Classical Information through quantum channels

Shannon's

noiseless channel coding theorem

...how many bits are required to store information?

noisy channel coding theorem

...how much information can be reliably transmitted through a noisy channel?

Information Source?

Classical : p_j , $j = 1, 2, \ldots d$

... letter j emitted with probability p_j

$\Rightarrow$ Compression :

e.g. letter "e" uses fewer bits than letter "z".

Noiseless channel coding theorem

... a classical source, $\{p_j\}$, can be compressed so that each source emission requires

$\approx$

$$H(p_j) = -\sum_j p_j \log(p_j) \quad \text{bits}$$

$H(p_j)$ is Shannon Entropy

.... using fewer bits than this results in a high probability of error after decomposition.

Shannon's noisy channel coding theorem:

Encode information using error-correcting codes so that channel noise can be corrected.

.... redundancy introduced.

e.g.

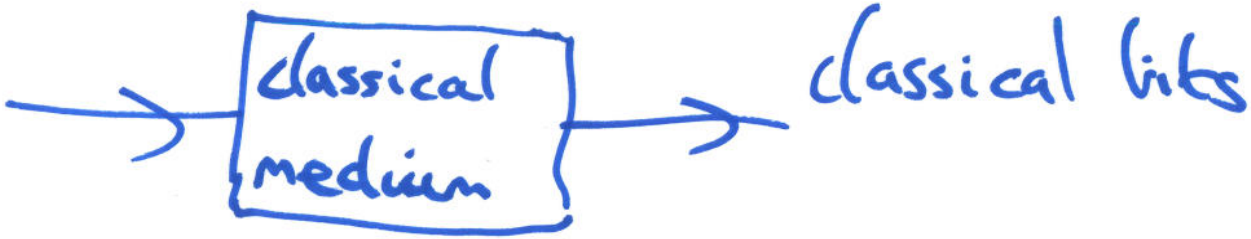
Suppose noise in channel requires encoding up to two bits per bit of information.

Then,

channel capacity is $\frac{1}{2}$ bit.

$\Rightarrow$ noisy channel coding theorem leads to a procedure for calculating channel capacity

Shannon,



what about

in fact, for the noiseless case, qubits do not allow any significant saving in the amount of communication required to transmit information over a noiseless channel.

Noisy Quantum channel?

Quantify capacity of quantum channel?

Problem:

Huge variety of noise models for quantum mechanics

.... use entangled states?

.... decode using entangled measurements?

Holevo-Schumacher-Westmoreland theorem (HSW)

provides a lower bound on channel capacity

Conjecture: actually HSW is an exact evaluation?

.... no complete proof yet.

Remaining issue:

can entanglement be used to raise the capacity beyond the HSW lower bound

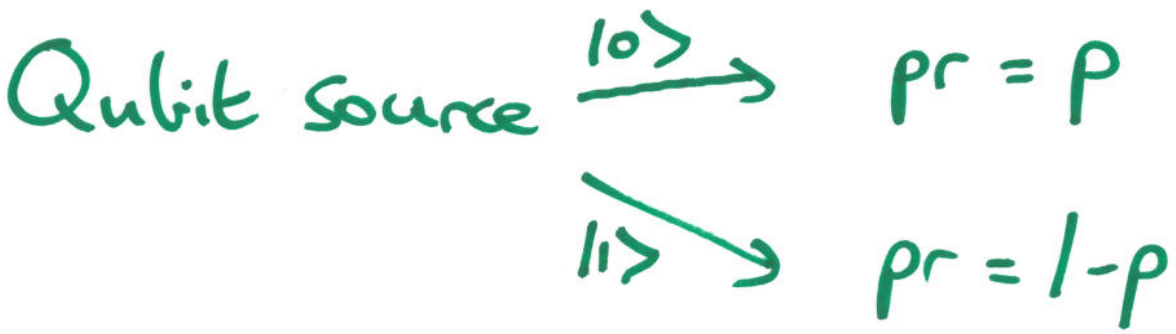
.... (thereby disproving the conjecture)

Quantum Information through Quantum Channels

Quantum Source:

set of probabilities, p_j,
corresponding to states, $|\psi_j\rangle$.

