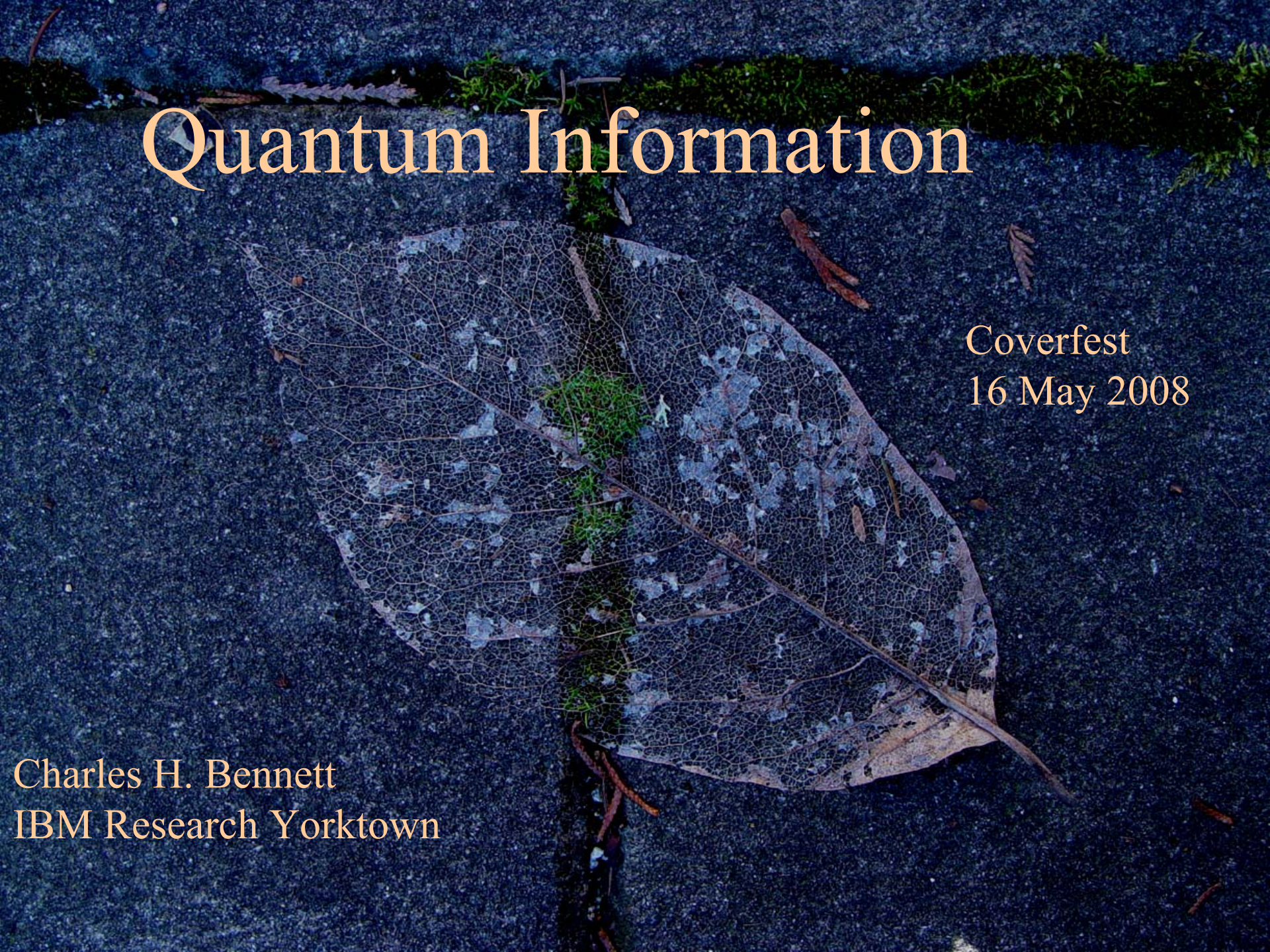
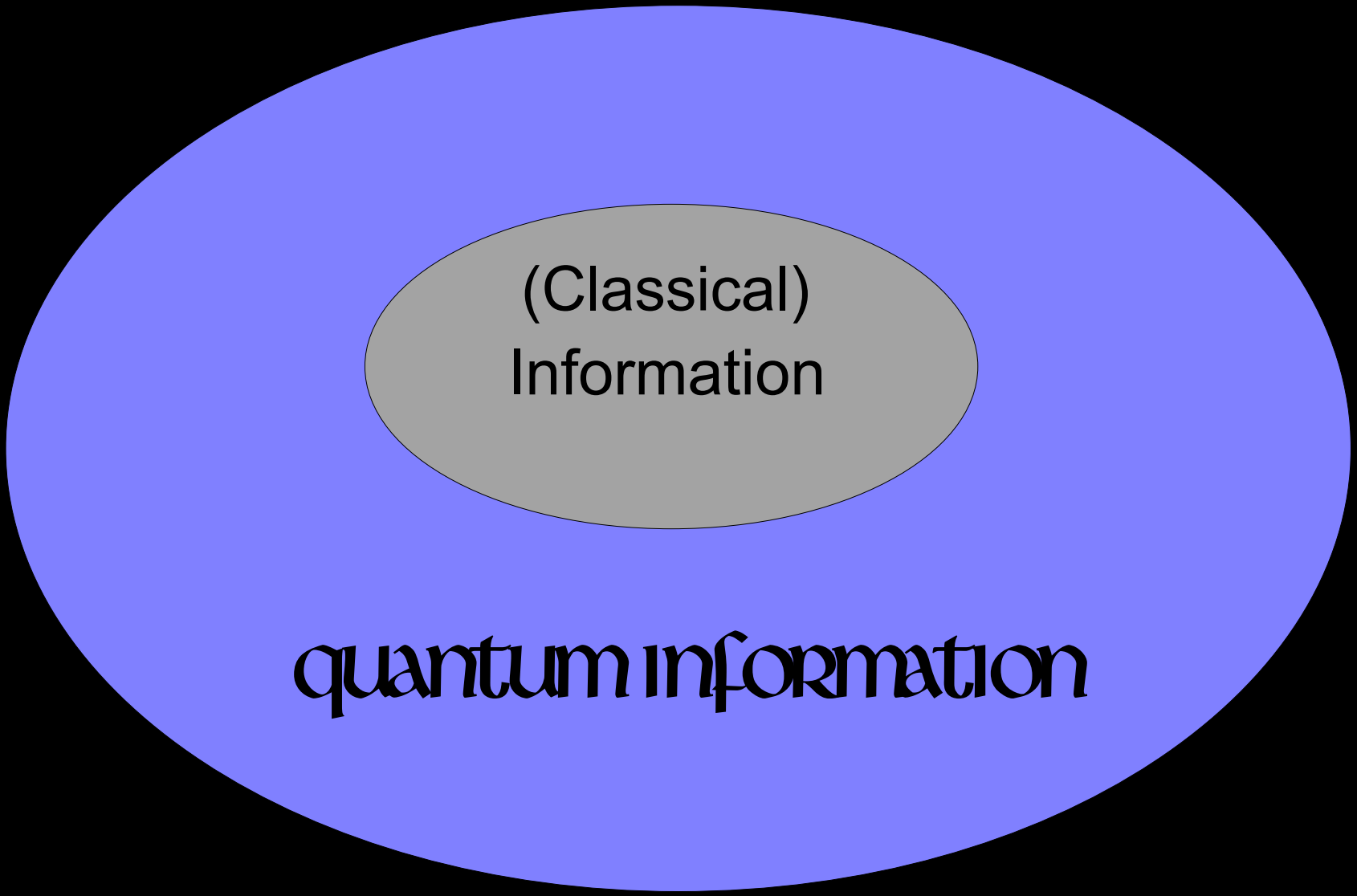


Quantum Information

Coverfest
16 May 2008

Charles H. Bennett
IBM Research Yorktown


(Classical)
Information
quantum information

Information = Distinguishability.

(Using a pencil, a piece of paper can be put into a various states distinguishable at a later time.)

- Information is reducible to bits (**0** ,**1**)

- Information processing, to reveal implicit truths, can be reduced to logic gates (**NOT**, **AND**)

- bits and gates are *fungible*, independent of physical embodiment, making possible Moore's law

- (classical) information
  - can be copied at will without disturbing it
  - cannot travel faster than light or backward in time

But information in microsopic bodies such as photons or nuclear spins obeys quantum laws. Such quantum information

- cannot be read or copied without disturbance.

- can connect two spacelike separated observers by a correlation too strong to be explained by classical communication. However, this "entanglement" cannot be used to send a message faster than light or backward in time.

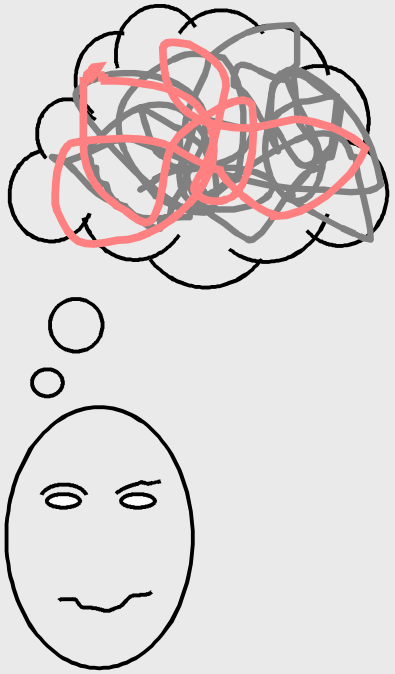
Quantum information is reducible to **qubits** i.e. two-state quantum systems such as a photon's polarization or a spin-1/2 atom.

Quantum information processing is reducible to one- and two-qubit gate operations.

Qubits and quantum gates are fungible among different quantum systems

Ordinary classical information, such as one finds in a book, can be copied at will and is not disturbed by reading it.

Quantum information is more like the information in a dream



• Trying to describe your dream changes your memory of it, so eventually you forget the dream and remember only what you've said about it.

• You cannot prove to someone else what you dreamed.

• You can lie about your dream and not get caught.

But unlike dreams, quantum information obeys well-known laws.

