

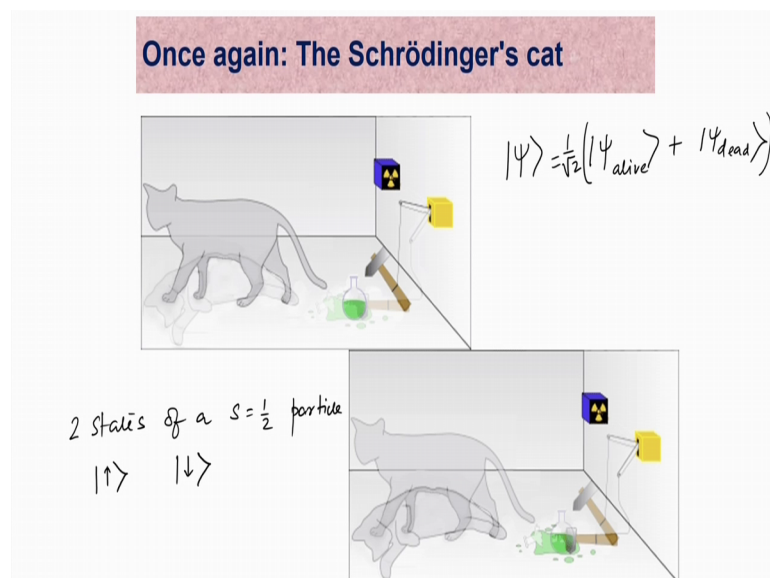
Advanced Quantum Mechanics with Applications
Prof. Saurabh Basu
Department of Physics
Indian Institute of Technology, Guwahati

Lecture - 15
Introduction to Quantum Computing

So, let us start a new subject or rather new module in the study of quantum mechanics that we have engaged in and it is called as the Quantum Computing. And, possibly it is one of the most interesting topics that keep the scientist busy over the next decade or so because, there are lots of developments that are happening and lots of open problems which need to be solved and attended.

So, in this particular lecture or the section of the lecture, I will give a brief introduction to this quantum computing and sort of this will be more like a popular introduction which should be acceptable or rather understandable for more general public. And then, I will go on to the details of various subtopics that we will mention in this lecture.

(Refer Slide Time: 01:35)



So, once again we go back to this Schrodinger's cat which we have talked about earlier. So, just to remind you of the situation that there is a cat which is left alone in a room and nobody is watching it. There is hammer that you can see which is hanging on a green colored portion kept in a bottle and this hammer is connected to a pulley. So, if the cat comes and disturbs the pulley, the hammer will fall onto the glass tube and the portion

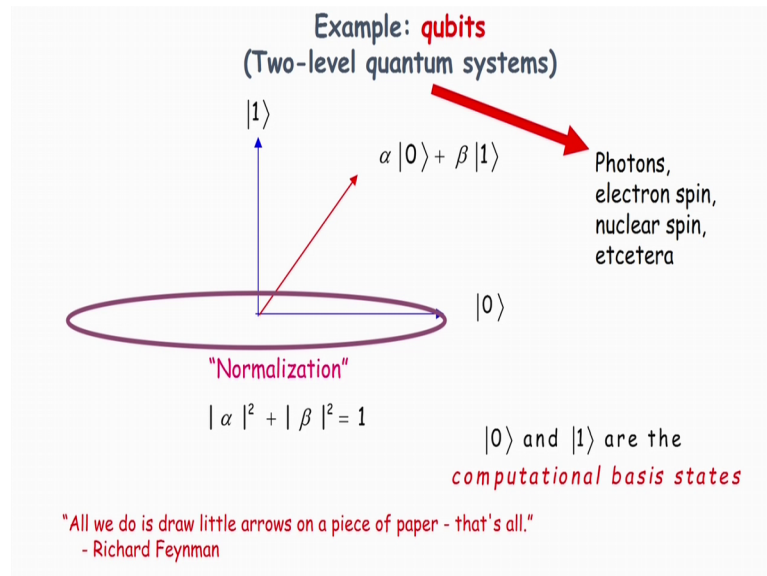
will come out and the portion is assumably poisonous. So, the cat will die and if he decides to stay away from, then it will be alive and if it does not you know I mean tamper with the pulley, then the hammer will be where it is and there will be no spilling out of that poison and it will be safe.

So, unless one does a measurement, one does not know whether it is dead or alive. So, it is in the superposition of state in the mind of an observer before an observation is made. So, it is in a state which may be given by a superposition superpose state which is a ψ alive plus, ψ dead. And, just to have proper normalization, we can write $1/\sqrt{2}$, so that the probability of being it alive is half and the probability of being dead is also half. Now, as soon as one does a measurement, it collapses into one of the available states which is either dead or alive. And say it is alive, then the amplitude that is associated with alive becomes 1 and the other amplitude that is associated with the state dead is equal to 0. So, as long as one has not made any measurement, it is in the superposition of state.

