

**NPTEL**

**NATIONAL PROGRAMME ON  
TECHNOLOGY ENHANCED LEARNING**

**IIT BOMBAY**

**CDEEP  
IIT BOMBAY**

**Quantum Information and  
Computing**

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

**Modul No.04**

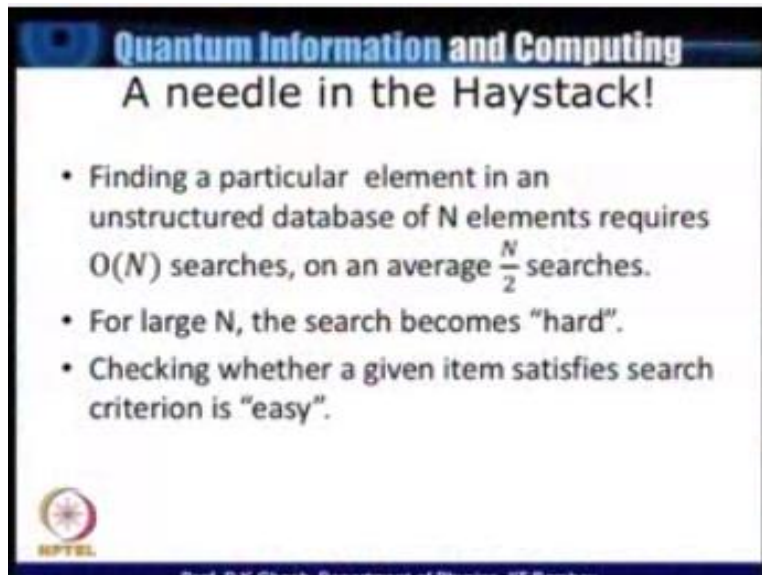
**Lecture No.19**

**Grover's Search Algorithm-I**

In the last lecture we talked about a problem called Simon's problem in some sense among the minor algorithm that was one of the significant development in quantum computing. In the next couple of lectures this one and the next couple of lectures I will be discussing one of the more significant algorithms which along with another algorithm that I will be talking about have been so far the most significant results of quantum computing.


The algorithm that we talk about today is due to Grover actually he is an Indian love Grover the algorithm is a database search it is popularly known as Grover's searcher.

(Refer Slide Time: 01:09)



**Quantum Information and Computing**  
**A needle in the Haystack!**

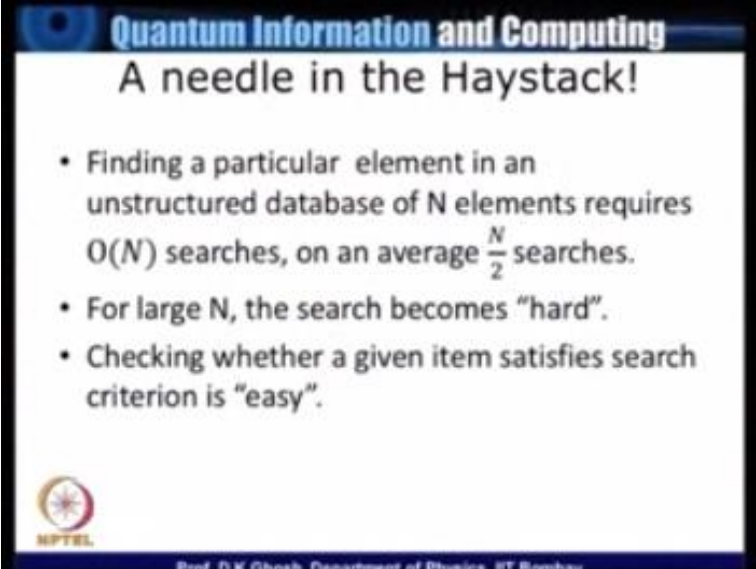
- Finding a particular element in an unstructured database of  $N$  elements requires  $O(N)$  searches, on an average  $\frac{N}{2}$  searches.
- For large  $N$ , the search becomes "hard".
- Checking whether a given item satisfies search criterion is "easy".

 NPTEL  
Prof. D.V. Ghosh, Department of Physics, IIT Bombay

The problem is something like this that suppose I have an unstructured data base, the unstructured data base is basically a database in which there is no particular order if you take a telephone directory for example the old classical telephone directory that was the structured database because you could go through the names in an alphabetical order and then find out the person that you want that telephone number..

But suppose I give you the same telephone directory and ask you to find out the name corresponding to a person whose telephone number then give now and you do it by a classical search that is obviously a very tall order they typically if I have a database of a capital  $N$  which is our short notation for  $2^n$ ,  $n$  is the number of pivots then I would require order  $n$  searches and in a probabilistic way I can say by Cirque will be successful with approximately  $N/2$ .


(Refer Slide Time: 02:25)



**Quantum Information and Computing**

### A needle in the Haystack!

- Finding a particular element in an unstructured database of  $N$  elements requires  $O(N)$  searches, on an average  $\frac{N}{2}$  searches.
- For large  $N$ , the search becomes "hard".
- Checking whether a given item satisfies search criterion is "easy".

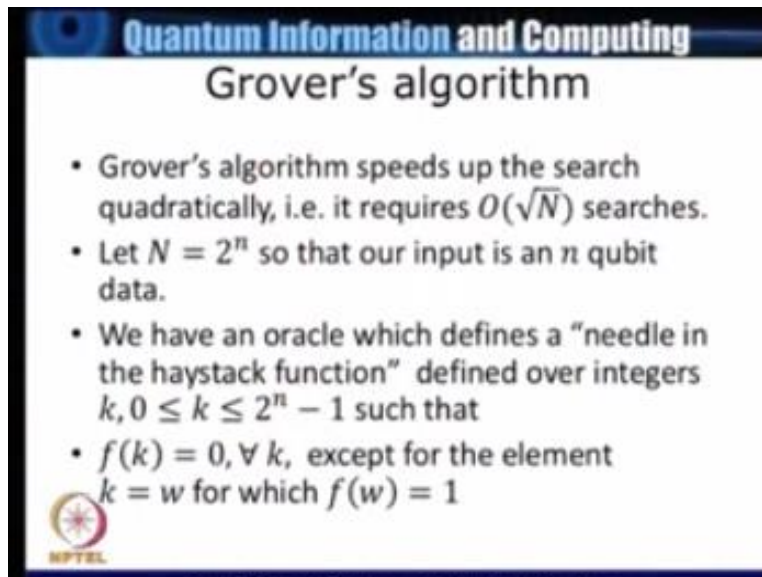
 NPTEL

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

So this is the classical algorithm and this for large  $n$  it becomes a hard problem. Now I have already discussed earlier what is the hard problem that it takes it cannot be done in a polynomial time, but this is the type of problem whether were given a solution checking whether the criterion for the search is satisfied is not easy problem that is if I have a certain characteristic given then I can always put the solution back into my statement of the problem and find out yes this is indeed a solution.


