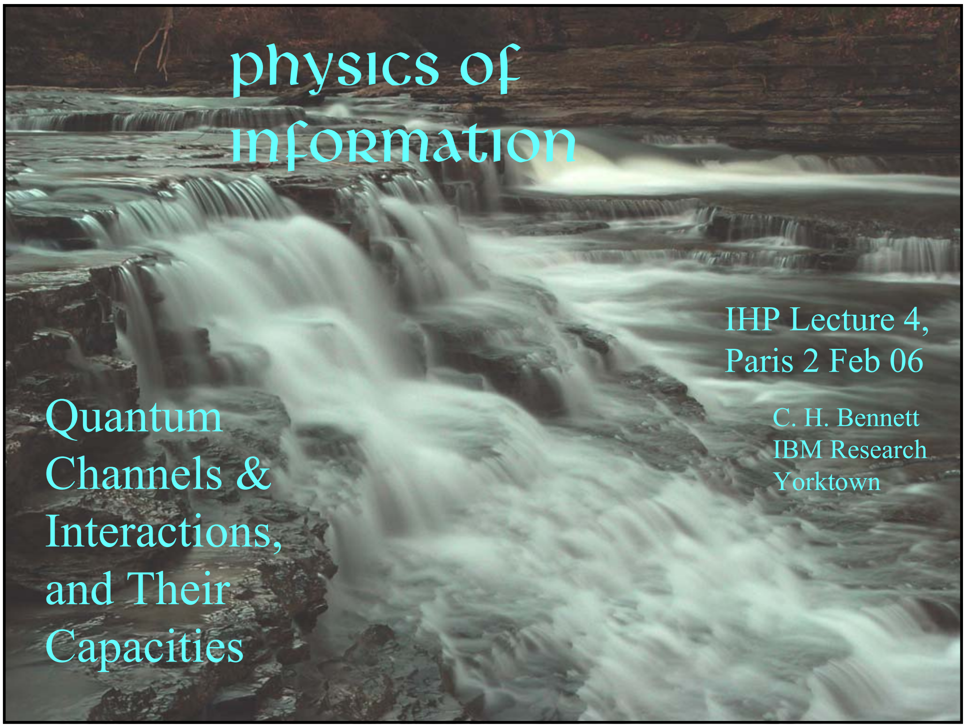


Classical Information Theory Background

- Why Auxiliary Resources (shared randomness and back communication) don't increase capacity
- Classical reverse Shannon theorem

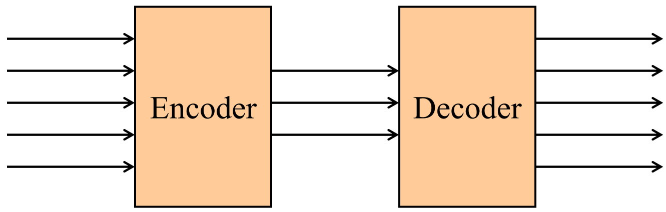
Quantum Channels: Why so many capacities?

- Why Entanglement can increase capacity
- Naturalness of Entanglement Assisted Capacity, quantum reverse Shannon theorem
- Why classical communication can increase quantum capacity

Approximate randomization and quantum data hiding

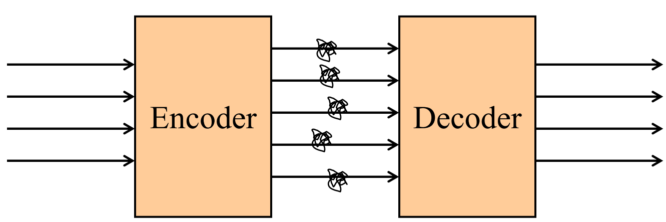
Interaction as a Resource: Capacities of interactions and isometries

Classical Communication Theory—central notions
•Data Compression and Source Entropy
•Error-correcting Codes and Channel Capacity



If an information source is redundant (due to unequal letter frequencies or correlations among letters) its output can be **compressed**, then faithfully recovered at the receiving end. A source's ***Shannon Entropy*** is the compressed size above which faithful recovery is possible, and below which it is impossible.

Classical Communication Theory—central notions
•Data Compression and Source Entropy
•Error-correcting Codes and Channel Capacity



Error correcting codes can be used to send information with arbitrarily high reliability through a noisy channel at any rate up to but not exceeding the channel's ***Capacity***. Simplest error correcting code is triple repetition.

