NPTEL

**NATIONAL PROGRAMME ON
TECHNOLOGY ENHANCED LEARNING**

IIT BOMBAY

**CDEEP
IIT BOMBAY**

Quantum Information and Computing

**Prof. D.K. Ghosh
Department of Physical IIT Bombay**

Modul No.01

Lecture No.1

Quantum Information & Computing
Why Quantum Computing?

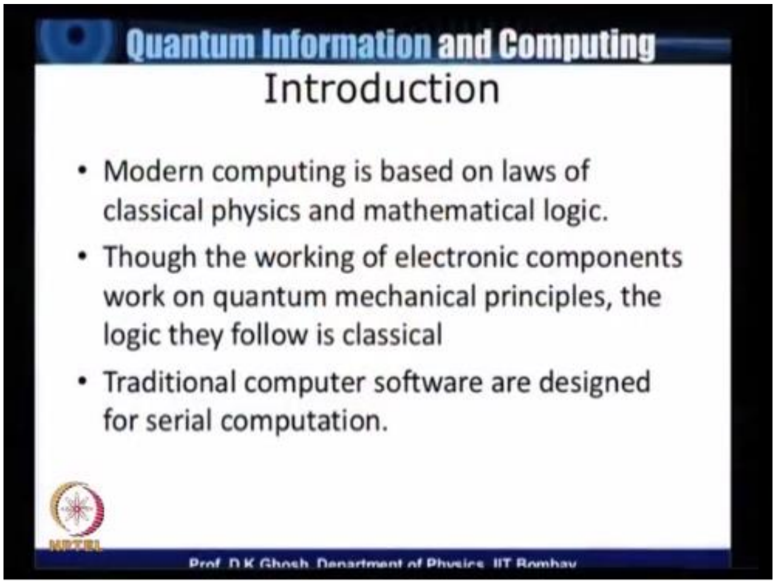
Hello, I welcome you all to this eight weeks 20 hour course.

(Refer Slide Time: 00:22)

On quantum computing and information under the edges of NPTEL platform. And in this very first lecture what I will do today is to tell you what is this quantum computing as you where all aware this is not been a traditional subject of physics or computer science for that matter and it is only during the last 20 years or so that this subject has come to prominence and it is still in a lot of developmental stage.

Now we will go through the scope of this course, but to begin with I would like to tell you why quantum computing after all we have add computers for quite some time.

(Refer Slide Time: 01:14)



Quantum Information and Computing

Introduction

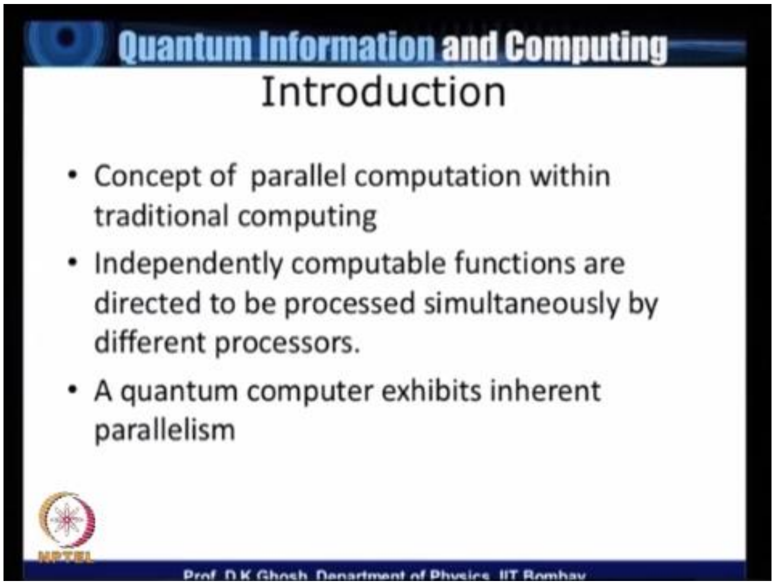
- Modern computing is based on laws of classical physics and mathematical logic.
- Though the working of electronic components work on quantum mechanical principles, the logic they follow is classical
- Traditional computer software are designed for serial computation.

