SoS: Quantum Information, Computing and Quantum Technologies

Prakriti Shahi

June 2022

1 Introduction

Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems.

Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories. For example, there is a physical theory known as quantum electrodynamics which describes with fantastic accuracy the interaction of atoms and light. Quantum electrodynamics is built up within the framework of quantum mechanics, but it contains specific rules not determined by quantum mechanics. The relationship of quantum mechanics to specific physical theories like quantum electrodynamics is rather like the relationship of a computer's operating system to specific applications software – the operating system sets certain basic parameters and modes of operation, but leaves open how specific tasks are accomplished by the applications.

2 History

In the early 1980s, interest arose in whether it might be possible to use quantum effects to signal faster than light – a big no-no according to Einstein's theory of relativity. The resolution of this problem turns out to hinge on whether it is possible to clone an unknown quantum state, that is, construct a copy of a quantum state. If cloning were possible, then it would be possible to signal faster than light using quantum effects. However, cloning – so easy to accomplish with classical information (consider the words in front of you, and where they came from!) – turns out not to be possible in general in quantum mechanics. This no-cloning theorem, is one of the earliest results of quantum computation and quantum information.

A related historical strand contributing to the development of quantum computation and quantum information is the interest, dating to the 1970s, of obtaining complete control over single quantum systems. For example, superconductivity has a superb quantum mechanical explanation. However, because a

superconductor involves a huge (compared to the atomic scale) sample of conducting metal, we can only probe a few aspects of its quantum mechanical nature, with the individual quantum systems constituting the superconductor remaining inaccessible. Since the 1970s many techniques for controlling single quantum systems have been developed. For example, 'atom traps' for trapping single atoms using scanning tunnel microscope, etc. By obtaining complete control over single quantum systems, we are exploring untouched regimes of Nature in the hope of discovering new and unexpected phenomena.

Quantum computation and quantum information provide a useful series of challenges at varied levels of difficulty for people devising methods to better manipulate single quantum systems, and stimulate the development of new experimental techniques and provide guidance as to the most interesting directions in which to take experiment. Conversely, the ability to control single quantum systems is essential if we are to harness the power of quantum mechanics for applications to quantum computation and quantum information. Despite this intense interest, efforts to build quantum information processing systems have resulted in modest success to date.

Small quantum computers capable of a few dozens of operations on qubits and experimental prototypes for doing quantum cryptography have been demonstrated. However, it remains a great challenge to physicists and engineers of the future to develop techniques for making large-scale quantum information processing a reality.

History of Computer Science

The modern incarnation of computer science was announced by the great mathematician Alan Turing in a remarkable 1936 paper. Turing showed that there is a Universal Turing Machine that can be used to simulate any other Turing machine. Furthermore, he claimed that the Universal Turing Machine completely captures what it means to perform a task by algorithmic means. That is, if an algorithm can be performed on any piece of hardware (say, a modern personal computer), then there is an equivalent algorithm for a Universal Turing Machine which performs exactly the same task as the algorithm running on the personal computer. This assertion, known as the Church–Turing thesis in honor of Turing and another pioneer of computer science, Alonzo Church, asserts the equivalence between the physical concept of what class of algorithms can be performed on some physical device with the rigorous mathematical concept of a Universal Turing Machine. The broad acceptance of this thesis laid the foundation for the development of a rich theory of computer science.

Computer hardware has grown in power at an amazing pace ever since, so much so that the growth was codified by Gordon Moore in 1965 in what has come to be known as Moore's law, which states that computer power will double for constant cost roughly once every two years. Moore's law has held true so far but most observers expect that this dream run will end some time during the first two decades of the twenty-first century. Conventional approaches to the

fabrication of computer technology are beginning to run up against fundamental difficulties of size. Quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller. One possible solution to this problem is quantum computation. Quantum computers offer an essential speed advantage over classical computers. This speed advantage is so significant that many researchers believe that no conceivable amount of progress in classical computation would be able to overcome the gap between the power of a classical computer and the power of a quantum computer.

'Efficient' vs 'Inefficient' simulations of a quantum computer

an efficient algorithm is one which runs in time polynomial in the size of the problem solved. In contrast, an inefficient algorithm requires super-polynomial (typically exponential) time. The strong Church-Turing thesis states: Any algorithmic process can be simulated efficiently using a Turing machine.

One class of challenges to the strong Church–Turing thesis comes from the field of analog computation. Unfortunately for analog computation, it turns out that when realistic assumptions about the presence of noise in analog computers are made, their power disappears in all known instances; they cannot efficiently solve problems which are not efficiently solvable on a Turing machine. This lesson – that the effects of realistic noise must be taken into account in evaluating the efficiency of a computational model – was one of the great early challenges of quantum computation and quantum information, a challenge successfully met by the development of a theory of quantum error-correcting codes and fault-tolerant quantum computation. Thus, unlike analog computation, quantum computation can in principle tolerate a finite amount of noise and still retain its computational advantages.

The first major challenge to the strong Church–Turing thesis arose in the mid 1970s, when Robert Solovay and Volker Strassen showed that it is possible to test whether an integer is prime or composite using a randomized algorithm. The algorithm could determine that a number was probably prime or else composite with certainty. Randomized algorithms pose a challenge to the strong Church–Turing thesis, suggesting that there are efficiently soluble problems which, nevertheless, cannot be efficiently solved on a deterministic Turing machine. This challenge appears to be easily resolved by a simple modification of the strong Church–Turing thesis: Any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

In 1985, David Deutsch attempted to define a computational device that would be capable of efficiently simulating an arbitrary physical system. Because the laws of physics are ultimately quantum mechanical, Deutsch was naturally led to consider computing devices based upon the principles of quantum mechanics. These devices, quantum analogues of the machines defined forty-nine years earlier by Turing, led ultimately to the modern conception of a quantum computer. Deutsch asked whether it is possible for a quantum computer to

efficiently solve computational problems which have no efficient solution on a classical computer, even a probabilistic Turing machine. He then constructed a simple example suggesting that, indeed, quantum computers might have computational powers exceeding those of classical computers.

Quantum computation and quantum information has taught us to think physically about computation, and we have discovered that this approach yields many new and exciting capabilities for information processing and communication. Computer scientists and information theorists have been gifted with a new and rich paradigm for exploration. Indeed, in the broadest terms we have learned that any physical theory, not just quantum mechanics, may be used as the basis for a theory of information processing and communication. The fruits of these explorations may one day result in information processing devices with capabilities far beyond today's computing and communications systems, with concomitant benefits and drawbacks for society as a whole. Quantum computation and quantum information certainly offer challenges aplenty to physicists, but it is perhaps a little subtle what quantum computation and quantum information offers to physics in the long term. We believe that just as we have learned to think physically about computation, we can also learn to think computationally about physics.