1. A linear vector space with complex coefficients and inner product

$$\langle \phi \mid \psi \rangle = \Sigma\, \phi_i^* \psi_i$$

2. For polarized photons two, e.g. vertical and horizonal

$$\leftrightarrow = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \updownarrow = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

3. E.g. for photons, other polarizations

$$\nearrow = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \searrow = \begin{pmatrix} +1 \\ -1 \end{pmatrix}$$

$$\circlearrowright = \begin{pmatrix} i \\ 1 \end{pmatrix} \quad \circlearrowleft = \begin{pmatrix} i \\ -1 \end{pmatrix}$$

4. Unitary = Linear and inner-product preserving.

quantum laws

I. To each physical system there corresponds a Hilbert space [1] of dimensionality equal to the system's maximum number of reliably distinguishable states. [2]

2. Each direction (ray) in the Hilbert space corresponds to a possible state of the system. [3]

3. Spontaneous evolution of an unobserved system is a unitary transformation on its Hilbert space. [4]

-- more --

4. The Hilbert space of a composite sysem is the tensor product of the Hilbert spaces of its parts. **1**

5. Each possible measurement **2** on a system corresponds to a resolution of its Hilbert space into orthogonal subspaces $\{\mathbf{P}_j\}$, where $\sum \mathbf{P}_j = 1$. On state ψ the result j occurs with probability $|\mathbf{P}_j\ \psi|^2$ and the state after measurement is

$$\frac{\mathbf{P}_j\ |\psi>}{|\mathbf{P}_j\ |\psi>|}$$

1. Thus a two-photon system can exist in "product states" such as ↔ ↔ and ↔ ↗ but also in "entangled" states such as

$$\frac{\leftrightarrow\leftrightarrow \;-\; \updownarrow\updownarrow}{\sqrt{2}}$$

in which neither photon has a definite state even though the pair together does

2 Believers in the "many worlds interpretation" reject this axiom as ugly and unnecessary. For them measurement is just a unitary evolution producing an entangled state of the system and measuring apparatus. For others, measurement causes the system to behave probabilistically and forget its pre-measurement state, unless that state happens to lie entirely within one of the subspaces $\mathbf{P}_j$.

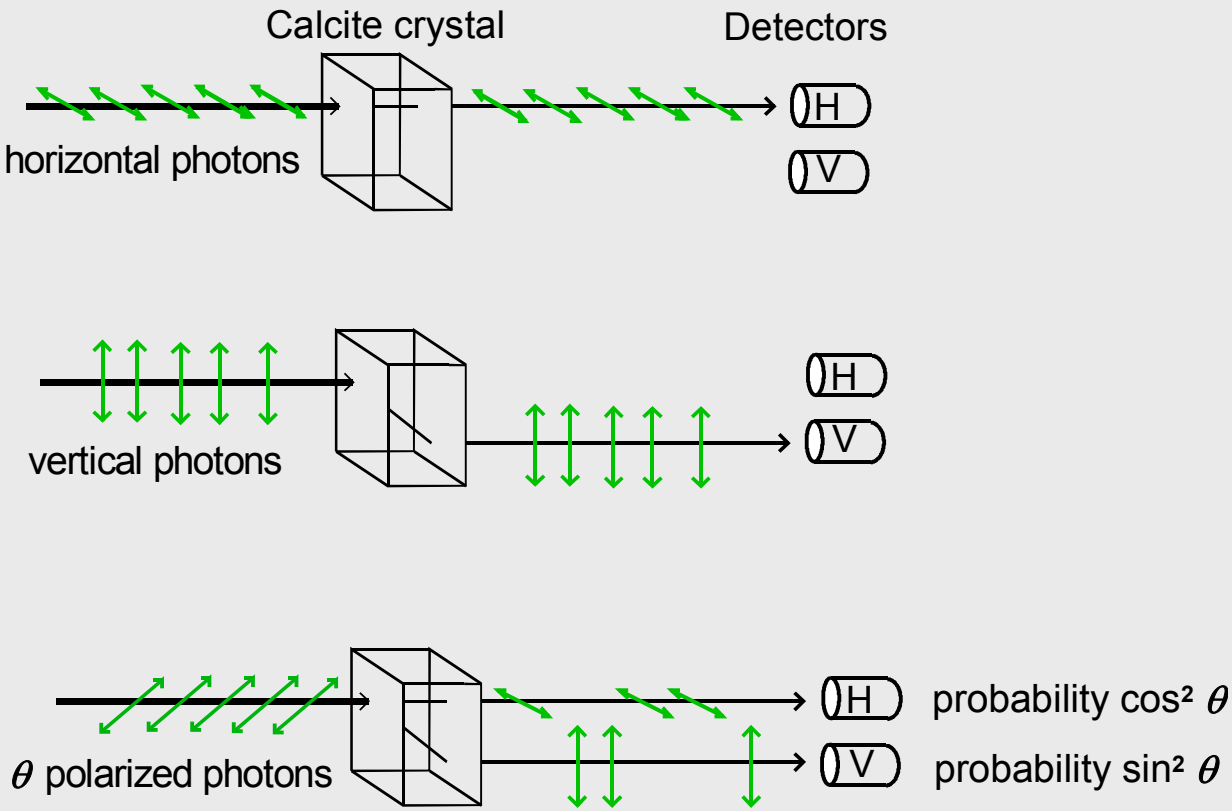
superposition principle

Between any two reliably distinguishable states of a quantum system

(for example horizontally and vertically polarized single photons)

there exists a continuum of intermediate states (representable as complex linear combinations of the original states) that in principle cannot be reliably distinguished from either original state.

(for example diagonal polarizations)



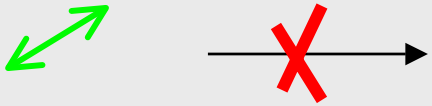
(Mathematically, a superposition is a weighted sum or difference, and can be pictured as an intermediate *direction* in space)

$$\nearrow\!\!\swarrow = \frac{\leftrightarrow + \updownarrow}{\sqrt{2}}$$

$$\nwarrow\!\!\searrow = \frac{\leftrightarrow - \updownarrow}{\sqrt{2}}$$

Non-orthogonal states like $\leftrightarrow$ and $\nearrow\!\!\swarrow$ are in principle imperfectly distinguishable. $\leftrightarrow$ always behaves somewhat like $\nearrow\!\!\swarrow$ and vice versa. This is the basis of quantum cryptography.

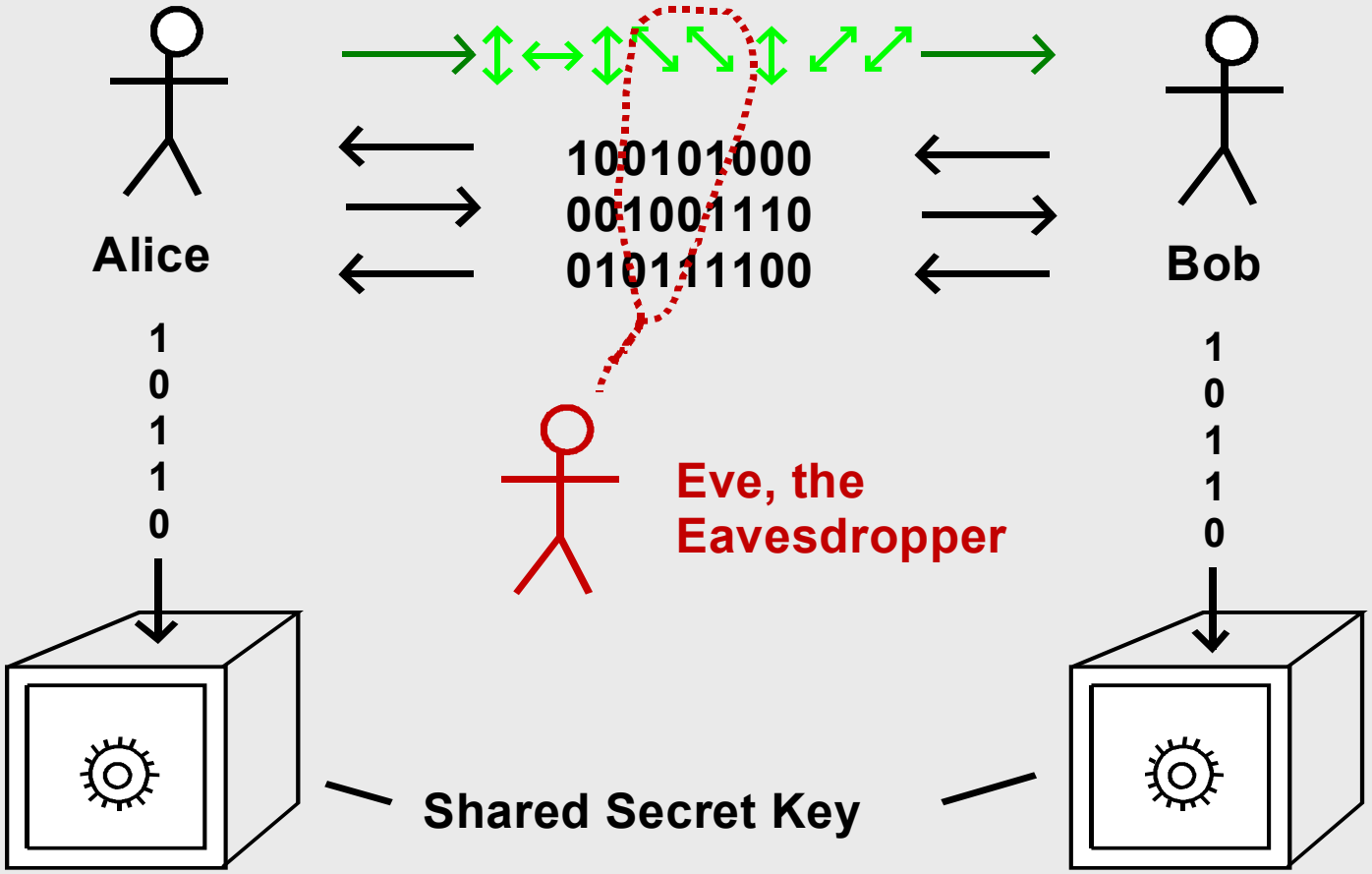
Measuring an unknown photon's polarization exactly is impossible (no measurement can yield more than 1 bit about it).



Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).

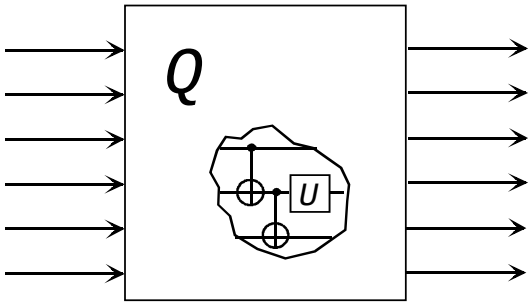
If you try to amplify an unknown photon by sending it into an ideal laser, the output will be polluted by just enough noise (due to spontaneous emission) to be no more useful than the input in figuring out what the original photon's polarization was.

Quantum Cryptographic Key Distribution



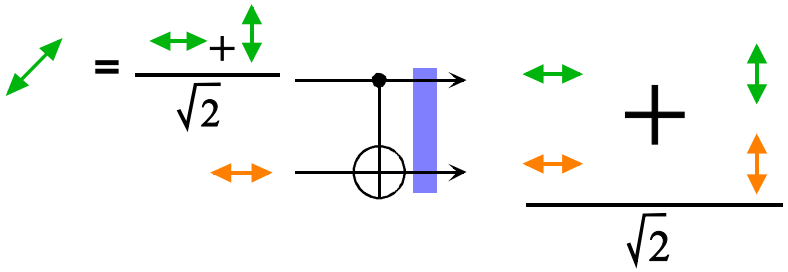
In the end, Alice and Bob will either agree on a shared secret key, or else they will detect that there has been too much eavesdropping to do so safely. They will not, except with exponentially low probability, agree on a key that is not secret.

Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.



The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.

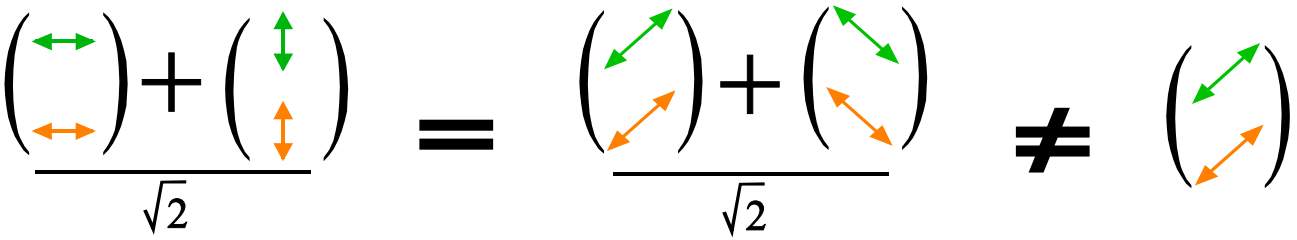
A superposition of inputs gives a superposition of outputs.



or EPR state

An entangled or EPR tate.

an entangled state is a state of a whole system that is not expressible in terms of states of its parts.



The two photons may be said to be in a definite state of *sameness* of polarization even though neither photon has a polarization of its own. (cf Haight-Ashbury, Summer of Love, 1967)

Entanglement is an intense and private kind of correlation

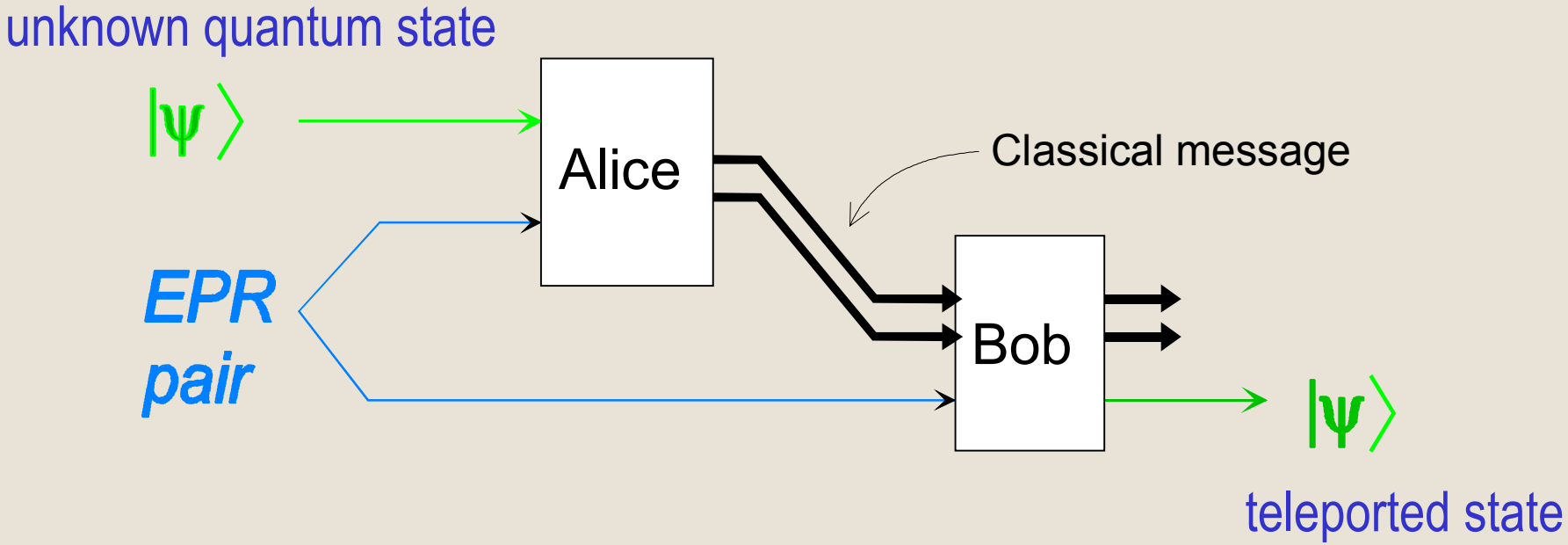
- A and B can be in a definite state, even though each is random
- Monogamy: If A and B are maximally entangled with each other, they cannot be even classically correlated with anyone else.

(Classical correlation is just a common, prosaic manifestation of entanglement)

BBCJPW '93

Entanglement is useful for Quantum Teleportation,

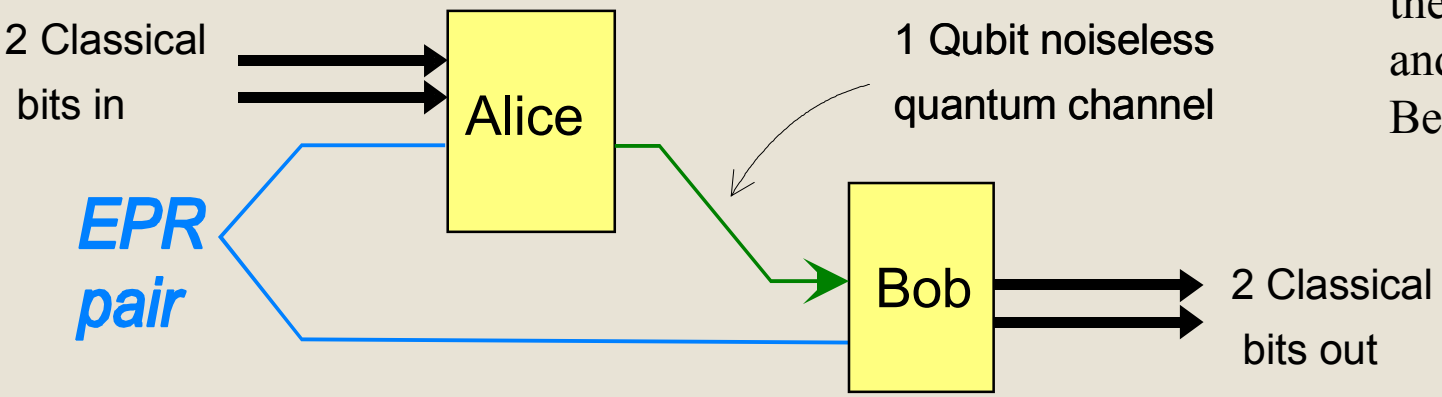
a way to transmit quantum information when no quantum channel is available.



Prior sharing of an EPR pair allows Alice to disembody an unknown qubit into a 2-bit classical message and preexisting entanglement. When Bob receives the classical message, he can reconstruct the unknown state exactly, but cannot copy it. The EPR link from Alice to Bob goes backward in time, but cannot by itself carry any meaningful message.

A dual process
to teleportation

Quantum Superdense Coding



Here Alice does the Pauli rotation and Bob does the Bell measurement.

doubles the classical capacity of any noiseless quantum channel

Alice's and Bob's roles in teleportation

Alice performs a joint measurement of the unknown input qubit ψ and her half of the shared EPR pair in the so-called Bell basis

$|00\rangle + |11\rangle$
$|00\rangle - |11\rangle$
$|01\rangle + |10\rangle$
$|01\rangle - |10\rangle$

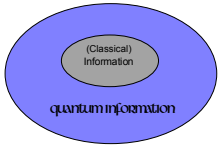
According to Alice's result, Bob performs one of four unitary transformations, the so-called Pauli operators `I`, `X`, `Y`, and `Z`, on his half of the EPR pair.

`I (do nothing)`	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
`Z phase shift`	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
`X bit flip`	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
`Y flip & shift`	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Result: Bob's qubit is left in the same state as Alice's was in before teleportation. If Alice's qubit was itself entangled with some other system, then Bob's will be when the teleportation is finished.

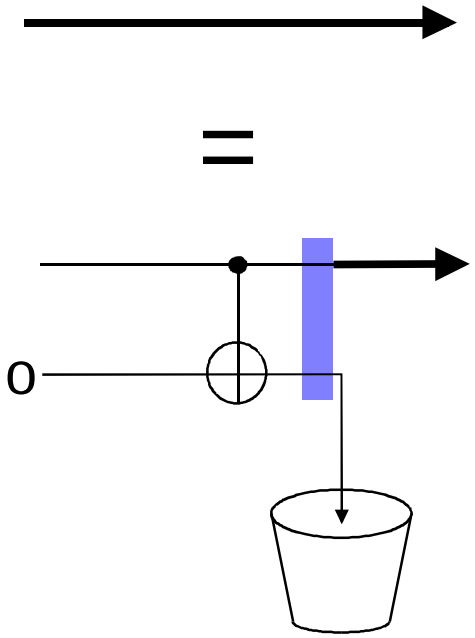
Expressing classical data processing in quantum terms.

