

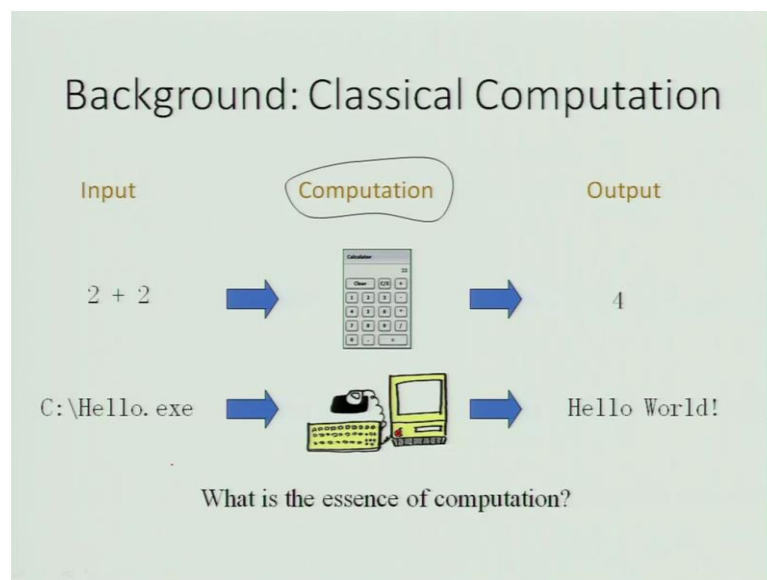
Implementation Aspects of Quantum Computing
Prof. Debabrata Goswami
Department of Chemistry
Indian Institute of Technology, Kanpur

Lecture – 37
Principles: Quantum Mechanics and Computers

This is the final week of our course on Implementation of Quantum Computing. So, what we will try to do in this week is go back to the basic ideas that we started from and give you all the summary of the implementations and the aspects of the quantum computing that we have learnt as a part of this course.

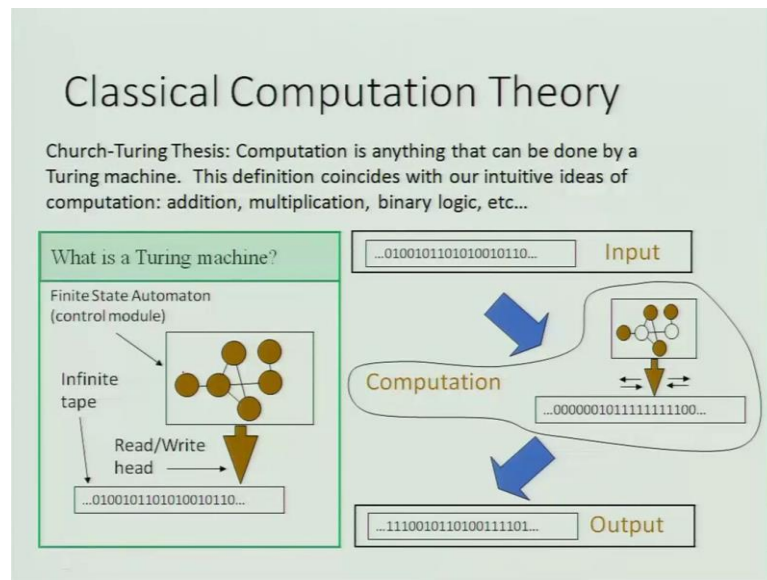
So perhaps, this week we will have a longish in terms of the number of lectures and the amount of material, just to make sure that we are able to cover most of the materials that we have presented in this course. Also we will try to look at some of the difficulties that some of you had in your responses in the forum and other places. So, there may be places where I also referred to the areas of difficulty that you had while doing this course so that we can sort of finish all that parts which who had not possible to be addressed during the course.

(Refer Slide Time: 01:21)



So, I have set it up in such a way, so that we go from the point of the background where we started this course which was classical computation.

(Refer Slide Time: 01:38)