Prof. D.K Ghosh, Department of Physics, IIT Bombay

At least for five decades and what is so special about quantum computing. The first thing that you might try to tell me that even the classical computing is based on transistors and other electronic components. So which means that these things like transistors and other electronic components which are parts of the integrated circuits which are used in a classical computer, they are also based on quantum mechanics. So what is so special about it the difference is the following that the modern computing as we know it is based on lose of classical physics.

And of course there may based on mathematical logic. We will still continue to have a lot of dependence on mathematical logic, but we will see that the laws of classical physics which seem to operate on the computers that we have become a costume to, they are gradually becoming a little detailed. The first thing that I would like to point is this, it traditional computer software is designed for serial computers.

(Refer Slide Time: 02:33)



Quantum Information and Computing

Introduction

- Concept of parallel computation within traditional computing
- Independently computable functions are directed to be processed simultaneously by different processors.
- A quantum computer exhibits inherent parallelism

Prof. D.K Ghosh, Department of Physics, IIT Bombay

What serial computation essentially means is that when you write an algorithm the logic flow takes place from one point to other in terms of time. Now what it means is that a particular process must be completed before another process is taken out. Now you will say that but we have heard about the parallel computers even in our traditional sense, but there is a very big difference.

Yes there are parallel computers in classical computers I am using the phrase classical computers to mean the computes which we have today which we have become a costume to over the last nearly half a century or so. The concept of a parallel computer within our traditional computing platform is the following, that supposing I have a problem which can be broken up into independent logics which could be executed at the same time. Just to give you an example supposing you are computing the product of a matrix.

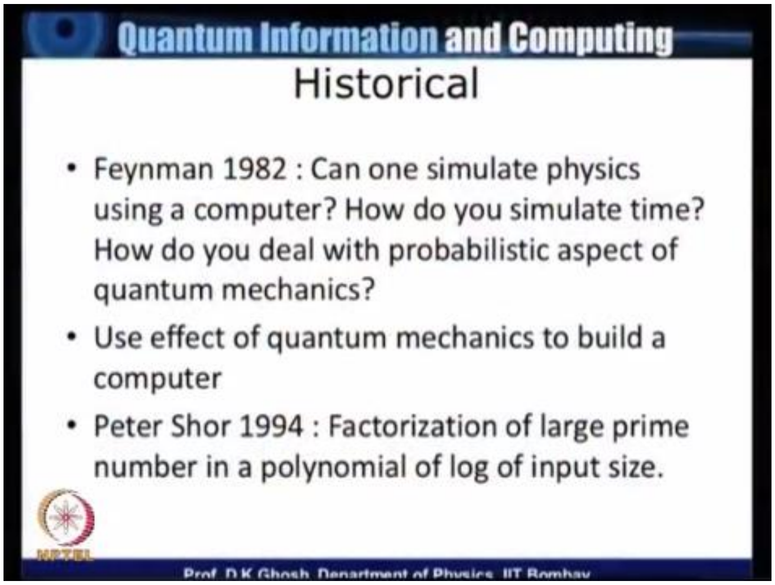
Now when you are computing the product up to matrices then when you want to compute the first element of let us say product of AB=C when you want to compute the first element of C what we require is the first row of A and the first column of B, so that I can multiply them one after another and add them. But during that time in principle I could be using let us say the second row of A and a second row or any other column of B to my advantage also without interfering with the first computation.

Now but how do I do it, the only way to do it is if these different computations which can beat taken up simultaneously are given to different processors and they are directed that at this same time you could do it. In other words each one still does a serial computation, but it is at the algorithm stage that I split up my logic into processors which can be executed at the same time by different processors.

So in others a traditional parallel computer must have n number of processers which could take up the job at the same time and then we should integrate with the results. Now what is the difference a quantum computer has what I will call as inherent parallelism. Now let me try to explain what it is, but before that let me also tell you a little bit which will give you an idea about what the history of quantum computer.

As I told you it is not a very old thing, but the first person who can credited with an idea of may be having a quantum computer, he might not have quite thought of it that way is Richard Feynman all of you must have heard a great scientism and probably better known because he a was a very effective communicator and the greatest teachers that the physics has seen, Feynman in 1982 published a paper.

(Refer Slide Time: 06:13)



Quantum Information and Computing

Historical

- Feynman 1982 : Can one simulate physics using a computer? How do you simulate time? How do you deal with probabilistic aspect of quantum mechanics?
- Use effect of quantum mechanics to build a computer
- Peter Shor 1994 : Factorization of large prime number in a polynomial of log of input size.