The checking a solution becomes easy but finding that becomes hard now Grover search algorithm actually accelerates this search from order  $n$  to order  $\sqrt{M}$  that is it a quadratically as period of search.

(Refer Slide Time: 03:31)



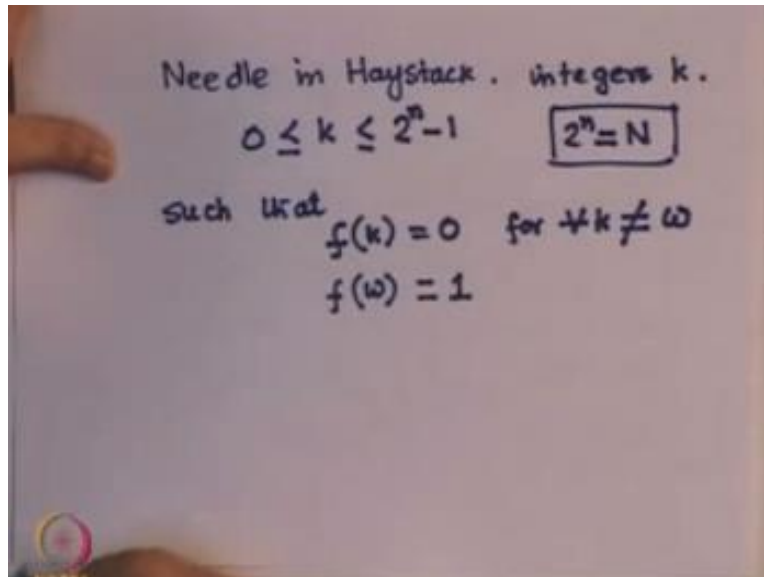
**Quantum Information and Computing**  
**Grover's algorithm**

- Grover's algorithm speeds up the search quadratically, i.e. it requires  $O(\sqrt{N})$  searches.
- Let  $N = 2^n$  so that our input is an  $n$  qubit data.
- We have an oracle which defines a "needle in the haystack function" defined over integers  $k, 0 \leq k \leq 2^n - 1$  such that
- $f(k) = 0, \forall k$ , except for the element  $k = w$  for which  $f(w) = 1$

 NPTEL

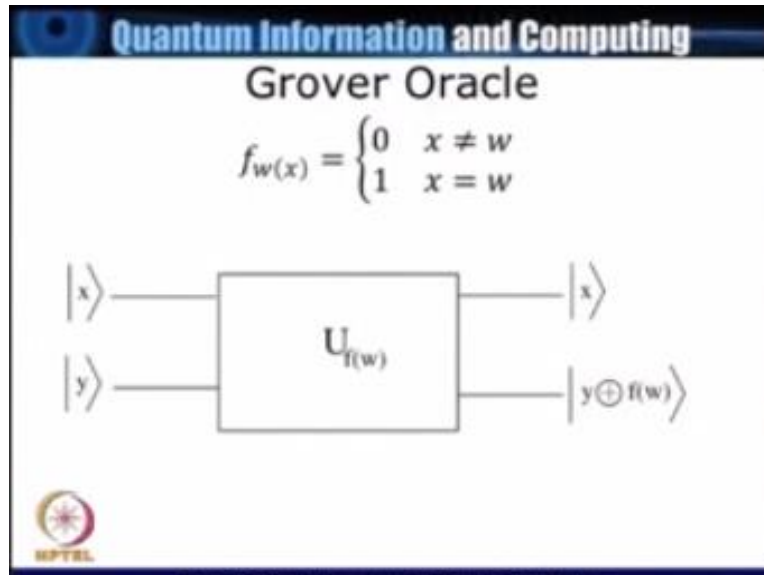
And this is a reasonable acceleration of this number of searches that we need so as we had already said that let  $N = 2^n$ , which is our  $n$  qubit data, now I need an oracle which will calculate a function and this function is what I would call as a needle in the haystack function.

(Refer Slide Time: 03:57)



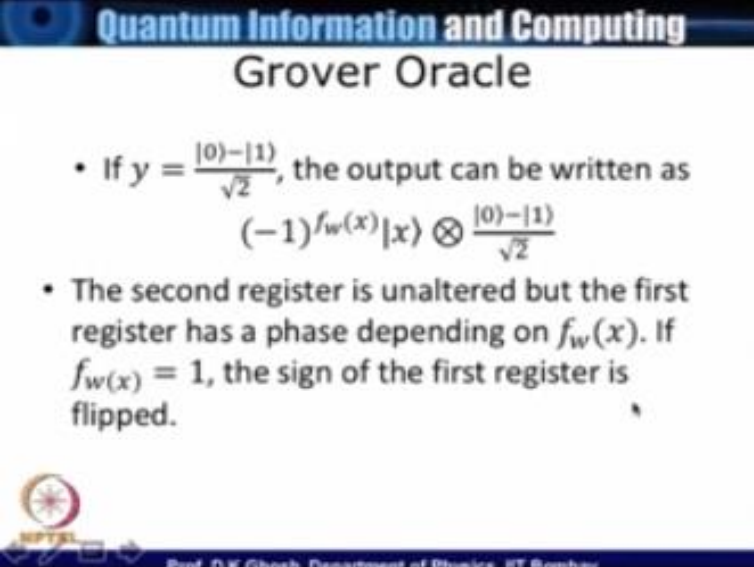
So the needle in the haystack function this is defined over set of integers  $K$ , so let us call it integers  $k$ . So  $k$  is the number which runs from 0 to  $2^n - 1$  remember  $2^n$ , I will frequently be writing as equal to  $N$ . Such that the oracle can calculate a function  $f$  value of  $f(k) = 0$  for all  $k$  not equal to a particular value  $w$ , now if  $k$  happens to be equal to  $w$  then the function evaluates to 1. Our problem is that given a large number of  $k$  which is capital number of case a an oracle which can calculate  $f(k)$  at every stage how do I find out what is this string  $w$  for which  $f(w)$  happens to be equal to 1 while all others evaluate to 0.

(Refer Slide Time: 05:28)




Grover's Oracle schematically is as written here that oracle calculates  $F$ , I have put argument  $w(x) = 0$  if  $x$  is not equal to  $W$  and is equal to  $1$  if  $X = W$ , so as again this is something which will be repeating several times because this is the crux of many things I have an input  $X$  I have a target  $y$  and the function is calculated by the oracle the input remains unchanged but the target will now store  $y$  addition modulo 2 with this function that we have calculated.