The Shannon entropy of a source X and the capacity of a noisy channel $\mathcal{N}$ both have simple mathematical expressions.

$$H(X) = -\Sigma_x \; p(x) \log p(x),$$

where $p(x)$ is the probability that the random variable X takes the value x.

$$C(\mathcal{N}) = \max_X \; [\, H(X) + \mathrm{H}(\mathcal{N}(X)) - \mathrm{H}(X,\mathcal{N}(X)) \,]$$

In other words, a channel's capacity is the maximum, over input distributions, of the Shannon *mutual information* between input and output.

Besides characterizing sources and channels, classical information theory aims to understand the role of auxiliary resources, such as ***shared randomness*** between sender and receiver, and free ***back communication*** (feedback) from receiver to sender.

Their role is simple: neither shared randomness nor back communication increases the capacity of a classical channel.

$$C_R = C_B = C$$

(However shared randomness, in the form of a one-time pad, makes it possible to communicate ***secretly*** over a public channel. Back communication, though it doesn't increase capacity, reduces encoding/decoding effort and latency.)

Shared randomness is also useful in characterizing the ability of channels to simulate one another.

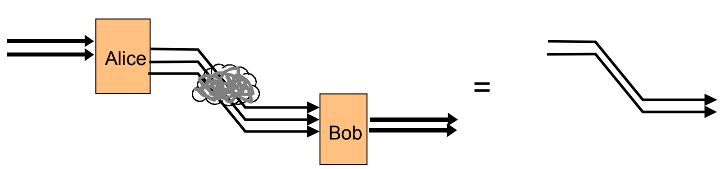
The classical *Reverse Shannon Theorem* states that in the presence of shared randomness the capacity of a channel $\boldsymbol{M}$ to simulate another channel $\boldsymbol{N}$ is simply the ratio of their plain capacities.

$$C_R(\boldsymbol{M},\boldsymbol{N}) = C(\boldsymbol{M}) / C(\boldsymbol{N})$$

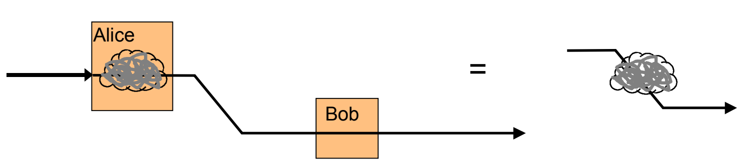
More precisely, it establishes the ability of $\boldsymbol{M}$, with shared randomness, to exactly simulate the input:output behavior of $\boldsymbol{N}$ on any block size, at an expected rate approaching $C(\boldsymbol{M})/C(\boldsymbol{N})$ in the limit of large block size. (BSST quant-ph/0106052, Winter quant-ph/0208131)

A question so silly it was not asked for the first 50 years of information theory: "Can a noiseless channel efficiently simulate a noisy one?"

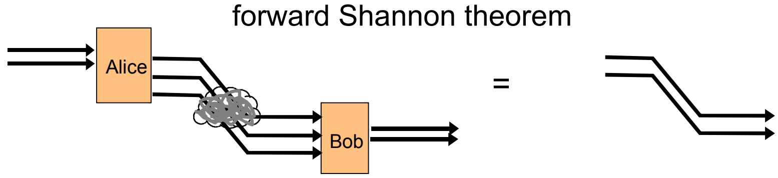
Classical Shannon Theorem:
A noisy channel can simulate a noiseless channel



Homer Simpson's Reverse Shanon's Theorem:
A noiseless channel can simulate a noisy channel.

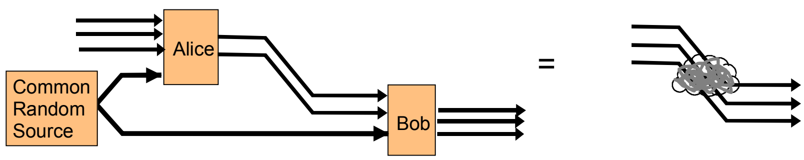


forward Shannon theorem



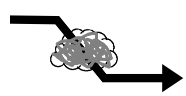
A Better Reverse Shannon Theorem *(quant-ph/0106052)*

In the presence of shared random information between sender and receiver, a noiseless channel can asymptotically simulate a noisy one ***of equal capacity.***

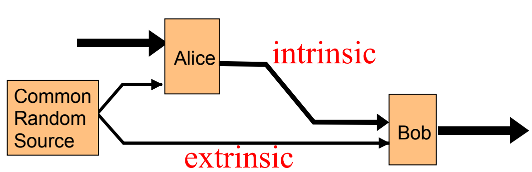


Therefore, in the presence of shared random information, all classical noisy channels are asymptotically equivalent.