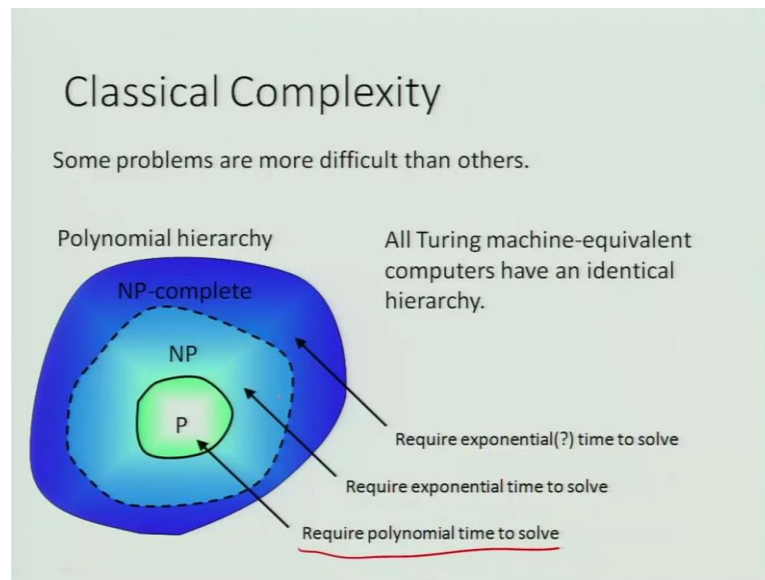


Wherein we gave examples of how classical computer can be essentially looked at in terms of the Church-Turing Thesis which essentially means that it is anything that can be done in a Turing machine. This definition coincides with our intuitive ideas of computation: addition, multiplication, binary logic etcetera.

So, in terms of a Turing machine we have discussed it as a machine which has a way to read write data on an infinite tape and have a control module, which is in a finite state automation so that it can achieve the computation on the input data to give rise to the result which is the output. So, in this principle problems which can be posed only in a way which can undergo specific answers are the ones which can be addressed. So that is the part which we discussed in terms of the concept of computing.

So, universal statements for instance are not information, which can be used for doing computation and so on and so forth. So, we had done quite a bit of discussion on this area of a computation.

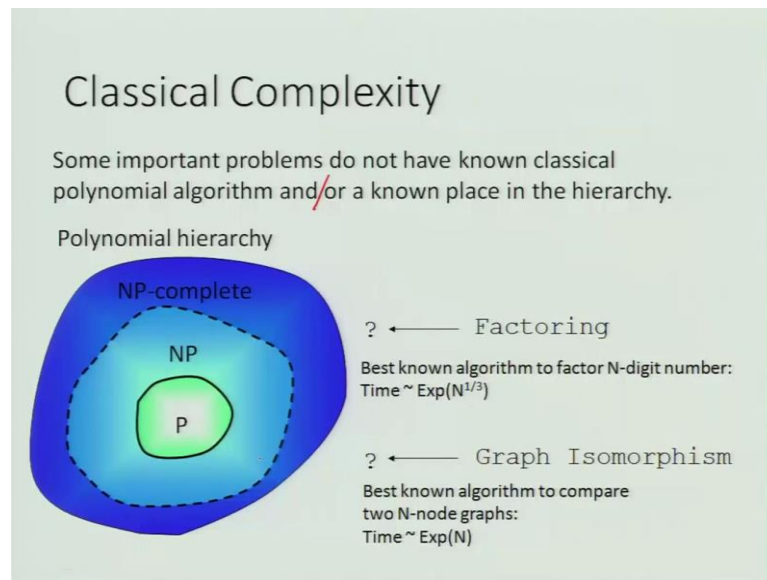
(Refer Slide Time: 02:58)



Now, the other important part of the computation lies in the concept of complexity which was also importantly addressed in this course, where we have discussed the levels of complexity that appears in computation, some problems are more difficult than the others. Generally speaking all the computable problems that I addressed through the Turing machines have polynomial hierarchy, and such all Turing machine-equivalent computers have identical hierarchy.

So, there is this typical way of presenting how the computer complexity looks like the part which is solved quite regularly by Turing machines or our computers are the ones which require polynomial time to solve which is the complexity in terms of P, and then the ones which have difficulty starts from the parts which are non determinate polynomials. So there are 2 parts to it: one which is known as non determinate polynomial and which require times which are definitely exponential to solve which are known as NP complete whereas, the others which are exponential requirement in time, but under certain conditions it can be transformed into certain levels of polynomial times; so those are the 2 different parts of the difficulty levels. So, it is either NP non determinate polynomial or NP complete which is the hardest part of the difficulty in terms of doing this work.