Let us talk about this coin, tossing of a coin and bias coin. So, it will be when it spins goes up and then, come down to the ground either between your palm or on the ground. It is found in one of the states that is head and tail. So, once you make a measurement, once you want to decide say who would bat first in cricket, it collapses into one of these head or tail. So, quantum mechanical coin in a sense is always spinning because, it is in the superposition of state and never comes down. The moment it comes down and you make a measurement, it becomes classical. So, measurement actually in some sense kills quantum mechanics.

So, there are various such examples of these 2 state systems just like it is mentioned here and we are given example of coin tossing giving head or tail or it could be just the 2 states of a spin half particle which are given as up down or take as on-off state of a switch or it could be the ground voltage v equal to 0 and an excited voltage which is say v equal to sum v . So, v can also be taken as a 2 state system. So, we will show that this 2 stage system and the superposition that goes along with, it forms an important part of this quantum computing or the quantum information has name course.

(Refer Slide Time: 06:02)



So, we will discuss what are called as qubits which are nothing, but just an amalgamation of the two words quantum and bits. A bit we are similar in the context of classical computers. Bits are 1 and 0 and every number is formed by the combination of 1 and 0 and when we discuss it in the context of quantum mechanics, then it is called as qubit. So, we are talking about particularly two level quantum system. We can actually talk about multi level quantum system if we just briefly will touch, but the two level systems are most important and convenient for us to discuss.

So, as we have just said that there are two level quantum systems, many of them such as photons having the polarization of photons, the spins of the electrons, the nucleus spins and a large variety of them as we have just seen. So, let us just draw two coordinate axis and label them as 1 and 0. You can also label them as dead or alive, you can also label them as up or down in the context of the spin of particles, but let us just talk about 1 and 0 just like the classical bits are being introduced. So, these are the 0's and 1's are the computational basis states which are going to be useful for our discussion.

So, we are just looking at a vector which is formed by the combination of the superposition of 0 and 1. Just recall that we have written down state like this in the last slide of the cat being dead and alive. So, the 0 state corresponds to dead and 1 corresponds to alive with their individual amplitudes given by alpha and beta. So, this is a vector that is drawn in that space which is spanned by 0 and 1 kets. There is a course

on normalization condition which is what we have seen; there is a half possibility of the cat being dead and the half of it being alive. So, the amplitude square should be normalized that is the alpha mod alpha square plus mod beta square should be equal to 1. So, this is a statement made by Richard Feynman.

He said that all we do is draw little arrows on a piece of paper. So, you see that with 0 and 1, one could write an unique classical number which is usually the numbers that are you know fed into the classical computers that we all are familiar with. However, in this particular case, there can be infinite number of numbers that can be formed with different choices of alpha and beta and the only constraint being alpha square plus beta square of the mod alpha square plus the mod beta square equal to 1.

So, say for example, alpha equal to or alpha square equal to 0.99 and beta square equal to 0.01 would give rise to a particular state and another distance that can be obtained by taking alpha mod alpha square equal to 0.98 and mode beta square equal to 0.02. So, they are distinct quantum states and could be made to carry distinct information, and there are infinite number of such combinations that are possible. So, just by using bits 0 and 1 in a super positions sense, we can actually built an infinite number or rather store infinite number of numbers.

(Refer Slide Time: 10:20)

Postulate 1

Associated to any quantum system is a complex vector space known as state space.

The state of a closed quantum system is a unit vector in state space.

Example: we'll work mainly with qubits, which have state space \mathcal{C}^2 .

$$\alpha |0\rangle + \beta |1\rangle \equiv \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

So, in some sense this talk about postulate or other piece of information which is important in this context. So, it is associated with any quantum system there is a complex

vector space known as State Space, and the state space that we are aware of are all complete which means they are orthogonal to each other. Each entry is orthogonal to the other and they are also normalized. So, they are orthonormalized and in that sense they are complete and an infinite vector space, he has a special name which is called as a Hilbert space; after the name of a mathematician called Hilbert. The state of a closed quantum system is a unit vector in the state space, just as in the slide that we have seen that this is that vector. So, a state of a system is represented by this vector which is α_0 and β_1 where clearly 0 and 1 form the coordinate axis for this particular problem.