In the large m limit, sending m bits through the noisy channel



can be simulated by sending about mC noiseless "intrinsic" bits, which Alice chooses with the help of the input,



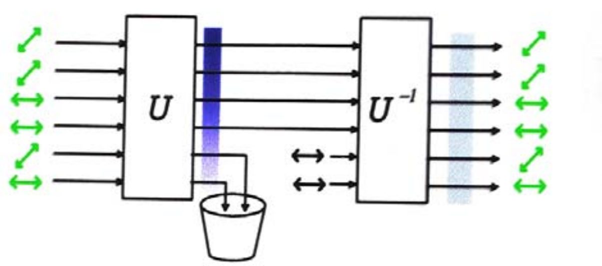
together with "extrinsic" random bits, which have nothing to do with the channel input, and so can be preagreed before Alice receives the input.

Why don't shared randomness and feedback improve the capacity of a classical channel?

Shared randomness doesn't help because any encoder/ decoder pair trying to simulate a noiseless channel can be *derandomized:* If the encoder/decoder pair works when the shared information R is chosen randomly, there must be a particular value $R=r$ for which it also works. Picking this r and always using it gives a deterministic encoder/decoder that works at least as well as the randomized one.

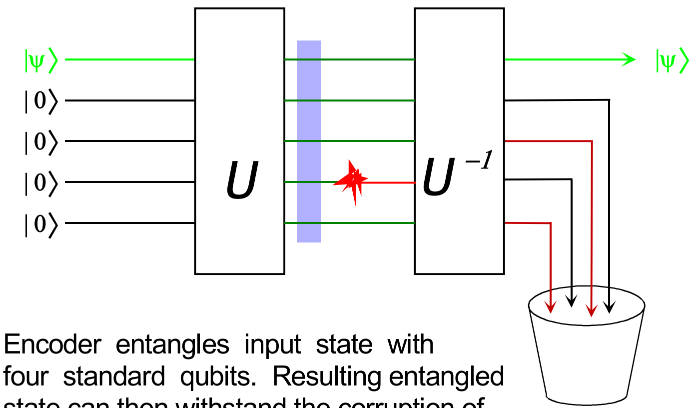
Feedback doesn't help because of the reverse Shannon theorem. If feedback helped a noisy channel, it would help a noiseless one, which would violate causality. If I say n bits to you and by talking back you could learn more than n bits about what I intend to say, you could learn something by preemptively guessing.

Quantum Data Compression



A source emitting 0 and 45 degree photons has a peculiarly quantum kind of redundancy because the states are nonorthogonal. Schumacher compression squeezes out this redundancy with arbitrarily little disturbance in the limit of large block size. More generally any quantum source ρ can be compressed to a size equal to its von Neumann entropy $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$, but no smaller.

Quantum Error Correcting Code

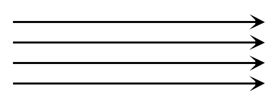


Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

Some Simple Quantum Channels

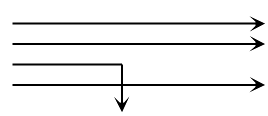
Noiseless Qubit Channel

input qubit undisturbed



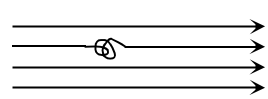
Quantum Erasure Channel

input qubit sometimes lost



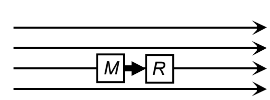
Depolarizing Channel

input qubit sometimes randomized

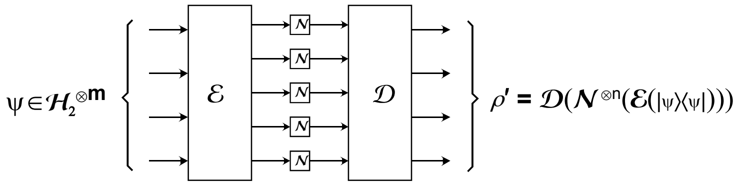


Dephasing Channel

input qubit sometimes gets measured and re-sent en route.



