

Theory of Computation
Prof. Kamala Krithivasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture No. # 36
NP-Complete Problems Cook's Theorem

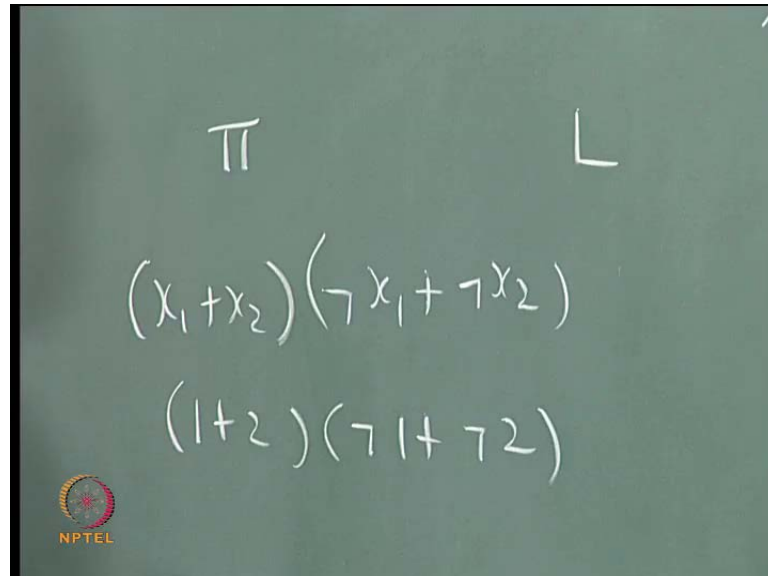
(Refer Slide Time: 00:20)



We were considering what is a problem? What is NP? NP is the class of languages accepted by non deterministic Turing machine in polynomial time. P is the class of languages accepted by deterministic Turing machine in polynomial time. Is NP equal to P is still an open problem. Just recall the connection between problems and languages for example, does M accept w is the problem and the corresponding language is denoted by strings having the form $\langle M, w \rangle$. So, every problem we can have a language representation. So, is CFG ambiguous? Given a CFG, is the language accepted by it ambiguous? A language corresponding to that will be L which will be accepted by all grammars which are ambiguous. So, you can talk about problems usually we use the symbol Π and the corresponding languages L.

So you talk about pi in NP, pi in P or L in NP, L in P both are equivalent. Now, when you look at a language representation for a problem certain things you have to consider. For example, if you have a Boolean expression is the Boolean expression satisfiable.

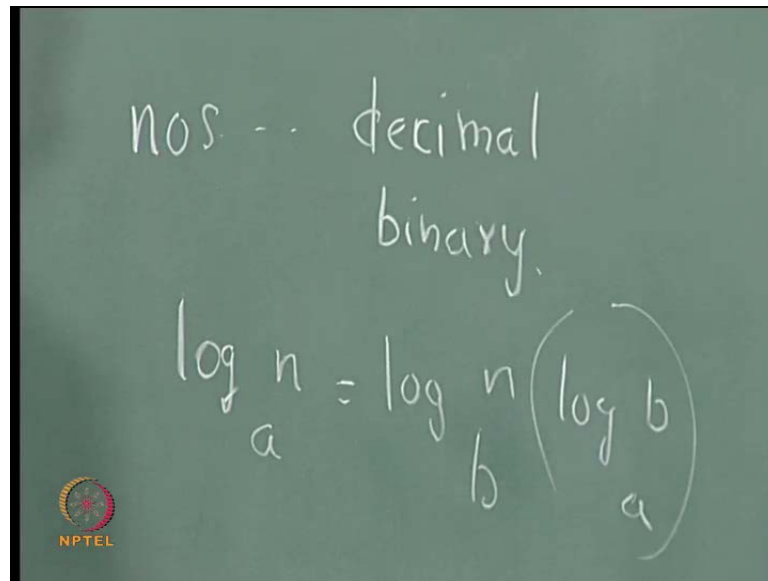
(Refer Slide Time: 02:21)



The image shows a chalkboard with the Greek letter pi (Π) on the left and the letter L on the right. Below them, the Boolean expression $(x_1 + x_2)(\neg x_1 + \neg x_2)$ is written. Underneath that, the expression is simplified to $(1 + 2)(\neg 1 + \neg 2)$. In the bottom left corner of the chalkboard, there is a small circular logo with the text "NPTEL" below it.