We will of course mainly work with qubits as I told which have a state space which we write as \mathbb{C}^2 because these are complex vector spaces. So, we write it with \mathbb{C} which denotes a complex vector space and 2 denotes a two-dimensional complex vector space. So, a qubit α_0 and β_1 is actually written by two column vector which is $\begin{bmatrix} \alpha_0 \\ \beta_1 \end{bmatrix}$. So, this is a notation that is somewhat universally accepted and one can simply write within like a column vector $\begin{bmatrix} \alpha_0 \\ \beta_1 \end{bmatrix}$. It would mean that we are talking about qubit with amplitudes α_0 and β_1 corresponding to 0 and 1 state.

(Refer Slide Time: 12:29)

A few conventions

We write vectors in state space as: $|\psi\rangle$

This is the *ket* notation.

We ^{nearly} *always* assume that our physical systems have *finite-dimensional* state spaces.

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \dots + \alpha_{d-1}|d-1\rangle$$

$$= \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{d-1} \end{bmatrix}$$

Qudit
 \mathbb{C}^d

Few more conventions if would actually help us to understand things better. So, we write vectors in state space as $|\psi\rangle$, which is equal to $\alpha_0|0\rangle + \beta_1|1\rangle$. So, is called as ket notation, which you are aware of and we nearly assumed that all are physical systems are finite dimensional state spaces. Of course, for

the sake of learning quantum mechanics, we have seen that they are actually they could be infinite dimensional. In fact, all these x and p , the position in the momentum the basis in which they are written are actually infinite dimensional. But, for the needs for this particular subject, we can think of finite dimensional state spaces and they are orthogonal orthonormal to each other and not only that if they are not orthogonal, they can be organized by a technique which is called as a Gram Schmidt Orthogonalization.

So, we can actually think of d dimensional space instead of two-dimensional space and we can write down the state space or a state vector ψ as $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \dots + \alpha_{d-1} |d-1\rangle$ and all that and all the way going up to α_{d-1} multiplied by the ket $d-1$. And, in a shorthand notation, it will be $\alpha_0 \alpha_1 \alpha_2 \dots \alpha_{d-1}$ and as we have learnt earlier that this corresponds to d dimensional complex vector space. So, this is called as qudit, instead of qubit dit for d dimensional space.

(Refer Slide Time: 14:33)

Quantum Entanglement

Quantum Entanglement is a uniquely quantum mechanical phenomenon.

It is a property of a multi-qubit (tensor product of individual qubits) and can be thought of as a resource in quantum computing.

The key to entanglement is the property that the **state space CAN NOT be decomposed into component spaces.**

In summary, by measuring one qubit, it is possible to affect the measurement of other qubit(s) in the system.

EPR paradox (**Can Quantum Mechanics be complete?**).

Hidden variables and Bell's inequality.

How these concepts of quantum entanglement and various other things would be elaborated later in the next lecture on the next discussion, but let us priory define them and try to at least get ourselves motivated that these are important things to study in the context of quantum information. So, quantum entanglement is uniquely quantum mechanical phenomena and has no classical analogue and this is what it means. It is a property of a multi qubit which is a tensor product of individual qubits and can be thought of as a resource in quantum computing. The key to entanglement is the property

that the state space cannot be decomposed into component spaces. So, the composite space remains composite and no combination or rather no choice is of some complex corporations. We would be able to write that as a product of two spaces or two qubits.

So, in summary if you want to just say before we do things in details, in summary by measuring 1 qubit it is possible to affect the measurement of other qubits or qubits in the system and this also has relevance to EPR paradox. This EPR are the first letters of the names of Einstein Podolsky and Rosen and these are, so Einstein actually question that can quantum mechanics be complete because, this quantum entanglement actually gives rise to the possibility of faster than light communications and since relativity clearly states that there cannot be anything which moves faster than light. So, is quantum mechanics is in a confrontation with relativity and whether it is complete and Einstein had this idea of that there are hidden variable, however they are negated by Rosen and by Bell's inequality.

(Refer Slide Time: 16:58)

Quantum Teleportation

Quantum Teleportation is about carrying a fixed amount of information through the system of qubits.

QT is a means to replace the state of one qubit with that of another.

The interesting name derives from the fact that the state is *transmitted* by setting up an entangled state space of 3 qubits and then removing two of them from the entanglement via measurement.

Since information of the source qubit is preserved by these measurements the information lands up in the third, that is, the destination qubit.

There is another very interesting concept in physics which has found a lot of mention in the science fiction books and movies. It is called as Quantum Teleportation. So, quantum teleportation is about carrying fixed amount of information through the system of qubit. So, this certain amount of information is being carried, and basically this if this transmission of information happens at a speed which is faster than the speed of light, then we can say that there are you know teleportation of information that happens

and it means that to replace the state of qubit with that of another, and the interesting name, the person name is very interesting is quantum teleportation.