A classical bit is just a qubit with one of the Boolean values **0** or **1**.



A classical wire is a quantum channel that conducts **0** and **1** faithfully, but randomizes superpositions of **0** and **1**.

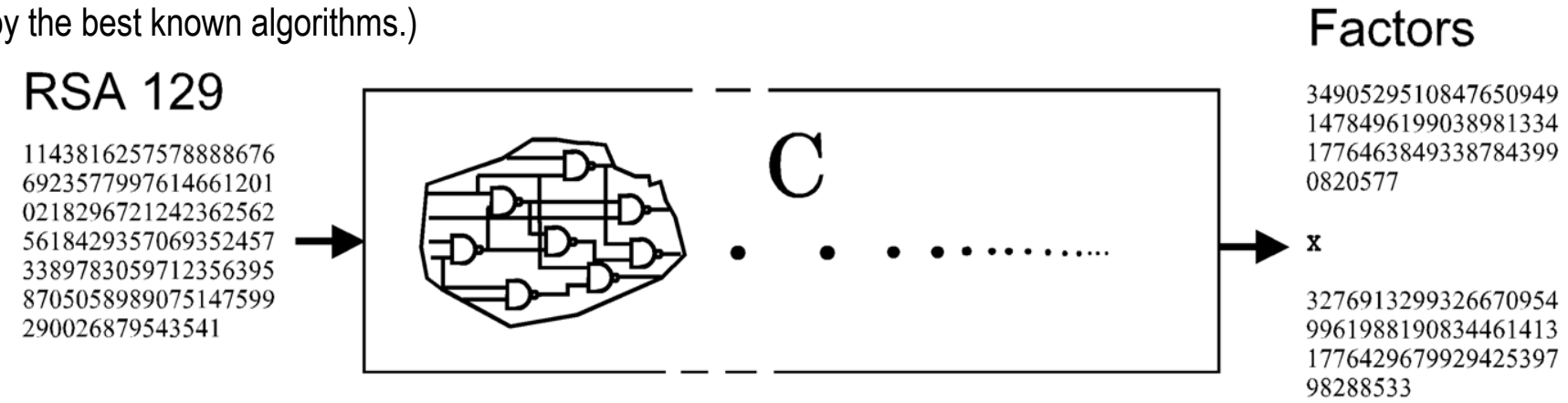
(This occurs because the data passing through the wire interacts with its environment, causing the environment to learn the value of the data, if it was **0** or **1**, and otherwise become entangled with it.)



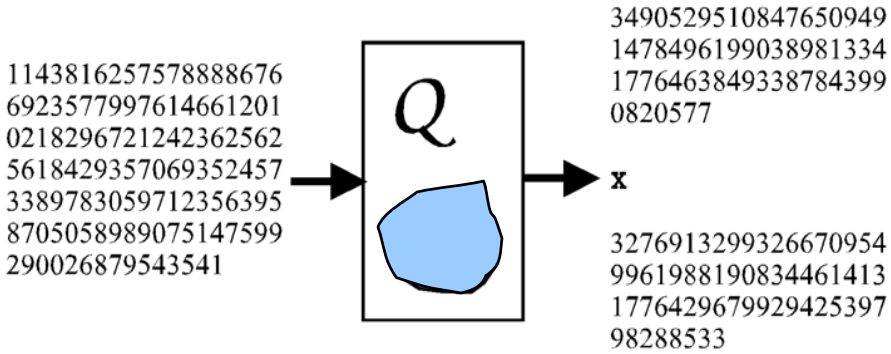
A classical channel is a quantum channel with an eavesdropper.

A classical computer is a quantum computer handicapped by having eavesdroppers on all its wires.

(For a classical computer, factoring appears to be exponentially harder than multiplication, by the best known algorithms.)



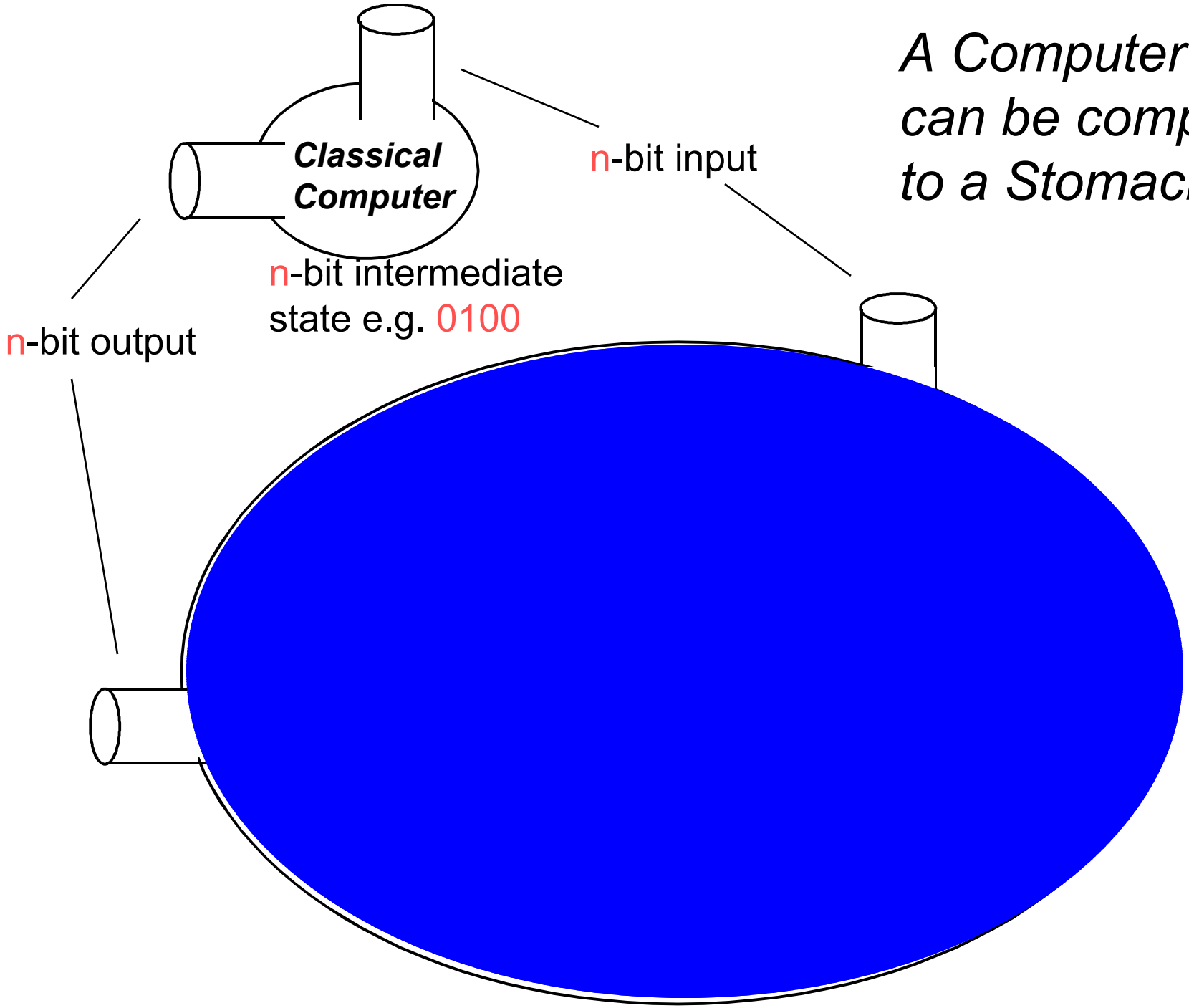
Same Input and Output, but Quantum processing of intermediate data gives



Exponential speedup for Factoring (Shor algorithm)

Quadratic speedup for Search (Grover algorithm)

(For a quantum computer, factoring is about as easy as multiplication, due to the availability of **entangled** intermediate states.)



A Computer can be compared to a Stomach

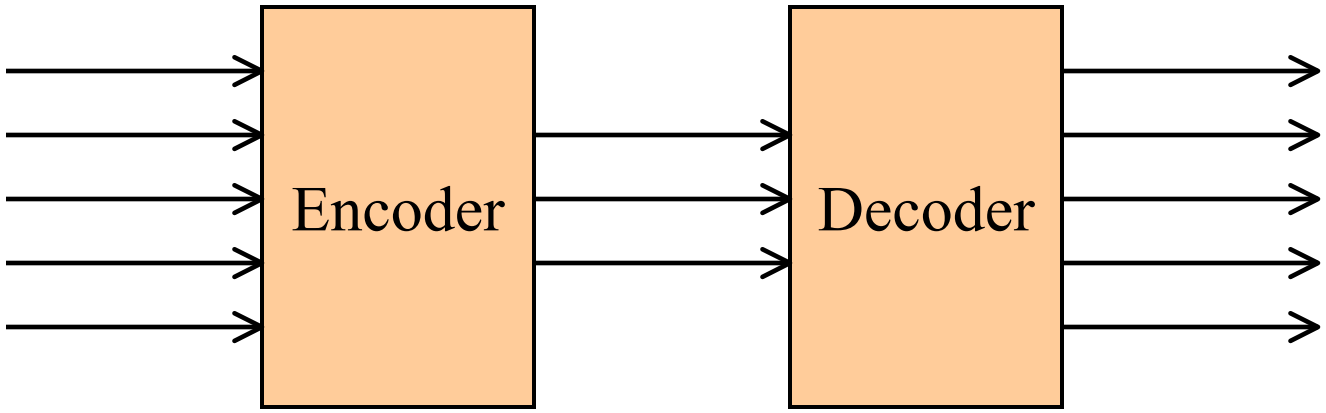
How Much Information is "contained in" n qubits, compared to n classical bits, or n analog variables?