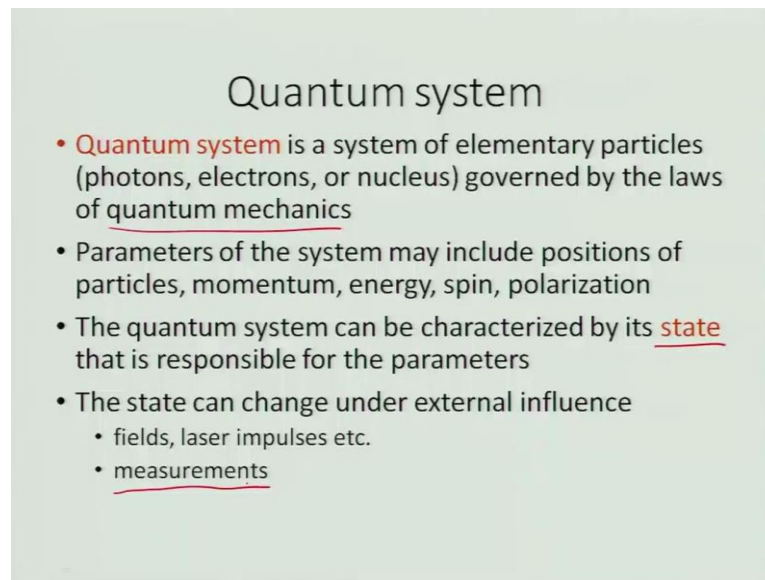
(Refer Slide Time: 04:46)



So, this is how we had discussed in terms of classical computing; we also refer to the fact that some important problems do not have the known classical polynomial algorithm and or a known place in the hierarchy. So, in this picture of polynomial hierarchy for instance a factoring is a problem, which works in exponential time for instance the best known algorithm to factor N-digit number takes time which is about exponential N to the power one-third.

So, those are the ones which go out of this polynomial hierarchy and they are classically difficult problems to be done. There is also this problem of graph isomorphism best known algorithm to compare 2 node graphs is also an exponential problem and similarly such problems can often run into regions which are not quite in the polynomial regions and they could be also non determinate polynomial in some sense.

(Refer Slide Time: 05:47)



Quantum system

- **Quantum system** is a system of elementary particles (photons, electrons, or nucleus) governed by the laws of quantum mechanics
- Parameters of the system may include positions of particles, momentum, energy, spin, polarization
- The quantum system can be characterized by its state that is responsible for the parameters
- The state can change under external influence
 - fields, laser impulses etc.
 - measurements

In this case we mentioned quantum systems can be of huge help to us. A quantum system is a system of elementary particles like photons, electrons, or nucleus governed by the laws of quantum mechanics. So, we deviate from the concepts of classical nature that we were discussing when we discuss in terms of quantum mechanics. So, in this regard of complexity, one of the concepts that we introduced was the idea of using quantum systems; when the systems becomes small such as a quantum system is a system of elementary particles such as photon, electrons or nucleus, which are governed by the laws of quantum mechanics and therein the concepts of classical mechanics are not quite applicable and thereby we can think of computations, which are no longer in the classical domain that we were discussing until now.

So, idea was to take the advantage of it. So, the parameters in this particular case or the system may include positions of particles, momentum, energy, spin, polarization. The quantum system can be characterized by it is state, that is responsible for the parameters. The state can change under external influence which could be fields, laser impulses etcetera it could and finally, those are to be realized or found out the results in terms of the measurements. So, these are the basic principles of the quantum system coming into the picture in place of the classical nature of objects that we just discussed.

(Refer Slide Time: 07:27)

Quantum mechanics distinction!

- Superposition: if a system can be in either of two states, it also can be in superposition of them }
- Some parameters of elementary particles are discrete (energy, spin, polarization of photons)
- Changes are reversible ←
- The parameters are undetermined before measurements }
- The original state is destroyed after measurement
- No Cloning Theorem: it is impossible to create a copy of unknown state
- Quantum entanglement and quantum teleportation

The distinction of quantum mechanics lies in certain points for example, in terms of super position: if a system can be in either of the 2 states simultaneously, it also can be in a super position of them this is distinct from what a classical nature of a system is supposed to be. Some parameters of elementary particles are discrete for example, energy, spin, polarization of photons and that is how they are quantum in nature. The changes in this particular case of quantum mechanics are all reversible, that is actually a very important parameter also and a critical part of quantum mechanics lies in the fact that the parameters are undermined before the measurements and so this plays a very vital role in terms of the application of quantum mechanics into the classical areas that we are discussing.

Another important aspect of quantum mechanics that is distinct from classical mechanics is that; the original state is destroyed after the measurement there is nothing which can be cloned and so that comes under the no cloning theorem, which says it is impossible to create a copy of unknown state and the point here is that once you make a state known then it does not remain as quantum anyway because it becomes classical. Finally, there is this concept of quantum entanglement and quantum teleportation, all of this has been a part of your course in great detail we are here just revising and refreshing it in order to make sure that we are completing all the parts of the course that we have covered in this series of lectures that we have done.