Prof. D.K Ghosh, Department of Physics, IIT Bombay

And which was titled simulation of physics on using a computer, the question that he asked is can one simulate physics using a computer? Now there are many problems with it, the first problem is how do you simulate time? As we now time is a continues variable the problem of stimulating time is that I must then some are the discredited time. Now you would immediately realize this is the problem but not that greater problem because after all we have been a custom to discrediting time in solving differential equations.

But the bigger problem is that we will see later in detail that the in quantum mechanics the measurements give you probably sticks at as you are aware that a state in quantum mechanics is a linear combination of certain steps and when you do a measurement that suppose I talk about linear combination of some bases stage and when we make a measurement of any physical property of the system.

One of the possible the values of that physical property is realized with certain probability. Now this is something which is totally new concept in quantum mechanics, and we have not seen a parallel like that in classical physics. So this probabilistic aspect is one of the problems that we come up with, but then the problem is that simulate a quantum processors using a quantum then can we use the quantum principle to our advantage to let us build a computer. Now this is the roughly the idea.

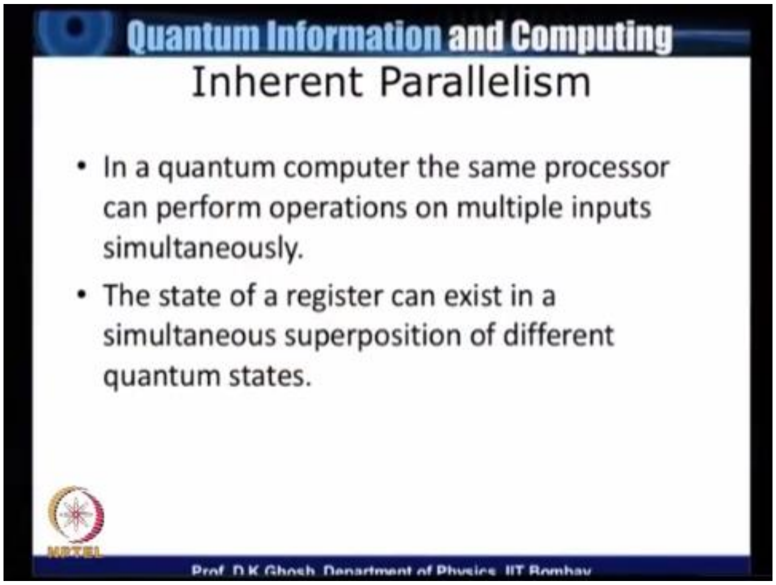
Now I could mention other people who have been involved in it is progress, but I think I would take a jump to about 12 years later there is Peter Shor who came up with an algorithm which we will be discussing in this course later. In 1994 he came up with an algorithm which showed that a very old problem that we have in computational science can be effectively solved if you had a quantum computer.

Now let me explain what that problem is, we will come to mathematical details of that during this course. The problem is connected with how to factorize a large composite number, now this has been known to be a very difficult problem or as computes scientists call it hard problem in computer science. And the reason why it is a hard problem is that there are no effective algorithms known which can compute the factors of a large composite number in what in compute science language is called in polynomial time.

If it could be done in polynomial time then of course it would be called an easy problem I would later on point out that even toady we depend on this difficulty in factorizing a large composite number to have encrypt some of data and in fact RSA algorithm which provides the data encryption depends on the relative hardness of the factorization problem and with respect to the multiplication which is relatively easy.

And if one can break this RSA Code which at least theoretically is possible today thanks to source algorithm, then it would mean a substantial advancement in both cryptography and in computer science. So what Peter Shor is that using the principles of quantum mechanics we can factorize a large composite number.

(Refer Slide Time: 10:33)



Quantum Information and Computing

Inherent Parallelism

- In a quantum computer the same processor can perform operations on multiple inputs simultaneously.
- The state of a register can exist in a simultaneous superposition of different quantum states.

Prof. D.K Ghosh, Department of Physics, IIT Bombay

Now you may say that this essentially gave us or heralded the coming of the quantum computers into the field even today there are no quantum computes which is available liberally, but there are prototype models and in fact the original number which was factorized using Peter Shor principle on a quantum computer is just the number 15 which of course does not require a quantum computer, but it was the principle of the thing that got established.