(Refer Slide Time: 06:09)



**Quantum Information and Computing**  
**Grover Oracle**

- If  $y = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ , the output can be written as  
$$(-1)^{f_W(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$
- The second register is unaltered but the first register has a phase depending on  $f_W(x)$ . If  $f_W(x) = 1$ , the sign of the first register is flipped.

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

Now suppose my Y is put to be equal to 0 – 1 bit let us look at.

(Refer Slide Time: 06: 18)

- 2-

$$1b \quad y = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Target  $y \oplus f_w(x)$

$$\underbrace{(-1)^{f_w(x)}}_{1b \quad f_w(x)=1} |z\rangle \otimes \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{2nd \text{ Register}}$$

Sign of 1st Register flipped

If  $Y = 0 - 1/\sqrt{2}$  remember my target is  $y + f(x)$  let me call it  $f_w(x)$  just to keep on reminding ourselves then there is a special  $w$  there then if  $Y$  is equal to 0 the output is just  $f(w)$  if  $Y$  is equal to 1 this is just the complement of  $w$ , so in other words I can write the target is equal to minus 1 to the power  $f_w(x)$ ,  $X$  which is this is my including my first register with  $0 - 1/\sqrt{2}$ .

Now remember my  $f_w(x)$  evaluates to either 0 or 1. Now when it is 0 when it is 0 this is 1 so therefore I of course expect what is if  $f_w(x)$  evaluates to 0 then the content is simply  $y$  which is equal to  $0$  minus one way. On the other hand if  $f_w(x)$  evaluates to 1 when my string happens to be equal to  $w$  then it is  $y + 1$  which is nothing but  $1 - 0/\sqrt{2}$  which is what I have indicated.

So since this is the one which has an  $x$  dependence I can put it along with the first register and write it in this fraction so therefore notice that my 2<sup>nd</sup> register is unchanged but my 1<sup>st</sup> register will have its sign flipped if  $f_w(x)=1$  in other words for the given string if  $f_w(x) = 1$  the sign of the 1<sup>st</sup> register will be flipped so let us look at what type of unitary operator will be it so I define a unitary operator.



(Refer Slide Time: 09:07)

- 3 -

$$U_w = I - 2|w\rangle\langle w|$$

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

↑ Standard State
→ Computational basis

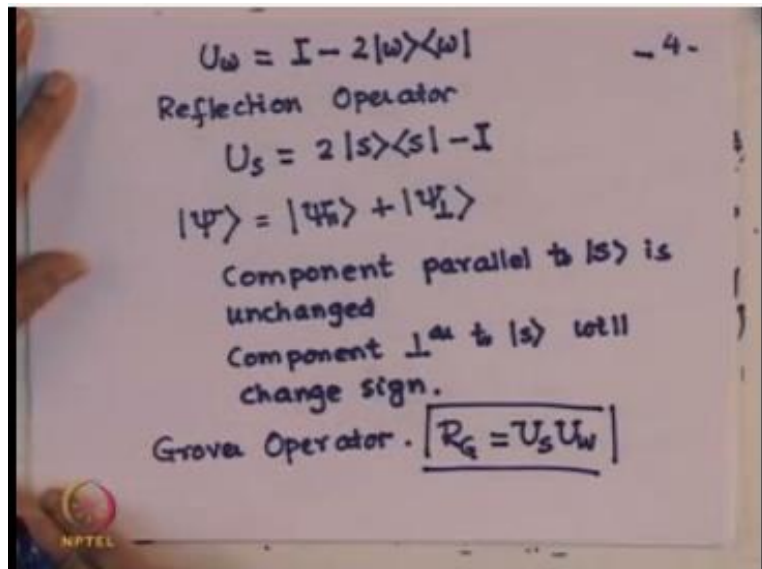
$$\langle w|s\rangle = \frac{1}{\sqrt{N}}$$

Corresponding to this  $w$  and I define this by  $I - 2|w\rangle\langle w|$  so look at how we are going to do this now when this acts on the state  $w$  then I get  $w - 2$  times  $w$  which is  $-w$  so if we have we will take a linear combination of the computational basics as all our inputs and there are  $N$  of them out of that there is a specific  $w$  and all these basis states are orthogonal to each other so if this  $U_w$  which is acting on a state  $w$  which by definition is orthogonal to all other members of the state's there then I get  $-w$ .

So this uniform linear combination let me instead of confusing with  $x$  let my  $x$  be the  $n$  qubit basics let me call it  $s$  standard state with which I start so this standard state as we have written several times  $1/\sqrt{N} \sum_{x=0}^{N-1} |x\rangle$  is a collection of all the states in the computational basics by definition then since  $w$  is the member of this collection then my scalar product of  $w$  with  $s$  remember in this  $\Sigma$  it is a uniform linear combination.

So as a result each one of the members has equal weight and this scalar product is then  $1/\sqrt{N}$  now Grover defined a second operator called reflection operator.

(Refer Slide Time: 11:43)

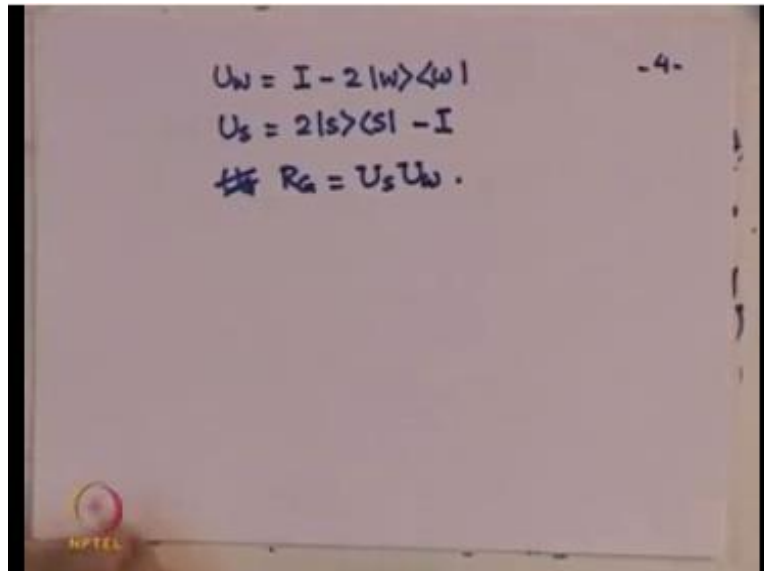


Grover defines a reflection of we will see why dissonant the reflection operator  $U_s$  is  $2|s\rangle\langle s| - I$  I remember the other operator which we are defined earlier was  $U_w = I - 2|w\rangle\langle w|$  there is a order in which these have to be written this why is this a reflection operator suppose I let it act on an arbitrary state  $\psi$  any state now any state  $\psi$  I can resolve into a component along the standard status and a component perpendicular to it now notice that if I write this  $\psi$  parallel +  $\psi$  particular this is parallel and perpendicular to the state  $s$ .