This name is derived from the fact that the state is transmitted by setting up an entangled state of 3 qubits and then, removing two of them from the entanglement via measurement we will of course these are this let them remain as words complicated that too, however we will make sure that one understands what is being conveyed here. So, the information of the source qubit is preserved by these measurements. The information lands up in the third that is the destination qubit. So, this is all about quantum teleportation and you would find them as I said that mentioned in the science fiction movies or books.

(Refer Slide Time: 18:55)

Super dense Coding

Super dense coding is in some sense the reverse of Quantum Teleportation.

The idea is to send two classical bits of information by sending one qubit.

It works by first pre-communication of this EPR pair that is shared between the receiver and the sender

Then, we would also discuss what is called as a super dense coding which is in some sense it is the reverse of quantum teleportation; so, the idea is to send two classical bits of information by sending 1 quantum bit or qubit. So, it works by first pre-communication of this EPR pair. So, EPR pair are those variables which one, when one being determined the other automatically gets determined. That is called as EPR pair that is shared between the receiver and the sender.

(Refer Slide Time: 19:37)

Quantum logic gates

Quantum not gate:

Input qubit

$X |0\rangle = |1\rangle; \quad X |1\rangle = |0\rangle.$

$\alpha |0\rangle + \beta |1\rangle \rightarrow ?$

$\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |1\rangle + \beta |0\rangle$

Matrix representation:

X

Output qubit

$U^\dagger U = \mathbb{1}.$

$$X = \begin{matrix} |0\rangle & |1\rangle \\ |0\rangle & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ |1\rangle & \end{matrix}$$

General dynamics of a closed quantum system (including logic gates) can be represented as a **unitary matrix**.

Let us just introduce the quantum logic gates which are analogous to the classical logic gates. So, if you have a quantum not gate, so an input qubit would pass through a quantum not gate and would give me. So, if it acts on 0 will give me 1 and if it acts on a 1 it will 0. So, the output qubit will be if the input qubits are 0 and 1 as it is written on the left hand side of those two equations, then the output qubit would be what appears in the right of those equations that is namely 1 and 0 corresponding to 0 and 1 qubit.

So, the question is that now if we want to do this operation on a qubit which is given by a combination or a super position of alpha 0 and beta 1, then what happens? So, alpha 0 actually goes to alpha 1 and beta 1 goes to beta 0. So, one actually gets the interchange, interchanging of the probability aptitudes or the amplitudes of this state spaces.


So, the matrix representation of such a thing can be written as 0 1 1 0, so that 0 is converted into 1 and 1 is converted into 0 and so on and so forth and this is nothing, but if you see that this is like the Pauli matrix. The x components of the Pauli spin matrix correspond to spin equal to half. So, the general dynamics of closed quantum systems including the logic gates can be represented by unitary matrix. We have given the definition of unitary matrix. Unitary matrix is defined as $U^\dagger U = I$ or $U U^\dagger = I$ is equal to an identity matrix. So, that is the definition or rather that is the test for unitary matrix.

(Refer Slide Time: 21:47)

Exercise: prove that $XY=iZ$


Pauli gates

X gate (AKA σ_x or σ_1)




$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle; \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Y gate (AKA σ_y or σ_2)



$Y|0\rangle = i|1\rangle; \quad Y|1\rangle = -i|0\rangle; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Z gate (AKA σ_z or σ_3)



$Z|0\rangle = |0\rangle; \quad Z|1\rangle = -|1\rangle; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Notation: $\sigma_0 \equiv I$

Exercise: prove that $X^2=Y^2=Z^2=I$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in terms of $\sigma_x, \sigma_y, \sigma_z$ and σ_0

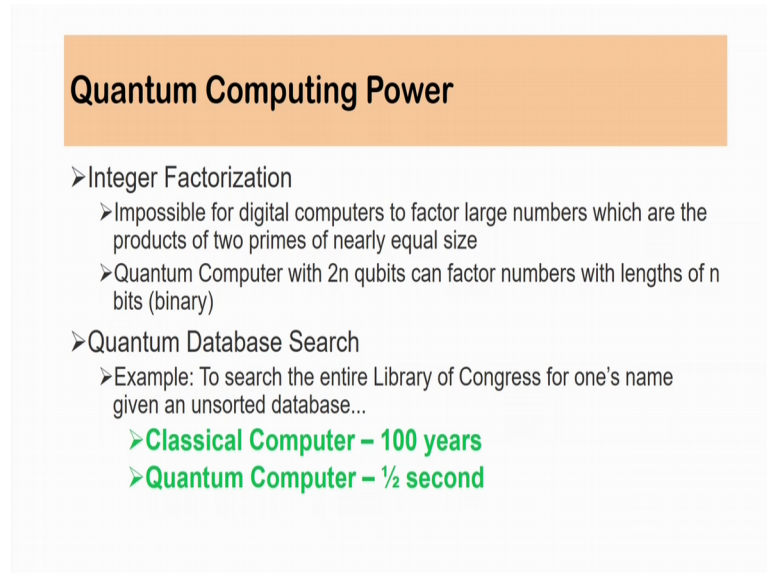
So, let us look at this Pauli gates which are sigma x or sigma 1 and that you know just acts like not gates. So, it converts 0 into 1 and 1 into 0 and also there is y gate which is written as sigma y or sigma 2 and this has a particular form which is 0 minus i 0. Do not mistake any of these having complex entries to be non-hermitian operators. They are all Hermitian operators and they have really eigenvalues. One can check that. So, this is y gate also known as the sigma y or sigma 2. As I told you and this is z gate also known as sigma z and sigma 3 and that just returns back the states excepting for the one state, it returns a minus 1. So, it is written as 1 0 0 minus 1 and this is nothing, but the z component of the Pauli matrix, ok.