(Refer Slide Time: 09:27)

Qubit → "Quantum Bit"

- Qubit is a unit of quantum information
- In general, one qubit simultaneously "contains" two classical bits
- Qubit can be viewed as a quantum state of one particle (photon or electron)
- Qubit can be modeled using polarization, spin, or energy level
- Qubit can be measured
- As the result of measurement, we get one classical bit: 0 or 1

So, one of the terms which we introduced in this was the idea of a qubit, which is the quantum bit. So, that is our unit of quantum operation; in general one qubit simultaneously contains 2 classical bits, and that is one of the important aspects of quantum mechanics which is inbuilt into the system. Qubits can be viewed as a quantum state of one particle photon or electron.

Qubits can be modeled using polarization spin or energy levels; all those which assume discrete values; qubit can be measured; as a result of measurement we get one classical bit either 0 or 1. So, until the point of measurement as has been correctly pointed out quantum mechanics ensures the result or the information can be embedded in terms of qubit, which can contain both the classical information simultaneously.

(Refer Slide Time: 10:59)

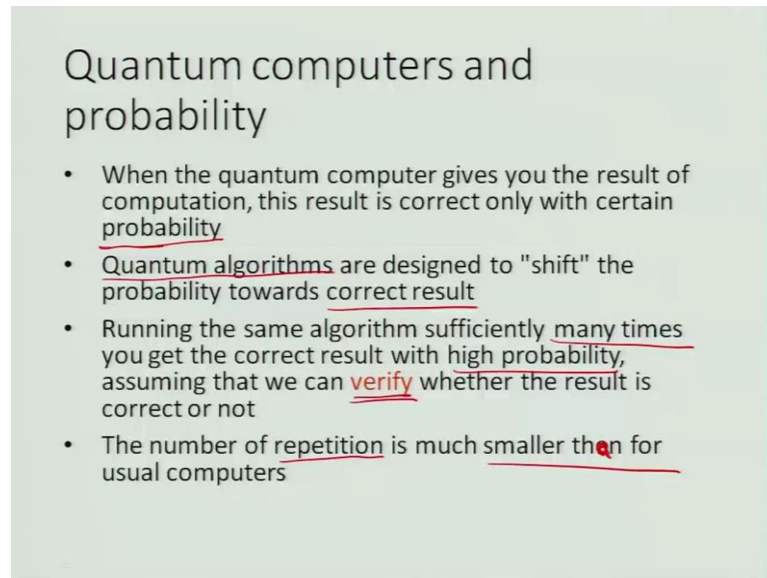
Quantum Computer

- Quantum computer uses properties of elementary particle that are predicted by quantum mechanics
- Usual computers: information is stored in bits
- Quantum Computers: information is stored in qubits = *qu + bits*
- Theoretical part of quantum computing is developed substantially
- Practical implementation is still a big problem

Therein comes the concept of quantum computer whenever we use quantum mechanics; quantum computers uses properties of elementary particles that are predicted by quantum mechanics and so that is how we arrived at this whole concept of quantum computer or quantum computing.

Usual computers as we have been showing in the very initial slides even today, the information is stored in terms of bits whereas, in quantum computers information is stored in terms of qubits quantum bits. Theoretical part of quantum computing is developed substantially as we have shown. However, practical implementation is still quite a big challenge although we have discussed in this course some of the even commercial approaches of quantum computing. So, this point the practical implementation point though is still an issue, it is not really a difficulty which has not been overcome as we yet.

(Refer Slide Time: 12:13)



Quantum computers and probability

- When the quantum computer gives you the result of computation, this result is correct only with certain probability
- Quantum algorithms are designed to "shift" the probability towards correct result
- Running the same algorithm sufficiently many times you get the correct result with high probability, assuming that we can verify whether the result is correct or not
- The number of repetition is much smaller than for usual computers

There is a strong connection of quantum computers with probability that is also another thing that we have discussed in length in this course; when the quantum computers gives you the result of computation, this result is correct with certain probability. Quantum algorithms are designed to shift the probability towards the correct result that is one of the most important aspects of quantum algorithms.

Running the same algorithm sufficiently in many times gets the correct answer with high probability, assuming that we can verify whether the result is correct or not. The number of repetition is much smaller than for usual computers and that is the power of quantum computer.