The reason why quantum computation is different from the classical computation is the fact that while a classical register can at a given time have or be in one state that is let us suppose, I am talking about a simple classical bit and I have a one bit register. The one bit register can stay either in state 0 or in state 1.

Similarly a two bit register can be in state 00,01,10,11. The difference between this statement and the corresponding quantum mechanical statement is that in a quantum mechanics not only I can have a register storing any of these four state in the second example that I give you but it can be simultaneously in a linear combination of these four steps. And not only that, that when you actually compute a function then one can compute the value of the function for this linear combination.

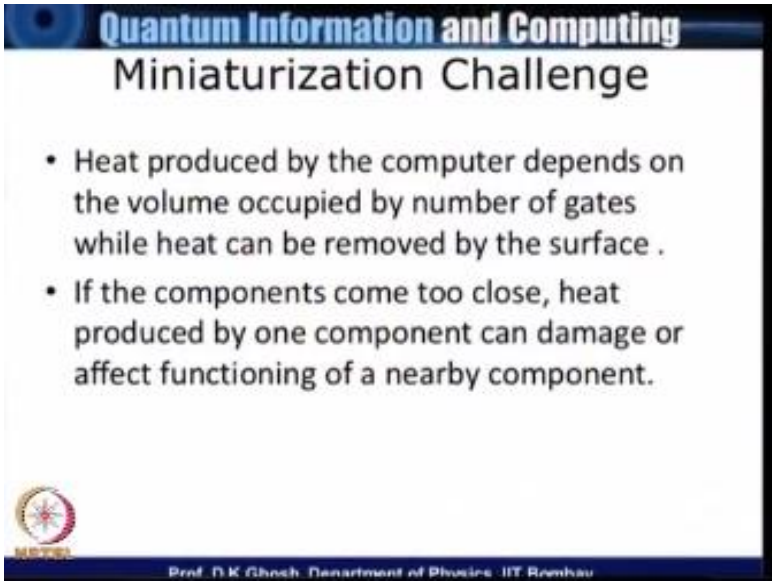
In other words, you compute the value of the function for each one of the inputs at the same time, in other words the parallelism that we are talking about for a quantum computer is inherent. And it is not an outside parallelism which has being trust on us by having number of process. So there is another important thing that comes up that quantum bits which we will later on give it a name call it cubits. They have another property interesting property known as entanglement, now an entanglement which of course requires a minimum two cubic system, is something which has no parallel in corresponding classical computer.

What it means is that the two bits or two cubits of a particular state are not individually realizable and if you measure one of them the state of the other one gets automatically different. We will be seeing a lot of this entanglement in this course. Now let us come back to what is the need of a quantum computer other than for solving hard problems. They main problem that is gradually coming up over the last several years you have seen the computers the classical computers as I will be using the term have generally increased in their speed.

Now how has it been possible, this is been possible because of great deal of miniaturization being achieved in integrated circuits. But that carried with it a problem there is a law of which the electronics engineers or the computer scientist referred to at Moore’s law which stated that the number density of transistors on an integrated circuit tumbles every 18 months of two years. Now if that were shown or if that is shown, then the spacing between the transistors or the other components they keep on decreasing.

Now when miniaturization proceeds like this there are two problems associated with, when the separation between different components they reach atomic dimension. You were all aware of quantum mechanical and certain difference may took high number now that has a lot of influence on what is happening when things reach atomic dimension. In other words, if the components come so close then the results that you get out of that computation will no longer be reliable. The other thing that will happen is that the heat produced by one of the components would naturally affect.

(Refer Slide Time: 15:43)



Quantum Information and Computing

Miniaturization Challenge

- Heat produced by the computer depends on the volume occupied by number of gates while heat can be removed by the surface .
- If the components come too close, heat produced by one component can damage or affect functioning of a nearby component.