3 Quantum bits (Qubits)

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, or qubit for short. A qubit is a mathematical object with certain specific properties. Rather remarkably, we cannot examine a qubit to determine its quantum state, that is, the values of α and β. When we measure a qubit we get either the result 0, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$

$$|\alpha|^2 + |\beta|^2 = 1$$

Some of the ways the realization of a qubit may occur are: as the two different polarizations of a photon; as the alignment of a nuclear spin in a uniform magnetic field; as two states of an electron orbiting a single atom.

But more interestingly, by reducing the time we shine the light, an electron initially in the state $|0\rangle$ can be moved 'halfway' between $|0\rangle$ and $|1\rangle$, into the $|+\rangle$ state.

because $|\alpha^2| + |\beta^2| = 1$ we can write equation as

$$|\psi\rangle = e^{i\gamma}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big)$$

here θ, ϕ and γ are real numbers. We can ignore the factor of $e^{i\gamma}$ out the front, because it has no observable effects, and for that reason we can effectively write

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

The numbers θ and ϕ define a point on the unit three-dimensional sphere. This sphere is often called the Bloch sphere An important two qubit state is the Bell state or EPR pair,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

These correlations have been the subject of intense interest ever since a famous paper by Einstein, Podolsky and Rosen, in which they first pointed out the strange properties of states like the Bell state. EPR's insights were taken up and greatly improved by John Bell, who proved an amazing result: the measurement correlations in the Bell state are stronger than could ever exist between classical systems

4 Quantum computation

It turns out that this linear behavior is a general property of quantum mechanics, and very well motivated empirically; moreover, nonlinear behavior can lead to apparent paradoxes such as time travel, faster-than-light communication, and violations of the second laws of thermodynamic The prototypical multi-qubit quantum logic gate is the controlled-`NOT` or `CNOT` gate. The action of the gate may be described as follows. If the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped. Another way of describing the is as a generalization of the classical gate, since the action of the gate may be summarized as $|A, B\rangle = |A, A \oplus B\rangle$ where $\oplus$ is addition modulo two, which is exactly what the `XOR` gate does. That is, the control qubit and the target qubit are `XOR`ed and stored in the target qubit.

The `XOR` and `NAND` gates are essentially irreversible or non-invertible. For example, given the output A $\oplus$ B from an `XOR` gate, it is not possible to determine what the inputs A and B were; there is an irretrievable loss of information associated with the irreversible action of the `XOR` gate. On the other hand, unitary quantum gates are always invertible, since the inverse of a unitary matrix is also a unitary matrix, and thus a quantum gate can always be inverted by another quantum gate.

Any multiple qubit logic gate may be composed from `CNOT` and single qubit gates. The proof is the quantum parallel of the universality of the `NAND` gate. Given any basis states $|a\rangle$ and $|b\rangle$ for a qubit, it is possible to express an arbitrary state as a linear combination $\alpha|a\rangle + \beta|b\rangle$ of those states. Furthermore, provided the states are orthonormal, it is possible to perform a measurement with respect to the $|a\rangle$, $|b\rangle$ basis, giving the result a with probability $|\alpha|^2$ and b with probability $|\beta|^2$. The orthonormality constraint is necessary in order that $|\alpha|^2 + |\beta|^2 = 1$ as we expect for probabilities. In an analogous way it is possible in principle to measure a quantum system of many qubits with respect to an arbitrary orthonormal basis.

There are a few features allowed in classical circuits that are not usually present in quantum circuits. First of all, we don't allow 'loops', that is, feedback from one part of the quantum circuit to another; we say the circuit is acyclic.

Second, classical circuits allow wires to be 'joined' together, an operation known as `FANIN`, with the resulting single wire containing the bitwise `OR` of the inputs. Obviously this operation is not reversible and therefore not unitary, so we don't allow `FANIN` in our quantum circuits. Third, the inverse operation, `FANOUT`, whereby several copies of a bit are produced is also not allowed in quantum circuits. In fact, it turns out that quantum mechanics forbids the copying of a qubit, making the `FANOUT` operation impossible!

4.1 Qubit copying circuit?

The `CNOT` gate is useful for demonstrating one particularly fundamental property of quantum information. Consider the task of copying a classical bit. This may be done using a classical gate, which takes in the bit to copy (in some unknown state x) and a 'scratchpad' bit initialized to zero Suppose we try to copy a qubit in the unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ in the same manner by using a `CNOT` gate. The input state of the two qubits may be written as

$$[a|0\rangle + b|1\rangle] = a|00\rangle + b|10\rangle$$

The function of `CNOT` is to negate the second qubit when the first qubit is 1, and thus the output is simply $a|00\rangle + b|11\rangle$.In the case where $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$ it is possible to use quantum circuits to copy classical information encoded as a $|0\rangle$ or a $|1\rangle$. However, for a general state $|\psi\rangle$ we see that

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

Comparing with $a|00\rangle + b|11\rangle$, we see that unless $ab = 0$ the 'copying circuit' above does not copy the quantum state input. In fact, it turns out to be impossible to make a copy of an unknown quantum state. This property, that qubits cannot be copied, is known as the no-cloning theorem, and it is one of the chief differences between quantum and classical information. There is another way of looking at the failure of the circuit. Based on the intuition that a qubit somehow contains 'hidden' information not directly accessible to measurement. Consider what happens when we measure one of the qubits of the state $a|00\rangle + b|11\rangle$. As previously described, we obtain either 0 or 1 with probabilities $|a|^2$ and $|b|^2$. However, once one qubit is measured, the state of the other one is completely determined, and no additional information can be gained about a and b. In this sense, the extra hidden information carried in the original qubit $|\psi\rangle$ was lost in the first measurement, and cannot be regained. If, however, the qubit had been copied, then the state of the other qubit should still contain some of that hidden information. Therefore, a copy cannot have been created.

4.1.1 Example: Bell states

Let's consider a slightly more complicated circuit which has a Hadamard gate followed by a `CNOT`, and transforms the four computational basis states according to the table given. As an explicit example, the Hadamard gate takes the input

$|00\rangle$ to $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$, and then the `CNOT` gives the output state $(|00\rangle + |11\rangle)/\sqrt{2}$. Note how this works: first, the Hadamard transform puts the top qubit in a superposition; this then acts as a control input to the `CNOT` , and the target gets inverted only when the control is 1. The output states

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\beta_{01}\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$|\beta_{00}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

are known as the Bell states, or sometimes the EPR states or EPR pairs, after some of the people – Bell, and Einstein, Podolsky, and Rosen – who first pointed out the strange properties of states like these.

4.1.2 Example: quantum teleportation

Quantum teleportation is a technique for moving quantum states around, even in the absence of a quantum communications channel linking the sender of the quantum state to the recipient. There are many interesting features of teleportation. Quantum teleportation does not enable faster than light communication, because to complete the teleportation one must transmit his/her measurement result to the receiver over a classical communications channel. Without this classical communication, teleportation does not convey any information at all. The classical channel is limited by the speed of light, so it follows that quantum teleportation cannot be accomplished faster than the speed of light, resolving the apparent paradox. A second puzzle about teleportation is that it appears to create a copy of the quantum state being teleported, in apparent violation of the no-cloning theorem. Quantum teleportation emphasizes the interchangeability of different resources in quantum mechanics, showing that one shared EPR pair together with two classical bits of communication is a resource at least the equal of one qubit of communication. Quantum computation and quantum information has revealed a plethora of methods for interchanging resources, many built upon quantum teleportation.