(Refer Slide Time: 13:09)

Short History

- 1970-e: the beginning of quantum information theory
- 1980: Yuri Manin set forward the idea of quantum computations *Paul Benioff*
- 1981: Richard Feynman proposed to use quantum computing to model quantum systems. He also describe theoretical model of quantum computer
- 1985: David Deutsch described first universal quantum computer
- 1994: Peter Shor developed the first algorithm for quantum computer (factorization into primes)

So, here is a short history of quantum computing which we have discussed in this course earlier also. From about 1970 onwards the beginning of quantum information theory started; at in 1980 Yuri Manin, first set forward the idea of quantum computations. Paul Benioff at about the same time discussed with Richard Feynman on the concept that as the computers becomes smaller, errors in computers become larger due to the probabilistic concept of quantum behavior and the solutions would becoming more and more probabilistic. Feynman thought about the problem and he independently proposed the use of quantum computing to model quantum systems, since quantum systems are the essential building block of nature, he thought that was one of the best ways of addressing quantum systems by building quantum computer rather than dreading the idea.

He also described the theoretical model of a quantum computer based on this third process. However, it was not until 1985 that the concept of how such a principle would become useful was given by the idea of David Deutsch, who described the first universal quantum computer. And then came the big breakthrough in 1994 where Peter Shor developed the first algorithm for quantum computer which is the factorization into primes. Now this was one of the most important developments perhaps in the area of quantum computing which essentially made people realize that it could really have a huge impact, because of the break of the RSI codes and other kinds of things.

So, this was a very important development and it took almost a decade to get there because a lot of error solving and other kinds of problems were being worked on during this period of initial development of quantum computer.

(Refer Slide Time: 16:02)

Short History

- 1996: Lov Grover developed an algorithm for search in unsorted database ↑
- 1998: the first quantum computers on two qubits, based on NMR (Oxford; IBM, MIT, Stanford)
- 2000: quantum computer on 7 qubits, based on NMR (Los-Alamos)
- 2001: 15 = 3 x 5 on 7- qubit quantum comp. by IBM
- 2005-2006: experiments with photons; quantum dots; fullerenes and nanotubes as "particle traps"
- 2007: D-Wave announced the creation of a quantum computer on 16 qubits

In 1996 Lov Grover developed an algorithm for searching in unsorted database and this was also extremely important because it turns out that for many problems it is known that the solution exists, but it is more of a searching of a solution which is the biggest step in computation and therefore, getting an algorithm which would be able to search for a solution has a huge impact in this area. In 1998 the first quantum computer on two qubits based on NMR was built in MIT Stanford and IBM in the year 2000 quantum computer on seven qubits based on NMR was built Los-Alamos.

Another major development in the year 2001 was when the number 15 was possible to be factored on the 7 qubit computer by IBM and this was achieved by Chuang and his group. In 2005 to 2006 experiments with photons and quantum dots; fullerenes and nanotubes as particle traps started becoming popular which resulted and developed this field further to finally, the first commercial computer quantum computer which came out in 2007 were D-Wave announced the creation of a computer on 16 qubits.

(Refer Slide Time: 17:48)

A model of qubit

$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$

vector (a_0, a_1)

- a_0 & a_1 are complex numbers such that $|a_0|^2 + |a_1|^2 = 1$
- $|\psi\rangle$ is a **superposition of basis states** $|0\rangle$ & $|1\rangle$
- The choice of basis states is not unique
- The measurement of $|\psi\rangle$ results in 0 with probability $|a_0|^2$ and in 1 with probability $|a_1|^2$
- After the measurement the qubit collapses into the basis state that corresponds to the result

Example: $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ $\begin{matrix} \xrightarrow{1/4} & |0\rangle \\ \xrightarrow{3/4} & |1\rangle \end{matrix}$

So, looking a little bit into the basics here, a model of a qubit as has been discussed several times, essentially can be represented by a vector with a ket representing vector having the state's 0 and 1; such that the coefficients a_0 and a_1 can be complex numbers with only the constraint that a mod squares add up to 1; this state or the qubit ψ ket is a superposition of the basis states 0 and 1, the choice of the basis states is not unique which means that several possibilities exists, the measurement of the wave functions ψ ket results in say the bit 0 with probability a_0 mod square and in bit 1 with probability a_1 mod square.

After the measurement the qubit collapses into the basis state that corresponds to the result and this particular part is essentially classical. So, the point of measurement brings back the classical information as we have been discussing. So, here is an example just to show that the coefficients basically give raise to the probability of the measure of individual states.

(Refer Slide Time: 19:32)

Computation with Qubits

How does the use of qubits affect computation?