Then for example, $x_1 + x_2$ or $\neg x_1 + \neg x_2$ or something like that this is a Boolean expression. Now, how do you represent this as a string you can represent it as a string but, you must use x_1 and x_2 instead of writing $x_1 x_2$, you can use numbers for the variables so for example, there are two variables. So, 0 and 1 or you can use the binary representation or just decimal representation 1 and 2 you can use. So, this 1 you can write as 1 plus 2 not 1 plus not 2 something like that you can use each variable is represented as a decimal number if there are n variables up to n decimal numbers you will use.

(Refer Slide Time: 03:15)



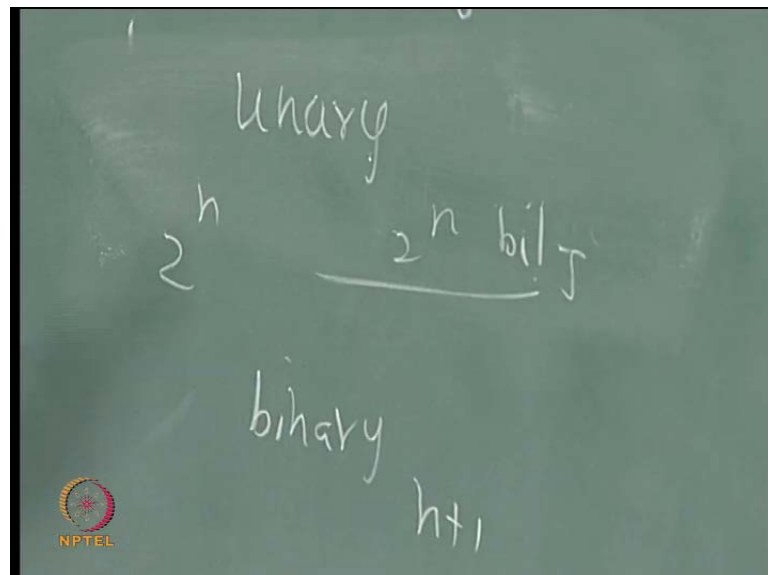
nos. -- decimal
binary.

$$\log_a n = \log_b n \left(\log_b a \right)$$

NPTEL

So, there are things which you have to be careful. Numbers you can represent as decimal or binary does not matter or any other base, because from one base the length will be only increased by a constant. Log to the base a is equal to log to the base b , log b to the base a .

(Refer Slide Time: 04:01)