So, as an exercise you can actually show that x into y is equal to i into z. So, this take, this matrix and multiplied with this matrix. So, let us do that for the moment so, x y equal to 0 1 1 0 and 0 minus i i 0. So, this is equal to 0 and i so, then 0 minus i and 1 0. So, this is equal to 0 1 0, this is also equal to 0 1 minus i. So, this minus i and this is equal to i and this is 1 0 0 minus 1. So, this is i into z, so on.

So, these are easy things and there is also another 2 by 2 matrix which is of importance here, that is sigma 0 which is equal to the identity matrix and it is important for you to know from the mathematical point of view that any 2 by 2 matrix call it a b c d, they can be written in terms of sigma x sigma y sigma z and sigma 0 by properly choosing

coefficients any 2 by 2 matrix, also as an exercise one can show that the x square equal to y square equal to z square equal to an identity matrix.

(Refer Slide Time: 24:41)



Quantum Computing Power

- Integer Factorization
 - Impossible for digital computers to factor large numbers which are the products of two primes of nearly equal size
 - Quantum Computer with $2n$ qubits can factor numbers with lengths of n bits (binary)
- Quantum Database Search
 - Example: To search the entire Library of Congress for one's name given an unsorted database...
 - **Classical Computer – 100 years**
 - **Quantum Computer – ½ second**

So, let us give very brief introduction to the quantum computing power. Why quantum computers will take a center stage in research and in learning? For the next you know maybe a decade or even more than that is because the integer factorization which is impossible for digital computers to factorize very large numbers which are the product of two primes of nearly equal size and quantum computer with $2n$ qubits can factor numbers with lengths n bits which are binary lengths. Quantum database search as an example one can see that to search the entire library of congress for a particular name and given an unsorted database in classical computers, it will take 100 years where as in a computer quantum computer, it should take half a second and that is a miraculous speed that we are talking about.

(Refer Slide Time: 25:45)

What is a Quantum Computer?

- Quantum Computer
A computer that uses quantum mechanical phenomena to perform operations on data through devices such as superposition and entanglement.
- Classical Computer (Binary)
A computer that uses voltages flowing through circuits and gates, which can be calculated entirely by classical mechanics.

So, what is the quantum computer? The computer that uses quantum mechanical phenomena to perform operations on data through devices, such as superposition in entanglement which is a little of it we have already seen. We will see more of that and classical computer as a post to the quantum computer. It uses voltages that flow through circuits and gates and can be calculated entirely by classical mechanics.

(Refer Slide Time: 26:13)

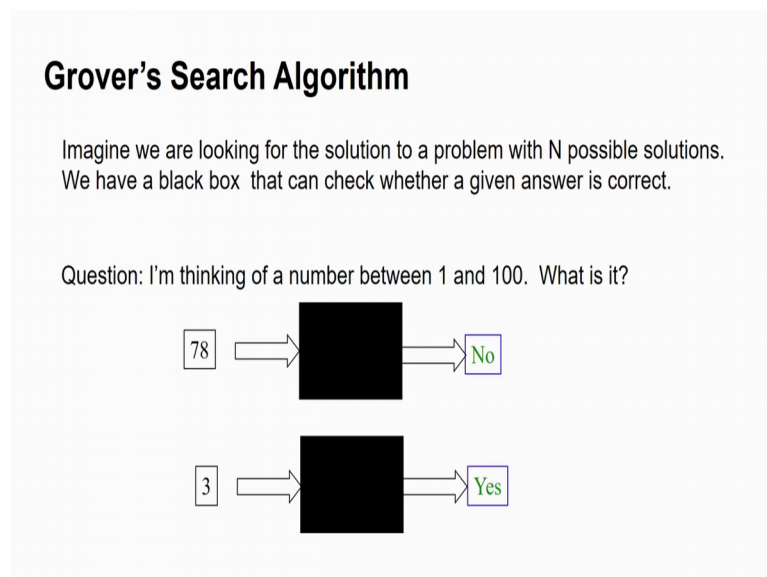
Shor's algorithm

- Shor's algorithm is used to factor numbers into their components which can potentially be prime. It does this in roughly $O(n^3)$ quantum operations.
- The best known classical algorithms are exponential.
- Since the difficulty of factoring is believed to be exponentially hard, it forms the basis of most crypto systems.
- Thus factoring in polynomial times has attracted significant interest.