	Digital	Analog	Quantum
Information required to specify a state	n bits	n real numbers	2^n complex numbers
Information extractable from state	n bits	n real numbers	n bits
Good error correction	yes	no	yes

Classical Communication Theory—central notions

•Data Compression and Source Entropy

•Error-correcting Codes and Channel Capacity

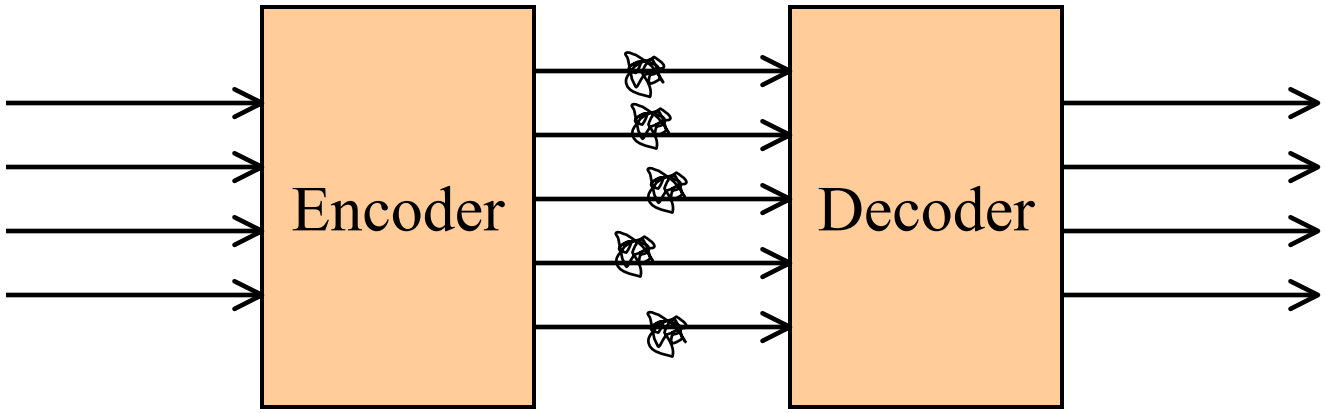


If an information source is redundant (due to unequal letter frequencies or correlations among letters) its output can be **compressed**, then faithfully recovered at the receiving end. A source's ***Shannon Entropy*** is the compressed size above which faithful recovery is possible, and below which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

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

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. (quant-ph/0106052=*IEEE Trans. Info. Theory* **48**, 2637-2655 ('02) with P. Shor, J. Smolin, A. Thapliyal; A. Winter quant-ph/0208131,)

Why doesn't shared randomness 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.

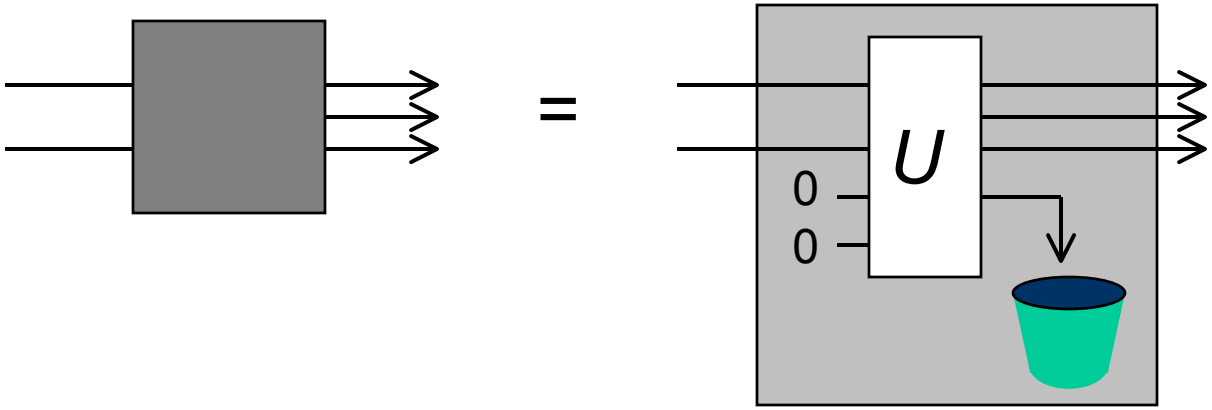
But entanglement *can* increase the capacity of a quantum channel because, unlike randomness, entanglement is not a kind of ignorance, and so cannot be derandomized.

Unitary evolution is reversible, preserving distinguishability.

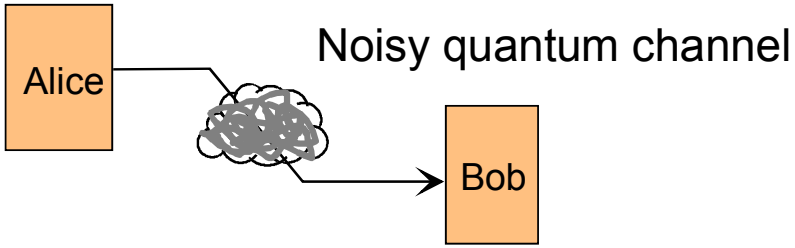
But quantum systems in interaction with an environment can undergo irreversible loss of distinguishability.

- noisy or lossy channels, which lose classical information
- classical wires, which spoil superpositions
- erasure, which destroys distinguishability completely

Any physically possible evolution of an open quantum system can be modeled as a unitary interaction with an environment, initially in a standard 0 state.



Multiple capacities of Quantum Channels



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

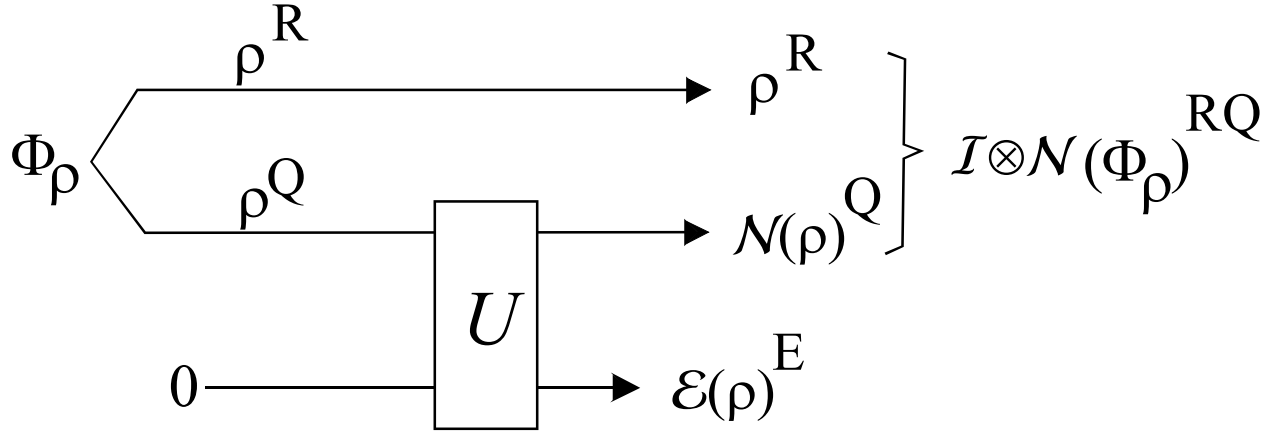
C plain classical capacity = bits faithfully trasmitted per channel use

Q_B quantum capacity assisted by classical back communication

Q_2 quantum capacity assisted by classical two-way communication

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.



= if min. output entropy is additive Shor '03

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

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

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

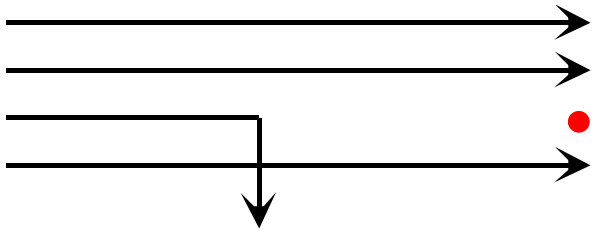
$Q_2 \approx$ Distillable entanglement = $\lim_{n\to\infty} \max_{\rho} D_2(\mathcal{I}\otimes\mathcal{N}^{\otimes n}(\Phi_\rho))/n$ = ?

(Unfortunately D_2 has no simple expression, may be nonconvex.
Even Q is grossly non-additive, as Smith and Yard showed last week.)

