NPTEL

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING

IIT BOMBAY

CDEEP IIT BOMBAY

Quantum Infromation and Computing

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

Modul No.04

Lecture No.18

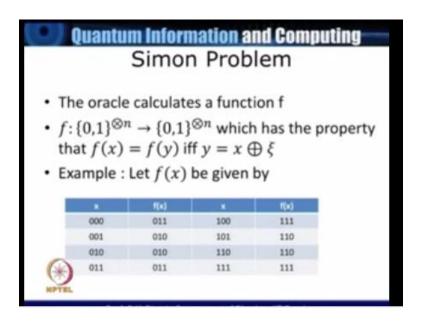
Simon Problem

In the last lecture we had introduced what we called as the Bernstein-Vazirani problem the slide sort of summaries.

(Refer Slide Time: 00:28)

What problem is so basically what happen in Bernstein Vazirani is that give in an n qubit input string x which is x_0 to x_{n-1} we need to find an unknown n qubit string a which is a_0 to n1 so that if I take the sum of the bitwise product if these two that $a_0x_0 + a_1x_1$ etc... and do it modulo 2 so this is a given single qubit output so given this single qubit output and the n qubit input string we need to find.

(Refer Slide Time: 01:07)



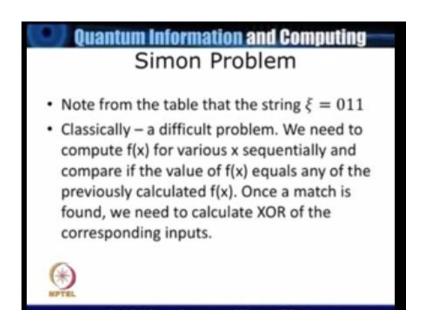
Unknown string which we called as the A what Simon problem is that just straightforward extension of the Bernstein-Vazirani problem in this case the oracle will calculate a function f will is called n qubit input to an n qubit output and it has the following property that for a pair of inputs x and y the function of the first input is equal to the function of the second input only if these two inputs are related by for examples if 1 is x the other one is y these two inputs are related by y equal to x+ that is addition modular 2 or x or ψ which is you are a unknown string and we need to find out the this unknown string ζ .

So let us look at this form as an example that I have given here so you this is a thick qubit example that we have listed here you notice here that the inputs 8 inputs are given 000001 right up to 111 and the corresponding effects are given and of course this is a frailly straight forward

thing if you look at it that f(000) happens to be 011 but f(011) also is 011 so therefore the ζ would be a string which is the bit wise x or of this 000 with 011 because if this is x and this is y the effects and f(y) or the same and likewise you can check that these are pairs are the same they have their same function and likewise here 100 as well as 111 they have the same.

Here of course it will being 3 qubits and there are only 8 entries you can even manually check what is the ζ input string that you have to find the problem becomes lot more complicated as I go along and increases the number of qubits.

(Refer Slide Time: 03:23)

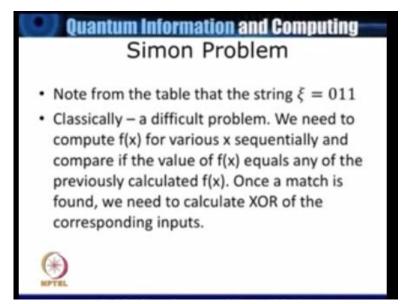


So in this particular case we had seen that the ζ was 011.

(Refer Slide Time: 03:27)

	Quantu		n Prob	nd Compu lem	IUIIY
• f:	{0,1}	a calculate $a \rightarrow \{0,1\}$ = f(y) if	\otimes^n which	has the p	roperty
	- C C C -	-/0/1	y = x d	55	
• Ex	ample :	Let $f(x)$	be given l	ру	
• Ex	ample :	Let $f(x)$	be given l	bγ f(x)	
• E>	-	,.,	be given		
۰Đ		f(x)	*	f(x)	
۰Đ	000	f(x) 011	× 100	f(s) 111	

That is fairly straight forward because you can see that these two pairs that is 000 as well as 011 they have the same value of the function so therefore your \emptyset x1 this with this then I see the string to be given by 011 now.