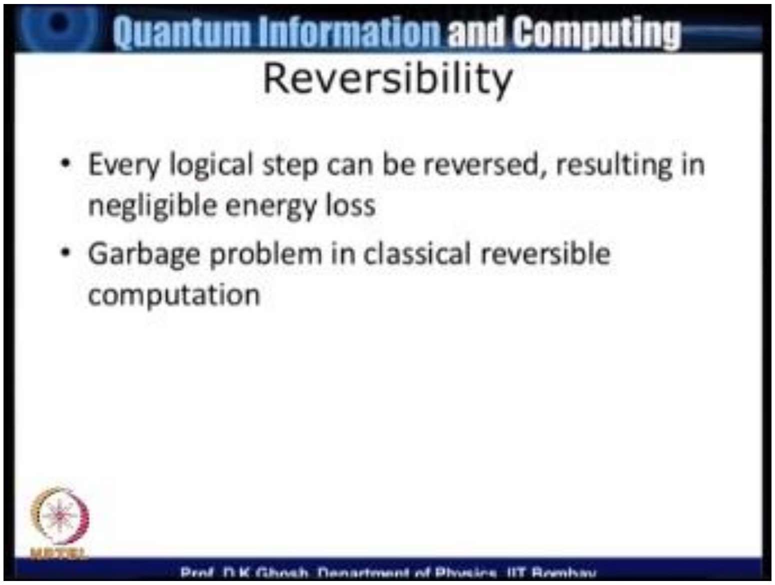
Prof. D.K Ghosh, Department of Physics, IIT Bombay

The performance of nearby components and so therefore, this will also make the computation on lab. There are this heat problem has certain other aspects for instance, the heat produced by a computer depends on the volume occupied by the number of bits. But you do not need remove the heat continuously and heat can be removed only from the surface. So as a result when the components come too close efficiency of removing heat will not be quite as good. There is a principle which is known as Landauer principle, which says every physically irreversible process.

You are all familiar with many reversible processes that take place while doing computation. For example, if you are AND gate it is irreversible process, most probably process is then classical computing are done irreversible. And this principle Landauer principles state that every n bit of information increases the thermodynamic entropy by nklog2, which would be that there is certain amount of loss of energy and the process becomes gradually inefficient as the number of components increase.

The present day computers dissipate much more energy than this limit. The quantum processes as we will see later, have to be carried out irreversibility, in fact the operators which will be doing it, will be unitary operation.

(Refer Slide Time: 17:35)



Quantum Information and Computing

Reversibility

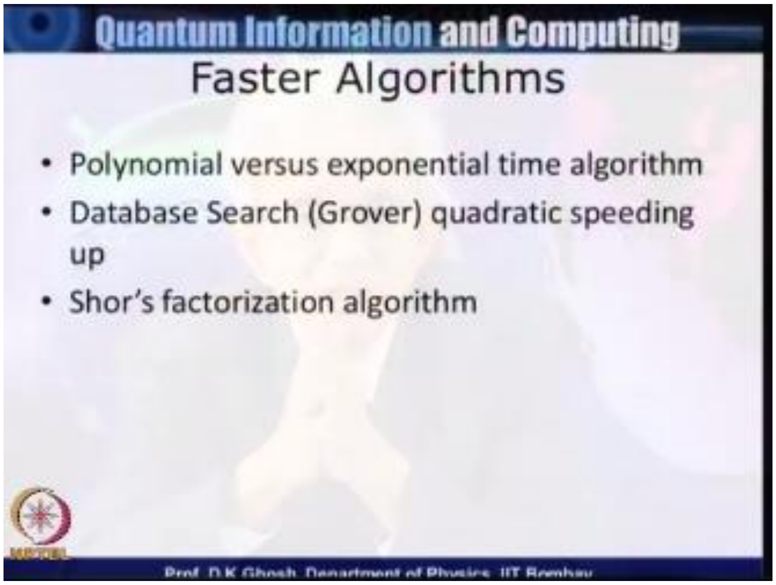
- Every logical step can be reversed, resulting in negligible energy loss
- Garbage problem in classical reversible computation

Prof. D K Ghosh, Department of Physics, IIT Bombay

Now it is also possible to do classical computing by means of reversible gets, but then there is always a problem of what we call as garbage. The garbage arises because for example, if I am using AND gate and I want it to be de reversibly, what it means is I have to store the inputs continuously, the, in fact the only classical gate which is a reversible gate is a NOT gate. But for all others if I want the process should be done reversibly I will need to collect the inputs which I do not later on require.

So that becomes a very big disposal problem and it also states unnecessary storage. So these are the two primary issues connected with the advent of quantum computers. Now let me tell you about what are the things that I am going to be doing in this course.

