-L region?

How classical and quantum networks best work together?

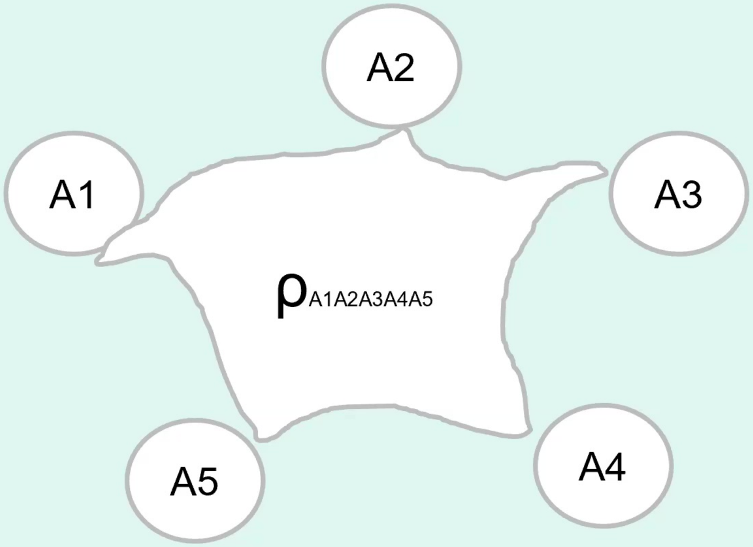


Outline

- ~~Information Theory Basics~~
- ~~Quantum Capacity~~
- ~~Additivity and nonadditivity~~
- ~~Quantum boost for classical networks~~
- Quantifying quantum correlations



Quantifying Quantum Correlations



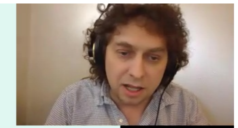
Given a mixed multiparty state ρ,
how much correlation does it hold,
and what kinds of correlations are they?
What are they good for?
How hard are they to make?
Are they classical or quantum?

Entanglement entropy works for two party pure states.

For two party mixed states, we know a lot.

We especially want to understand more than two parties:
Gives more refined information, Tools for understanding quantum networks, many body quantum systems (e.g., topological entanglement entropy appears to be at least 3 party)

Alhejji-Smith IEEE TIT 2020, Levin-Smith IEEE TIT 2020, DeWolfe-Levin-Smith PRD 2020



Optimized formulas

Coherent information:

$$Q^{(1)}(N) = \frac{1}{2} \max_{|\psi\rangle_{RA}} [I(R;B) - I(R;E)]$$

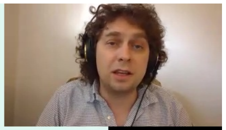
Entanglement assisted capacity:

$$C_e(N) = \max_{|\psi\rangle_{RA}} I(R;B)$$

Squashed entanglement:

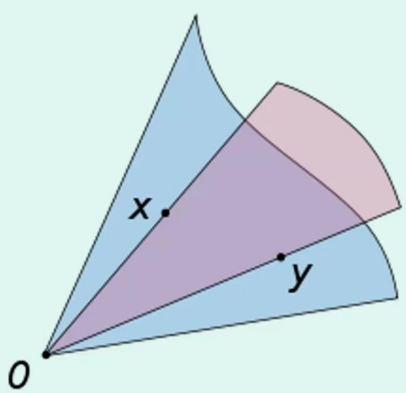
$$E_{sq}(\rho_{AB}) = \frac{1}{2} \inf I(A;B|E)$$

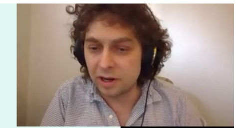
Where I(A;B|E) = S(AE)+S(BE)-S(ABE)-S(E) and $\rho_{AB} = Tr_E \rho_{ABE}$