unary

$$2^n \quad \underline{2^n \text{ bits}}$$

binary

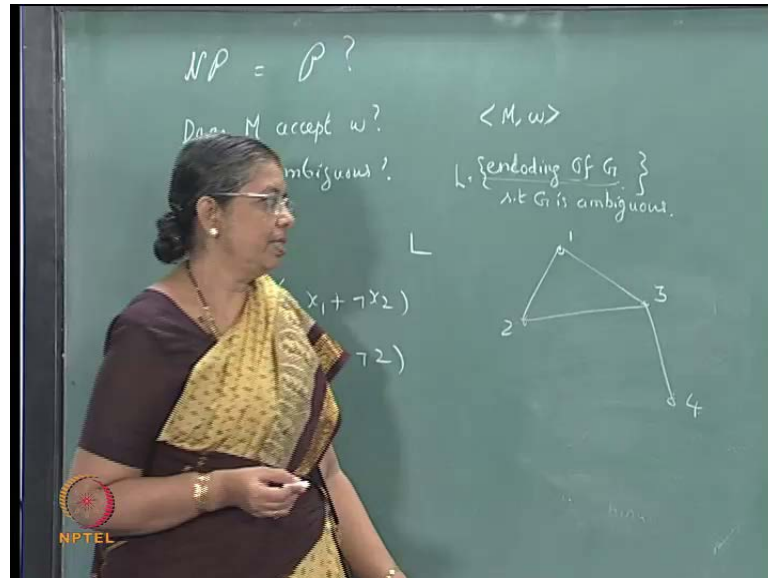
$n+1$

NPTEL

So this is a constant so, from one base to another the length will be affected only by a constant factor, but notice if you use unary representation 2^n will use 2^n bits. In binary this is in unary in binary it will use $n+1$ drastically changes.

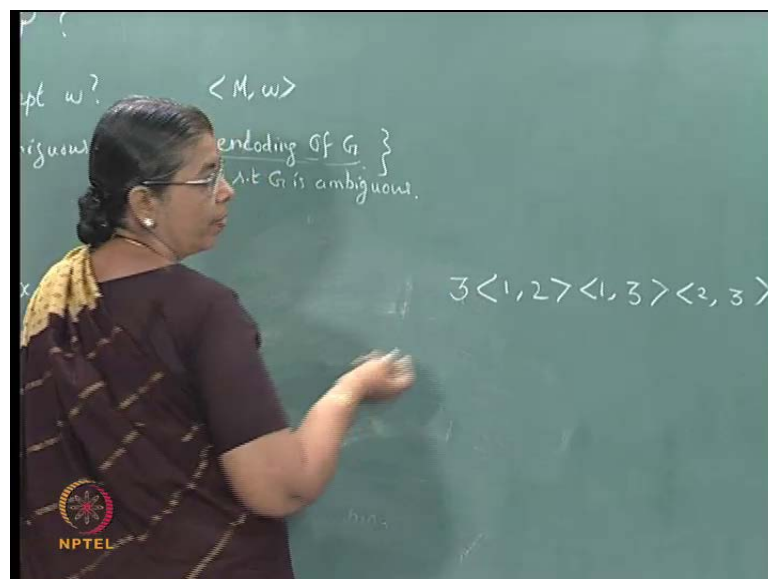
So you should not consider unary representation any other representation is, because you have to scan the whole input. If you are going to represent it unary time will be exponential increase exponential.

(Refer Slide Time: 04:44)



So, proper representation you have to choose. You can have graphs given a graph something like this with nodes 1, 2, 3, 4. The question is does it have a click of size three. A click is complete sub graph. Does this graph have a complete sub graph of size three. It has a triangle is there, but how do we represent this graph there are 4 nodes.

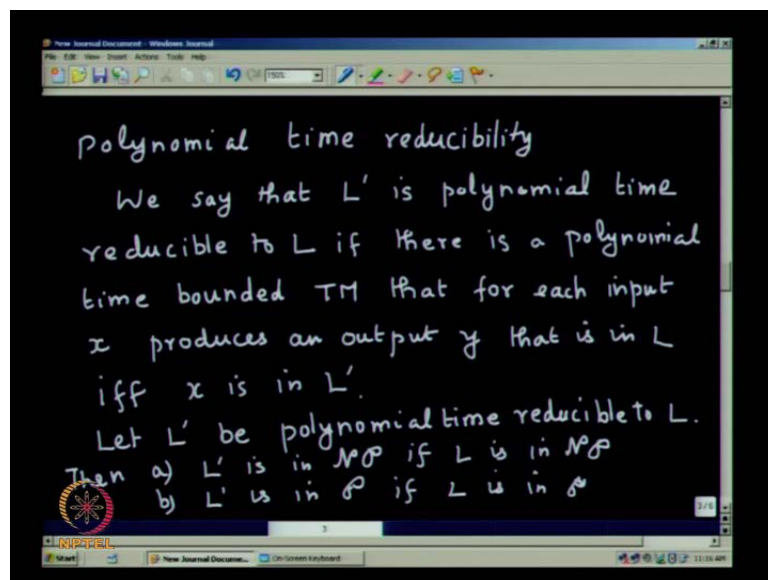
(Refer Slide Time: 05:15)



And some edges you choose some proper representation like 1,2 edges you represent 1,3,2,3, all edges starting from 1 first and all edges starting from 2 then all edges starting from 3,4 you can represent it as a string like this.