Classical Computation

Data unit: bit
 $\bullet = '1'$ $\circ = '0'$

Valid states:
 $x = '0'$ or $'1'$

$x = 0$

$x = 1$

Quantum Computation

Data unit: qubit
 $\uparrow = |1\rangle$ $\downarrow = |0\rangle$

Valid states:
 $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$

$|\psi\rangle = |0\rangle$

$|\psi\rangle = |1\rangle$

$|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$

So, this idea of using computation with qubits, how does it affect the concept of computer? So, in terms of classical computation, the data unit is as mentioned either 1 or 0. So, the valid states are either 0 or 1 and depending on how the switch is whether it is pointing towards 0 or towards 1, we get the values as 0 or 1. In terms of quantum computer; however, the data unit which is the qubit has the valid state in the superposition of both 0 and 1 and at any point of time before measurement it can assume any of the values that are possible.

(Refer Slide Time: 20:24)

Computation with Qubits

How does the use of qubits affect computation?

Classical Computation

Operations: **logical**

Valid operations:

NOT =

in	
0	1
1	0

 out 1-bit

AND =

in	
0	1
0	0
1	0
1	1

 out 2-bit

Quantum Computation

Operations: **unitary**

Valid operations:

$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$\sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ $H_d = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

CNOT =

1	0	0	0
0	1	0	0
0	0	0	1
0	0	1	0

In both cases logical operations are to be performed; however in classical computation logical operations need not be reversible. So, for instance not gate where that is a 1 input and 1 output is a 1 bit process is perfectly fine; however, it also admits 2 inputs and 1 output in terms of the and gate; in terms of quantum computation which is definitely going to be only unitary and reversible, the valid operations therefore involve for example, in terms of 1 qubit the poly matrices as we have discussed throughout this course as well as the hadamard operation, which basically produces an equal superposition of the states concerned.

In 2 qubit case there is this control not, which enables the switching of a bit based on the control. However, almost all the; however, it is important that all the logic gates in terms of quantum computation be reversible.

(Refer Slide Time: 21:48)

Computation with Qubits

How does the use of qubits affect computation?

Classical Computation		Quantum Computation							
Measurement: deterministic		Measurement: <u>stochastic</u>							
State	Result of measurement	State	Result of measurement						
x = '0'	'0'	$ \psi\rangle = 0\rangle$	'0'						
x = '1'	'1'	$ \psi\rangle = 1\rangle$	'1'						
		$ \psi\rangle = \frac{ 0\rangle + 1\rangle}{\sqrt{2}}$	<table style="border: none;"> <tr> <td style="border: none;">}</td> <td style="border: none;">'0'</td> <td style="border: none;">50%</td> </tr> <tr> <td style="border: none;">}</td> <td style="border: none;">'1'</td> <td style="border: none;">50%</td> </tr> </table>	}	'0'	50%	}	'1'	50%
}	'0'	50%							
}	'1'	50%							

In case of classical computation the measurement is deterministic if the state is a 0 then the result of the operation then the result of the measurement would be 0 whereas, if the state is 1 then the result of measurement will be 1.

On the other hand in quantum computer the measurement is probabilistic or stochastic, as a result we could land up having the measurement of either 0 or 1 as well as the case where both 0 and 1 occur with a 50 50 probability. So, these are the major distinctions which can be immediately looked at when we look at computation with qubits versus the computation with (Refer Time: 22:43).

(Refer Slide Time: 22:43)

Several qubits

- The system of n qubits "contain" 2^n classical bits (basis states)
- Thus the potential of a quantum computer grows exponentially
- We can measure individual qubits in the multi-qubit system
 - For example, in a two-qubit system we can measure the state of first or second qubit, or both
- The results of measurement are probabilistic
- After the measurement the system collapses in the corresponding state

When we are using several qubits, the subsystem of n qubits contains 2^n classical bits or the basis states. So, here come the exponential benefits in terms of the classical computing; the potential of quantum computer grows exponentially.

We can measure individual qubits in the multi qubit system for example in a 2 qubit system we can measure the state of the first or the second qubit or both, the results of measurement are probabilistic as we have just showed, after the measurement the system collapses in the corresponding state.

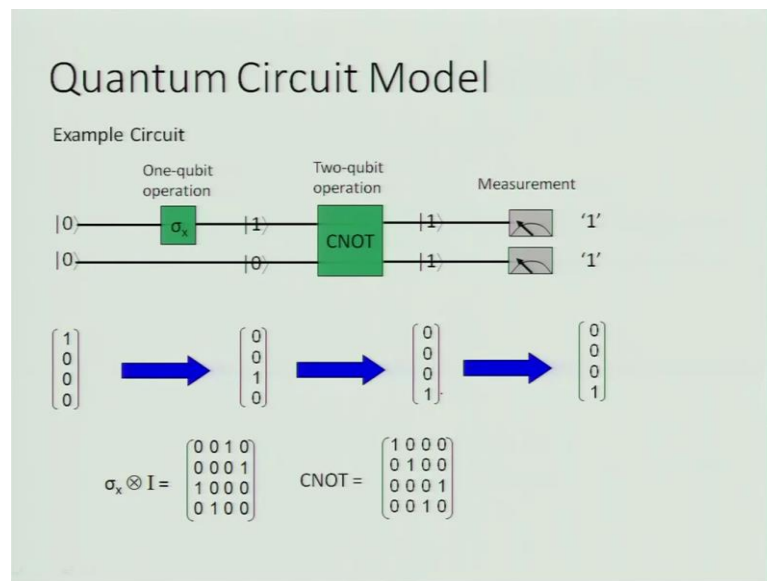
(Refer Slide Time: 23:31)