Bipartite Correlation measures

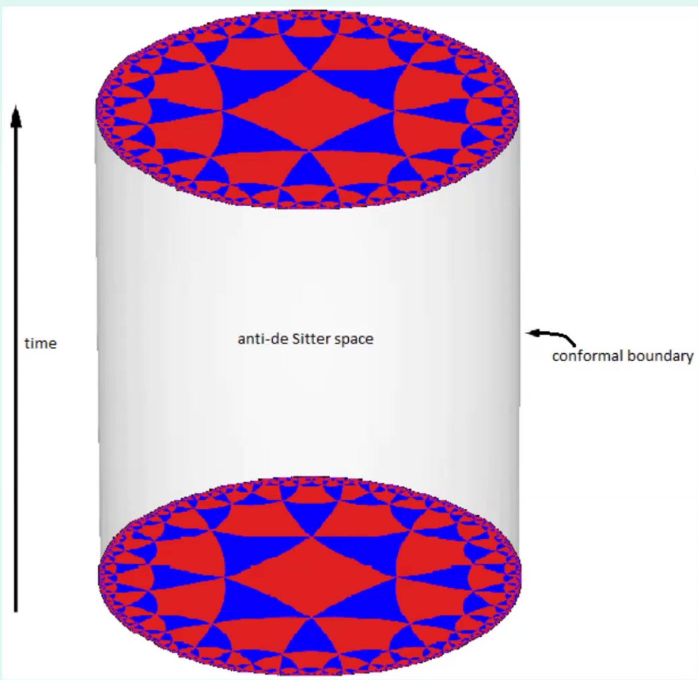
- $E_P = \underline{\inf\left(S(AV)\right)}$
- $E_Q = \frac{1}{2}\inf\left(S(A) + S(B) + S(AV) - S(BV)\right)$
- $E_R = \frac{1}{2}\inf(S(AB) + S(A|V) - S(B|AV))$

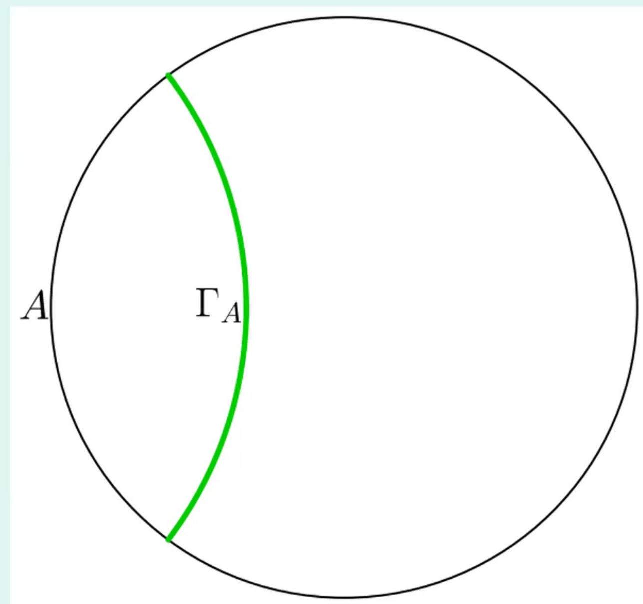




Detour: Correlations in the AdS/CFT Correspondence

CFT on boundary of asymptotically AdS spacetime <==>
Quantum gravity theory in the bulk