Plain C and Q capacities defined using block encoder and decoder



Quantum capacity Q of a noisy quantum channel $\mathcal{N}$:

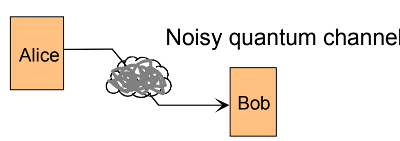
$$Q(\mathcal{N}) = \max\{\, r : \forall \varepsilon\ \overset{\infty}{\exists} mn\ (m/n > r)\ \&\ \forall_{\psi \in \mathcal{H}_2^{\otimes m}}\ \langle\psi|\rho'|\psi\rangle > 1-\varepsilon \,\}$$

Classical capacity C is given by a similar expression,

$$C(\mathcal{N}) = \max\{\, r : \forall \varepsilon\ \overset{\infty}{\exists} mn\ (m/n > r)\ \&\ \forall_{\mathbf{x} \in \{0,1\}^m}\ \langle\mathbf{x}|\rho'|\mathbf{x}\rangle > 1-\varepsilon \,\},$$

with inputs ψ restricted to product states $|\mathbf{x}\rangle$ of the $\{|0\rangle,|1\rangle\}$ basis.

Multiple capacities of Quantum Channels



Q plain quantum capacity = qubits faithfully trasmitted per channel use, via quantum error correcting codes

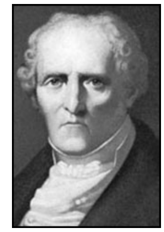
C plain classical capacity = bits faithfully trasmitted per channel use

Q_B quantum capacity assisted by classical back communication
Q_2 quantum capacity assisted by classical two-way communication
(also C_B and C_2 , but more about these later.)

C_E entanglement assisted classical capacity i.e. bit capacity in the presence of unlimited prior entanglement between sender and receiver.

For quantum channels, these assisted capacities can be greater than the corresponding unassisted capacities.

Does Free Stuff make the world better?



Robert Owen, Charles Fourier, Edward Bellamy:
Free goods & services will make everything better.

Fourier, Emma Goldman…Haight-Ashbury
Free Love will make everything better

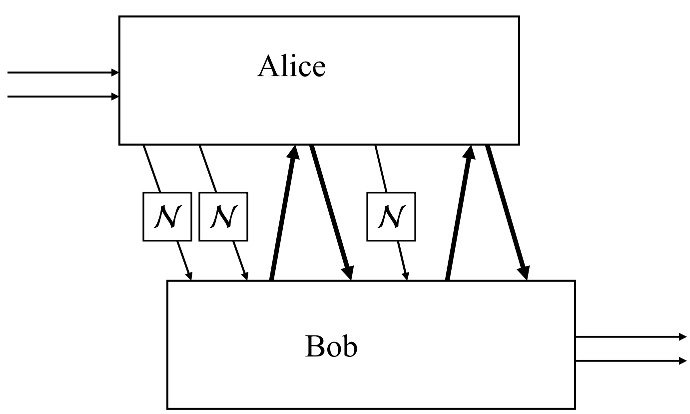
Timothy Leary, Ken Kesey:
Free LSD will make everything better

(Gutenberg, the Internet, LOCC)
Free Classical Communication

(Aram Harrow, ITP2001 poster session)
Will **Free Entanglement** change the world?

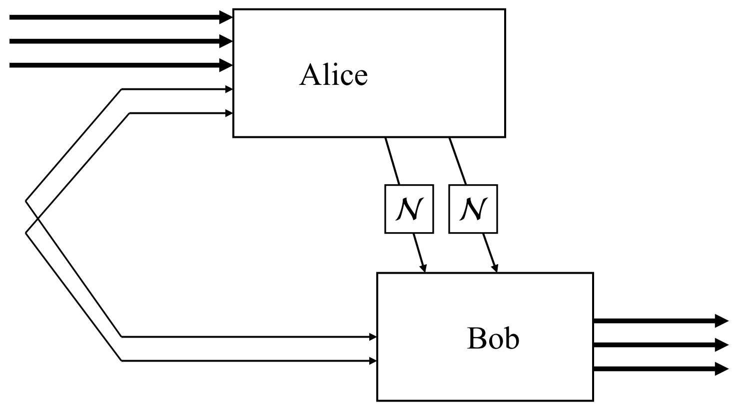
At least it simplifies the theory of quantum interactions & channels.