(Refer Slide Time: 18:37)



Quantum Information and Computing

Faster Algorithms

- Polynomial versus exponential time algorithm
- Database Search (Grover) quadratic speeding up
- Shor's factorization algorithm

Prof. D.K Ghosh, Department of Physics, IIT Bombay

I will be actually aiming to do quite a bit in detail to measure, the first one is known as Grovers database, this is a problem with requires of the order of enquires in classical computation. But as we see later quantum databases are of an unstructured database can speed this process up quadratically, that is require only square root of n number of queries that instead of n it depends up on square root of n.

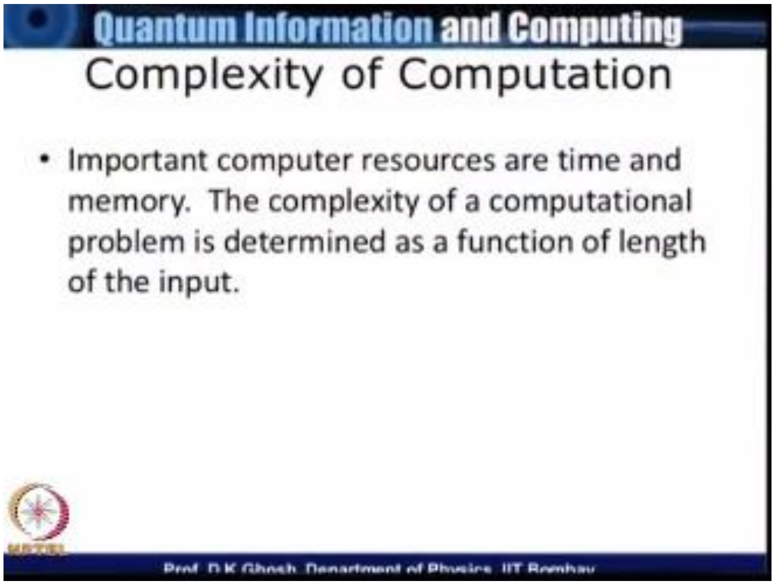
I started talking about the source algorithm more for historical reasons, but the source factorized algorithm is a major advancement in the area because till this algorithm has been known the classical computers could not solve a problem the problem of factorization in what we will call as a polynomial time. In computer science the complexity of a problem is determined by the dependence of the resources that the algorithm requires or the length of the input string.

By resources we mean time, memory, extra, let suppose I am multiplying two numbers, one could say that the way depends up on tine, depends on let us say n^2+ i. Now mind you these will not be the same for two different computers, but we are talking about order of magnitude. So I would then say that this complexity of this problem is order n^2. In general if I can express the complexity as a polynomial function or the length of the string, then I say this problem is complexity is polynomial time.

And in computer science an algorithm which can be executed in polynomial time is considered as an easy problem. Of course, you could have a problem which depends up on algorithm of the resources which also is an easy problem. Constant time algorithms are also easy problems, but supposing I cannot express it on the polynomial. If in depends up on 2^n 2 is the normal base of exponential in computation, then it is called as exponential time algorithm and the problem is now considered highly.

Factorization problem is one of the hard algorithms, what Peter Shor showed is that one can solved the.

(Refer Slide Time: 21:37)



Quantum Information and Computing

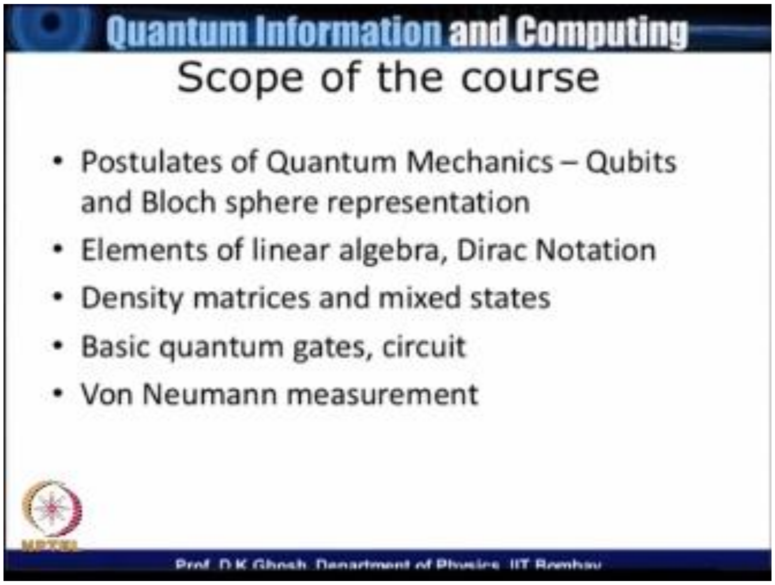
Complexity of Computation

- Important computer resources are time and memory. The complexity of a computational problem is determined as a function of length of the input.