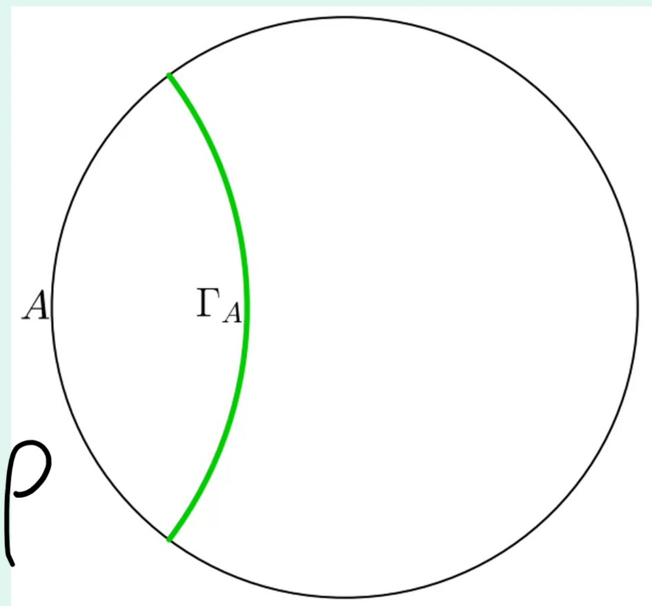




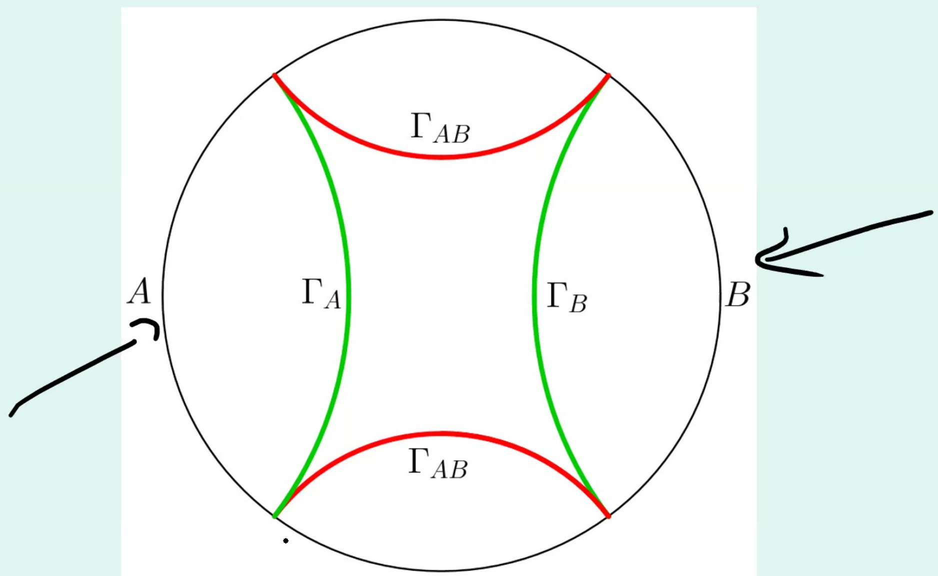
$$S(A) = \frac{Area(\Gamma_A)}{4G_N}$$

(Ryu and Takayanagi 2006)

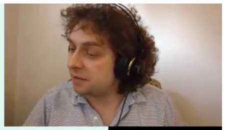
Ryu-Takayanagi formula and the entanglement wedge