5 Intro to Quantum Mechanics

The standard quantum mechanical notation for a vector in a vector space is the following: $|\psi\rangle$

Discussions of quantum mechanics often refer to Hilbert space. In the finite dimensional complex vector spaces that come up in quantum computation and quantum information, a Hilbert space is exactly the same thing as an inner

product space. Suppose A is any linear operator on a Hilbert space, V . It turns out that there exists a unique linear operator $A^\dagger$ on V such that for all vectors $|v\rangle$, $|w\rangle \in$ V ,

$$(|v\rangle, A|w\rangle) = \left(A^\dagger|v\rangle, |w\rangle\right).$$

5.1 Postulates of Quantum Mechanics

5.1.1 State space

The first postulate of quantum mechanics is about Hilbert space.
Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space. Quantum mechanics does not tell us, for a given physical system, what the state space of that system is, nor does it tell us what the state vector of the system is. Quantum electrodynamics (often known as QED), which describes how atoms and light interact provides a solution for that *specific* system with intricate and beautiful rules.
A qubit has a two-dimensional state space. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

where a and b are complex numbers. The condition that $|\psi\rangle$ be a unit vector, $\langle\psi|\psi\rangle = 1$, is therefore equivalent to $|a|^2+|b|^2=1$. The condition $\langle\psi|\psi\rangle = 1$ is often known as the normalization condition for state vectors . We say that any linear combination $\sum_i \alpha_i|\psi_i\rangle$ is a superposition of the states $|\psi_i\rangle$ with amplitude α_i for the state $|\psi_i\rangle$. So, for example, the state

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

is a superposition of the states $|0\rangle$ and $|1\rangle$ with amplitude $1/\sqrt{2}$ for the state $|0\rangle$, and amplitude $-1/\sqrt{2}$ for the state $|1\rangle$.

5.1.2 Evolution

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

Just as quantum mechanics does not tell us the state space or quantum state of a particular quantum system, it does not tell us which unitary operators U describe real world quantum dynamics. Quantum mechanics merely assures us that the evolution of any closed quantum system may be described in such a

way. In the case of single qubits, it turns out that any unitary operator at all can be realized in realistic systems. The X and Z Pauli matrices are also sometimes referred to as the bit flip and phase flip matrices: the X matrix takes $|0\rangle$ to $|1\rangle$, and $|1\rangle$ to $|0\rangle$, thus earning the name bit flip; and the Z matrix leaves $|0\rangle$ invariant, and takes $|1\rangle$ to -$|1\rangle$, with the extra factor of -1 added known as a phase factor, thus justifying the term phase flip. Another interesting unitary operator is the Hadamard gate, which we denote using H. This has the action $H|0\rangle \equiv(|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle \equiv(|0\rangle - |1\rangle)/\sqrt{2}$, and corresponding matrix representation

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Postulate 2 requires that the system being described be closed. In reality, of course, all systems (except the Universe as a whole) interact at least somewhat with other systems. Nevertheless, there are interesting systems which can be described to a good approximation as being closed, and which are described by unitary evolution to some good approximation. A more refined version of this postulate can be given which describes the evolution of a quantum system in continuous time.

Postulate 2' : The time evolution of the state of a closed quantum system is described by the Schrödinger equation,

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

If we know the Hamiltonian of a system, then (together with a knowledge of $\hbar$) we understand its dynamics completely, at least in principle. Because the Hamiltonian is a Hermitian operator it has a spectral decomposition. with eigenvalues E and corresponding normalized eigenvectors $|E\rangle$. The states $|E\rangle$ are conventionally referred to as energy eigenstates, or sometimes as stationary states, and E is the energy of the state $|E\rangle$. The lowest energy is known as the ground state energy for the system, and the corresponding energy eigenstate (or eigenspace) is known as the ground state.

5.1.3 Quantum measurement

Postulate 3: Quantum measurements are described by a collection M_m of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle,$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle$$

A simple but important example of a measurement is the measurement of a qubit in the computational basis. Each measurement operator is Hermitian, and $M_0^2 = M_0$, $M_1^2 = M_1$. Thus the completeness relation is obeyed, $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. Suppose the state being measured is $|\psi\rangle = a|0\rangle + b|1\rangle$. Then the probability of obtaining measurement outcome 0 is

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2$$

Similarly, the probability of obtaining the measurement outcome 1 is $p(1) = |b|^2$. The state after measurement in the two cases is therefore

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle$$

multipliers like $a/|a|$, which have modulus one, can effectively be ignored, so the two post-measurement states are effectively $|0\rangle$ and $|1\rangle$.

5.1.4 Distinguishing quantum states

In the classical world, distinct states of an object are usually distinguishable, at least in principle. Quantum mechanically, the situation is more complicated. Non-orthogonal quantum states cannot be distinguished.

5.1.5 Projective measurements

Projective measurements: A projective measurement is described by an observable, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition ,

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues, m, of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result m is given by

$$p(m) = \langle\psi|P_m|\psi\rangle$$

Given that outcome m occurred, the state of the quantum system immediately after the measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$$

By definition, the average value of the measurement is

$$E(M) = \langle\psi|M|\psi\rangle$$

From this formula for the average follows a formula for the standard deviation associated to observations of M,

$$[\Delta(M)]^2 = \langle(M - \langle M\rangle)^2\rangle = \langle M^2\rangle - \langle M\rangle^2$$

The standard deviation is a measure of the typical spread of the observed values upon measurement of M. In particular, if we perform a large number of experiments in which the state $|\psi\rangle$ is prepared and the observable M is measured, then the standard deviation $\Delta(M)$ of the observed values is determined by the formula $\Delta(M) = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$. This formulation of measurement and standard deviations in terms of observables gives rise an elegant way to results such as the Heisenberg uncertainty principle.

More generally, suppose $\vec{v}$ is any real three-dimensional unit vector. Then we can define an observable:

$$\vec{v}.\vec{\sigma} \equiv v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3.$$

Measurement of this observable is sometimes referred to as a 'measurement of spin along the $\vec{v}$ axis', for historical reasons.