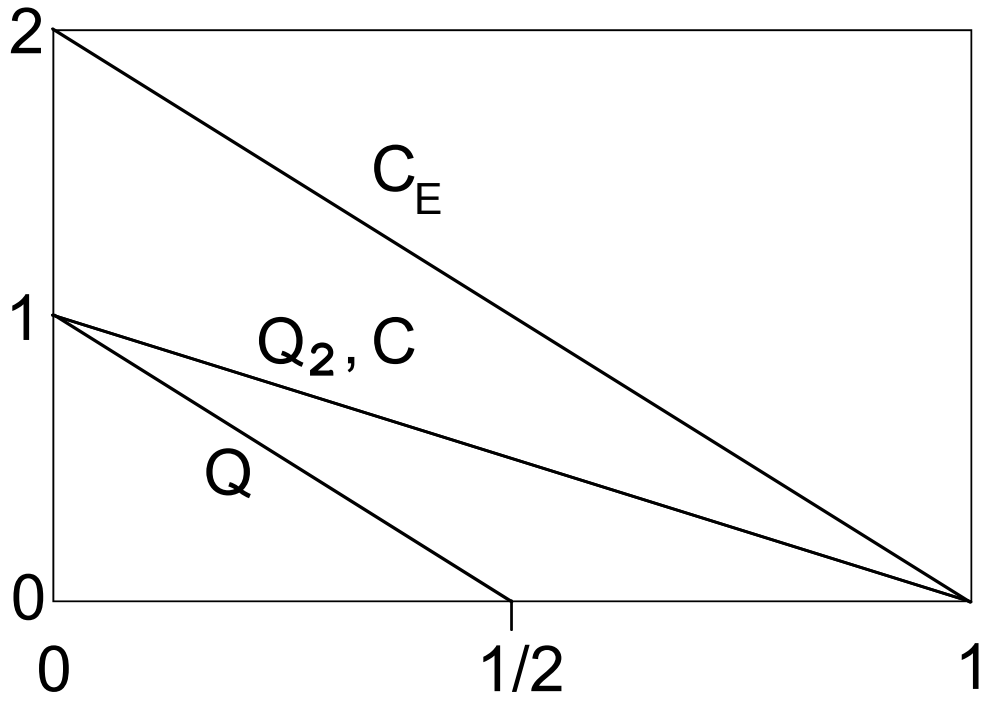
Simple illustrative example

Quantum Erasure Channel

input qubit sometimes lost

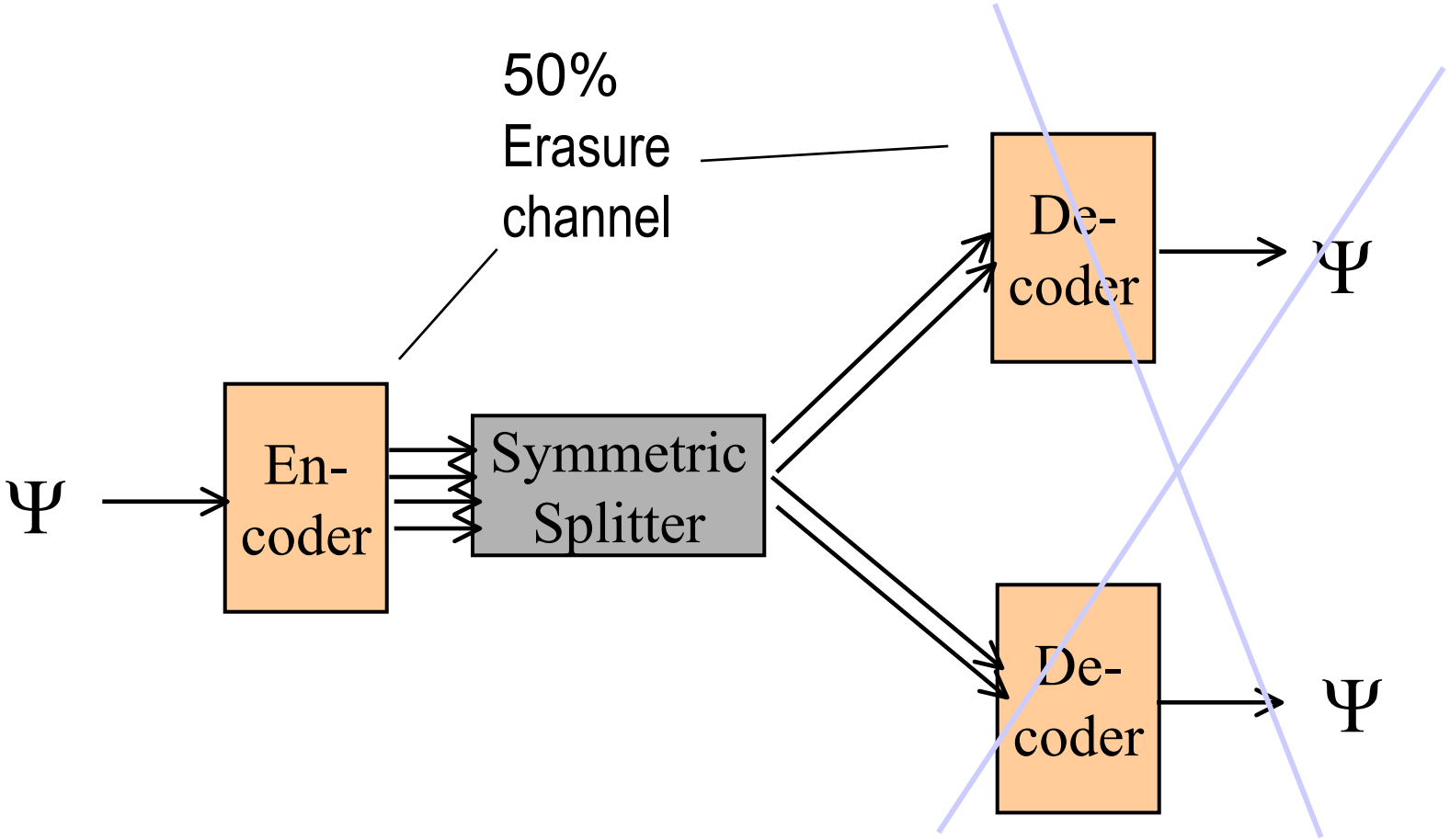


Capacities of Quantum Erasure Channel



Erasure Probability

A 50% erasure channel can be viewed as one output of a symmetric splitter.
Because of this its unassisted quantum capacity Q must be zero.
If this were not the case, the splitter could be used together with an encoder and two decoders to clone unknown quantum states.



But when assisted by classical communication or shared entanglement, the 50% erasure channel acquires a nonzero quantum capacity:

With Classical 2-way communication

- Alice uses the erasure channel to send Bob halves of EPR pairs.
- Bob reports back classically which ones arrived successfully.
- Alice uses these and forward classical communication to teleport the quantum input to Bob

With Shared Entanglement

- With the help of ordinary Shannon coding, Alice uses the erasure channel's forward classical capacity (50%) to send Bob the classical bits needed for teleportation. They already have the other resource required, viz Alice-Bob entanglement.

With Classical Back Communication alone

- Combine the two constructions above

Mixed States and Density Matrices

The quantum states we have been talking about so far, identified with rays in Hilbert space, are called *pure states.* They represent situations of minimal ignorance, where there is nothing more to know about the system. Pure states are fundamental in the sense that the quantum mechanics of any closed system can be completely described as a unitary evolution of pure states, without need of further notions. However, a very useful notion, the *mixed state*, has been introduced to deal with situations of greater ignorance, in particular

an ensemble $\mathcal{E}$ in which the system in question may be in any of several pure states ψ_1, ψ_2 ... with probabilities p_1, p_2 ....

a situation in which the system in question (call it A) is part of larger system AB, which itself is in an entangled pure state $\Psi(AB)$.

In open systems, a pure state may naturally evolve into a mixed state (which can also be described as a pure state of a larger system comprising the original system and its environment)

A mixed state is represented by a Hermitian, positive-semidefinite, unit-trace *density matrix*

$$\rho = \sum_i p_i \, | \psi_i \rangle \langle \psi_i |$$ for an ensemble

$$\rho(A) = \mathrm{Tr}_B \, | \Psi(AB) \rangle \langle \Psi(AB) |$$

for a subsystem

($\rho = | \psi \rangle \langle \psi |$ for a pure state)

Different ensembles can have the same density matrix. For example any equal mixture of two orthogonal polarizations has

$\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$ What common feature does ρ represent?

Meaning of the Density Matrix

The density matrix represents *all and only* that information which can be learned by sampling the ensemble or observing the *A* part of the compound system. Ensembles with the same ρ are indistinguishable. Pure states $\Psi(AB)$ with the same $\rho(A)$ are indistinguishable by observing the *A* part.

If Alice and Bob share a system in state $\Psi(AB)$, then, for any ensemble $\mathcal{E}$ compatible with $\rho(A)$, there is a measurement

Bob can do on his subsystem alone, which generates the ensemble, in the sense that the measurement yields outcome i with

probability p_i, and, conditionally on that outcome having

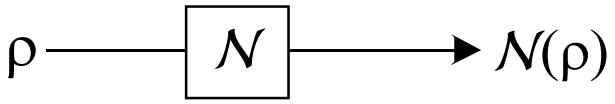
occurred, Alice's subsystem will be left in pure state ψ_i.

(Hughston-Jozsa-Wootters/Schroedinger theorem)

The Church of the Larger Hilbert Space

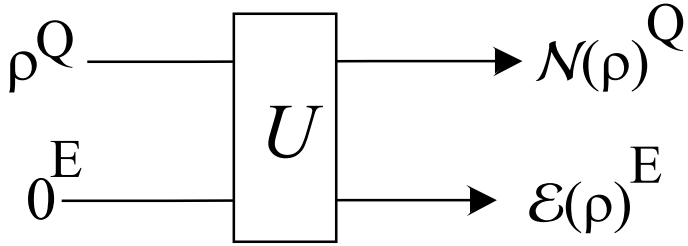
This is the name given by John Smolin to the habit of always thinking of a mixed state as a pure state of some larger system; and of any nonunitary evolution as being embedded in some unitary evolution of a larger system: No one can stop us from thinking this way; and Church members find it satisfying and helpful to their intuition:

This doctrine only makes sense in a quantum context; where because of entanglement a pure whole can have impure parts: Classically; a whole can be no purer than its most impure part. (Cf. Biblical view of impurity: If thy eye offend thee, cast it out.) But this does not bother Church members; who tend to believe that the classical (including Biblical) world is an emergent phenomenon from an underlying quantum reality.



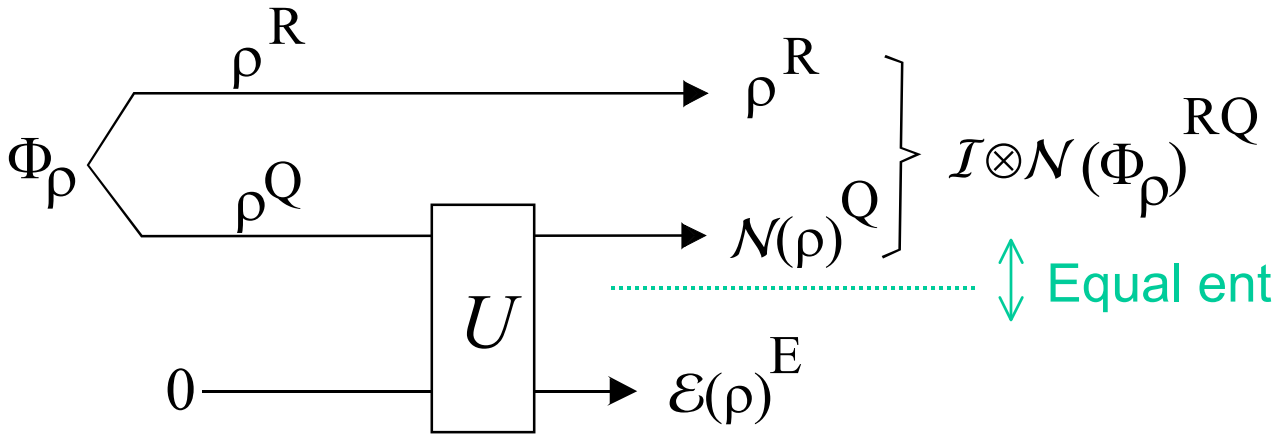
Noisy channel viewed as interaction with environment