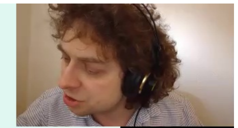


$$S(A) = \frac{Area(\Gamma_A)}{4G_N}$$

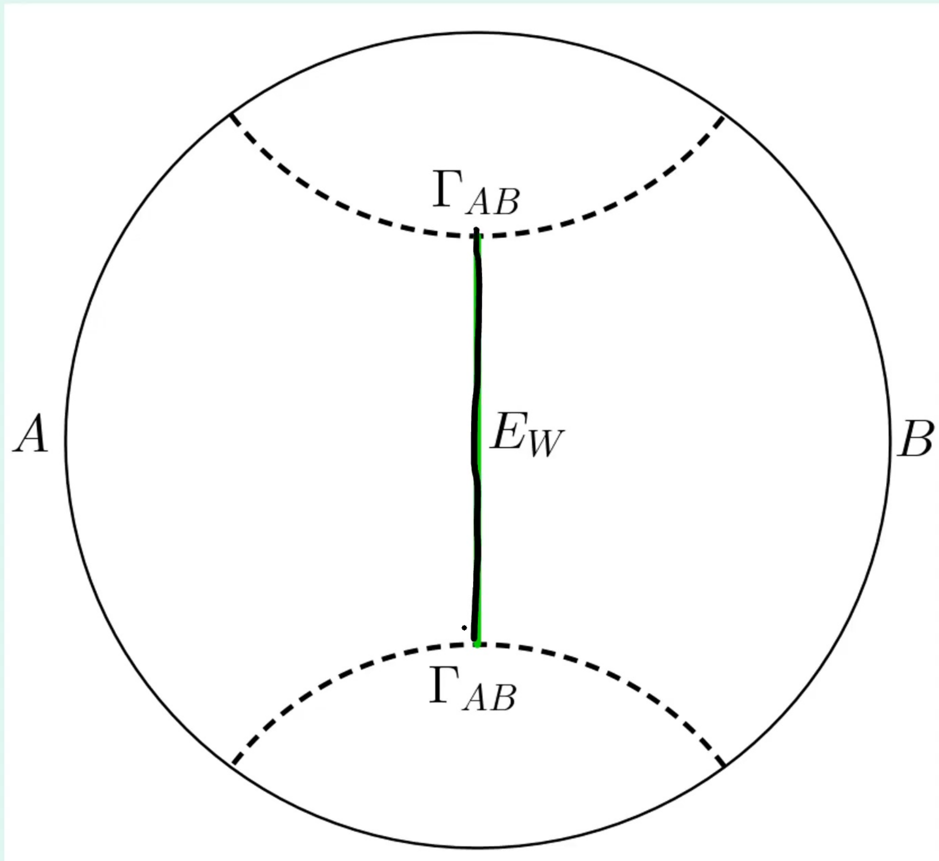


Entanglement wedge of A:
bulk region bounded by A and Γ_A.

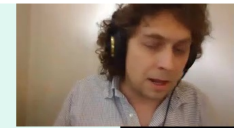




Conjecture: $E_P(\rho_{AB}) = \frac{E_W(\rho_{AB})}{4G}$

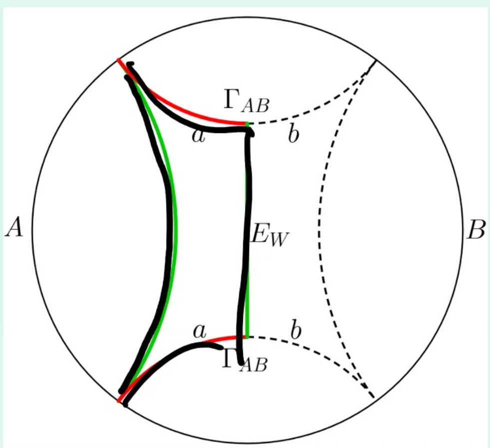


Takayanagi/Umemoto 18, Swingle et al 18

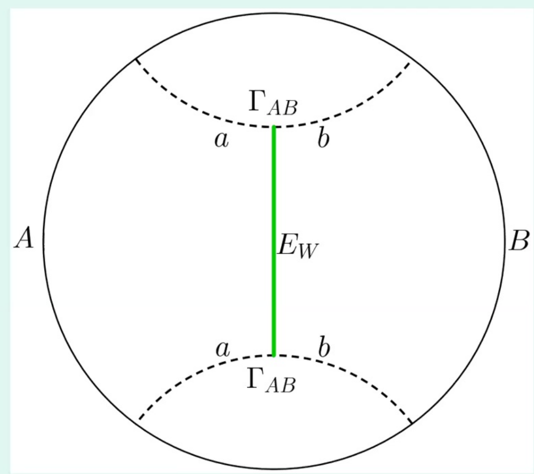


Bipartite correlation measures

- $E_Q = \frac{1}{2}\min[S(A) + S(B) + S(Aa) - S(Ba)]$
- $E_R = \frac{1}{2}\min[S(AB) + S(B|a) - S(A|Ba)]$
- $S(A) = E_Q(A{:}B) + I_{ss}(E\rangle A)$

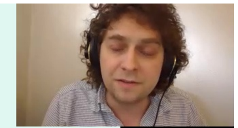


EQ



ER

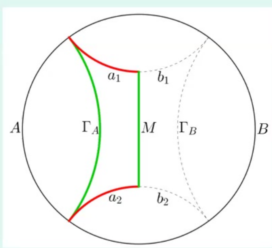
Levin-DeWolfe-Smith PRD 2020



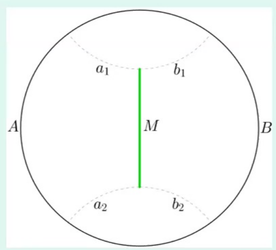
Multiparty correlations

Bipartite Optimized Correlation Measures

$$E_Q(A:B) = \frac{1}{2} \inf_{|\psi\rangle_{AaBb}} [I(Aa:B) + I(A:b)]$$
$$E_R(A:B) = \frac{1}{2} \inf_{|\psi\rangle_{AaBb}} [I(Aa:B) + I(A:b|a)]$$