5.1.6 POVM measurements

The acronym POVM stands for 'Positive Operator-Valued Measure'. Suppose a measurement described by measurement operators M_m is performed upon a quantum system in the state $|\psi\rangle$. Then the probability of outcome m is given by $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$.
Suppose we define

$$E_m M_m^\dagger M_m$$

Then from Postulate 3 and elementary linear algebra, E_m is a positive operator such that $\sum_m E_m = I$ and $p(m) = \langle\psi|E_m|\psi\rangle$ .Thus the set of operators E_m are sufficient to determine the probabilities of the different measurement outcomes. The operators E_m are known as the POVM elements associated with the measurement. The complete set $\{E_m\}$ is known as a POVM

5.1.7 Composite systems

The following postulate describes how the state space of a composite system is built up from the state spaces of the component systems.
Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

the superposition principle of quantum mechanics, which states that if $|x\rangle$ and $|y\rangle$ are two states of a quantum system, then any superposition $\alpha|x\rangle + \beta|y\rangle$ should also be an allowed state of a quantum system, where $|\alpha|^2 + |\beta|^2 = 1$. For composite systems, it seems natural that if $|A\rangle$ is a state of system A, and $|B\rangle$ is a state of system B, then there should be some corresponding state, which we might denote $|A\rangle|B\rangle$, of the joint system AB. Applying the superposition principle to product states of this form, we arrive at the tensor product postulate given above.

5.1.8 Quantum mechanics: a global view

Postulate 1 sets the arena for quantum mechanics, by specifying how the state of an isolated quantum system is to be described. Postulate 2 tells us that the dynamics of closed quantum systems are described by the Schrödinger equation, and thus by unitary evolution. Postulate 3 tells us how to extract information from our quantum systems by giving a prescription for the description of measurement. Postulate 4 tells us how the state spaces of different quantum systems may be combined to give a description of the composite system.

5.2 The density operator

5.2.1 Ensembles of quantum states

Suppose a quantum system is in one of a number of states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i. We shall call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i |\psi\rangle\langle\psi|$$

Suppose, for example, that the evolution of a closed quantum system is described by the unitary operator U. If the system was initially in the state $|\psi\rangle$ with probability p_i then after the evolution has occurred the system will be in the state $U|\psi_i\rangle$ with probability p_i. Thus, the evolution of the density operator is described by the equation

$$\rho \equiv \sum_i p_i |\psi\rangle\langle\psi| \xrightarrow{\mathrm{U}} \sum_i p_i U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger$$

Suppose we perform a measurement described by measurement operators M_m. If the initial state was $|\psi\rangle$, then the probability of getting result m is

$$\begin{aligned} p(m) &= \sum_i p(m|i)p_i \\ &= \sum_i p_i tr(M - m^\dagger M - m|\psi\rangle\langle\psi|) \\ &= tr(M_m^\dagger M_m \rho) \end{aligned}$$

If the initial state was $|\psi\rangle$ then the state after obtaining the result m is

$$|\psi_i^m\rangle = \frac{M_m|\psi - i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}}$$

Thus, after a measurement which yields the result m we have an ensemble of states $|\psi_i^m\rangle$ with respective probabilities $p(i|m)$. The corresponding density operator ρ_m is therefore

$$\rho_m = \sum_{[} ip(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}$$

But by elementary probability theory, $p(i|m) = p(m,i)/p(m) = p(m|i)p_i/p(m)$. Substituting we obtain

$$\begin{aligned} \rho_m &= \sum_i p_i \frac{M_m|\psi_i le\langle\psi_i|M_m^\dagger}{tr(M_m^\dagger M_m \rho)} \\ &= \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)} \end{aligned}$$

TF

A quantum system whose state $|\psi\rangle$ is known exactly is said to be in a pure state. In this case the density operator is simply $\rho = |\psi\rangle\langle\psi|$. Otherwise, ρ is in a mixed state; it is said to be a mixture of the different pure states in the ensemble for ρ.

Finally, imagine a quantum system is prepared in the state ρ_i with probability p_i. It is not difficult to convince yourself that the system may be described by the density matrix $\sum_i p_i p_i$. A proof of this is to suppose that ρ_i arises from some ensemble $\{p_{ij}, |\psi_{ij}\rangle\}$ (note that i is fixed) of pure states, so the probability for being in the state$|\psi_{ij}\rangle$ is $p_i p_{ij}$. The density matrix for the system is thus

$$\rho = \sum_{ij} p_i p_{ij}|\psi_{ij}\rangle\langle\psi_{ij}| = \sum_i p_i \rho_i$$

where we have used the definition $\rho_i = \sum_j p_{ij}|\psi_{ij}\rangle\langle\psi_{ij}|$. We say that ρ is a mixture of the states ρ_i with probabilities p_i.

5.2.2 General properties of the density operator

Theorem 2.5: (Characterization of density operators) An operator ρ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if it satisfies the conditions:

1. (Trace condition) ρ has trace equal to one.
2. (Positivity condition) ρ is a positive operator.

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its density operator, which is a positive operator ρ with trace one, acting on the state space of the system. If a quantum system is in the state ρ_i with probability p_i, then the density operator for the system is $\sum_i p_i \rho_i$

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state ρ of the system at time t_1 is related to the state ρ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$\rho' = U \rho U^\dagger$$

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is ρ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = tr(M_m^\dagger M_m \rho)$$

and the state of the system after the measurement is

$$\frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)}$$

. The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state ρ_i, then the joint state of the total system is $\rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n$.

the density operator approach really shines for two applications: the description of quantum systems whose state is not known, and the description of subsystems of a composite quantum system.

Theorem 2.6: (Unitary freedom in the ensemble for density matrices) The sets $|\tilde{\psi_i}\rangle$ and $|\tilde{\phi_j}\rangle$ generate the same density matrix if and only if

$$|\tilde{\psi_i}\rangle = \sum_j u_{ij}|\tilde{\phi_j}\rangle$$

where u_{ij} is a unitary matrix of complex numbers, with indices$i$ and j, and we 'pad' whichever set of vectors $|\tilde{\psi_i}\rangle$ or $|\tilde{\phi_i}\rangle$ is smaller with additional vectors 0 so that the two sets have the same number of elements

As a consequence of the theorem, note that $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_j q_j|\phi_j\rangle\langle\phi_j|$ for normalized states $|\psi_i\rangle$,$|\phi_j\rangle$ and probability distributions p_i and q_j if and only if

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\phi_j\rangle.$$

for some unitary matrix u_{ij} , and we may pad the smaller ensemble with entries having probability zero in order to make the two ensembles the same size. Thus, Theorem 2.6 characterizes the freedom in ensembles $\{p_i, |\psi_i\rangle\}$ giving rise to a given density matrix ρ.

5.2.3 The reduced density operator

Perhaps the deepest application of the density operator is as a descriptive tool for sub-systems of a composite quantum system. Such a description is provided by the reduced density operator. The reduced density operator is so useful as to be virtually indispensable in the analysis of composite quantum systems. Suppose we have physical systems A and B, whose state is described by a density operator ρ^{AB}. The reduced density operator for system A is defined by

$$\rho^A \equiv tr_{_B}\rho^{AB}$$

where $tr_{_B}$is a map of operators known as the partial trace over system B. The partial trace is defined by

$$tr_{_B}(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2|tr(|b_1\rangle\langle b_2|)$$

where $|a_1\rangle$ and $|a_2\rangle$ are any two vectors in the state space of A, and$|b_1\rangle$and $|b_2\rangle$ are any two vectors in the state space of B. The trace operation appearing on the right hand side is the usual trace operation for system B, so $tr(|b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle$. We have defined the partial trace operation only on a special subclass of operators on AB;

Quantum teleportation and the reduced density operator: A useful application of the reduced density operator is to the analysis of quantum teleportation.