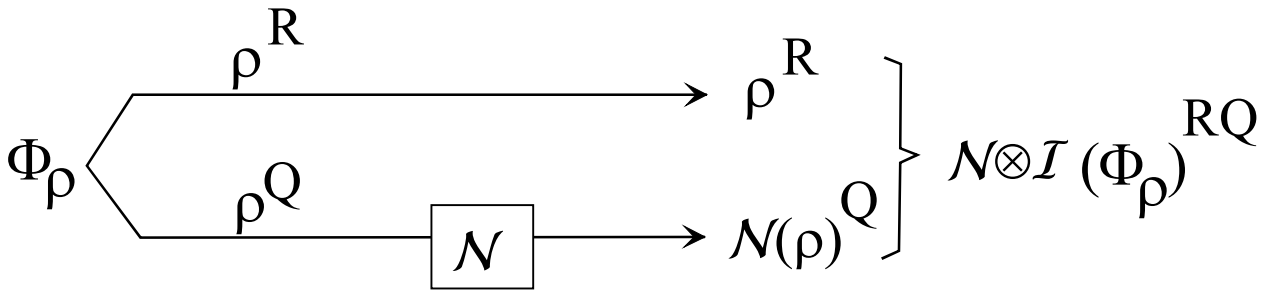
CLHS invoked to purify noisiness of channel



CLHS invoked again to purify mixedness of input

Input viewed as entangled with a reference system R





(entangled purification of ρ)

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

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).

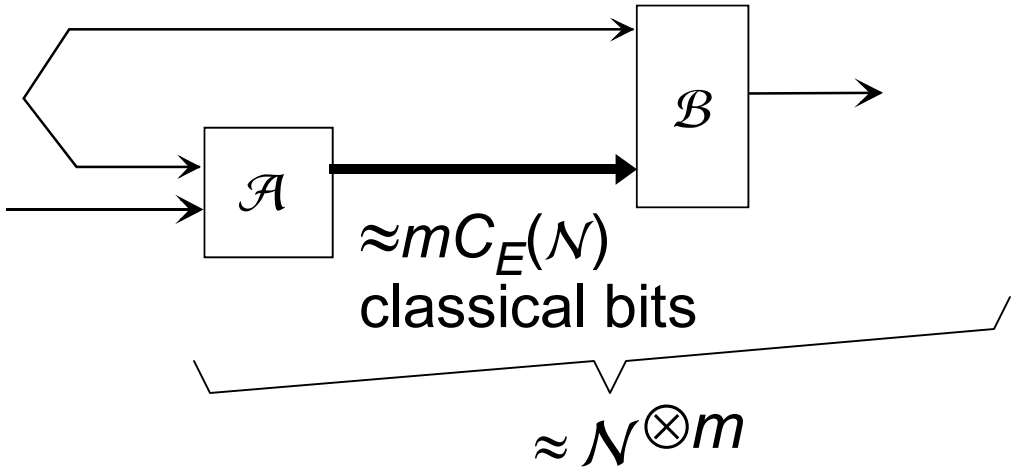
In retrospect, ***entanglement-assisted capacity***, not plain classical capacity, is the natural quantum generalization of the classical capacity of a classical channel. What Shannon actually found in 1948 was a nice formula for the entanglement-assisted capacity of a classical channel.

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

Quantum Reverse Shannon Theorem

(I.Devetak, A. Harrow, P. Shor and A. Winter, and CHB)

With some restrictions on the source ρ and channel $\mathcal{N}$ (or some enlargement of the notion of entanglement) any quantum channel $\mathcal{N}$ can be simulated asymptotically perfectly in the limit of large block size by prior entanglement and an amount of classical communication approaching the channel's entanglement assisted capacity.



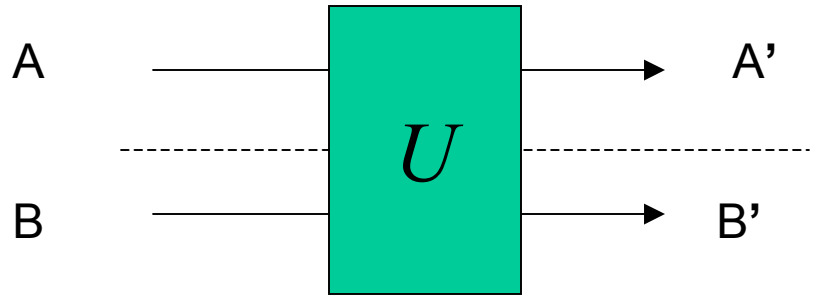
In particular, for all channels on tensor power sources $\rho = \rho^{\otimes m}$ (the quantum analog of classical Independent Identically Distributed sources)

$C_E(\mathcal{M},\mathcal{N}) = C_E(\mathcal{M}) \,/\, C_E(\mathcal{N})$.

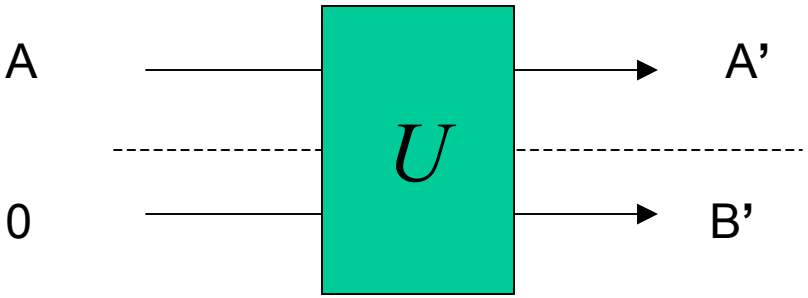
Thus, for these sources, in the presence of a shared entanglement, all quantum channels can be characterized by a single parameter, C_E .