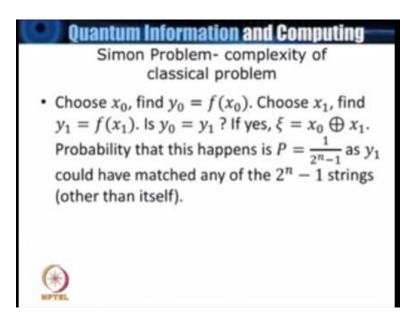


I will assume the functions to because there is always a possibility of the function being 1 to 1 in which case the unknown string is rather trivial it has to be simply 000 so we will assume that is not true but we have 2 to 1 function so let us look at this problem classically and then we will see how does it change if I consider the corresponding quantum mechanical analog so how does one proceed classically so what we will do is that I have a collection n inputs and I'm going to examine each input sequentially without replacement because once I have calculated the value I can tabulate so I think of the first input calculate what is the value of effects corresponding to this the first one goes no information other than the fact that I have x and I have an effects then I pick up next one since I am doing it sequentially.

Supposes I pick up 000001 then I calculate the value of the function again and this time I compare weather there is a match between the effects that I have calculated for the second string and that calculated for the first string now in the rare case that it is then of course I have already found out what is ζ because ζ then would be simply obtained by taking a bit wise XOR of the first input and second input.

Now of course you realize that unless one is extremely lucky this is not going to happen and particularly when my number of inputs is there in large this is very unlikely that we will find a match so quickly.

(Refer Slide Time: 05:45)



So let us look at how does one proceed little more systematically so what we will do is we will first pick up let us say x_{0} .

(Refer Slide Time: 05:54)

= f(x.) $y_1 = f(x_1)$ $y_0 = y_1$? $g = x_0 \oplus x_1$ classical probability

So when I pick up x_0 I found out let us say y_0 which is $f(x_0)$ so this does not give us any information because I need to have a starting point after that I pick up and string x_1 and I calculate the value of the function of the second string x_1 remember all of these are n qubit string and then compare is y_0 equal to y_1 now if the answer is the yes then we know that your ζ is nothing but x_0 XOR with x_1 which is each bit is done and you can find it out now what is the probability but such a thing happening.

So this is classical probability so notice that in calculating the classical probability then y_1 in principle could have matched with any of the 2^{n-1} remember that there are total in number of input is 2^n and I have picked up y_1 and I am comparing with the rest so it could have matched it is value y_1 value could have matched with the function of any of the other 2^{n-1} input and as a result my classical probability is $1/2^{n-1}$ so this have n increases is obviously n it is small probability now so let us suppose I have computed the value for let us say case strings so first case strings we have calculated.

(Refer Slide Time: 07:50)

And we have not found the match. Now if I picked up case strings and I calculate it the effects value corresponding to each one of the strip then in principle I have calculated kc2 which is simply k(k-1) divided by factorial 2 which is 2 this many strings are been checked. Now i pick up the (k+1)th string so pick up (k+1)th string and evaluate its f(x) the function and the question that I am asking is, what is the probability that the function that is y(k+1) if you like.

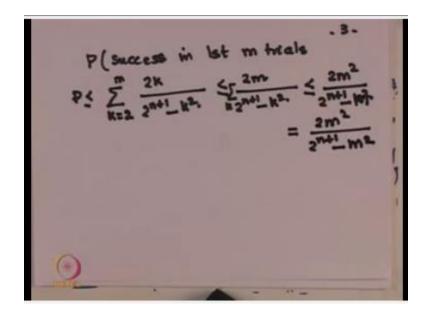
Well $(k+1)^{th}$ string I am saying so since I started from 0 it is y_k , so what is the probability that this y_k matches with one of these number sub strings that I have, now the probability of that happening is this, see remember that there were 2^{n-1} which is my number of strings that where there, so the balance number of strings that I have left with is k(k-1) / 2 and of course this probability has to be multiplied with k.

And that quantity this is a quantity which has an find out a limit and this limit I will do by simply reducing the value of the denominator so put it back say find that this will be 2k on the top divided by I have got when I multiplied this with 2 I get $2^{(n+1)}$ so let me write that one, there is a -2 since -2 is well that there is a negative number so theretofore by removing that and then I have I will come to this minus rooting.