5.3 The Schmidt decomposition and purifications

Theorem 2.7: (Schmidt decomposition) Suppose $|\psi\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_A\rangle$ for system A, and

orthonormal states $|i_B\rangle$ of system B such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle \| i_B\rangle$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as Schmidt coefficients. Let $|\psi\rangle$ be a pure state of a composite system, AB. Then by the Schmidt decomposition $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$ and $\rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$, so the eigenvalues of ρ^A and ρ^B are identical, namely λ_i^2 for both density operators. Many important properties of quantum systems are completely determined by the eigenvalues of the reduced density operator of the system, so for a pure state of a composite system such properties will be the same for both systems. The Schmidt number is an important property of a composite quantum system, which in some sense quantifies the 'amount' of entanglement between systems A and B. Algebraic invariance properties make the Schmidt number a very useful tool.

5.4 EPR and the Bell inequality

When we speak of an object such as a person or a book, we assume that the physical properties of that object have an existence independent of observation. That is, measurements merely act to reveal such physical properties. As quantum mechanics was being developed in the 1920s and 1930s a strange point of view arose that differs markedly from the classical view. According to quantum mechanics, an unobserved particle does not possess physical properties that exist independent of observation. Rather, such physical properties arise as a consequence of measurements performed upon the system. For example, according to quantum mechanics a qubit does not possess definite properties of 'spin in the z direction, σ_z', and 'spin in the x direction, σ_x' ,each of which can be revealed by performing the appropriate measurement. Rather, quantum mechanics gives a set of rules which specify, given the state vector, the probabilities for the possible measurement outcomes when the observable σ_z is measured, or when the observable σ_x is measured.

Many physicists rejected this new view of Nature. The most prominent objector was Albert Einstein. In the famous 'EPR paper', co-authored with Nathan Rosen and Boris Podolsky, Einstein proposed a thought experiment which, he believed, demonstrated that quantum mechanics is not a complete theory of Nature.

EPR were interested in what they termed 'elements of reality'. Their belief was that any such element of reality must be represented in any complete physical theory. The goal of the argument was to show that quantum mechanics is not a complete physical theory, by identifying elements of reality that were not included in quantum mechanics. The way they attempted to do this was by introducing what they claimed was a sufficient condition for a physical property to be an element of reality, namely, that it be possible to predict with certainty the value that property will have, immediately before measurement.

The goal of EPR was to show that quantum mechanics is incomplete, by demonstrating that quantum mechanics lacked some essential 'element of reality', by their criterion. They hoped to force a return to a more classical view of the world, one in which systems could be ascribed properties which existed independently of measurements performed on those systems. Unfortunately for EPR, most physicists did not accept the above reasoning as convincing.

Nearly thirty years after the EPR paper was published, an experimental test was proposed that could be used to check whether or not the picture of the world which EPR were hoping to force a return to is valid or not. It turns out that Nature experimentally invalidates that point of view, while agreeing with quantum mechanics. The key to this experimental invalidation is a result known as Bell's inequality.

Imagine we perform the following experiment, Charlie prepares two particles. It doesn't matter how he prepares the particles, just that he is capable of repeating the experimental procedure which he uses. Once he has performed the preparation, he sends one particle to Alice, and the second particle to Bob. Once Alice receives her particle, she performs a measurement on it. Imagine that she has available two different measurement apparatuses, so she could choose to do one of two different measurements. These measurements are of physical properties which we shall label P_Q and P_R, respectively. Alice doesn't know in advance which measurement she will choose to perform. Rather, when she receives the particle she flips a coin or uses some other random method to decide which measurement to perform. We suppose for simplicity that the measurements can each have one of two outcomes, +1 or -1. Suppose Alice's particle has a value Q for the property P_Q. Q is assumed to be an objective property of Alice's particle, which is merely revealed by the measurement, much as we imagine the position of a tennis ball to be revealed by the particles of light being scattered off it. Similarly, let R denote the value revealed by a measurement of the property P_R.

Similarly, suppose that Bob is capable of measuring one of two properties, P_S or P_T , once again revealing an objectively existing value S or T for the property, each taking value +1 or -1. Bob does not decide beforehand which property he will measure, but waits until he has received the particle and then chooses randomly. The timing of the experiment is arranged so that Alice and Bob do their measurements at the same time. Therefore, the measurement which Alice performs cannot disturb the result of Bob's measurement (or vice versa), since physical influences cannot propagate faster than light. We are going to do some simple algebra with the quantity $QS + RS + RT - QT$.

Notice that

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T.$$

Because $R, Q = \pm 1$ it follows that either $(Q + R)S = 0$ or $(R - Q)T = 0$. In either case, it is easy to see that $QS + RS + RT - QT = \pm 2$. Suppose next that $p(q, r, s, t)$ is the probability that, before the measurements are performed, the system is in a state where $Q = q, R = r, S = s$, and $T = t$. These probabilities

may depend on how Charlie performs his preparation, and on experimental noise. Letting E$(\cdot)$ denote the mean value of a quantity, we have

$$\begin{aligned} E(QS + RS + RT - QT) &= \sum_{qrst} p(q,r,s,t)(qs + rs + rtqt) \\ &\leq \sum_{qrst} p(q,r,s,t) \times 2 \\ &= 2. \end{aligned}$$

Also,

$$\begin{aligned} E(QS + RS + RTQT) = &\sum_{qrst} p(q,r,s,t)qs + \sum_{qrst} p(q,r,s,t)rs \\ &+ \sum_{qrst} tp(q,r,s,t)rt - \sum_{qrst} p(q,r,s,t)qt \\ =&E(QS) + E(RS) + E(RT) - E(QT) \qquad TF \end{aligned}$$

Comparing, we obtain the Bell inequality,

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2.$$

By repeating the experiment many times, Alice and Bob can determine each quantity on the left hand side of the Bell inequality. It's time to put some quantum mechanics back in the picture. Imagine we perform the following quantum mechanical experiment. Charlie prepares a quantum system of two qubits in the state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

He passes the first qubit to Alice, and the second qubit to Bob. They perform measurements of the following observables

$$Q = Z_1 \qquad S = \frac{-Z_2 - X_2}{\sqrt{2}}$$

$$R = X_1 \qquad T = \frac{Z_2 - X_2}{\sqrt{2}}$$

Simple calculations show that the average values for these observables, written in the quantum mechanical $\langle\cdot\rangle$ notation, are:

$$\langle QS\rangle = \frac{1}{\sqrt{2}}; \langle RS\rangle = \frac{1}{\sqrt{2}}; \langle RT\rangle = \frac{1}{\sqrt{2}}; \langle QT\rangle = -\frac{1}{\sqrt{2}}$$

Thus,

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$$

We learned previously that the average value of QS plus the average value of RS plus the average value of RT minus the average value of QT can never exceed 2. Yet here, quantum mechanics predicts that this sum of averages yields $2sqrt2$!
Fortunately, we can ask Nature to resolve the apparent paradox for us. Clever experiments using photons – particles of light – have been done to check the prediction of quantum mechanics versus the Bell inequality which we were led to by our common sense reasoning. the results were resoundingly in favor of the quantum mechanical prediction. The Bell inequality is not obeyed by Nature. It means that one or more of the assumptions that went into the derivation of the Bell inequality must be incorrect.