Gates, Isometries and Channels

Gate

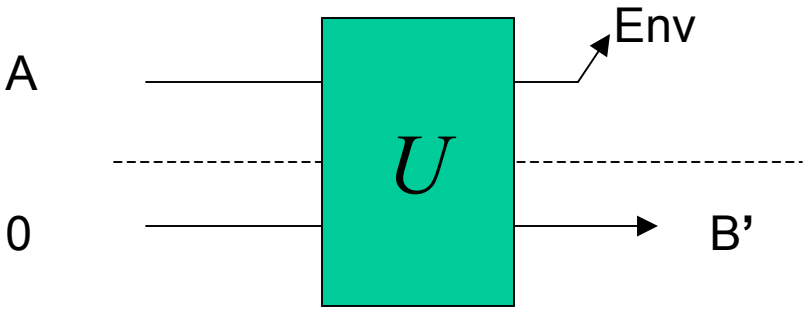


Isometry,
a.k.a.
channel
with quantum
feedback

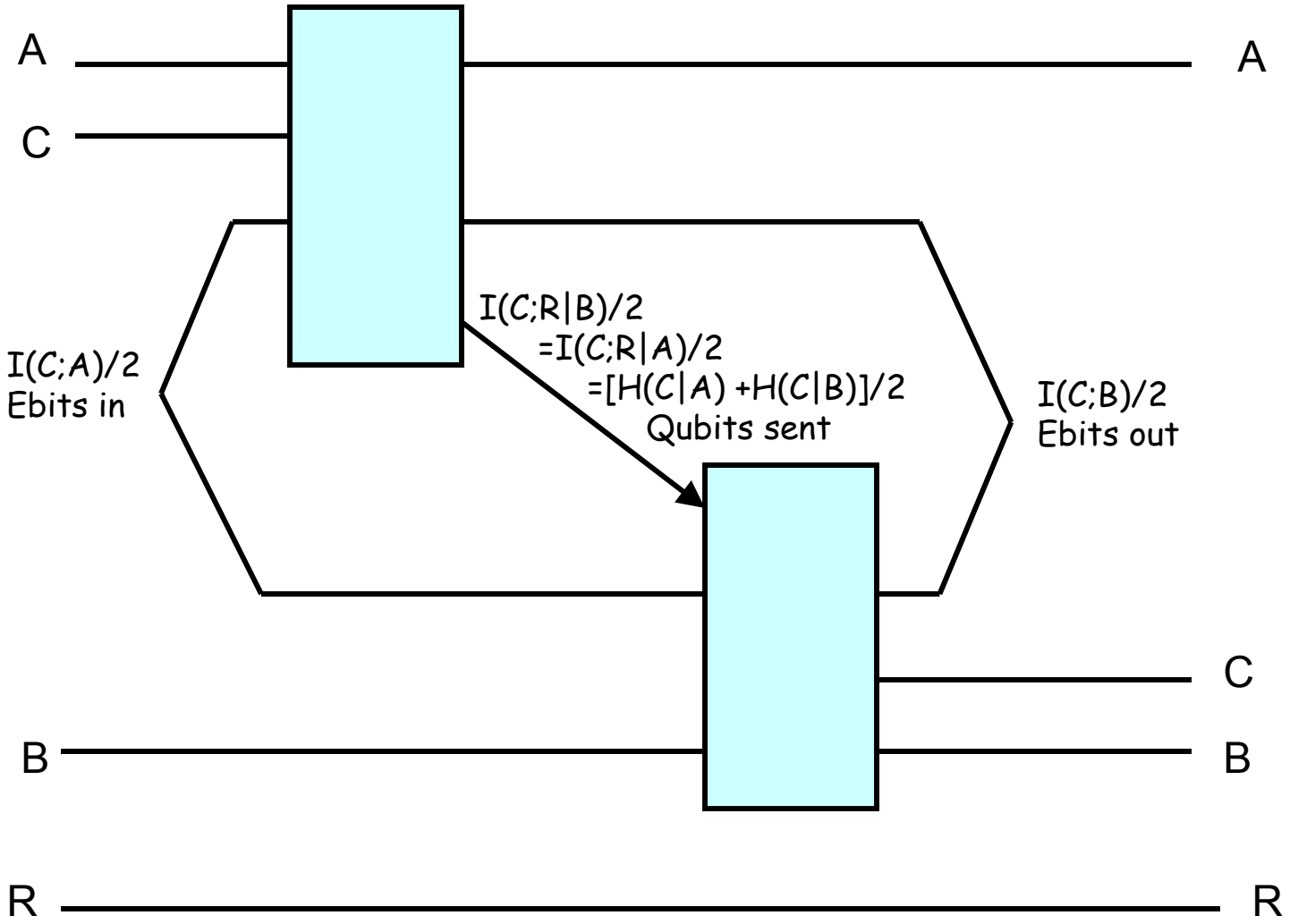


Cf classical feedback, where wlog Bob gets a *copy* of output

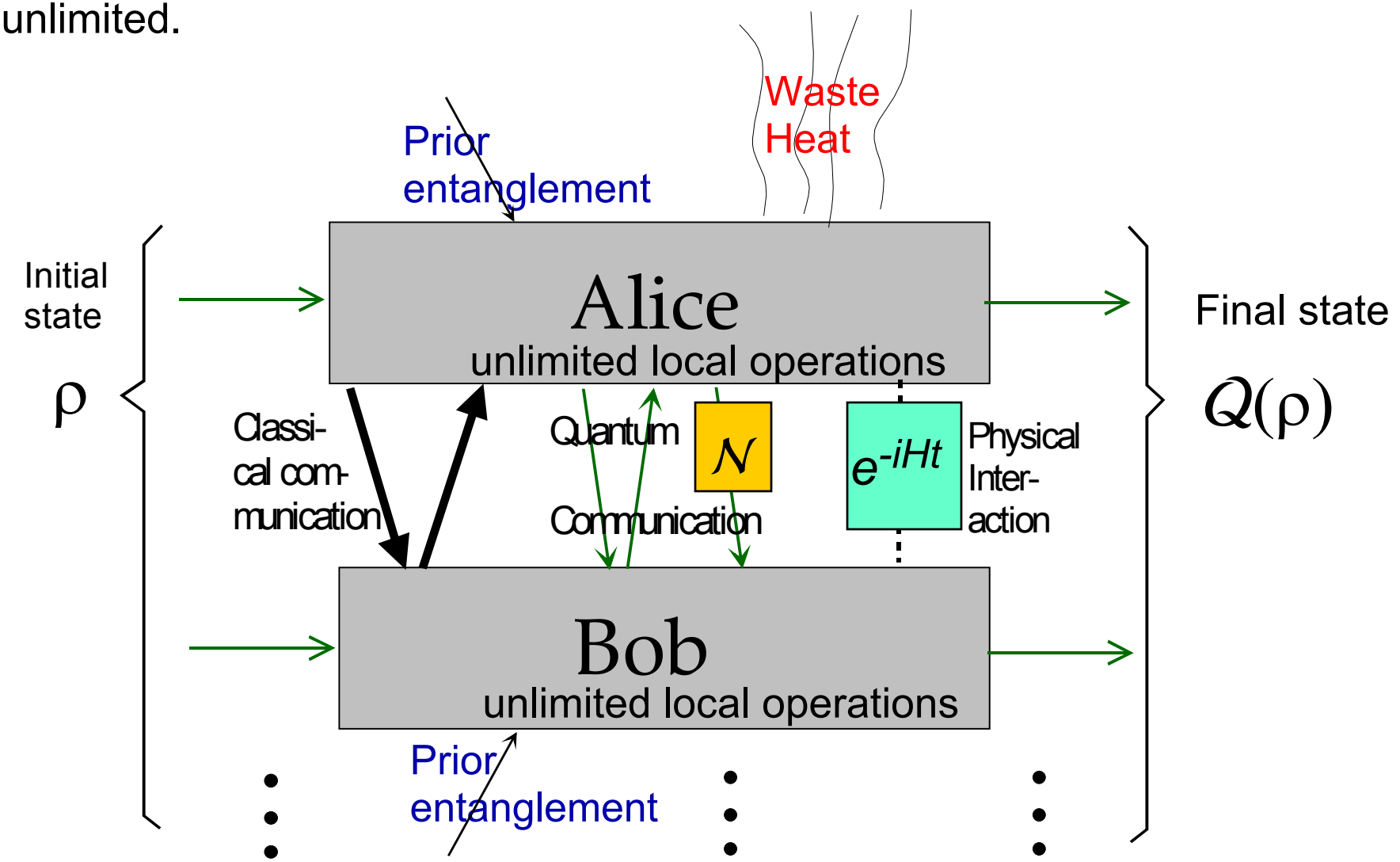
Channel,
a.k.a.
CPTP map



Quantum State Redistribution (Devetak & Yard; Oppenheim):
Reversible Communication and Entanglement costs of transferring subsystem C from Alice's lab to Bob's, in the presence of non-moving local subsystems A and C, while maintaining intact entanglement with a passive reference system R.



An important general 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.



Summary and Conclusion

- The quantum arena is simpler and grander

- Many classical notions, when carried over straightforwardly to the quantum realm, get ugly and complicated.
    - Additivity of classical capacity
    - Quantum capacity

- But when appropriately generalized, they can become simple again
    - Entanglement-assisted capacity
    - Coherent, channel simulation and state redistribution

- In the quantum realm, there are more toys to play with and resources to trade off against one another: classical and quantum communication, interaction, entanglement..

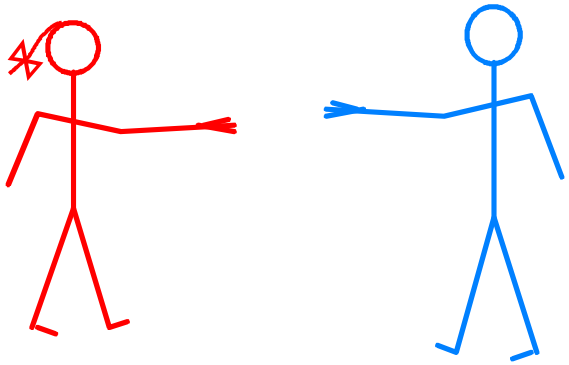
Extra slides

One way in which quantum laws are simpler than classical is the universality of interaction.

Classically, there are distinct kinds of interaction that cannot be substituted for one another. For example, if I'm a speaker and you're a member my audience, no amount of talking by me enables you to ask me a question.

Quantumly, interactions are intrinsically bidirectional. Indeed there is only one kind of interaction, in the sense that any interaction between two systems can be used to simulate any other.

A quantum love story, based on the classic tale of Pyramus and Thisbe.



Alice and Bob are young and in love.

Unfortunately, their parents oppose their relationship, and have forbidden them to visit, or talk, or exchange email.

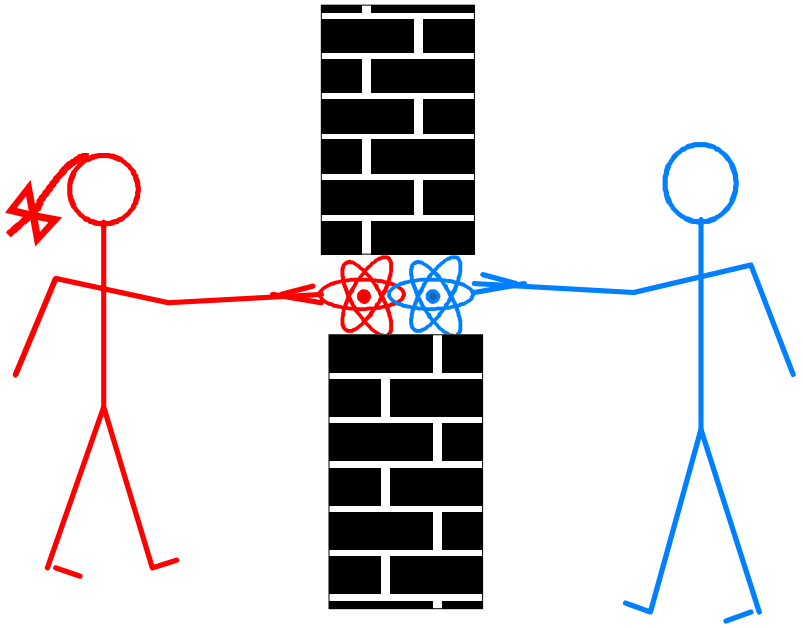
Fortunately, they live next door to one another.

Unfortunately, there's a wall between their two houses.

Fortunately, there's a hole in the wall.

-- more --

Unfortunately, the hole is only big enough for one atom of Alice to interact with one atom of Bob, via an interaction ***H'*** .

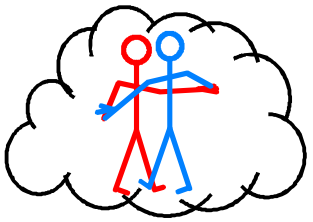


Fortunately, Alice and Bob know quantum mechanics. They know that any interaction can be used to create entanglement, and that interactions are intrinsically bidirectional and private: A cannot affect B without B affecting A. If C interferes or eavesdrops, the joint state of A and B will be degraded and randomized.

-- more --

The young lovers wish to experience the life they would have had if they had been allowed to interact not by the one-atom interaction **H'** but by the many-atom interaction **H**, which is a physicist's way of saying always being in each other's arms.

How can they use the available **H'** to simulate the desired **H** ?



They can of course separately prepare their respective interacting atoms in any initial states, and thereafter alternate through-the-wall interactions under H' with local operations among their own atoms, each on his/her own side of the wall.

Using the hole in the wall, they can prepare entangled states. We assume each has a quantum computer in which to store and process this entanglement. Whenever they need to communicate classically, to coordinate their operations, they can use the interaction **H'** to do that too. Thus the joint states they can experience are all those that can be achieved by shared entanglement and classical communication. Of course it will take a lot of time and effort.

-- more --

The joint states they can experience are all those that can be achieved by shared entanglement and classical communication.

But this is *all* quantum states of A and B!

If their parents had only plugged the hole in the wall and allowed them unlimited email, their future would have been much bleaker.

They could never have become entangled, and their relationship would have remained Platonic and classical. In particular, it would have had to develop with the circumspection of knowing that everything they said might be overheard by a third party.

As it is, with the hole remaining open, by the time they get to be old lovers, they can experience exactly what it would have been like to be young lovers (if they are still foolish enough to want that).

-- The End --