Free classical communication gives Q_2, the classically assisted quantum capacity, e.g. by entanglement sharing, distillation, and teleportation



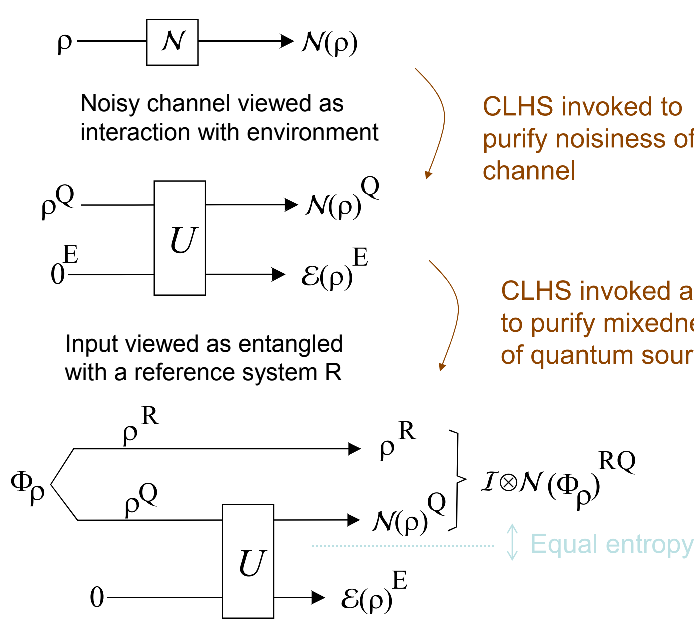
Unfortunately, no simple expression is known for this capacity.

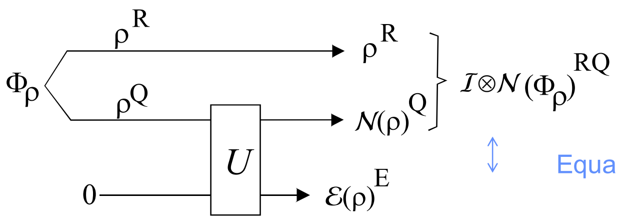
Providing unlimited free entanglement gives C_E ,
the entanglement-assisted classical capacity.



By contrast free entanglement does greatly simplify capacity theory: C_E is given by a simple expression; and in the presence of free entanglement all quantum channels of equal C_E can simulate one another with unit asymptotic efficiency.

Church-of-the-Larger-Hilbert-Space view of quantum sources and channels





Entropic quantities related to channel capacities.

= if min. output entropy is additive Shor '03

C =? Holevo capacity = $\max_{\{p_i,\rho_i\}} \; S(\mathcal{N}(\rho)) - \Sigma p_i\, S(\mathcal{N}(\rho_i))$

Shor, Lloyd, Devetak '02-'03

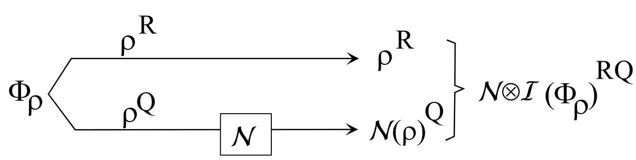
Q = Coherent Info. = $\lim_{n\to\infty} \max_{\rho} \; S(\mathcal{N}^{\otimes n}(\rho)) - S(\mathcal{E}^{\otimes n}(\rho))/n$

C_E = Quantum Mutual Info. = $\max_{\rho} \; S(\rho) + S(\mathcal{N}(\rho)) - S(\mathcal{E}(\rho))$ BSST '01

$Q_2 \approx$ Distillable entanglement = $\lim_{n\to\infty} \max_{\rho} D_2(\mathcal{I}\otimes\mathcal{N}^{\otimes n}(\Phi_\rho))/n$ = ?