So, any problem you can represent in a proper manner as a language. Now, does it have a click of size 3 that 3 you can put in front. So, any problem proper way you can consider a language. So, you can talk about the problem being in NP being a language being in NP without any difficulty.

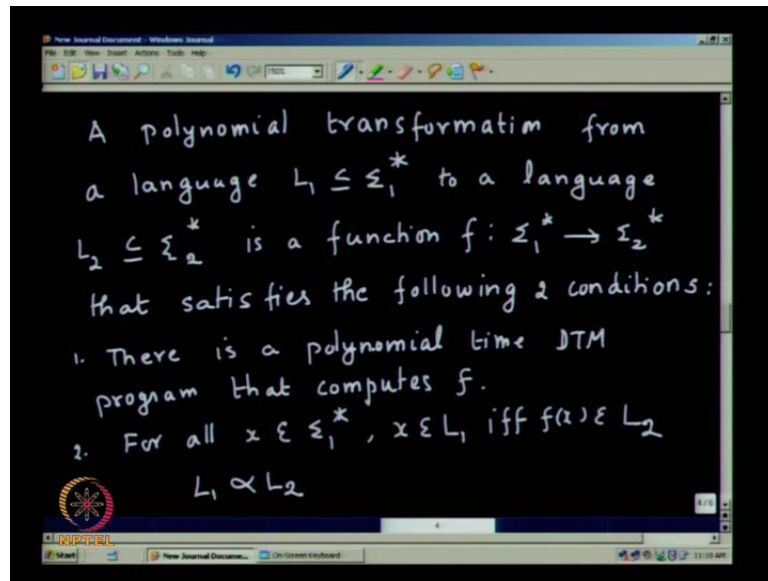
(Refer Slide Time: 06:16)



Now, let us see what is polynomial time reducibility? We say that L' is polynomial time reducible to L . If there is a polynomial time bounded Turing machine that for each input x produces an output y . That is in L , if and only if x is in L' . So, from one language it is transforming into another language that is and the transformation is done by a deterministic Turing machine in polynomial time this is called polynomial time reducible. I will read again, we say that a language L is polynomial time reducible to L' , L' is polynomial time reducible to L , if there is a polynomial time bounded Turing machine that for each input x produces an output y , that is in if and only if x is in L' .

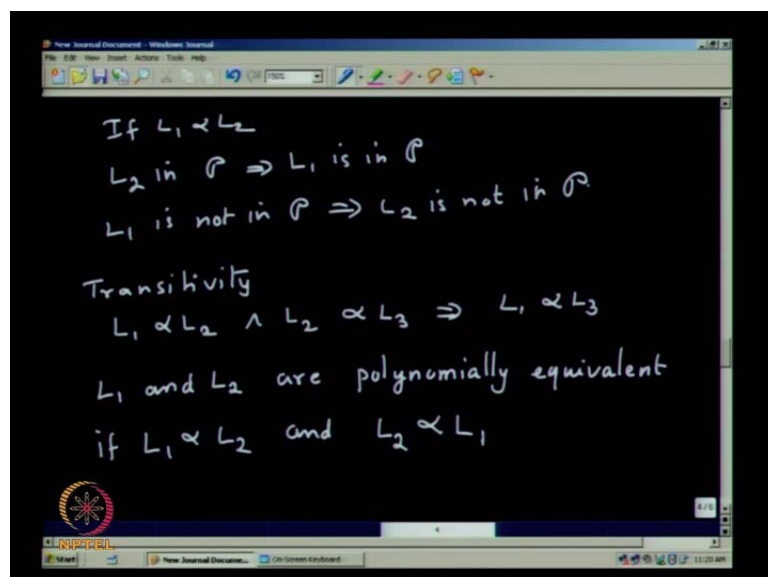
If L' is polynomial time reducible to L then, if L' is in NP then, a L' will be in NP if L is in NP and if L' is in P L is in NP if one L' is polynomial time reducible to L and if L is in NP L' will be in NP if L is in P L' will be in P slightly.