Prof. D K Ghosh, Department of Physics, IIT Bombay

Factorization problem in polynomial time if you had a quantum computer.

(Refer Slide Time: 21:43)



Quantum Information and Computing

Scope of the course

- Postulates of Quantum Mechanics – Qubits and Bloch sphere representation
- Elements of linear algebra, Dirac Notation
- Density matrices and mixed states
- Basic quantum gates, circuit
- Von Neumann measurement

Prof. D K Ghosh, Department of Physics, IIT Bombay

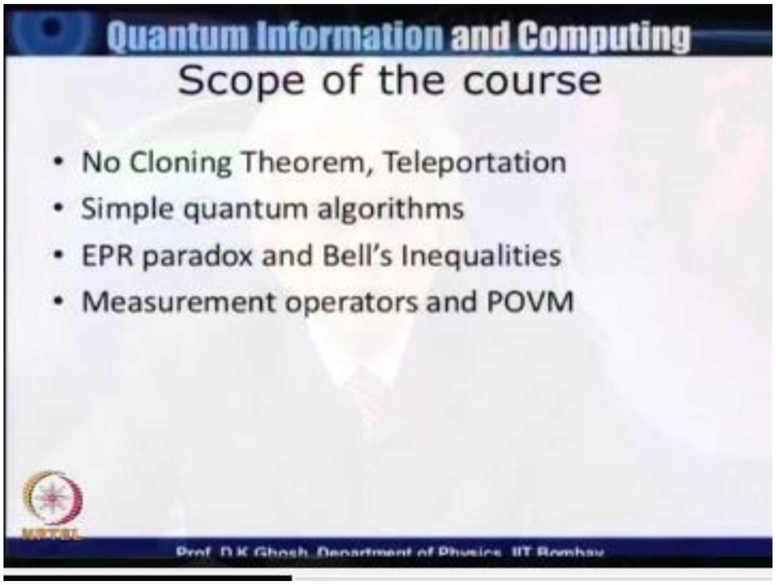
I will begin this course with the review of the postulates of quantum mechanics. The postulates of quantum mechanics that I will be talking about are basically what are known as the [indiscernible][00:22:01] and interpretation. I will be introducing the concept of a cubit it quantum bit which is similar to the classical bits, but as I already mentioned that my registers can simultaneously score linear combination of such cubits. We will see an attractive geometrical interpretation of these cubits on a sphere called Block sphere.

Since this course is heavily dependent on linear algebra and we spending a bit of a time on elements of the linear algebra, and will be introducing the direct notation of quantum mechanics which is commonly used in discussing quantum computing. We will see that the traditional quantum mechanics which we learn in universities they depend on or they describe what are called pure systems. In reality we rarely have your systems but we are likely to have either mix systems or even pure systems which interact with surroundings.

We will be introducing the concept of density matrix which is more appropriate way of defending or discussing the quantum mechanics for such mix systems or ensemble of systems. After that we will be bringing up the idea of what we call at the circuit model of quantum computer and that is basically to introduce various gates which are similar to the classical gates that we have, but with certain prescription that these gates must execute tasks unitarily and reversibly.

One of the biggest problems that we have in quantum computers is the problem of measurement, as we have seen that measurement in quantum mechanics does not give you the state of the system at that time, because the state of the system could be a linear combination of the real states. And so what will happen is that you will get on measurement only one of those states coming up. And this state which is projected out due to measurement is probably stick in nature, so this actually causes a very big problem but we will see.