There are two assumptions made in the proof of the Bell inequality which are questionable:

1. The assumption that the physical properties PQ, PR, PS, PT have definite values Q, R, S, T which exist independent of observation. This is sometimes known as the assumption of realism.
2. The assumption that Alice performing her measurement does not influence the result of Bob's measurement. This is sometimes known as the assumption of locality.

These two assumptions together are known as the assumptions of local realism. They are certainly intuitively plausible assumptions about how the world works, and they fit our everyday experience. Yet the Bell inequalities show that at least one of these assumptions is not correct.The world is not locally realistic. Most physicists take the point of view that it is the assumption of realism which needs to be dropped from our worldview in quantum mechanics, although others have argued that the assumption of locality should be dropped instead. Regardless, Bell's inequality together with substantial experimental evidence now points to the conclusion that either or both of locality and realism must be dropped from our view of the world if we are to develop a good intuitive understanding of quantum mechanics.

6 Quantum Computation

6.1 Quantum algorithms

Practically speaking, many interesting problems are impossible to solve on a classical computer, not because they are in principle insoluble, but because of the astronomical resources required to solve realistic cases of the problem. The spectacular promise of quantum computers is to enable new algorithms which render feasible problems requiring exorbitant resources for their solution on a classical computer. Two broad classes of quantum algorithms are known which fulfill this promise. The first class of algorithms is based upon Shor's quantum Fourier transform, and includes remarkable algorithms for solving the factoring and discrete logarithm problems, providing a striking exponential speedup over

the best known classical algorithms. The second class of algorithms is based upon Grover's algorithm for performing quantum searching. These provide a less striking but still remarkable quadratic speedup over the best possible classical algorithms. The quantum searching algorithm derives its importance from the widespread use of search-based techniques in classical algorithms, which in many instances allows a straightforward adaptation of the classical algorithm to give a faster quantum algorithm

The quantum searching algorithm has many potential applications. It can be used to extract statistics, such as the minimal element, from an unordered data set, more quickly than is possible on a classical computer. It can be used to speed up algorithms for some problems in **NP** – specifically, those problems for which a straightforward search for a solution is the best algorithm known. Finally, it can be used to speed up the search for keys to cryptosystems such as the widely used Data Encryption Standard (DES). The quantum Fourier transform also has many interesting applications. It can be used to solve the discrete logarithm and factoring problems. These results, in turn, enable a quantum computer to break many of the most popular cryptosystems now in use, including the RSA cryptosystem. The Fourier transform also turns out to be closely related to an important problem in mathematics, finding a hidden subgroup (a generalization of finding the period of a periodic function). coming up with good quantum algorithms seems to be a difficult problem. There are at least two reasons for this. First, algorithm design, be it classical or quantum, is not an easy business! Finding good quantum algorithms is made doubly difficult because of the additional constraint that we want our quantum algorithms to be better than the best known classical algorithms. A second reason for the difficulty of finding good quantum algorithms is that our intuitions are much better adapted to the classical world than they are to the quantum world. If we think about problems using our native intuition, then the algorithms which we come up with are going to be classical algorithms. It takes special insights and special tricks to come up with good quantum algorithms.

6.2 Single qubit operations

A single qubit is a vector $|\psi\rangle = a|0\rangle + b|1\rangle$ parameterized by two complex numbers satisfying $|a|^2 + |b|^2 = 1$. Operations on a qubit must preserve this norm, and thus are described by 2×2 unitary matrices. Of these, some of the most important are the Pauli matrices; it is useful to list them again here:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Three other quantum gates will play a large part in what follows, the Hadamard gate (denoted H), phase gate (denoted S), and $\pi/8$ gate (denoted T)

$$H \equiv \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

A couple of useful algebraic facts to keep in mind are that $H = (X+Z)/\sqrt{2}$ and $S = T^2$. A single qubit in the state $a|0\rangle + b|1\rangle$ can be visualized as a point θ, ϕ on the unit sphere, where $a = \cos(\theta/2), b = e^{i\phi}\sin(\theta/2)$, and a can be taken to be real because the overall phase of the state is unobservable. This is called the Bloch sphere representation, and the vector $(\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$ is called the Bloch vector.
. *Theorem*: ($Z-Y$ decomposition for a single qubit) Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha}R_x(\beta)R_y(\gamma)R_z(\delta)$$

Corollary: Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha}A \times B \times C$ where α is some overall phase factor.

6.3 Controlled operations

Controlled operation is one of the most useful in computing, both classical and quantum. The prototypical controlled operation is the controlled-`NOT` , which is a quantum gate with two input qubits, known as the control qubit and target qubit, respectively. In terms of the computational basis, the action of the `CNOT` is given by $|c\rangle|t\rangle \longrightarrow |c\rangle|t \oplus c\rangle$; that is, if the control qubit is set to $|1\rangle$ then the target qubit is flipped, otherwise the target qubit is left alone. Thus, in the computational basis $|control, target\rangle$ the matrix representation of `CNOT` is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

more generally, suppose U is an arbitrary single qubit unitary operation. A controlled U operation is a two qubit operation, again with a control and a target qubit. If the control qubit is set then U is applied to the target qubit, otherwise the target qubit is left alone; that is, $|c\rangle|t\rangle \Longrightarrow |c\rangle U^c|t\rangle$.

Apply the phase shift $e^{i\alpha}$ on the target qubit, controlled by the control qubit. That is, if the control qubit is $|0\rangle$, then the target qubit is left alone, while if the control qubit is $|1\rangle$, a phase shift $e^{i\alpha}$ is applied to the target . To verify that this circuit works correctly, note that the effect of the circuit on the right hand side is

$$|00\rangle \longrightarrow |00\rangle, |01\rangle \longrightarrow |01\rangle, |10\rangle \longrightarrow e^{i\alpha}|10\rangle, |11\rangle \longrightarrow e^{i\alpha}|11\rangle,$$

which is exactly what is required for the controlled operation on the left hand side. U may be written in the form $U = e^{i\alpha}AXBXC$, where A, B and C are single qubit operations such that $ABC = I$. Suppose that the control qubit is set. Then the operation $e^{i\alpha}AXBXC = U$ is applied to the second qubit. If, on the other hand, the control qubit is not set, then the operation $ABC = I$

is applied to the second qubit; that is, no change is made. That is, this circuit implements the controlled-U operation.