More than one qubit

	Single qubit	Two qubits
Hilbert space	$ 0\rangle, 1\rangle$ $\mathcal{H}_2 = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$	$ 00\rangle, 01\rangle, 10\rangle, 11\rangle$ $\mathcal{H}_2^{\otimes 2} = \mathcal{H}_2 \otimes \mathcal{H}_2 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$
Arbitrary state	$ \psi\rangle = c_1 0\rangle + c_2 1\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$	$ \Psi\rangle = c_1 00\rangle + c_2 01\rangle + c_3 10\rangle + c_4 11\rangle = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$ <div style="text-align: right; color: red; font-size: small;"> 2^n $n=2$ </div>
Operator	$U \psi\rangle = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$	$U \Psi\rangle = \begin{pmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ u_{21} & u_{22} & u_{23} & u_{24} \\ u_{31} & u_{32} & u_{33} & u_{34} \\ u_{41} & u_{42} & u_{43} & u_{44} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$

So, here is the how it is looks like; we are in terms of quantum computer working in the Hilbert space, for a single qubit we have already seen how it works when we have 2 qubits they work as tensor products and so there is an exponential growth in the space. For any arbitrary state for a single qubit the coefficients are just a 2 coefficients of the 2 states; however, for 2 qubits there are 4 possibilities which is 2 to the power n, in this case n is equal to 2 and the operator is supposed to be always unitary, which acts on the given state as has been shown here.

(Refer Slide Time: 24:28)



So, we have basically explored the entire process by using the quantum circuit model in most of the cases throughout the discussion in this course; where for example, we have shown circuits which are lines which are drawn with the operations and the path and finally, we have used measurement as the final result. So, whenever we looked at the inputs, we had the inputs provided and then we had certain operations. For example, in this case there is a 1 qubit operation of a poly x and then after the 2 qubits are in to the CNOT gate which is the 2 qubit operation, the CNOT gate operates and we can have the measurement with gives rise to whatever the processes happened.

So, here is the principle of applying how the state goes, so we have the particular state coming in spin put into this one qubit operation which switches it to 1 the other unit state as 0 continuous after going through the CNOT, because the control is a 1, it does it is not operation so it switches the last 2 bits and that can be measured as the final result.

(Refer Slide Time: 26:00)

Operations on one qubit

- **Quantum NOT**
 $\text{NOT}(a_0 |0\rangle + a_1 |1\rangle) = a_0 |1\rangle + a_1 |0\rangle$
 $|0\rangle \rightarrow |1\rangle$
 $|1\rangle \rightarrow |0\rangle$

$$\text{NOT} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$
- **Hadamard gate**
 $H(a_0 |0\rangle + a_1 |1\rangle) = 1/\sqrt{2} [(a_0 + a_1)|0\rangle + (a_0 - a_1)|1\rangle]$
 $|0\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
 $|1\rangle \rightarrow \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle$

$$H \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

So, here is another way of looking at operations on 1 qubit, quantum not gate for instance it switches the values of the operations. So, 0 goes to 1 1 goes to 0 and not operation is therefore, is just a matrix which looks like, this the hadamard gate as I mentioned before essentially creates an equal superposition of the 2 states and so, here is an operation of hadamard which is shown here in terms of the matrices. So, we have this equivalent approaches either through vectors or through matrices, which go through this processes.