I have go taken $-k^2 + k/s$ so I reduce that k/2 in the denominator and since n is large base number 2 is rather you know small number so I can actually neglect it, so this is probability that the $(k+1)^{th}$ string matches n of the previous strings. Now so question now is this, I have to ask supposing I have made if m attempt so far, okay. Now what is the probability of success in the first mth

Now remember this k is a number which is going 1, 2, 3,4 or 0, 1, 2, 3, 4, 0 is the first one and so therefore what is do is this, I will say that there is a possibility of its success in the first m trials.

(Refer Slide Time: 11:33)



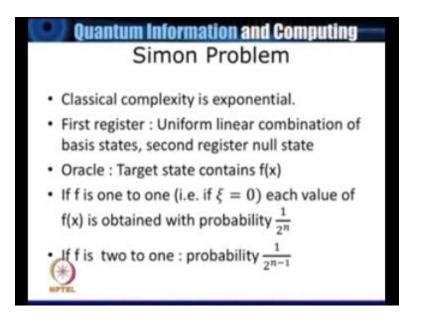
So I need to simply sum over k = 2 because I started from the second one to m 2k factorization probability is less than that $2^{(n+1)} - k^2$ so this quantity is \leq now k is the number which is running from 2 to n so supposing I replace k/m then it is decreasing the denominator and increasing the numerator so therefore this will be $\leq 2m/2^{(n+1)} - k^2$ and which is obviously less than $2m^2 / 2^{m+1} - k^2$.

So the well basically what I have done is this, okay I should put the sub back because what I have done is in each term is I have done this change replace k/m^2 and then I say the following let me write it clearly $2m^2 / 2^{(m+1)} m^2$ sop each of the term I just make it equal so naturally the probability P is less than this. So this is a reasonable estimate of the probability of success and we will say the probability of success remains less than this, now so what is the you know requirement that an algorithm is probabilistically successful, there is no particular rule regarding it but it seems like a good thing to say that in this probability is at least 3 course.

You will see half is nothing great because there is either a terms of success or not a chance of success.

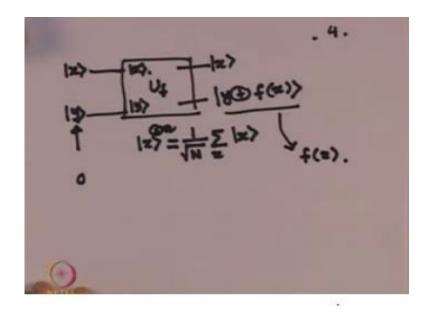
(Refer Slide Time: 13:53)

So we say if it is $2m^2 - 2^{n+1} - m^2$ happens to be $\leq \frac{3}{4}$ then there is a algorithm has a reasonable chance of success. This very trivial top work out what this tell us of m because we have 8 and square $-3m^2$ on the right hand side, so you get m to be given by the number of items that will be is given by $6/11 \ge 2^n$ is remains here this, now this you realize is an exponential complexity the complexity is exponential. Let us now go over to Simon's problem.



And try to find out the quantum equivalent of this problem, so we will find out the corresponding quantum cumuli, now as with many of our algorithms I have an oracle and in this oracle, the standard oracle like we have drawn it several times.

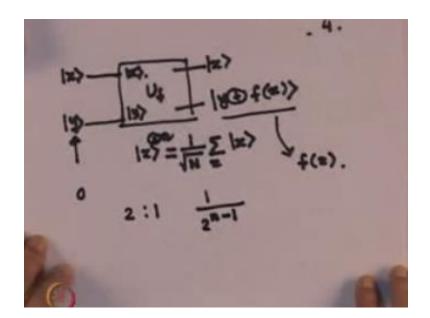
(Refer Slide Time: 15:15)



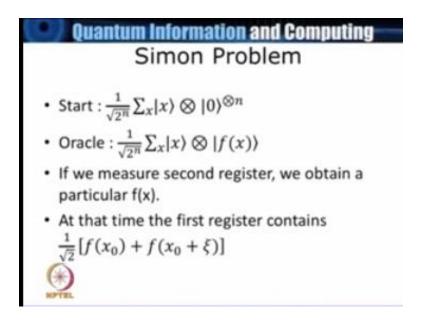
So this is your input $|x\rangle$ and this is your target bit $|y\rangle$ and we know that here directs elements are changed and here we get y+f(x) this is almost a standard thing that we can be marking out several times. Now suppose I start with a uniform linear combination of the computational basis so my $|x\rangle$ then I will use the same notation on this side $1/\sqrt{N\sum x}|x\rangle$ okay, so this is so may be just you make sure I put this and this as you know by passing a null string through a series of Hadamard gate if you can get this.