So, one of the very important thing about quantum computation, quantum computation is factorization of very large numbers and there was an algorithm put forward by Peter Shor

in which it is this algorithm is used to factor numbers into their components which can potentially be prime just like we have seen just a while back and it does this in roughly order of n^3 quantum operations, ok. So, the best known classical algorithms are at the best exponential. Since the difficulty of factoring is believed to be exponentially hard, it forms the basis of most cryptosystems, ok. This factoring in polynomial times is so basically because a quantum computing does it in polynomial times which is n^3 , it has attracted significant amount of attention.

(Refer Slide Time: 27:11)

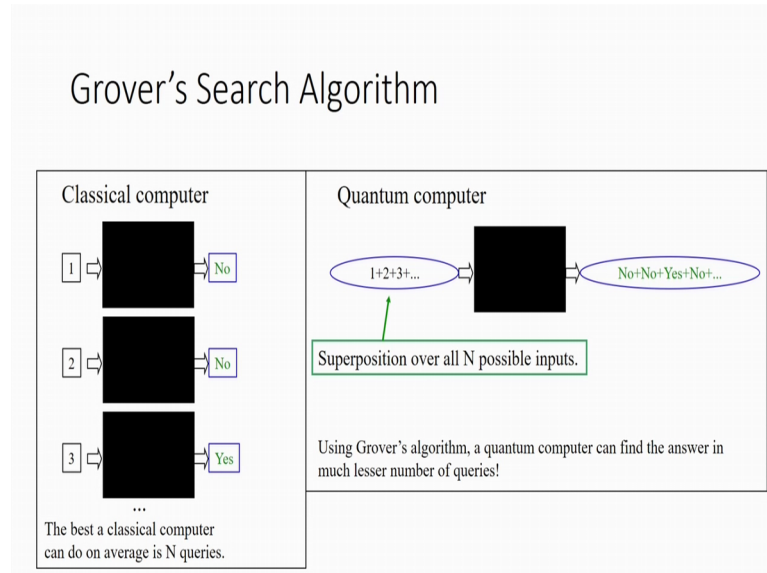


Let us look at this Grover's search algorithm which says that in some sense you know the parallel version of the classical computer is already built into that. So, if you want to understand how the classical computers work, they actually work with the flow in time which means that one job gets over and the next job starts like if you think about the multiplication of two large matrices, it will multiply the row of the left one to the column of the first, the second one and then, store it as the first element some all these entries and store it as the first element of that resulted matrix and then, it will go on to do it for the second row and the second column, however all these things are done in a parallel fashion in a quantum computer.

Let us see how that happens. So, let us say that we are I am thinking of a number between 1 and 100 and say have thought about the number which is 3. So, the classical

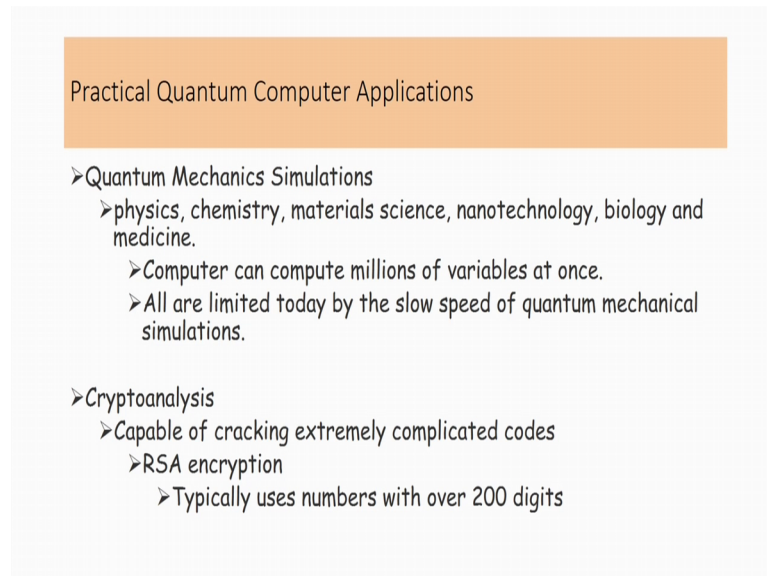
computer will keep asking that is the number 1 is the number 2 is the number 3 is the number 4 and all that and then, once it gets the answer, yes it stops its operations.