(Refer Slide Time: 07:55)



The same definition putting in a slightly different manner, same definition only is stated in a slightly different way that is all. A polynomial transformation from a language L_1 contained in Σ_1^* to a language L_2 contained in Σ_2^* is a function f . Which transforms strings in Σ_1^* to strings in Σ_2^* that satisfies the following two conditions, one there is a polynomial time deterministic Turing machine that computes the function f . That is it transforms L_1 into L_2 for all x in Σ_1^* x belongs to L_1 , if and only if f of x belongs to L_2 then, you use the symbol L_1 is reducible to L_2 , $L_1 \propto L_2$ this symbol is used.

(Refer Slide Time: 09:04)

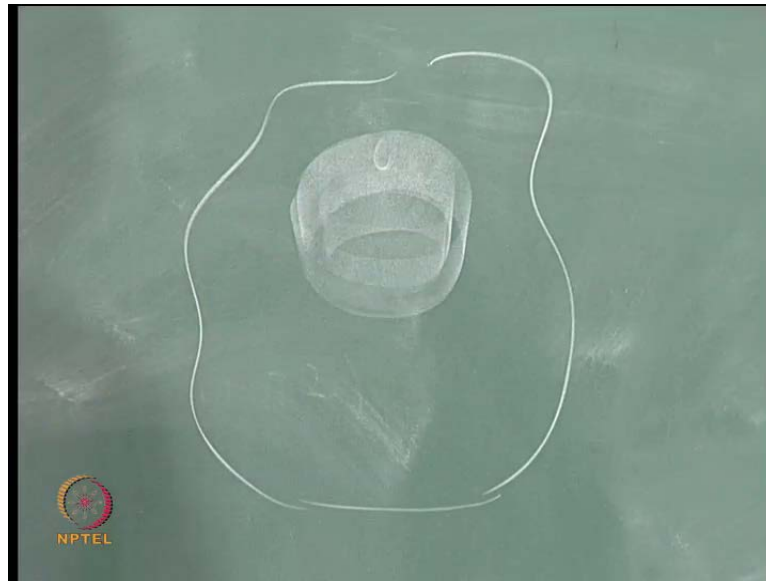


Now, having defined this let us see some more things. If L_1 is polynomial time reducible to L_2 then, if L_2 is in P then L_1 will be in P , because L_1 polynomially you can transform to L_2 and you can accept L_2 in polynomial time. If L_2 is in P that means L_2 can be accepted in polynomial deterministic Turing machine can accept it in polynomial time. L_1 can be accepted by a deterministic Turing machine in polynomial time, because from L_1 you can convert it to L_2 and then accept it L_2 polynomial time this is also a polynomial and acceptance of L_2 is also polynomial. So, L_1 can be accepted by a deterministic Turing machine in polynomial time.

Now, transitivity you can very easily see, if L_1 can be polynomially transformed to L_2 and L_2 can be polynomially transformed to L_3 then, obviously combining the one Turing machine can transform L_1 to L_2 . And that is a deterministic Turing machine working in polynomial time and another Turing machine can transform L_2 to L_3 . That is also done by a deterministic Turing machine in a polynomial time. So, combining the two you can have a Turing machine which transforms L_1 to L_3 in polynomial time. So, if L_1 is polynomial time reducible to L_2 and L_2 is polynomial time reducible to L_3 then, L_1 is polynomial time reducible to L_3 . When do you say L_1 and L_2 are polynomially equivalent, if you can reduce L_1 in polynomial time to L_2 and you can also reduce L_2 in polynomial time to L_1 .