(Unfortunately D_2 has no simple expression, may be nonconvex)

(entangled purification of ρ)

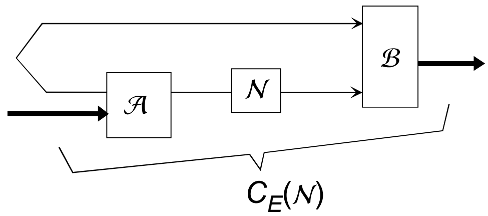


$$C_E(\mathcal{N}) = \max_\rho \quad S(\rho) + S(\mathcal{N}(\rho)) - S(\mathcal{N}\otimes\mathcal{I}(\Phi_\rho))$$

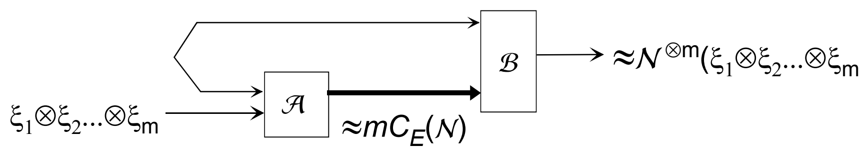
Entanglement-Assisted capacity C_E of a quantum channel $\mathcal{N}$ is equal to the maximum, over channel inputs ρ, of the input (von Neumann) entropy plus the output entropy minus their "joint" entropy (more precisely the joint entropy of the output and a reference system entangled with the late input) (BSST 0106052, Holevo 0106075).

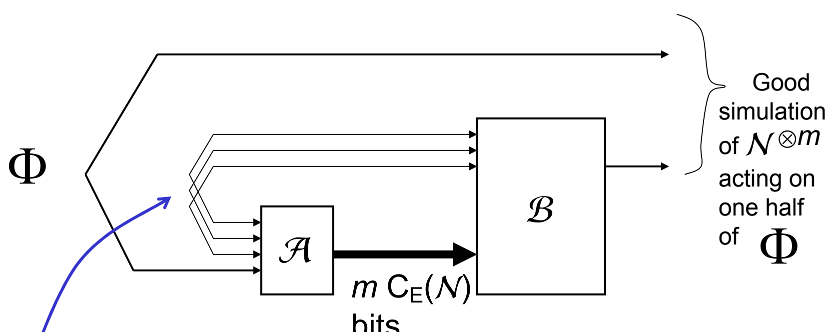
In retrospect, ***entanglement-assisted capacity***, not plain classical capacity, is the natural quantum generalization of the classical capacity of a classical channel.

$Q_E = C_E / 2$ for all channels, by teleportation & superdense coding.



Quantum Reverse Shannon Theorem (QRST): Any quantum channel can be simulated by shared entanglement and an amount of classical communication equal to the channel's entanglement-assisted capacity. Therefore, in a world full of entanglement, all quatum channels are qualitatively equivalent, and quantitatively can be characterized by a single parameter.

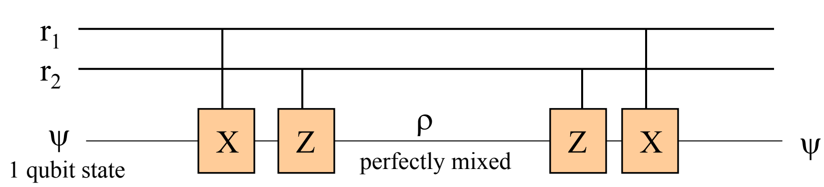




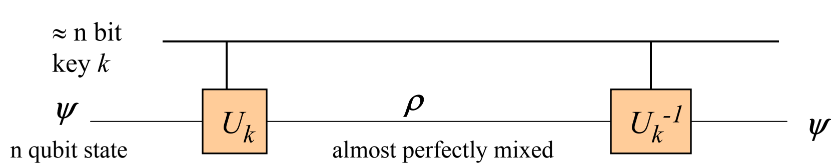
Unexpected complication: Some quantum channels, on general non-product inputs, require a stronger form of entanglement resource than standard EPR pairs, the so-called entanglement-embezzling states of Hayden and van Dam (quant-ph/0201041) in order to be simulated at a forward communication cost not exceeding their C_E. Or they can be simulated with standard EPR pairs and some *backward* communication in addition to the forward communication.

Private Quantum Channels:

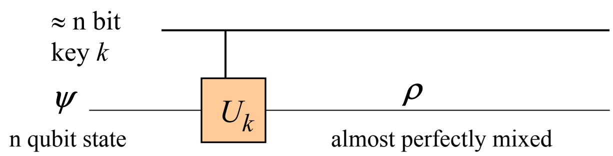
It is well known that two random key bits are necessary and sufficient to perfectly encrypt a qubit, so that regardless of the input ψ, the intermediate "ciphertext" looks completely mixed. Quantum analog of One Time Pad.