Now what I do is supposing this f I put it to be equal to 0 the null then my target register will have f(x). As I have already pointed out that if the function with 1 to 1 then my is the $\psi=0$ and if you measure the second register you will get a particular value of f(x) with probability 1^n if the function happens to be 1 to 1, and then of course we know that the string I am looking for is just a null string. But suppose my function is 2:1.

(Refer Slide Time: 17:01)

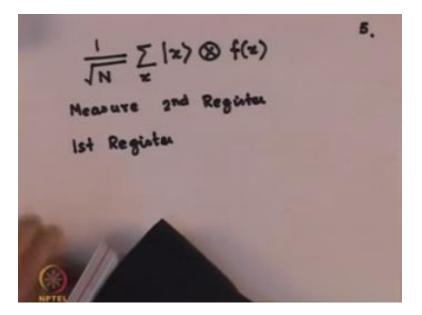


Then my probability of obtaining a particular string if I measure the first register is simply 2^{n-1} . So I do this same thing that we have been doing for several times. (Refer Slide Time: 17:17)



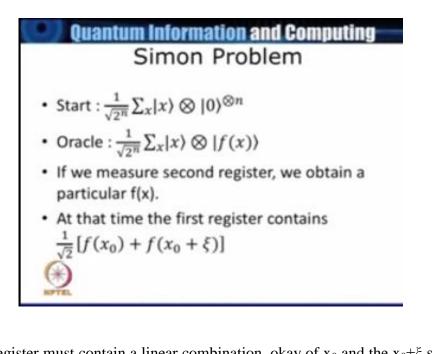
So my starting point is as I said $1/\sqrt{N}$ is just a short form for 2^n n is the number of qubits, so I start with that so after the oracle I get.

(Refer Slide Time: 17:33)



 $1/\sqrt{N} \sum x$ which is the uniform basis and of course f(x), now at this stage if I measure the second register I would get a particular value of f(x), but what does the first register contain, okay so the first register because of the fact that a particular f(x) could have arisen from two different values of the input. Let us suppose one of the inputs is executed.

(Refer Slide Time: 18:25)

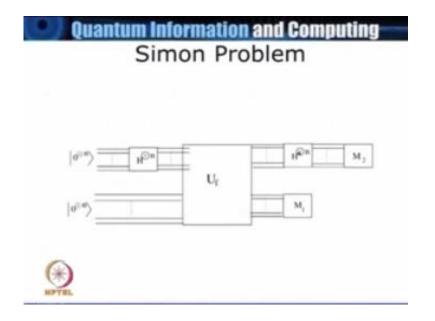


Then my first register must contain a linear combination, okay of x_0 and the $x_0+\xi$ so first register contains.

(Refer Slide Time: 18:38)

. 5. ∑ 12) ⊗ f(=) and Register Measure Ist Register contains _ [1x07 + 1x0+ \$?] -

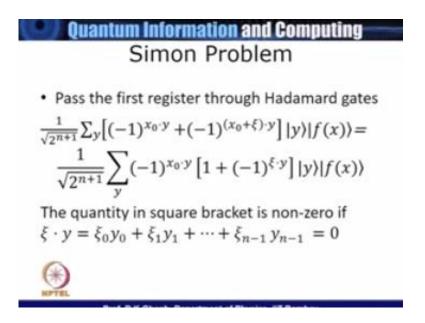
 $|x_0\rangle + |x_0 + \xi\rangle$ and of course we normalize it to $1/\sqrt{2}$, the reason is for both of these my f(x) happens to be the same and this is what we point it out and they are look at the.