(Refer Slide Time: 28:37)



So, it is like this the classical computer you keep going 1 no, 2 no, 3 no and so on. So, there will be n such queries by which it will be resolved that actually the number that I have thought about is 3, however in a quantum computer this is done very differently way. It is put as the entire you know 1 to 100 is put as superposition and so, there is an input that is given to the quantum computer is 1 plus 2 plus 3 plus 4 and so on. So, it will keep doing it no, no, no and then, yes for third and then no, no, no, no and for the rest you know 97 entries or 96 entries. So, this is called is the Grover's Search Algorithm. So, at the quantum computer will find to the query in very lesser number of you know queries as compared to the classical computer.

(Refer Slide Time: 29:35)

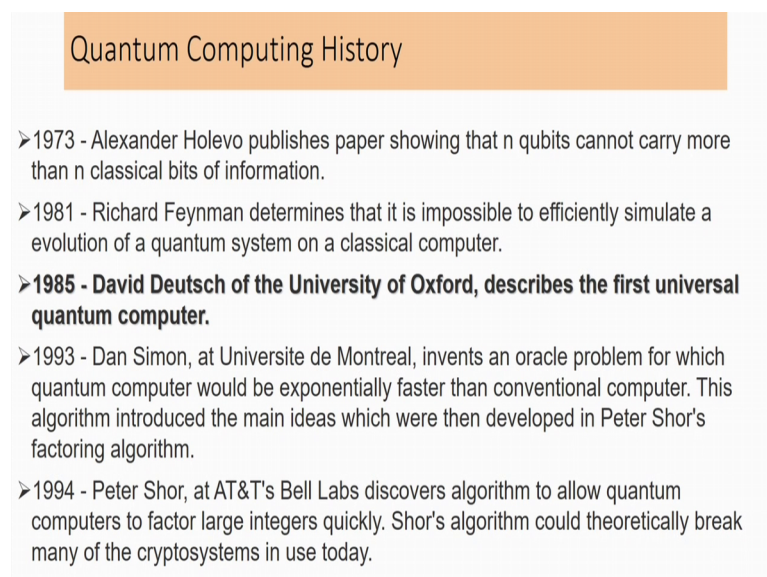


Practical Quantum Computer Applications

- Quantum Mechanics Simulations
 - physics, chemistry, materials science, nanotechnology, biology and medicine.
 - Computer can compute millions of variables at once.
 - All are limited today by the slow speed of quantum mechanical simulations.
- Cryptoanalysis
 - Capable of cracking extremely complicated codes
 - RSA encryption
 - Typically uses numbers with over 200 digits

So, the practical quantum computer applications is that the quantum mechanics simulations in physics, in chemistry, material science, nanotechnology, biology, medicine, computers can simulate millions of variables at once and all are limited today by the slow speed of the quantum mechanical simulation and then, there is something called as cryptoanalysis is capable of cracking extremely complicated codes and this RSA encryption as a name goes and typically uses numbers with 200 digits.

(Refer Slide Time: 30:11)



Quantum Computing History

- 1973 - Alexander Holevo publishes paper showing that n qubits cannot carry more than n classical bits of information.
- 1981 - Richard Feynman determines that it is impossible to efficiently simulate a evolution of a quantum system on a classical computer.
- **1985 - David Deutsch of the University of Oxford, describes the first universal quantum computer.**
- 1993 - Dan Simon, at Universite de Montreal, invents an oracle problem for which quantum computer would be exponentially faster than conventional computer. This algorithm introduced the main ideas which were then developed in Peter Shor's factoring algorithm.
- 1994 - Peter Shor, at AT&T's Bell Labs discovers algorithm to allow quantum computers to factor large integers quickly. Shor's algorithm could theoretically break many of the cryptosystems in use today.

So, let us have brief at the history and the main ones. In fact, this the quantum computing history in 1993 Alexandra Holevo published a paper showing that the qubits can carry more than classical mechanics bits of classical bits of information. 1981 Richard Feynman determines that it is possible to efficiently simulate a evolution of quantum system on a classical computer. 1985 David Deutsch of the University of Oxford described the first universal quantum computer.

1993 Dan Simon at Montreal, he invented the Oracle program or problem for which quantum computer would be exponentially faster than the conventional classical computer. This algorithm introduced the main ideas which were then developed in Peter Shor's Factoring Algorithm. We will give a detailed account of this Shor's algorithm and Shor's problem, the factorization problems. In 1994 Peter Shor at T bell labs, it discovers an algorithm to allow quantum computers to factor large integers quickly. Shor's algorithm could theoretically break many of the cryptosystems in use.