(Refer Slide Time: 26:43)

Two qubits: controlled NOT (CNOT)

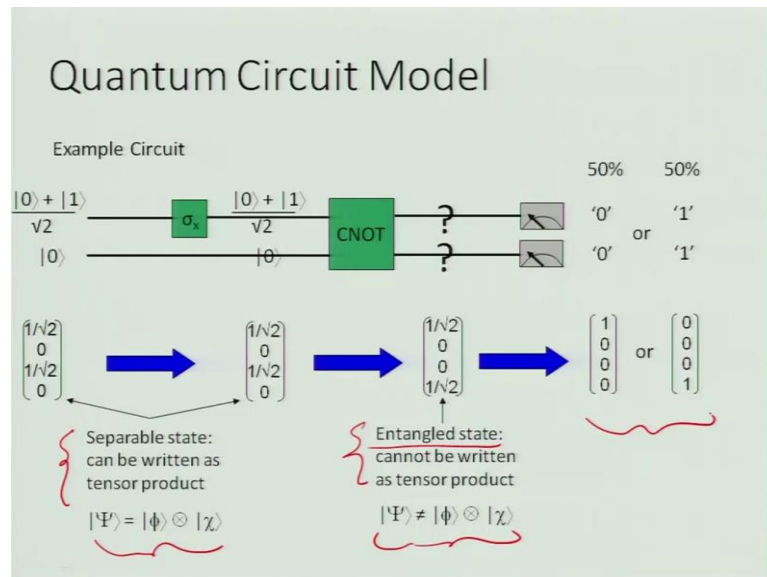
CNOT (x,y) = (x, x XOR y) = (x, x⊕y)
 $0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$

CNOT(a₀|00⟩+a₁|01⟩+a₂|10⟩+a₃|11⟩) = a₀|00⟩+a₁|01⟩+a₃|11⟩+a₂|10⟩

$$\begin{matrix} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{matrix} \quad \text{CNOT} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

There is another representation of the controlled not operation, where we have used the matrices and the gates vectors in this operation procedure and as can be seen this can be represented in many possible ways and these are the ways that we have discussed in the classes we have gone through.

(Refer Slide Time: 27:10)



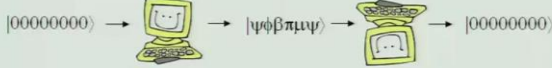
So, here is another example where instead of the 2 pure states coming we have 1 state 0 and the other 1 is hadamard state, which comes in and as we go through the operations how they go and change it depends and so in this particular case for example, it is a 50 50 mixture of either getting a 0 or a 1. So, the states can be of 2 kinds where 1 case where they can be separated and can be written as a tensor products as has been shown here those are called superposition states.

However the other kinds of states where the states cannot be written as tensor products then those are known as entangled states as we show it here. So, these states are entangled states and in case of entangled states our results are always going to be probabilistic


(Refer Slide Time: 28:08)

Some Interesting Consequences


Reversibility
Since quantum mechanics is reversible (dynamics are unitary), quantum computation is reversible.



Quantum Superordinacy
All classical quantum computations can be performed by a quantum computer.



No cloning theorem
It is impossible to exactly copy an unknown quantum state



So, the interesting consequences result of this quantum concept is the principle of reversibility, because quantum mechanics is reversible, dynamics are unitary, quantum computations are reversible. The other is the quantum superordinacy where all quantum computations can be performed by a quantum computer; however, one very important thing is there is no cloning possible it is impossible to exactly copy an unknown quantum state. one of the important things to realize; however, that although quantum superordinacy exists it is not true that every principle of a classical computer will be more efficient when we go into the quantum computer domain. It might take more steps because of the requirements of the reversibility of the quantum computing process; however, at the end of the day we all know reversible computers are going to be more efficient at least energy wise, so it has it is advantages.

(Refer Slide Time: 29:25)

What is a quantum computer good for?

- Many practical problems require too much time if we attempt to solve them on usual computers
 - It takes more than the age of the Universe to factor a 1000-digits number into primes! ←
- The increase of processor speed slowed down because of limitations of existing technologies ←
- Theoretically, quantum computers can provide "truly" parallel computations and operate with huge data sets ←

So we may ask; what is a quantum computer good for? This is one of the things which we have looked into. Many practical problems require too much time if we attempt solve them by usual computers. For example, it takes more than the age of the universe to factor a 1000-digit number into primes, because this is an exponential problem. The increase of processor speed slowed down because of limitations of existing technologies; this is one of the facts which has happened. Theoretically quantum computers can provide truly parallel computations and operate with huge data sets. So, these are the major aspects of quantum computing advantage, why there is a huge research to a quantum computation.

So, with this we would like to actually end this first lecture where we basically bring out the essence of why we were studying quantum computations and its implementation. In the next lecture we will go into some more details of the very basics that we introduced here in terms of where this entire idea of quantum computer started, how we dealt with it and how we have benefited from learning more and more about the aspects of quantum developments over these years and how we have managed to go to a point where we can do implementations.

So, from the next lecture on we look more into these kinds of aspects that we have already discussed in this course.

Thank you.