(Refer Slide Time: 24:46)



Quantum Information and Computing

Scope of the course

- No Cloning Theorem, Teleportation
- Simple quantum algorithms
- EPR paradox and Bell's Inequalities
- Measurement operators and POVM

Prof. D.K Ghosh, Department of Physics, IIT Bombay

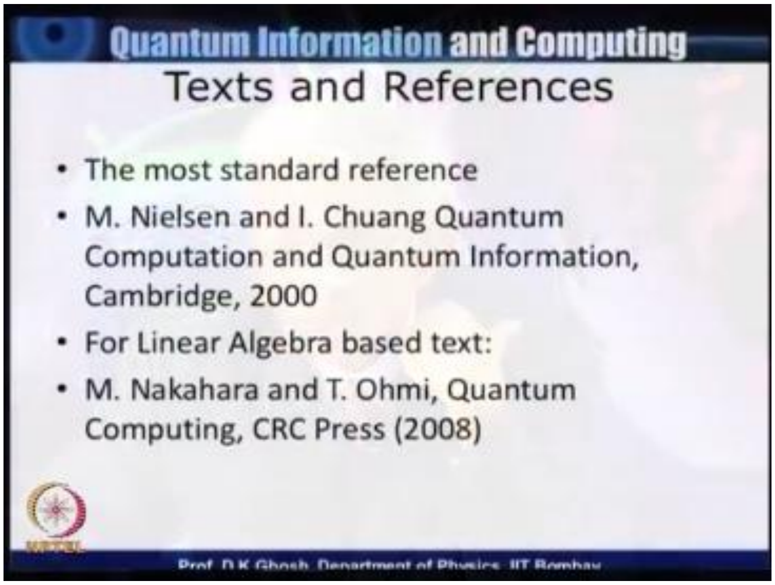
How to use this to our advantage and extract quantum require. We will be bringing up a theorem known as quantum no cloning theorem which tells us that we cannot duplicate a quantum state. And we will see that how a quantum state can be transported from one place to another by a very interesting algorithm known as quantum teleportation. We will be done introducing simple quantum algorithms, but in addition to making a logical conclusion of the course towards the two major algorithms that we talk about we will the bringing up something which are fairly interesting tests of quantum mechanics.

One of the paradox of quantum mechanics was pointed out to by Einstein Prodowsky and Rosen as you might recall that one of the persons who never believed the [indiscernible][00:25:57] interpretation of quantum mechanics was under Einstein himself. And this he presented a paradox which is known APR paradox and that has become a subject of in terms debate among the leaders of quantum mechanics and those who believed in the alternate theory known as the invariant theory.

John Bell provided what we make all as a conclusive test to determine which one of the theories variety. These require certain equalities known as Bellson equality and we will be talking about them of this course. Once we have completed the quantum computing part we will be spending the last few lectures on the aspects of quantum information theory. But before that we have a quick review of classical information.

We all understand what is information in some lose sense it will, means knowledge but we will see what is the way of quantifying or majoring information. Both classical information and quantum information and we will see that interestingly a quantity known as entropy with which you have familiarity in your terminal course comes to our rescue.

(Refer Slide Time: 27:29)



Quantum Information and Computing

Texts and References

- The most standard reference
- M. Nielsen and I. Chuang Quantum Computation and Quantum Information, Cambridge, 2000
- For Linear Algebra based text:
- M. Nakahara and T. Ohmi, Quantum Computing, CRC Press (2008)

Prof. D.K Ghosh, Department of Physics, IIT Bombay

And finally towards the last one or two lectures we will be giving you an overview of practical realization of a quantum computer. This course will be primarily based on the most standard reference that is there by Nielsen and Chuang quantum computation and quantum information but as I will be doing a lot of linear Algebra there is a linear Algebra based it text by Nakahara and Ohmi on quantum computing.

I will also be giving a detail list of other books that are available in the market for quantum computer, with this I will begin by regular exposition of quantum computing starting with the postulates of quantum mechanics.

NATIONAL PROGRAMME ON TECHNOLOGY
ENHANCED LEARNING
(NPTEL)

NPTEL
Principal Investigator
IIT Bombay

Prof. R.K. Shevgaonkar

Head CDEEP
Prof. V.M. Gadre

Producer
Arun kalwankar

Online Editor
& Digital Video Editor
Tushar Deshpande

Digital Video Cameraman
& Graphic Designer
Amin B Shaikh

Jr. Technical Assistant
Vijay Kedare

Teaching Assistants
Pratik Sathe
Bhargav Sri Venkatesh M.

Sr. Web Designer
Bharati Sakpal

Research Assistant
Riya Surange

Sr. Web Designer
Bharati M. Sarang

Web Designer
Nisha Thakur

Project Attendant
Ravi Paswan

Vinayak Raut

NATIONAL PROGRAMME ON TECHNOLOGY
ENHANCED LEARNING

(NPTEL)