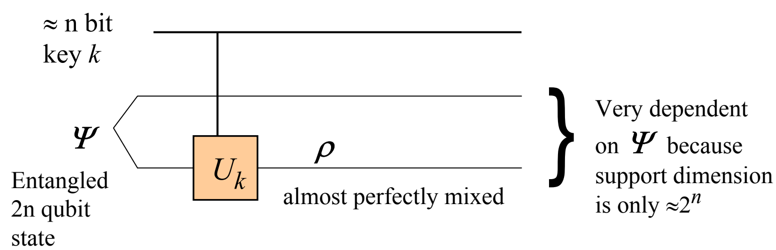


But if we are willing to settle for asymptotically perfect encryption, then in the limit of large block size, only half as much key is needed.

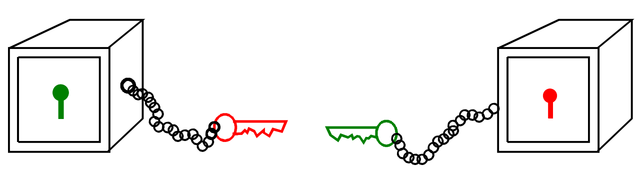


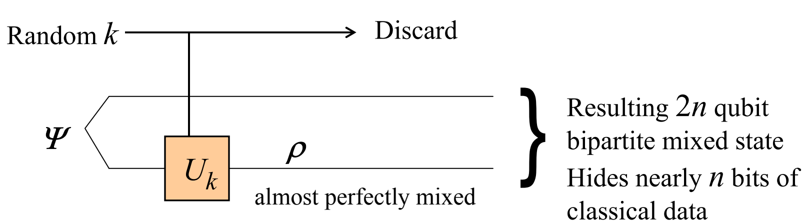
Curiously, this encryption, while hiding pure states almost perfectly, does not hide entangled states well at all. (Hayden, Leung, Shor, Winter 0307104)





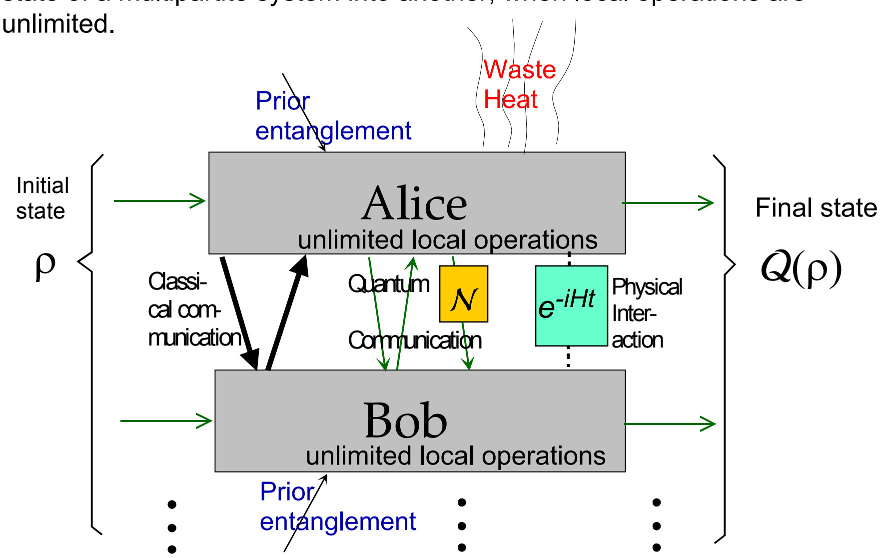
Data Hiding: A multipartite state which stores classical data that can be recovered by a joint measurement, but not by any sequence of local measurements and classical communication. Like 2 locked boxes each chained to the other's key .





Interaction as a Resource

An important goal of quantum information theory is to understand the nonlocal resources, and tradeoffs among them, needed to transform one state of a multipartite system into another, when local operations are unlimited.