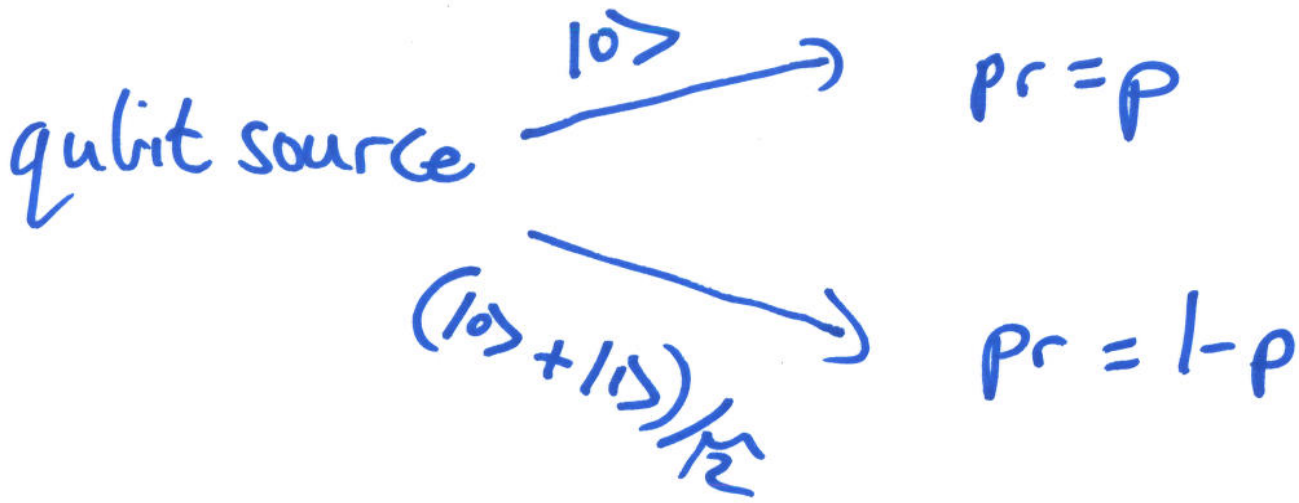
Can we compress the output from a quantum-mech. source?



... only $H(p, 1-p)$ qubits are required to store the compressed source,

where H is the Shannon entropy.

What about



Problem:

$|0\rangle$ and $(|0\rangle + |1\rangle)/\sqrt{2}$ not completely distinguishable

.... compression still possible but not necessarily error-free.

We consider compression with small distortion that becomes negligible, in the limit (i.e. for large blocks of source).

Distortion quantified using fidelity

Think of fidelity as the probability of doing decompression correctly.

Schumacher's noiseless channel coding theorem quantifies resources required for quantum data compression, assuming it is possible to recover the source with fidelity close to 1.

For orthogonal states (ie. completely distinguishable), Schumacher's theorem reduces to compression down to but not beyond $H(p)$

For non-orth. states, compression limit is Von Neumann entropy where,

Von Neumann entropy $\leq$ Shannon entropy $= H(p_j)$

.... with equality when states are orthogonal.

How much compression is possible?

Source $\xrightarrow{|0\rangle}$ $pr = p$

$\xrightarrow{(|0\rangle + |1\rangle)/\sqrt{2}}$ $pr = 1-p$

Emit n times: $|0\rangle^{\otimes np} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n(1-p)}$

$\approx$ superposition of $|0\rangle^{\otimes np} \left[|0\rangle^{\otimes n(1-p)/2} |1\rangle^{n(1-p)/2}\right]$

$\approx$ superposition of $|0\rangle^{\otimes n(1+p)/2} |1\rangle^{\otimes n(1-p)/2}$

There are $\approx \binom{n}{n(1+p)/2} \approx 2^{nH\left[(1+p)/2, (1-p)/2\right]}$ such states

... using Stirlings approximation.

Label these $N = 2^{nH[(1+p)/2,(1-p)/2]}$ states as $|c_1\rangle$ to $|c_N\rangle$.

