1.6 Quantum information

The term "*quantum information*":

1. All manner of operations that might be interpreted as related to informatin processing using quantum mechanics.(*e.g. q–computation, q–teleportation, the no-cloning theorem*)
2. The study of elementary quantum information process tasks.
   - q info. theory $\Longleftrightarrow$ (classical) info. theory

A few fundamental goals uniting work on quantum information theory :

1. Identify elementary classes of static resources in quantum mechanics
   - qubits
   - bits
   - bell states shared between two distant parties.
2. Identify elementary classes of dynamical processes in quantum mechanics
   - memory – storing q-st. over some period of time
   - q-information transmission between two parties
   - copying(or trying to copy) a quantum state
   - noise protecting quantum communication
3. Quantify resource tradeoffs incurred performing elementary dynamics
   - What are the minimal resources to transfer quantum information between two parties using noisy quantum channel.

The quantum information theory includes all the static and dynamic elements of classical information theory, as well as additional static and dynamic elements $\Rightarrow$ Broader.

Some information theoretic questions have been studied as samples:
Exploring Semi-classical elements (*sending classical information through q-channel*)

$$\Downarrow$$

The new static and dynamic processes present in quantum mechanics (*quantum error-correction, the problem of distinguishing quantum states, and entanglement transformation.*)

1.6.1 Quantum information theory: example problems

Classical information through quantum channels

Classical elements Shannon's noiseless channel coding theorem and Shannon's noisy channel coding theorem : The fundamental results of classical information theory.

noiseless How many bits are required to store information being emitted by a source of information

noisy How much information can be reliably transmitted through a noisy commnunication channel

A classical information source is described by a set of probabilities p_j, $j = 1, 2, 3...d$ (*eg. English text* - the numbers j : the alphabet and punctuation, with the probabilities p_j giving the relative frequencies with which the different letters appear in regular English text)

Regular text includes redundancy, the redundancy have the possibility of compress the text.
→ Shannon's noiseless channel coding theorem quantifies exactly how well such a compression scheme can be made to work.

The noiseless channel coding theorem tells

- A classical source described by probabilities p_j can be compressed so that on average each use of a classical source can be represented using $H(p_j)$ bits of information, where

  $$H_(p_j) \equiv -\sum_j p_j \log p_j$$

  is a function of the source probability distribution known as the *Shannon entropy*.
- to attempt to represent the source using fewer bits than this will result in a high probability of error when the information is decompressed.

Shannon's noiseless coding theorem provides a good example where the goals of information theory

goal 1 Two static resources are identified (the bit and the information source)

goal 2 Two-stage dynamic process is identified (compressing, decompressing)

goal 3 A quantitative criterion for determining the resources consumed (an optimal data compression scheme)

The noisy channel coding theorem

- quantifies the amount of information that can be reliably transmitted through a noisy channel.
  In particular, to transfer the information being produced by some source to another location (that location : at another point in space, or at another point in time - storing information in the presence of noise -)
- The idea in both instances is to encode the information being produced using *error–correcting codes*, so that any noise introduced by the channel can be corrected at the end of the channel.
- The error–correcting codes achieve this is by introducing *enough redundancy* into the information sent through the channel, so that even after some of the information has been corrupted it is still possible to recover the original message.
- provieds a general procedure for calculating the capacity of an arbitrary noisy channel. (for one bit information transmission through noisy channel, one must encode using two bits : such a channel has a capacity of half a bit)

Shannon's noisy channel coding theorem also achieves the three goals of information thoery

goal 1 Two static resources are involved (the bit and the information source)

goal 2 Three dynamic processes are involved (noise, encoding and decoding the state in an error–correcting code)

goal 3 How much redundancy must be introduced by an optimal error–correction scheme, for a fixed noise channel

Semi-classical elements A natural question for q-information theory : what happens if the storage medium is canged so that classical information is transmitted using quantum states as the medium.

In Ch. 12 : Using qubits allows a better compression rate than is possible classically and we will prove that qubits do not allow any significant saving in the amount of communication required to transmit information over a noiseless channel.