Then acting on this the component parallel to  $s$  will be unchanged. But the sign of the state perpendicular to  $s$ , see if a perpendicular to  $s$  is there then this term will give me 0 because this is parallel to  $s$  perpendicular to  $s$  is the scalar product is zero and the component perpendicular this is an important point to note component perpendicular to  $s$  will be flipped will change sign.

Grovers operator which will call simply as a Grover operator rover rotation operators also it is called  $R_G$  is defined as  $U_w$  followed by  $U_s$ , now what we will do next is to look at a geometrical interpretation of what this means. So let us collect our thoughts again.

(Refer Slide Time: 14:34)



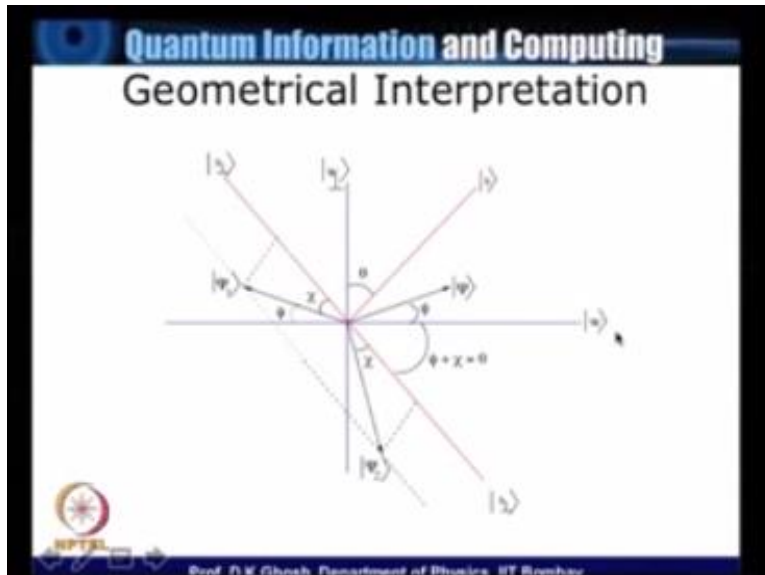
A photograph of a whiteboard with handwritten mathematical equations. The equations are:

$$U_w = I - 2|w\rangle\langle w|$$
$$U_s = 2|s\rangle\langle s| - I$$
$$\# R_G = U_s U_w .$$

The number "-4-" is written in the top right corner. An NPTEL logo is visible in the bottom left corner of the whiteboard.

We have  $U_w$  equal to  $I - 2|w\rangle\langle w|$   $U_s$  is  $2|s\rangle\langle s| - I$  and  $U_G R_G = U_s U_w$  in that order.

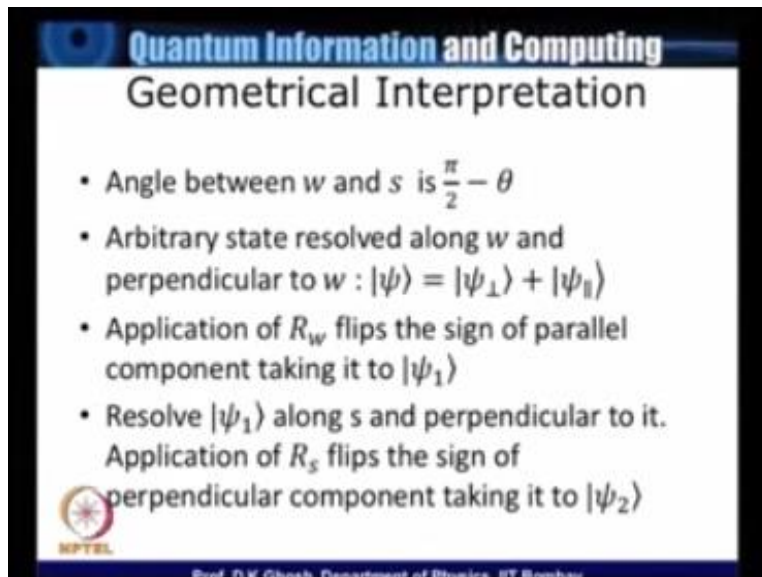
(Refer Slide Time: 14:56)



So let us look at this for the geometrical interpretation of what does the Grover operator do, so what I am going to do here, is the following that I have taken an arbitrary states  $I$  here and this arbitrary state is let us say making some angle  $\phi$  with the  $W$ , now look at the colored things that are there, they  $W$  is a member here. So I have got a  $W$  and  $W$  perpendicular, this is the representation of a vector.


Now  $s$  is given by this redline and perpendicular to that is your  $s$  perpendicular direction and there is an arbitrary angle between  $s$  and the  $W$  perpendicular. Now supposing I just talked about an arbitrary vector sign they have an arbitrary vector sign which is making an angle of  $\phi$  with  $DW$ , so what does this do?

(Refer Slide Time: 16:11)



**Quantum Information and Computing**  
**Geometrical Interpretation**

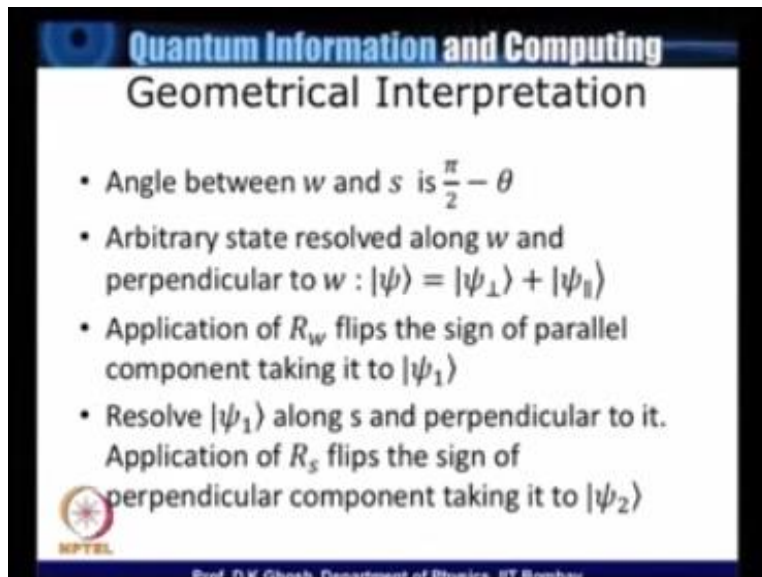
- Angle between  $w$  and  $s$  is  $\frac{\pi}{2} - \theta$
- Arbitrary state resolved along  $w$  and perpendicular to  $w$  :  $|\psi\rangle = |\psi_{\perp}\rangle + |\psi_{\parallel}\rangle$
- Application of  $R_w$  flips the sign of parallel component taking it to  $|\psi_1\rangle$
- Resolve  $|\psi_1\rangle$  along  $s$  and perpendicular to it. Application of  $R_s$  flips the sign of perpendicular component taking it to  $|\psi_2\rangle$