These questions can be asked in an exact setting

$$\rho \longrightarrow Q(\rho)$$

or in the regularized asymptotic setting characteristic of information theory, where one seeks to transform many copies of the input state into a high-fidelity approximation to many copies of the desired output state

$$\rho^{\otimes n} \longrightarrow \approx Q(\rho)^{\otimes n}$$

By appropriate choice of the transformation Q which one seeks to implement (a completely positive trace preserving map on multipartite states), one can define state properties like distillable entanglement, and many sorts of channel capacity

Interaction between two systems, by a gate or Hamiltonian, is a fundamental physical resource, which may be viewed as a bidirectional channel

How efficiently can interactions be used
- to generate entanglement
- to perform classical communication
- to simulate other interactions

Kinds of Interaction

Unitary gate or Hamiltonian: U or e^{-iHt}

Nonunitary (interaction involves other, inaccessible systems): nonlocal TPCP map

$\mathcal{N}$ or $d\rho/dt = \mathcal{L}[\rho]$

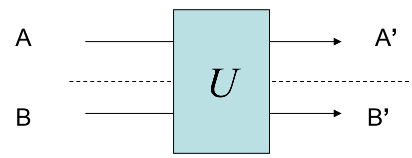
All nonlocal unitary interactions are *qualitatively* equivalent because they can produce entanglement and perform bidirectional classical communication. These resources are sufficient to perform any other nonlocal action, eg by teleportation.

But is there a single scalar measure of an interaction's "strength"? Or are some interactions better for some jobs and others for other jobs?

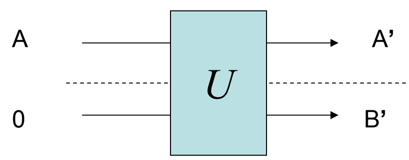
Nonunitary interactions (bilocal TPCP maps), are not even qualitatively equivalent: eg some can generate entanglement but not communicate, some can communicate but only classically, or only unidirectionally, and some, such as the Popescu-Rohrlich "Non-local boxes" cannot communicate in either direction and yet are a nontrivial resource in that they reduce communication complexity.

Gates, Isometries and Channels

Gate

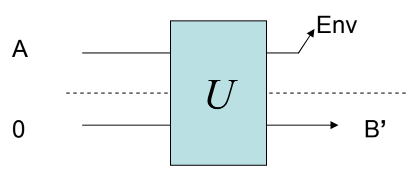


Isometry,
a.k.a.
channel
with quantum
feedback

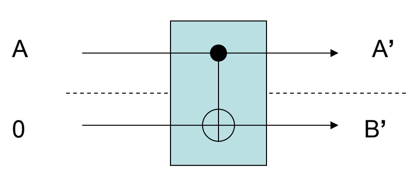


Cf classical feedback, where wlog Bob gets a *copy* of output

Channel,
a.k.a.
CPTP map



A useful isometry, the *cobit* or coherent bit (Harrow)

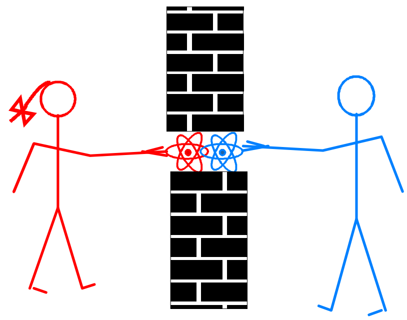


2 cobits $\rightleftarrows$ 1 ebit + 1 forward qubit

Qualitatively all interactions are equivalent:

Any nontrivial interaction can

- communicate from Alice to Bob
- communicate from Bob to Alice
- generate entanglement



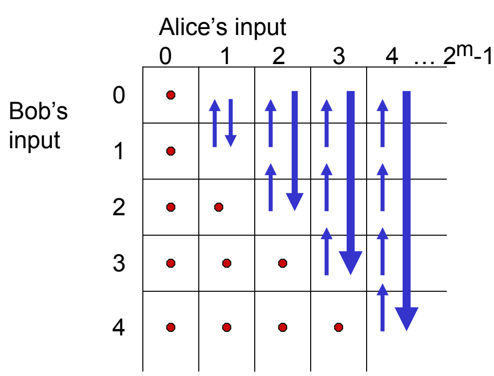
But are a gate's capacities for doing so necessarily equal?

Yes for 2x2 gates.

No for gates acting on larger Hilbert spaces

Harrow, Shor 0511219
Linden, Smolin, Winter 0511217

Gate with Asymmetric Capacities



In computational basis, gate performs a cyclic permutation of Bob's data whenever it is less than or equal to Alice's.

doesn't change Alice's data or any other data of Bob

For large *m*, forward classical capacity (A=>B) is *m* bits per channel use.

But reverse capacity is only O($\log^k(m)$)

(Harrow QIP2006 talk, HS 0511217, nontrivial proof)