Slide this is simply talking about the same thing that I have been pointing out again and again that you have a null string pass it through a series of Hadamard gate and so that here I have got a linear combination of all the computational basis and my target which I have been calling as y they are just the null string. Now when that happens we have already seen what will I get, so if I measure the second now remember it very important the order into the measurement we do your measurement.

The second measurement has to be measurement of the second line has to come first, now when you will be back one of the values of f(x) will come out with the probability $1/2^{n-1}$ as I have pointed out earlier, and at that stage when I am doing this measurement this line contains a linear combination of x_0 and $x_0+\xi$ and suppose these two things I now pass through Hadamard gate now what do I get.

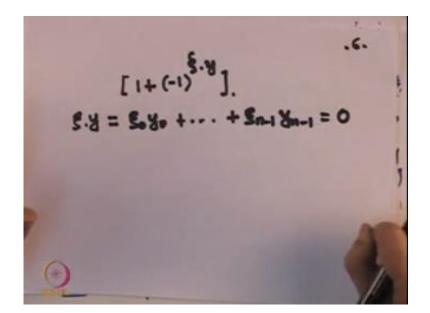
(Refer Slide Time: 20:18)



Now when I put the first register through the Hadamard gate this is the algebra that I had worked out in connection of the Bernstein-Vazirani problem so we would get is this that remember that I have got x_0 and $x_0+\xi$ passing through the Hadamard gate. Second register of course is already fixed when I pass it through the Hadamard gate because of the fact that Hadamard gate changes x to $0+(-1)^x$ times 1, so I get since one of my string is x_0 the another string is $x_0+\xi$ this is that I will get by the same logic as I have given in Bernstein-Vazirani problem.

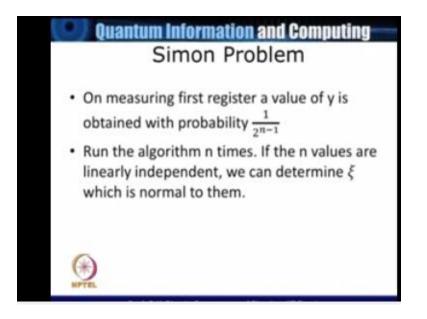
Now if you extract the $(-1)^{x_0}$, y out we get $1+(-1)^{\xi,y}$ |y> now notice the quantity in this square bracket which is there so let me write it down.

(Refer Slide Time: 21:23)



The quantity in the $[1+(-1)^{\xi,y}]$ now this quantity in the bracket will be non 0 only if ξ .y or ψ .y, okay so any making mistakes so $\xi_0y_0 + \xi_{n-1}y_{n-1}=0$. Remember these are bitwise things so therefore I either get a 0 or I get a 1, and if it is 1 it will be 1-1=0, so this is what I will get so what it means is the strings are and the string y they are perpendicular now support the n values.

(Refer Slide Time: 22:19)



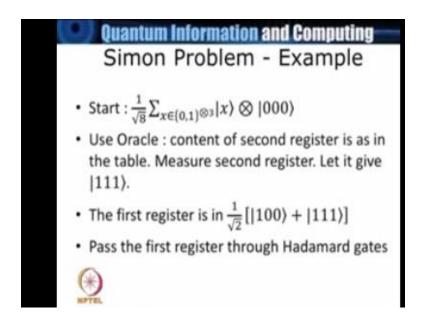
Are linearly independent then I can run the algorithm n number of times n number of times this is very important because n was simply the number of two bits not capital N which was 2n value and we can determine ϵ which is normal so let us look at.

(Refer Slide Time: 22:43)

	4(x)		η.
000	011	100	11
001	010	101	11
010	010	110	11
011	011	111	11

This by mean of an example well I have again given an example with only three K bits but it could be few and little more advent there are equal to want be more so look at this here. So here what I am going to start it is this is table I will come back to.