Suppose we have$n+k$ qubits, and U is a k qubit unitary operator. Then we define the controlled operation $C^n(U)$ by the equation

$$C^n(U)|x_1x_2...x_n\rangle|\psi\rangle = |x_1x_2...x_n\rangle U^{x_1x_2...x_n}|\psi\rangle$$

where $x_1x_2...x_n$ in the exponent of U means the product of the bits $x_1, x_2, ..., x_n$. That is, the operator U is applied to the last k qubits if the first n qubits are all equal to one, and otherwise, nothing is done.

For the following we assume that $k = 1$, for simplicity. Larger k can be dealt with using essentially the same methods, however for $k \geq 2$ there is the added complication that we don't (yet) know how to perform arbitrary operations on k qubits.

Suppose U is a single qubit unitary operator, and V is a unitary operator chosen so that $V^2 = U$. Then the operation $C^2(U)$ may be implemented using a particular circuit. Defining $V \equiv (1-i)(I+iX)/2$ and noting that $V^2 = X$, we get the implementation of the Toffoli gate in terms of one and two qubit operations. any unitary operation can be composed to an arbitrarily good approximation from just the Hadamard, phase, controlled-`NOT` and $\pi/8$ gates. Because of the great usefulness of the Toffoli gate it is interesting to see how it can be built from just this gate set.

In the controlled gates we have been considering, conditional dynamics on the target qubit occurs if the control bits are set to one. Of course, there is nothing special about one, and it is often useful to consider dynamics which occur conditional on the control bit being set to zero. For instance, suppose we wish to implement a two qubit gate in which the second ('target') qubit is flipped, conditional on the first ('control') qubit being set to zero. Generically we shall use the open circle notation to indicate conditioning on the qubit being set to zero, while a closed circle indicates conditioning on the qubit being set to one.

6.4 Measurement

There are two important principles that are worth bearing in mind about quantum circuits. Both principles are rather obvious; however, they are of great utility. The first principle is that classically conditioned operations can be replaced by quantum conditioned operations:

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations. Often, quantum measurements are performed as an intermediate step in a quantum circuit, and the measurement results are used to conditionally control subsequent quantum gates. This is the case, for example, in the teleportation circuit. However, such measurements can always be moved to the end of the circuit.The

second principle is even more obvious - and useful!

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured. Imagine a quantum circuit containing just two qubits, and only the first qubit is measured at the end of the circuit. Then the measurement statistics observed at this time are completely determined by the reduced density matrix of the first qubit. However, if a measurement had also been performed on the second qubit, then it would be highly surprising if that measurement could change the statistics of measurement on the first qubit.The role of measurements in quantum circuits, as an interface between the quantum and classical world is generally considered to be an irreversible operation, destroying quantum information and replacing it with classical information. In certain carefully designed cases, however, this need not be true, as is vividly illustrated by teleportation and quantum error-correction. What teleportation and quantum error-correction have in common is that in neither instance does the measurement result reveal any information about the identity of the quantum state being measured. In order for a measurement to be reversible, it must reveal no information about the quantum state being measured!

6.5 Universal quantum gates

A set of gates is said to be universal for quantum computation if any unitary operation may be approximated to arbitrary accuracy by a quantum circuit involving only those gates. Any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, `CNOT` , and $\pi/8$ gates.
The first construction shows that an arbitrary unitary operator may be expressed exactly as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states. The second construction combines the first construction with the results of the previous section to show that an arbitrary unitary operator may be expressed exactly using single qubit gates. The third construction combines the second construction with a proof that single qubit operation may be approximated to arbitrary accuracy using the Hadamard, phase, `CNOT` , and $\pi/8$ gates. This in turn implies that any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, `CNOT` , and $\pi/8$ gates. Our constructions say little about efficiency – how many (polynomially or exponentially many) gates must be composed in order to create a given unitary transform. Of course, the goal of quantum computation is to find interesting families of unitary transformations that can be performed efficiently.

6.5.1 Two-level unitary gates are universal

Consider a unitary matrix U which acts on a d-dimensional Hilbert space. In this section we explain how U may be decomposed into a product of two-level

unitary matrices; that is, unitary matrices which act non-trivially only on two-or-fewer vector components. A corollary of the above result is that an arbitrary unitary matrix on an n qubit system may be written as a product of at most $2^{n-1}(2^n-1)$ two-level unitary matrices. For specific unitary matrices, it may be possible to find much more efficient decompositions, but as you will now show there exist matrices which cannot be decomposed as a product of fewer than $d-1$ two-level unitary matrices!

6.5.2 Single qubit and gates are universal

Single qubit and gates together can be used to implement an arbitrary two-level unitary operation on the state space of n qubits. Single qubit `CNOT` and gates can be used to implement an arbitrary unitary operation on n qubits,and therefore are universal for quantum computation. to construct a circuit built from single qubit `CNOT` and gates.we need to make use of Gray codes. Suppose we have distinct binary numbers, s and t. A Gray code connecting s and t is a sequence of binary numbers, starting with s and concluding with t, such that adjacent members of the list differ in exactly one bit. For instance, with $s = 101001$ and $t = 110011$ we have the Gray code.

$$\begin{array}{cccccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array}$$

Let g_1 through g_m be the elements of a Gray code connecting s and t, with g_1 = s and $g_m = t$. Note that we can always find a Gray code such that $m \leq n+1$ since s and t can differ in at most n locations.

6.5.3 Approximating unitary operators

Obviously, a discrete set of gates can't be used to implement an arbitrary unitary operations exactly, since the set of unitary operations is continuous. Rather, it turns out that a discrete set can be used to approximate any unitary operation. To understand how this works, we first need to study what it means to approximate a unitary operation. Suppose U and V are two unitary operators on the same state space. U is the target unitary operator that we wish to implement, and V is the unitary operator that is actually implemented in practice. We define the error when V is implemented instead of U by

$$E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$$

where the maximum is over all normalized quantum states $|\psi\rangle$. In the state space this measure of error has the interpretation that if $E(U,V)$ is small, then any measurement performed on the state $V|\psi\rangle$ will give approximately the same

measurement statistics as a measurement of $U|\psi\rangle$, for any initial state $|\psi\rangle$. More precisely, we show that if M is a POVM element in an arbitrary **POVM**, and P_U (or P_V) is the probability of obtaining this outcome if U (or V) were performed with a starting state $|\psi\rangle$, then

$$|P_U - P_V| \leq 2E(U, V)$$

Thus, if $E(U, V)$ is small, then measurement outcomes occur with similar probabilities, regardless of whether U or V were performed. If we perform a sequence of gates $V_1, ..., V_m$ intended to approximate some other sequence of gates $U_1, ..., U_m$ then the errors add at most linearly,

$$E(U_m U_{m-1} ... U_1, V_m V_{m-1} ... V_1) \leq \sum_{j=1}^{M} E(U_j, V_j)$$

Suppose we wish to perform a quantum circuit containing m gates, U_1through U_m. Unfortunately, we are only able to approximate the gate U_j by the gate V_j . In order that the probabilities of different measurement outcomes obtained from the approximate circuit be within a tolerance $\Delta \geq 0$ of the correct probabilities, it suffices that $E(U_j, V_j) \leq \frac{\Delta}{2m}$