Perform unitary transform, U, such that

$$U|c_j\rangle = |j\rangle|0\rangle^{\otimes n - nH[(1+p)/2,(1-p)/2]}$$

Drop the final $n - nH[(1+p)/2,(1-p)/2]$ qubits

$\Rightarrow$ compressed state of

$$nH\left[\frac{(1+p)}{2},\frac{(1-p)}{2}\right] \text{ qubits}$$

(to decompress, append $|0\rangle^{\otimes n - nH[(1+p)/2,(1-p)/2]}$ and perform U^{-1}).

Result:

Storage requirement of $H\left[\frac{(1+p)}{2}, \frac{(1-p)}{2}\right]$ qubits per source use.

When $p \geq \frac{1}{3}$ then this is an improvement over $H(p, 1-p)$.

.... when $p < \frac{1}{3}$, the scheme outlined actually increases the redundancy!

Quantum Distinguishability

Unlike classical states, it is not always possible, in principle, to distinguish between two quantum states.

e.g. try distinguishing $|0\rangle$ from $(|0\rangle + |1\rangle)/\sqrt{2}$

.... measure in computational basis

... measuring $|1\rangle$ identifies $(|0\rangle + |1\rangle)/\sqrt{2}$

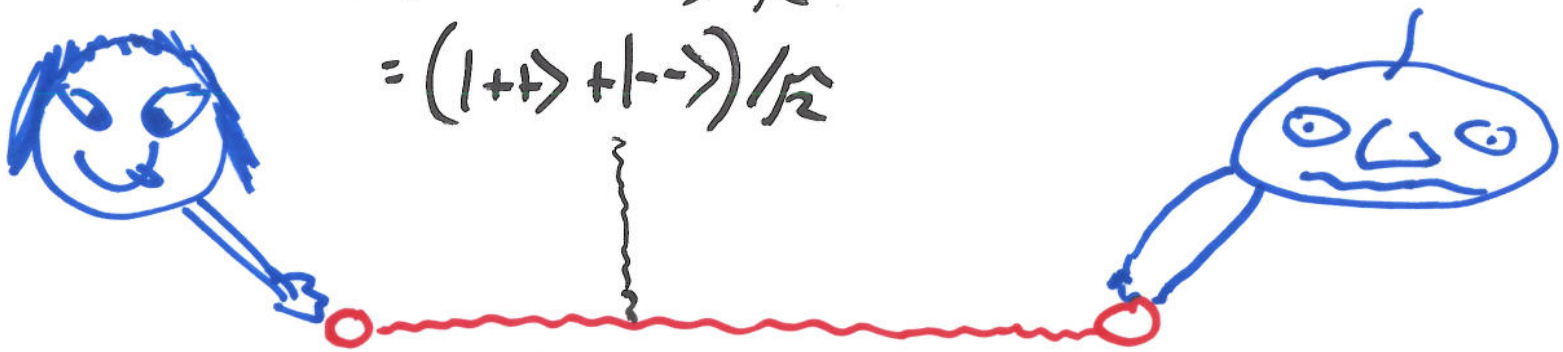
.... but measuring $|0\rangle$ is no help.

If two arbitrary states are deterministically distinguishable, then,

we can communicate faster than the speed of light using entanglement.