(Refer Slide Time: 23:02)



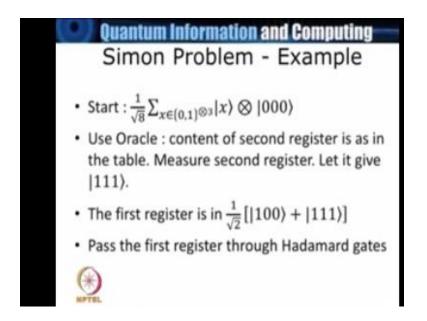
So I would start with first linear combination of all the computer technology basis so normalize some of the one over start I get one over $\sqrt{2}$ some x, x and the second register 100 I use an oracle content of the second register is given in the table I will be back and 4th and suppose.

(Refer Slide Time: 23:28)

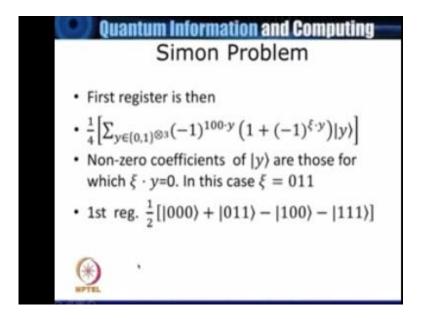
	4(x)		() ()
000	011	100	111
001	010	101	110
010	010	110	110
011	011	111	111

Look at this table of here suppose i got 111 now look at if I got 111 you could take any value and with that during point of SC then my first yeah discuss must have 100 and 111.

(Refer Slide Time: 23:44)



So my first register is contain this normalize to on over study of that group get 100+ get 111 now at this if I put the first register so Hadamard gates now if I put the first register.

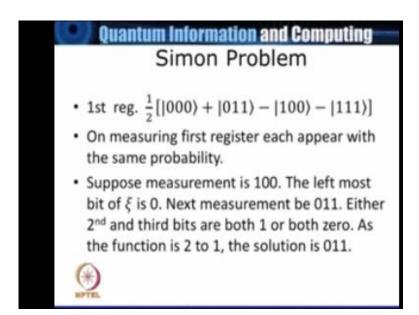


So the Hadamard get what did I get where even where I had 100 and 100+ that so therefore my one passing through the Hadamard gate I get - 1^{100} that y x 1+ - $1\varepsilon^{y}$ this is what I wrote down now in this case what I want is that this quantity here so they known here in order that my mother man something so my Non-zero coefficient of(y) are only those for it we can so in this case my first register after passing to the Hadamard see what I am doing is to do at that calculation.

Because I already know from examination that my value could be 011 so since I know that most factor I just put it back input application and find out what was back to be the content of mine prospects so my first my register would can have $\frac{1}{2}$ 000, 011- because there is a in factor there – $1^{100.y}$ so based on that I get to from this – 100 and 11 so this is actually my first register ask her two step I measured the second register after measured in the second register when the first register is in linear combination of the two inputs corresponding to which the outputs depend the same.

These two outputs when a linear combination higher past way high and since Hadamard gate act in one bit gives the 2 0 goes to 0 + 1 maybe etc so my terms that I get there are four of them and indicate so look at the slide again.

(Refer Slide Time: 26:17)



So of this is what is I have brought now I now measure the first page I would get one of this four things that I would be get one of this four things I would be get now and on measuring the first page in each one of them with complete now suppose are first measures happens to be 1 yeah sign is in no since I know ε is orthogonal to this and these are 0 here obviously I can immediately come to that the left most to become that difficult so 1 bit is it is this way that we need to one of the other bits that be fixed but in this particular example is a much similarity.

Supporting my next that the mean 011 this now in that case they I have already said that the left one bit is 0 so if got this then either the second one the third bit are = 1 or = that if it is in both them are 0 the function out then become 1 to 1 but we have already made a experiment that have

function is two bit so therefore the second one the third bit must be 1 each giving the solution 011 it at so what we have done in this lecture is to experiment the [indiscernible][00:27:58] to the case of a two, two one function and what the that supporting we in the 221 function where the pare of inputs give you the same output if the two inputs are related by $x = y + \varepsilon$ our problem is to determine what is this unknown string ε and we are seen that classically it is an exponention that algorithm.

Requiring 2n-2 number of terms but what do we found there is that n there is the number of bits but we would what we found is that with the reasonable degree of success looking Simon algorithm with only need to have attempt only are the number of cubic's number of runs and then is expect to that is reasonable answer.

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