 NPTEL

Prof. D.V. Choudhary, Department of Physics, IIT Bombay


First thing that I do as I told you, I resolve the arbitrary state along  $w$  and perpendicular to  $w$ .  
Now when I apply  $R_w$  to it.

(Refer Slide Time: 16:26)



**Quantum Information and Computing**  
**Geometrical Interpretation**

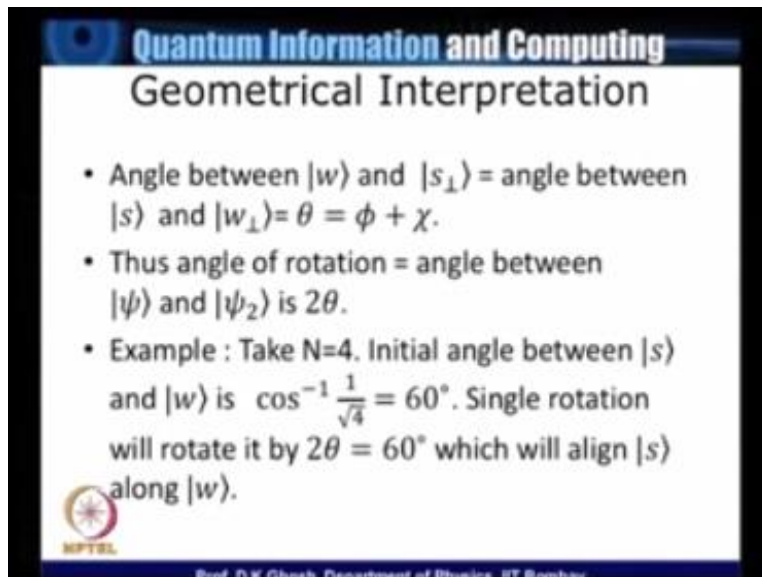
- Angle between  $w$  and  $s$  is  $\frac{\pi}{2} - \theta$
- Arbitrary state resolved along  $w$  and perpendicular to  $w$  :  $|\psi\rangle = |\psi_{\perp}\rangle + |\psi_{\parallel}\rangle$
- Application of  $R_w$  flips the sign of parallel component taking it to  $|\psi_1\rangle$
- Resolve  $|\psi_1\rangle$  along  $s$  and perpendicular to it. Application of  $R_s$  flips the sign of perpendicular component taking it to  $|\psi_2\rangle$

 NPTEL

Prof. D.V. Choudhary, Department of Physics, IIT Bombay


It will flip the sign of the component parallel to the my  $w$ , so let us look at.

(Refer Slide Time: 16:33)



**Quantum Information and Computing**  
**Geometrical Interpretation**

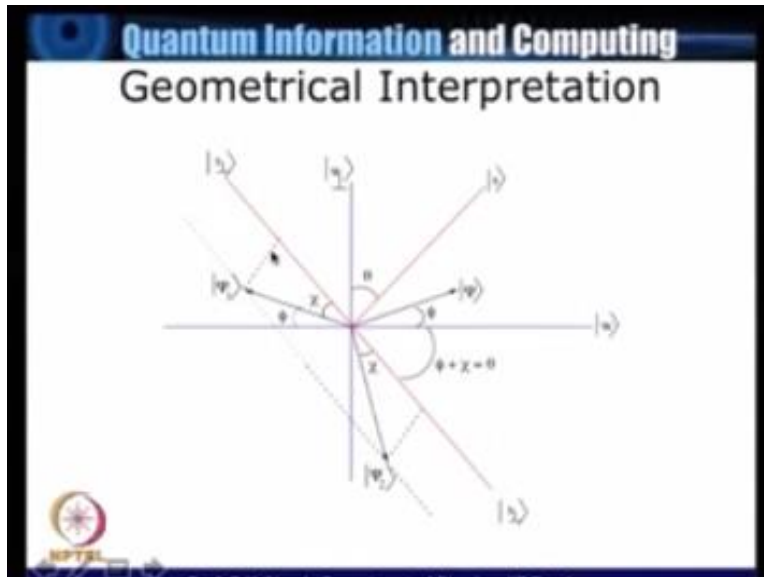
- Angle between  $|w\rangle$  and  $|s_{\perp}\rangle$  = angle between  $|s\rangle$  and  $|w_{\perp}\rangle$  =  $\theta = \phi + \chi$ .
- Thus angle of rotation = angle between  $|\psi\rangle$  and  $|\psi_2\rangle$  is  $2\theta$ .
- Example : Take  $N=4$ . Initial angle between  $|s\rangle$  and  $|w\rangle$  is  $\cos^{-1} \frac{1}{\sqrt{4}} = 60^\circ$ . Single rotation will rotate it by  $2\theta = 60^\circ$  which will align  $|s\rangle$  along  $|w\rangle$ .

 NPTEL

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

What it takes me to.