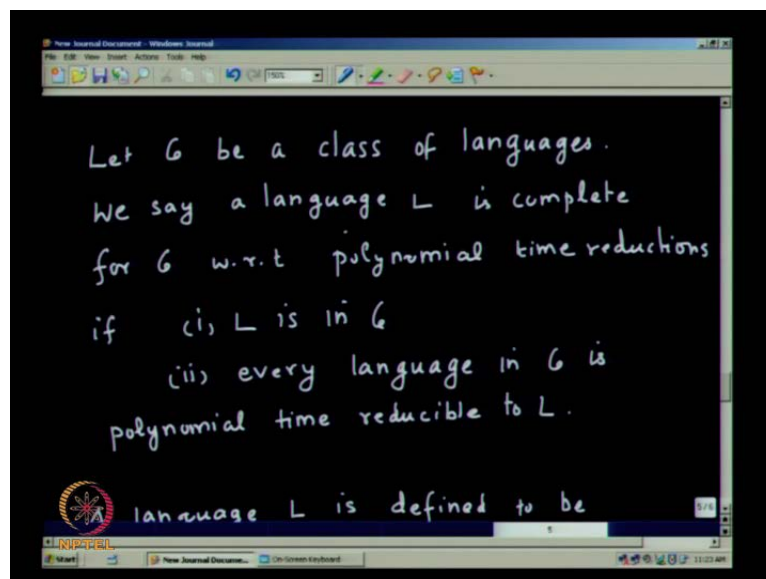
There is something else called log-space reducibility, I will not consider it now. So, this all these reductions which we are going to consider of polynomial time reduction so, with this we will proceed further. In a way what is a complete problem you have a class in that class you pick up some problems and show that they are as difficult as any other problem in that class those problems are called complete problems.

(Refer Slide Time: 11:44)



This need not be in NP we are going to study about NP by NP complete problems, but it can be other class also. Any class you take you make you find out some problems and these problems you show that they are as difficult as any other problems in that class. So, those problems are known as complete problems for that class you have also have PSPACE complete problems and so on.

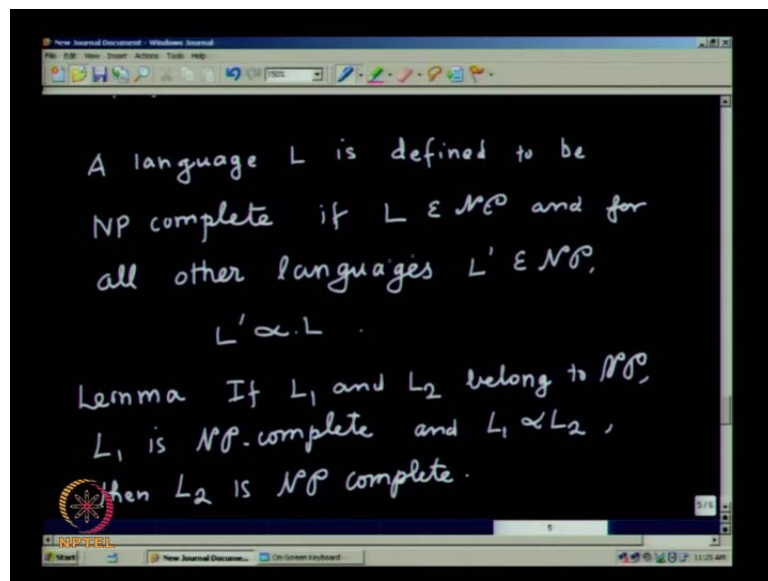
(Refer Slide Time: 12:19)



Let c be a class of languages it is a general definition then we will define for NP. What is an NP complete problem.

Let c be a class of languages we say a language L is complete for c with respect to polynomial time reductions. If L is in c and every language in c is polynomial time reducible to L . There are two conditions to be satisfied generally, we take polynomial time reducible sometimes certain cases you have to take log space reductions and so on. So, that is for some other class here generally we are taking polynomial time reductions. So, I will repeat this definition again, let c be a class of languages this is a class say and a language L is said to be complete for that class, it is as difficult as any other problem in the class.