Transmission classical information through a noisy channel:
Might it be advantageous, for example, to encode the classical information using *entangled* states, which are then transmitted one piece at a time through the noisy channel?
Perhaps it will be advantageous to decode using entangled measurements?

HSW(Holevo-Schumacher-Westmoreland) theorem

- provides a lower bound on the capacity of a channel.
- is believed to provide an exact evaluation of capacity

Encoding using entangled does not help raise the capacity beyond the lower bound by the HSW theorem. (but still open problem)

Semi-classical schemes are concerned with Eavesdropping of orthogonal quantum key distribution

Quantum information through quantum channels - pure quantum elements

def) probabilities p_j and corresponding quantum states $|\psi_j\rangle$

A quantum source with output states $|0\rangle$ with probability p and $|1\rangle$ with probability $1-p$ can be compressed so that $H(p, 1-p)$ qubits are required to store the compressed source.

If the source had been producing the state $|0\rangle$ with probability p, and the state $(|0\rangle + |1\rangle)/\sqrt{2}$ with probability $1-p$, the standard techniques of classical data compression no longer apply. (we can not distingush $|0\rangle$ and $|+\rangle$)

A type of compression is still possible, but the compression may no longer be *error-free* (the quantum state being produced by the source may be slightly distorted by the compression-decompression procedure)

Suppose the distortion is small and ultimately neglibigle in limit of large blocks of source output being compressed.

A *fidelity* measure for the compression scheme

- measures the average distortion introduced by compression scheme.
- The idea of quantum data compression is that the compressed data should be recovered with very good fidelity.
- is thought to be analogues to the probability of doing the decompression correctly (large data block limit $\rightarrow$ no error limit of 1)

Schumacher's noiseless channel coding theorem

- quantifies the resources required to dot quantum data compression, with the restriction that it be possible to recover the source with fidelity close to 1.
- In the case of a source producing orthogonal quantum states $|\psi_j\rangle$ with probabilities p_j the theorem reduces to telling that the source may be compressed down to but beyond the classical limit $H(p_j)$.
- In the more general case of non-orthogonal states being produced by the source, the theorem tells how much a quantum source may be compressed (the new entropic quantity *von Neumann* entropy)

The von Neumann entropy for the sourced p_j, $|\psi_j\rangle$ is in general strictly smaller than the Shannon entropy $H(p_j)$. (*eg.* $|0\rangle$ with p and $(|0\rangle + |1\rangle)/\sqrt{2}$ with probability $1-p$ can be reliably compressed using fewer than $H(p, 1-p)$ qubits per use of the source)

Suppose above sources, and use the large # limit law with high probability the source emits about np copies of $|0\rangle$ and $n(1-p)$ copies of $(|0\rangle + |1\rangle)/\sqrt{2}$. It has the form

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

up to re-ordering of the systems involved. Approximately, the state emitted by the source has the form

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

How many states of this form are there? Roughly n choose $n(1+p)/2$, which by Stirling's approximation is equal to $N \equiv 2^{nH[(1+p)/2,(1-p)/2]}$

$$\left(\frac{n!}{(n-n(1+p)/2)!\,(n(1+p)/2)!} = \frac{n!}{(n(1-p)/2)!\,(n(1+p)/2)!}, \right.$$
$$\left. n! \approx n^n e^{-n} \sqrt{2\pi n}, \qquad H(p_i) = -\sum_i p_i \log_2 p_i \right)$$

A simple compression method then is to label all states of the form $|0\rangle^{\otimes n(1+p)/2} |1\rangle^{\otimes n(1-p)/2}$ $|c_1\rangle$ through $|c_N\rangle$.

It is possible to perform a unitary transform on the n qubits emitted from the source that takes $|c_j\rangle$ to $|j\rangle|0\rangle^{\otimes n - nH[(1+p)/2,(1-p)/2]}$, since j is an $nH\left[(1+p)/2,(1-p)/2\right]$ bit number. The compression operation is to perform this unitary trasformation, and then drop the final $n - nH\left[(1+p)/2,(1-p)/2\right]$ qubits, leaving a compressed state of $nH\left[(1+p)/2,(1-p)/2\right]$ qubits. To decompress, we append the state $|0\rangle^{n-nH[(1+p)/2,(1-p)/2]}$ to the copressed state, and perform the inverse unitary transformation.