(Refer Slide Time: 16:35)

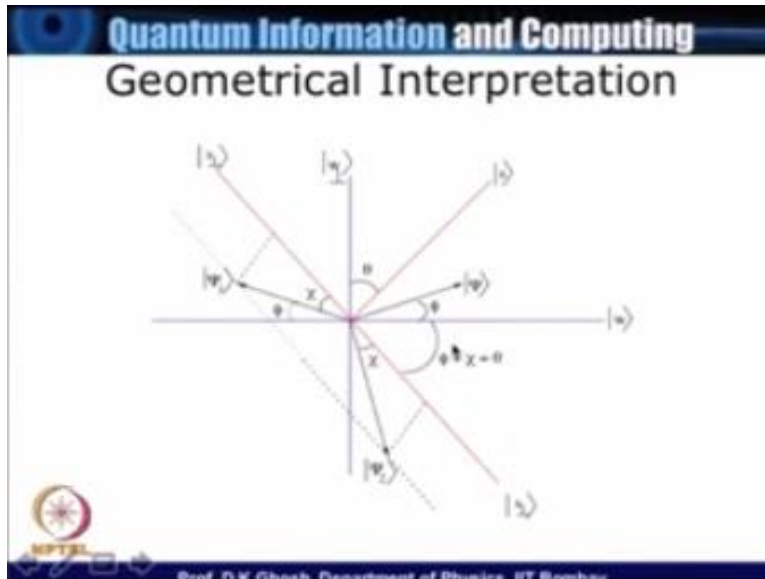


So this picture if you look at it, I have my  $\psi$  here, so the component of  $\psi$  parallel and perpendicular to  $w$  you can mentally resolve this, this will be parallel to  $W$  and this much will be perpendicular to. When I apply the  $U_W$  operator on this, we have seen that the component parallel to  $W$  will be flipped. So therefore this just turns back on this  $\psi$  this is  $\psi_1$ . So this angle  $\phi$  must be the same as identified.

So that  $\psi$  becomes  $\psi_1$  when we apply them, my second job will be to apply  $U_s$  to it, now remember what is  $U_s$  my  $U_s$  was  $2|s\rangle\langle s| - I$ , so what I do is I resolve  $\psi_1$  now into a component parallel to  $s$  which is not shown here the component perpendicular to  $S$  as mentioned there and of course you can immediately see that if I had extended this red line then I will have this much or this much we just parallel to  $S$ . Now what the  $U_s$  operator will do, will be to flip.

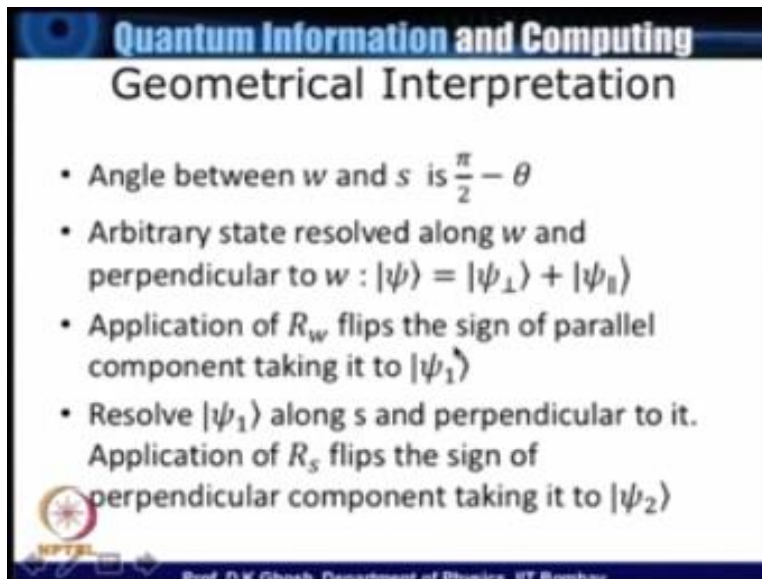


(Refer Slide Time: 18:01)




Will be to flip the component perpendicular to  $s$ , so therefore this one will now come to  $\psi_1$  this one will come to  $\psi_2$  and so therefore this is  $s$  perpendicular component has been change and these are fairly straightforward angles this angle must be equal to that angle because that is the way I have reflected it and if this angle happens to be  $\phi$  now this is  $\phi$ . Now look at the geometry here they this angle between this line and that line here so this must be equal to  $\psi + \phi$  which is here this is should be read as  $\Theta$  both of them like  $\theta$  in the picture. The slide says  $\Theta$  and so therefore this is what happens.

(Refer Slide Time: 18:57)

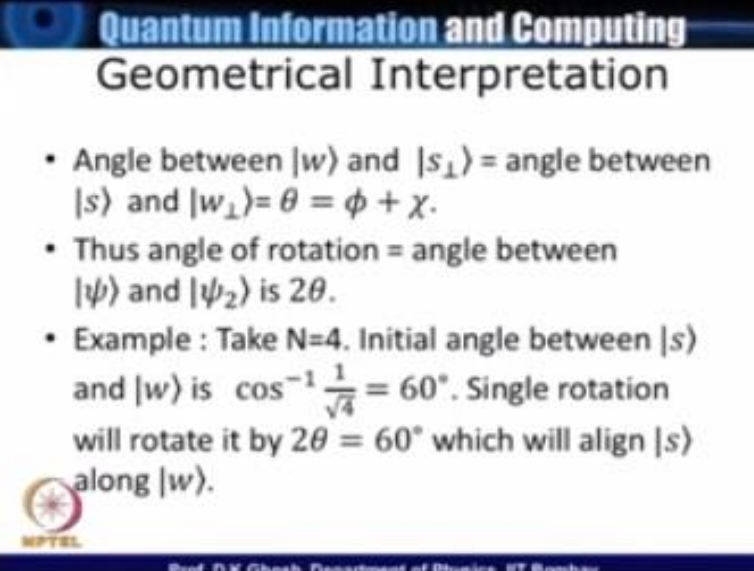


**Quantum Information and Computing**  
**Geometrical Interpretation**

- Angle between  $w$  and  $s$  is  $\frac{\pi}{2} - \theta$
- Arbitrary state resolved along  $w$  and perpendicular to  $w$  :  $|\psi\rangle = |\psi_{\perp}\rangle + |\psi_{\parallel}\rangle$
- Application of  $R_w$  flips the sign of parallel component taking it to  $|\psi_1\rangle$
- Resolve  $|\psi_1\rangle$  along  $s$  and perpendicular to it. Application of  $R_s$  flips the sign of perpendicular component taking it to  $|\psi_2\rangle$


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

(Refer Slide Time: 18:59)



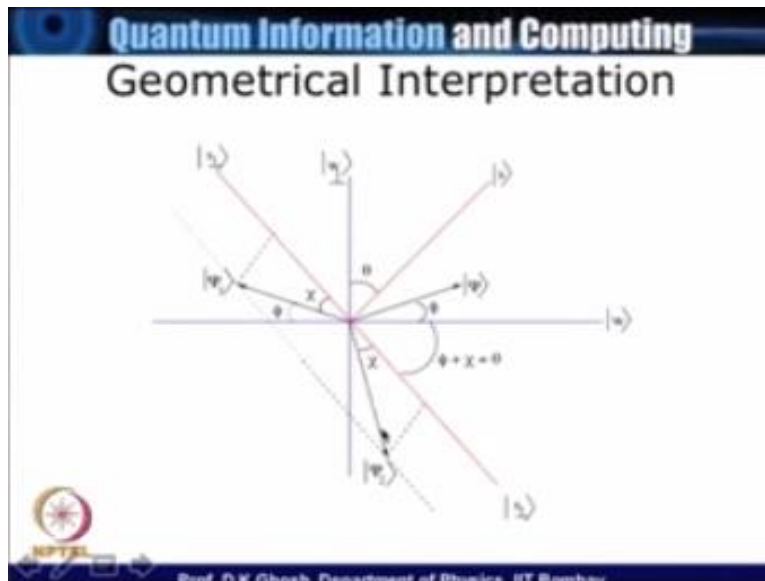
**Quantum Information and Computing**  
**Geometrical Interpretation**