Proof

$$(|00\rangle + |11\rangle)/\sqrt{2}$$
$$= (|++\rangle + |--\rangle)/\sqrt{2}$$



Alice measures computational basis

or

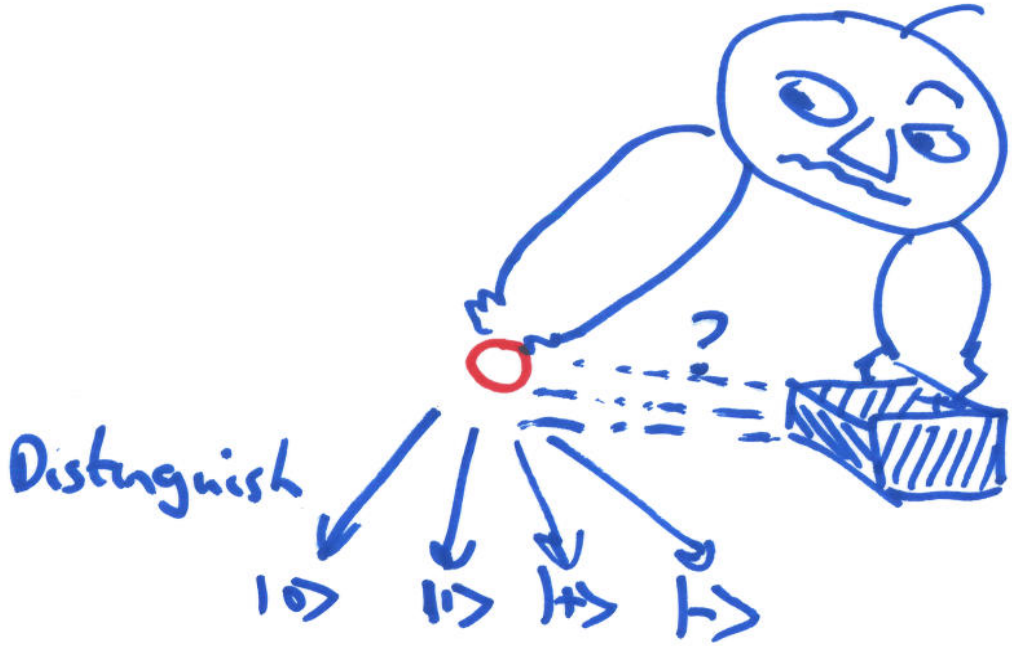
Alice measures $|+\rangle, |-\rangle$ basis

$|0\rangle$ $pr=\frac{1}{2}$ $\longrightarrow$ $|0\rangle$, $pr=\frac{1}{2}$

$|1\rangle$ $pr=\frac{1}{2}$ $\longrightarrow$ $|1\rangle$, $pr=\frac{1}{2}$

$|+\rangle$ $pr=\frac{1}{2}$ $\longrightarrow$ $|+\rangle$, $pr=\frac{1}{2}$

$|-\rangle$ $pr=\frac{1}{2}$ $\longrightarrow$ $|-\rangle$, $pr=\frac{1}{2}$

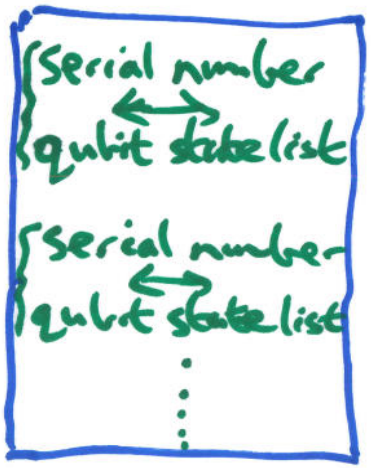

?
Distinguish
|0>
|1>
|+>
|->
If Bob has access to a device that can distinguish the four states |0>, |1>, |+>, |->, then he could tell whether Alice had measured in the computational or |+>, |-> basis....
.... instantaneously ....
...as soon as Alice had made the measurement.

Banks can exploit indistinguishability

Banks produce banknotes:

classical serial number
qubit sequence in either $|0\rangle$ or $(|0\rangle+|1\rangle)/\sqrt{2}$ states

Bank possesses secret list,



Impossible to counterfeit

... counterfeiter cannot determine states with certainty.

... merchant asks bank for

{serial number ⟷ qubit state list}

.... measures note in $|0\rangle$, $|1\rangle$, $(|0\rangle+|1\rangle)/\sqrt{2}$ or $(|0\rangle+|1\rangle)/\sqrt{2}$ basis, according to

There is an exponential increase in probability of counterfeit detection as more qubits checked.

Creation and transformation of entanglement

Creating: How many qubits must two parties exchange so as to create a specified entangled state?

Transforming: One entangled form $\overset{?}{\Rightarrow}$ another entangled form

... is classical and/or quantum communication needed?