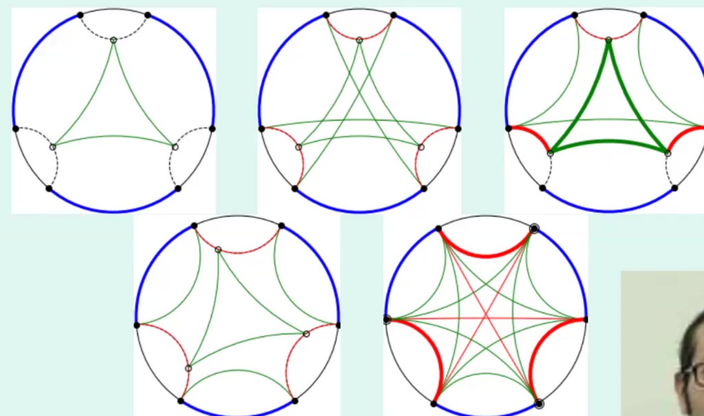


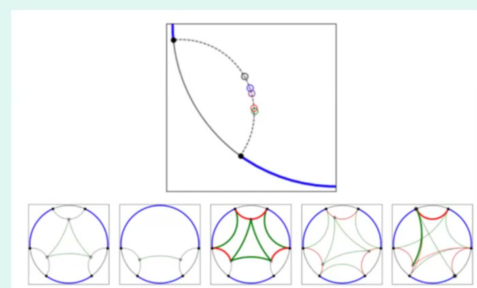
$2E_Q(A:B)$

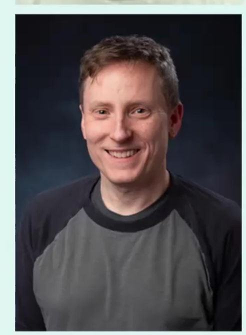


$E_R(A:B) = E_P(A:B)$

Tripartite Optimized Correlation Measures



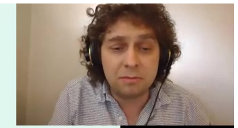




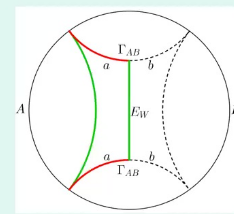
Even the vacuum is very interesting!

Goal: use these correlation measures to access geometrical information about the entanglement wedge

DeWolfe-Levin-Smith PRD 2020

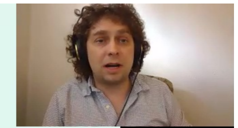


Multiparty correlations and holography



- Holographic states: useful tool for understanding quantum information
- Gives a care where we can evaluate distillable entanglement $I_{ss}(E\rangle A)$
- Seem nice enough that additivity is more common ($E_P$is not thought to be additive in general, but is here)
- Seeds conjectures: e.g.,

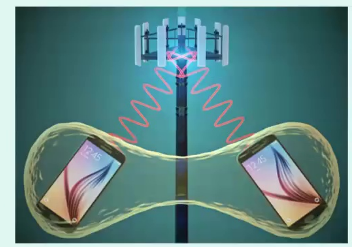
$$E_P^{\infty}(\rho_{AB}) = \lim \frac{1}{\mathrm{n}} E_P\left(\rho_{AB}^{\otimes n}\right) = E_R(\rho_{AB})\ ?$$



Summary

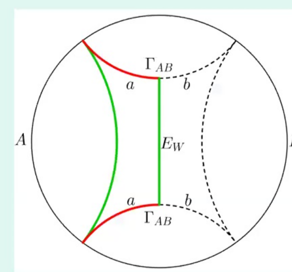
- Interaction between many quantum resources is nonadditive.

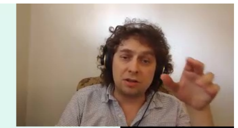
Challenge: hard to evaluate capacities, understand
Opportunity: possibility of finding better recipes, effects



- Classical MAC + entanglement: specific nontrivial interaction. Unexpected richness of classical network.

- Nice/axiomatic correlation measures capture different sorts of multiparty correlations. Operational understanding TBD. Admit geometrical interpretations for holographic states.





THANK YOU