- Angle between  $|w\rangle$  and  $|s_{\perp}\rangle$  = angle between  $|s\rangle$  and  $|w_{\perp}\rangle = \theta = \phi + \chi$ .
- Thus angle of rotation = angle between  $|\psi\rangle$  and  $|\psi_2\rangle$  is  $2\theta$ .
- Example : Take  $N=4$ . Initial angle between  $|s\rangle$  and  $|w\rangle$  is  $\cos^{-1} \frac{1}{\sqrt{4}} = 60^\circ$ . Single rotation will rotate it by  $2\theta = 60^\circ$  which will align  $|s\rangle$  along  $|w\rangle$ .

 NPTEL  
Prof. T.K. Ghosh, Department of Physics, IIT Bombay

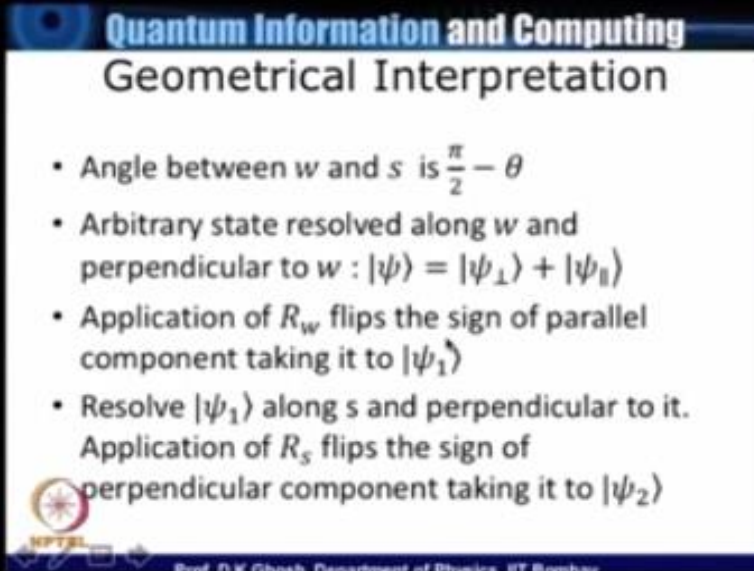
Now you can immediately check that by a trivial geometry that the angle by which you have to rotate  $\psi$  in order to get to  $\psi_2$  is twice the original at the  $\Theta$ .

(Refer Slide Time: 19:17)



There is a  $\theta$  and in order to come from this  $\psi$  to this  $\psi_2$  you have to rotate it by twice this is  $\psi + \phi + \theta$  so there is a  $\psi + \phi$  here, there is  $\psi + \phi$  here, there is  $\psi + \phi$  here so that is  $2\theta$ .

(Refer Slide Time: 19:38)



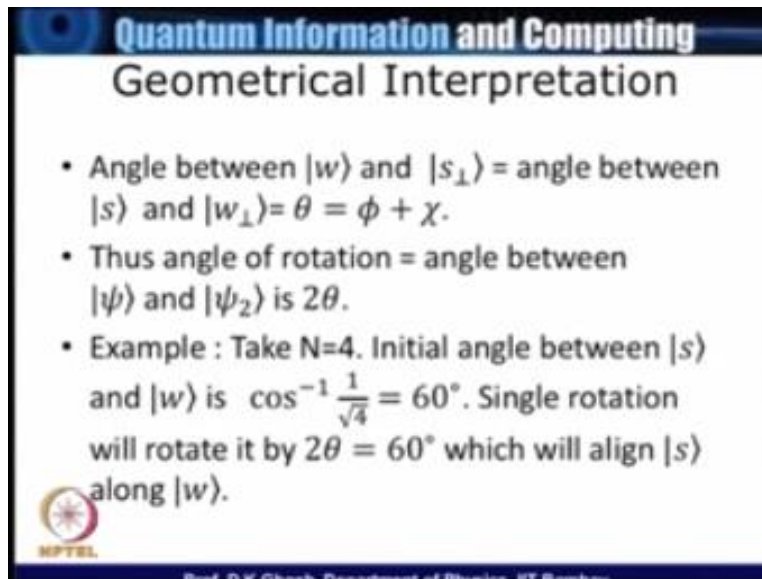
**Quantum Information and Computing**  
**Geometrical Interpretation**

- Angle between  $w$  and  $s$  is  $\frac{\pi}{2} - \theta$
- Arbitrary state resolved along  $w$  and perpendicular to  $w$  :  $|\psi\rangle = |\psi_{\perp}\rangle + |\psi_{\parallel}\rangle$
- Application of  $R_w$  flips the sign of parallel component taking it to  $|\psi_1\rangle$
- Resolve  $|\psi_1\rangle$  along  $s$  and perpendicular to it. Application of  $R_s$  flips the sign of perpendicular component taking it to  $|\psi_2\rangle$

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


But this is what would happen to an arbitrary sum, now what do you do is, now that you have realized that what Grover operator does is to acting on a state any state rotates it by  $2\Theta$  where  $\Theta$  was defined by us earlier. Then the, I can apply it on the standard state  $s$  itself, instead of arbitrary state make an application what is it doing to a standards.