Universality of Hadamard + phase + `CNOT` + $\pi/8$ gates: We're now in a good position to study the approximation of arbitrary unitary operations by discrete sets of gates. We're going to consider two different discrete sets of gates, both of which are universal. The first set, the standard set of universal gates, consists of the Hadamard, phase, `CNOT` and $\pi/8$ gates. The second set of gates we consider consists of the Hadamard gate, phase gate, the `CNOT` gate, and the Toffoli gate. These gates can also all be done fault-tolerantly; however, the universality proof and fault-tolerance construction for these gates is a little less appealing.

6.5.4 Approximating arbitrary unitary gates is generically hard

We've seen that any unitary transformation on n qubits can be built up out of a small set of elementary gates. Is it always possible to do this efficiently?

The answer to this question turns out to be a resounding no: in fact, most unitary transformations can only be implemented very inefficiently. One way to see this is to consider the question: how many gates does it take to generate an arbitrary state of n qubits? A simple counting argument shows that this requires exponentially many operations, in general; it immediately follows that there are unitary operations requiring exponentially many operations. To see this, suppose we have g different types of gates available, and each gate works on at most f input qubits. These numbers, f and g, are fixed by the computing hardware we have available, and may be considered to be constants. Suppose we have a quantum circuit containing m gates, starting from the computational basis state $|0\rangle^{\otimes n}$ For any particular gate in the circuit there are therefore at most $\begin{bmatrix} n \\ f \end{bmatrix}^g = O(n^{fg})$ possible choices. It follows that at most $O(n^{fgm})$ different

states may be computed using m gates to within a polynomial factor the construction for universality we have given is optimal; unfortunately, it does not address the problem of determining which families of unitary operations can be computed efficiently in the quantum circuits model.

6.5.5 Quantum computational complexity

There is considerable interest in developing a theory of quantum computational complexity, and relating it to classical computational complexity theory. We content ourselves with presenting one result about quantum complexity classes, relating the quantum complexity class BQP to the classical complexity class PSPACE. PSPACE was defined as the class of decision problems which can be solved on a Turing machine using space polynomial in the problem size and an arbitrary amount of time. BQP is an essentially quantum complexity class consisting of those decision problems that can be solved with bounded probability of error using a polynomial size quantum circuit. Slightly more formally, we say a language L is in BQP if there is a family of polynomial size quantum circuits which decides the language accepting strings in the language with probability at least 3/4, and rejecting strings which aren't in the language with probability at least 3/4. In practice, what this means is that the quantum circuit takes as input binary strings, and tries to determine whether they are elements of the language or not. At the conclusion of the circuit one qubit is measured, with 0 indicating that the string has been accepted, and 1 indicating rejection. By testing the string a few times to determine whether it is in L, we can determine with very high probability whether a given string is in L. Of course, a quantum circuit is a fixed entity, and any given quantum circuit can only decide whether strings up to some finite length are in L. For this reason, we use an entire family of circuits in the definition of BQP; for every possible input length there is a different circuit in the family. We place two restrictions on the circuit in addition to the acceptance / rejection criterion already described. First, the size of the circuits should only grow polynomially with the size of the input string x for which we are trying to determine whether $x \in L$. Second, we require that the circuits be uniformly generated his uniformity requirement arises because, in practice, given a string x of some length n, somebody will have to build a quantum circuit capable of deciding whether x is in L. To do so, they will need to have a clear set of instructions – an algorithm – for building the circuit. For this reason, we require that our quantum circuits be uniformly generated, that is, there is a Turing machine capable of efficiently outputting a description of the quantum circuit. This restriction may seem rather technical, and in practice is nearly always satisfied trivially, but it does save us from pathological examples

One of the most significant results in quantum computational complexity is that BQP $\subseteq$ PSPACE. It is clear that BPP$\subseteq$ BQP, where BPP is the classical complexity class of decision problems which can be solved with bounded probability of error using polynomial time on a classical Turing machine. Thus we have the chain of inclusions BPP $\subseteq$BQP $\subseteq$ PSPACE. Proving that BQP $\neq$

BPP – intuitively the statement that quantum computers are more powerful than classical computers – will therefore imply that BPP $\neq$ PSPACE. However, it is not presently known whether BPP $\neq$ PSPACE, Therefore, the class of problems solvable on a quantum computer with unlimited time and space resources is no larger than the class of problems solvable on a classical computer. Stated another way, this means that quantum computers do not violate the Church–Turing thesis that any algorithmic process can be simulated efficiently using a Turing machine. Of course, quantum computers may be much more efficient than their classical counterparts, thereby challenging the strong Church–Turing thesis that any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

6.6 Summary of the quantum circuit model of computation

the key elements of the quantum circuit model of computation:

1. **Classical resources:** A quantum computer consists of two parts, a classical part and a quantum part. In principle, there is no need for the classical part of the computer, but in practice certain tasks may be made much easier if parts of the computation can be done classically. For example, many schemes for quantum error-correction are likely to involve classical computations in order to maximize efficiency. While classical computations can always be done, in principle, on a quantum computer, it may be more convenient to perform the calculations on a classical computer.
2. **A suitable state space:** A quantum circuit operates on some number, n, of qubits. The state space is thus a 2^n-dimensional complex Hilbert space. Product states of the form $|x_1, ..., x_n\rangle$, where $x_i = 0, 1$, are known as computational basis states of the computer. $|x\rangle$ denotes a computational basis state, where x is the number whose binary representation is $x_1...x_n$.
3. **Ability to prepare states in the computational basis**: It is assumed that any computational basis state $|x_1, ..., x_n\rangle$ can be prepared in at most n steps.
4. **Ability to perform quantum gates:** Gates can be applied to any subset of qubits as desired, and a universal family of gates can be implemented. For example, it should be possible to apply the `CNOT` gate to any pair of qubits in the quantum computer. The Hadamard, phase, `CNOT` and $\pi/8$ gates form a family of gates from which any unitary operation can be approximated, and thus is a universal set of gates. Other universal families exist.
5. **Ability to perform measurements in the computational basis:** Measurements may be performed in the computational basis of one or more of the qubits in the computer.

The quantum circuit model of quantum computation is equivalent to many other models of computation which have been proposed, in the sense that other models result in essentially the same resource requirements for the same problems.