The Storage requirement : $H\left[(1+p)/2,(1-p)/2\right]$ qubits per use of the source.

Schumacher's noiseless channel coding theorem allows us to do somewhat better even than this (Ch. 12)

For $|0\rangle$ and $(|0\rangle + |1\rangle)/2$, the states contain some redundancy since both have a components in the $|0\rangle$ direction.

Shumacher's noiseless channel coding theorem is an analogue of Shannon's but there's no fully satisfactory analogue of Shannon's on noisy channel. (however, it has been made with quantum error-correcting codes)

Quantum distinguishability

Up to now, compression, decompression, noise, encoding and decoding error correcting codes have been considered in both classical and quantum information theory. The new types of information (such as quantum state) enlarges the class of dynamical processes.

The problem of distinguishing quantum state : it is not always possible to distinguish between arbitrary states (*eg.* $|0\rangle$ and $|+\rangle$ are not distinguishable)

However, this indistinguishability of non-orthogonal quantum states is at the heart of QC and QI.

A quantum state contains **hidden** information that is not accessible to measurement, and thus plays a key role in quantum algorithm and quantum cryptography.

One of the central problems of quantum information theory is to develop measures quantifying how well non-orthogonal quantum state may be distinguished. (Ch.9, Ch.12)

The distinguishability between non-orthogonal quantum states implies the ability to communicate faster than light, using entanglement.

Alice and Bob share an entangled pair of qubits in the state $(|00\rangle + |11\rangle)/\sqrt{2}$. Then if Alice measures in the computational basis, the post-measurement state will be $|00\rangle$ with probability 1/2, and $|11\rangle$ with 1/2. Thus Bob has same probabilities in both states.

If Alice had instead measured in the $|+\rangle$, $|-\rangle$ basis, the state of Bob's system after the measurement will be $|+\rangle$ or $|-\rangle$ with probability 1/2 each.

If Bob had access to a devie that could distinguish the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ from one another, then he could tell whether alice had measured in the computational basis, or in the $|+\rangle$, $|-\rangle$ basis. Moreover he could get that information *instantaneously*, as soon as Alice had made the measurement. (faster-than-light communication)

Quantum money : banknotes imprinted with a serial #, and a sequence of qubits each in either the state $|0\rangle$ or $(|0\rangle+|1\rangle)/\sqrt{2}$. The bank maintains a list matching serial # to embedded states. The note is impossibel to counterfeit exactly, because it is impossible for a would-be counterfeiter to determine with certainty the state of the quvits in the original note, without destroying them.

This idea is the basis for numerous other quantum cryptographic protocols, and demonstrates the utility of the indistinguishability of non-orthogonam quantum states.

Creation and transformation of entanglement Engtanglement is another elementary static resource of quantum mecanics.
→ Amazingly different; HOWEVER note yet well understood

eg. Two information-theoretic problems related to entanglement Creating entanglement
Transfering entanglement : A, B share Bell state, and wish to transform it into some other type of entanglement.

- What resources do they need to accomplish this task?
- Can they do it without communicating?
- With classical communication only?
-

1.6.2 Quantum information in a wider context

Quantum information theory : PART III

especially
Ch. 11 : deals with fundamental properties of entropy in quantum and classical information theory.
Ch. 12 : focuses on pure quantum information theory

Quantum information theory is the most abstract part of quantum computation and quantum information, yet in some sense it is also the most fundamental.

What is it that separates the quantum and the classical world?
What resources, unavailable in a classical world, are being utilized in a quantum computation?

Existing answers to these questions are foggy and incomplete; ti is our hope that the fog may yet lift in the years to come, and we will obtain a clear appreciation for the possibilities and limitations of quantum information processing.