(Refer Slide Time: 20:08)



**Quantum Information and Computing**  
**Geometrical Interpretation**

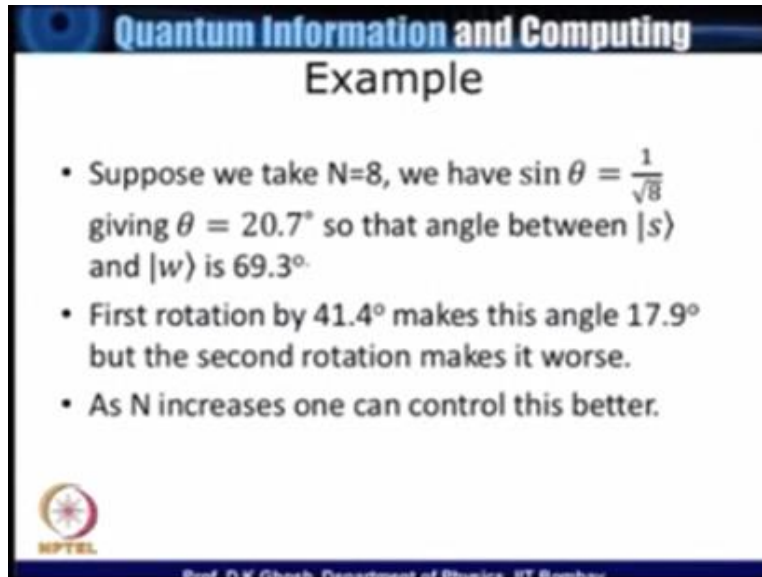
- Angle between  $|w\rangle$  and  $|s_{\perp}\rangle$  = angle between  $|s\rangle$  and  $|w_{\perp}\rangle$  =  $\theta = \phi + \chi$ .
- Thus angle of rotation = angle between  $|\psi\rangle$  and  $|\psi_2\rangle$  is  $2\theta$ .
- Example : Take  $N=4$ . Initial angle between  $|s\rangle$  and  $|w\rangle$  is  $\cos^{-1} \frac{1}{\sqrt{4}} = 60^\circ$ . Single rotation will rotate it by  $2\theta = 60^\circ$  which will align  $|s\rangle$  along  $|w\rangle$ .

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

An example will sort of explain to you what I am doing, suppose I take just four elements of course you would say four elements is so trivial that I could do it classically but that is not the point, point is that if you have four elements in principle to find the match you need on an average. Okay, I mean three will definitely make sure which is it but on the other hand let us say on an average between 2 to 3 or 1 to 3 you will take. But then in this case the angle between  $s$  and  $w$  is 60 degrees.


Now single rotation remember  $\theta$  was 30 degrees in that case because  $1/\sqrt{4}$  that is  $1/2\psi$  inverse is 30degrees. So if I now rotate it by  $2\theta$  since  $\theta$  is 30 degree  $2\theta$  is 60 degrees which will immediately align  $s$  with  $w$ . In other words a single rotation Grover rotation is good enough to align the standard state  $s$  along a marked step, you would say now this is incidentally not always true.

(Refer Slide Time: 21:22)



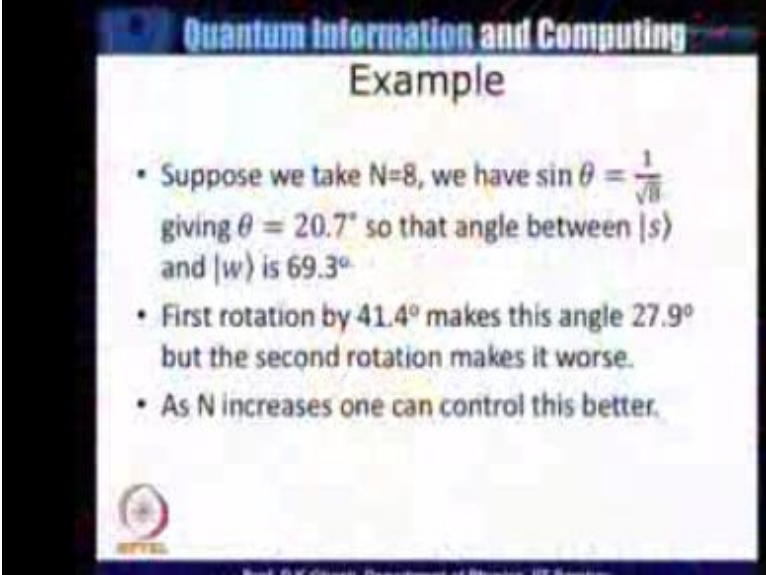
**Quantum Information and Computing**  
**Example**

- Suppose we take  $N=8$ , we have  $\sin \theta = \frac{1}{\sqrt{8}}$  giving  $\theta = 20.7^\circ$  so that angle between  $|s\rangle$  and  $|w\rangle$  is  $69.3^\circ$ .
- First rotation by  $41.4^\circ$  makes this angle  $17.9^\circ$  but the second rotation makes it worse.
- As  $N$  increases one can control this better.

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

Look at what happens if I have  $N=8$  so we have seen that in principle I would need classically about half of the such as, in this case my  $\sin\theta$  is  $1/\sqrt{8}$  and if you calculate using a calculator you will find  $\theta$  happens to be 20.7 degrees approximately 21 degrees. Now if  $\theta$  is 21 degrees they angle between  $s$  and  $w$  here is 69 degrees.

(Refer Slide Time: 21:58)



The slide is titled "Quantum Information and Computing" and "Example". It contains three bullet points:

- Suppose we take  $N=8$ , we have  $\sin \theta = \frac{1}{\sqrt{8}}$  giving  $\theta = 20.7^\circ$  so that angle between  $|s\rangle$  and  $|w\rangle$  is  $69.3^\circ$
- First rotation by  $41.4^\circ$  makes this angle  $27.9^\circ$  but the second rotation makes it worse.
- As  $N$  increases one can control this better.

And a single rotation will rotate it by 21 degrees to 42 degrees of functional it is actually 20.7 so it is 41.4 but does not matter I am just giving you approximate idea so the first rotation will make this angle 70 degrees you know in other words it has decreased a bit but if you do a second rotation to make it worse but the so therefore the idea is I must know a priori how many rotations I want if your  $n$  increases then the steps of every rotation is small and then I can control it much greater.

And I can then use much less number of rotation in order to get the  $S$  if it is not exactly aligned closely aligned with the marked I will continue with the Grover problem for the next as well as the following lectures they but let me summarize for today what is it that we have done what we have done is to start with an unstructured data base of  $n$  number of elements corresponding to each one of the elements there is a member of my basis States  $n$  cubed basis I have an Oracle which calculates the function corresponding to every member of this computational basis there is a needle.

In the haystack function which the Oracle calculates which evaluates to 1 if the input string happens to be the marked string  $W$  and is equal to 0 if it is equal it is not the much having done



that we gave a geometrical interpretation to the Grover rotation operator so what you found is this that starting with a uniform linear combination of basic and it given market state having that property application of Grover rotation would make my standard state come closer and closer to the market and this the number of attempts.

That you will require as we will see in the next lecture is of the order square root of  $n$  instead of order  $n$  which we require for a classical search you.

## **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)**

**Copyright NPTEL CDEEP IIT Bombay**