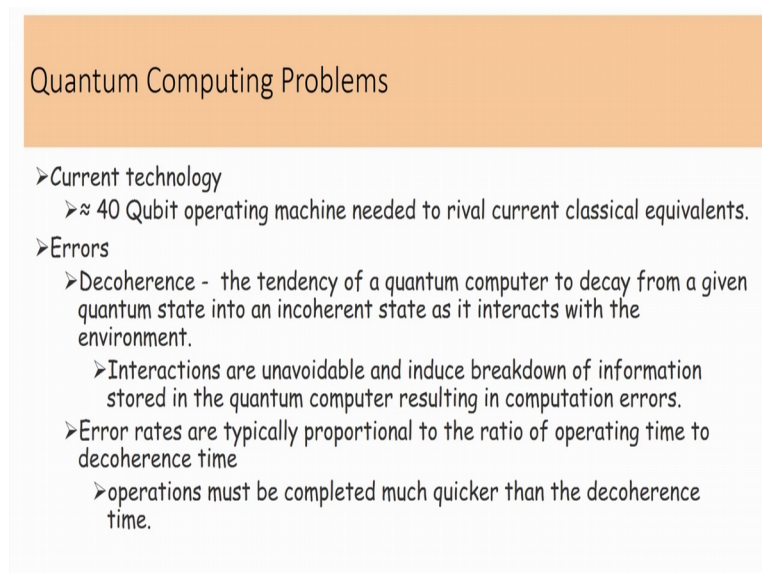
(Refer Slide Time: 31:31)

- 1995 - Shor propos the first scheme for quantum error correction.
- 1996 - Lov Grover, at Bell Labs, invents quantum database search algorithm.
- 1997 - David Cory, A.F. Fahmy, Timothy Havel, Neil Gershenfeld and Isaac Chuang publish the first paper on quantum computers.**
- 1998 - First working 2-qubit NMR computer demonstrated at University of California, Berkeley.
- 1999 - First working 3-qubit NMR computer demonstrated at IBM's Almaden Research Center. First execution of Grover's algorithm.
- 2000 - First working 5-qubit NMR computer demonstrated at IBM's Almaden Research Center.
- 2001 - First working 7-qubit NMR computer demonstrated at IBM's Almaden Research Center.**

Today in 1995, Shor proposes the first scheme for quantum error correction. In 96 Grover which is we mentioned his work and Bell Labs, invents a quantum databases search algorithm. So, that is Grover search algorithm. In 97 David Cory, A. F. Fahmy, Timothy Havel and Gershenfeld and Isaac Chuang published the first paper on quantum computing.

So, it is not very old. It is about 20- years old. When the first paper had come out in 1998, the first working 2 bit 2 qubit NMR computer demonstrators at the university of California at Berkeley, 1999 first working 3 qubit NMR computer demonstrate is at IBMS Almaden Research Centre. The first execution of Grover's algorithm was achieved in 2000, first working 5 qubit NMR computer demonstrated as IBMS Almaden Research Centre and in 2001, first working 7 qubit NMR computer demonstrated as IBMS, again Almaden Research Centre and of course, these activities are going on. It has not stopped at 2001, but I have just given a brief history of that how it developed in the initial days and so are the quantum computing problems.

(Refer Slide Time: 33:01)



Quantum Computing Problems

- Current technology
 - \approx 40 Qubit operating machine needed to rival current classical equivalents.
- Errors
 - Decoherence - the tendency of a quantum computer to decay from a given quantum state into an incoherent state as it interacts with the environment.
 - Interactions are unavoidable and induce breakdown of information stored in the quantum computer resulting in computation errors.
 - Error rates are typically proportional to the ratio of operating time to decoherence time
 - operations must be completed much quicker than the decoherence time.

The current technology or 40 qubit operations, operating machines needed to rival current the classical equivalent errors are caused by the decoherence. There is the tendency of the quantum computer to dk from a given quantum state into an incoherent state as it interacts with environment. Interactions are unavoidable and induced breakdown of information stored in the quantum computer resulting in computational errors and error rates are typically proportional to the ratio of the operating time to the decoherence time. So, that is the errors rates or one can estimate errors by that and the operations must be complicated, much quicker than the difference time.

So, these are some of the problems that are going to come up or that are already come up, however there are also efforts to negotiate or mitigate those difficulties and problems.

So, with this I will end this somewhat popular introduction to quantum computing, however I will take on each of the topics or most of the topics in detail for a better understanding of the subject.