(Refer Slide Time: 14:04)



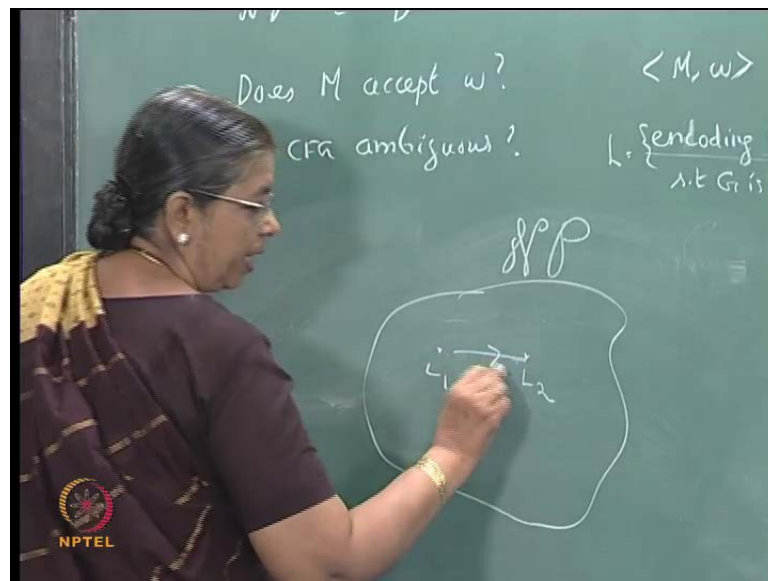
A language L is complete for c with respect to polynomial time reductions. If L is in c and every language in c is polynomial time reducible to L , two conditions have to be satisfied.

Now, let us go to the definition of NP complete in a same thing, but we will specify NP specifically. A language L is defined to be NP complete if L belongs to NP and for all other languages L' belonging to NP, L' is polynomial time reducible to L . Now, we are restricting our to one class the class NP. A language L will repeat again, because these definitions are important. A language L is defined to be NP complete, if L belongs to NP and for any other language L' belongs to NP, L' is polynomial time reducible to L .

Now, what is NP hard? There are two conditions, one is this, the second is this any other language L is polynomial time reducible to L . There are two conditions, if the first condition is not there, but only the second condition is there the language is said to be NP hard. The language means you can also talk for problems when, you talk about languages corresponding problems also you can talk.

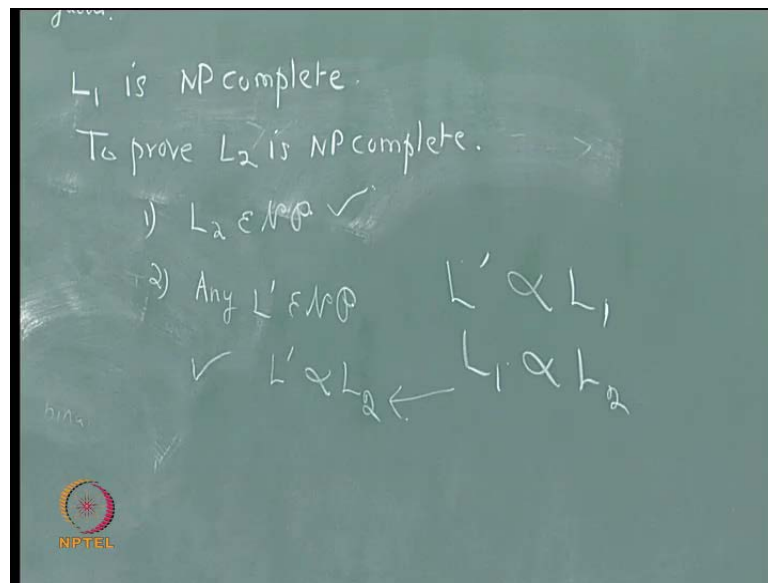
Lemma if L_1 and L_2 belong to NP and L_1 is NP complete and L_1 can be polynomially reduced to L_2 then, L_2 is NP complete.

(Refer Slide Time: 16:06)



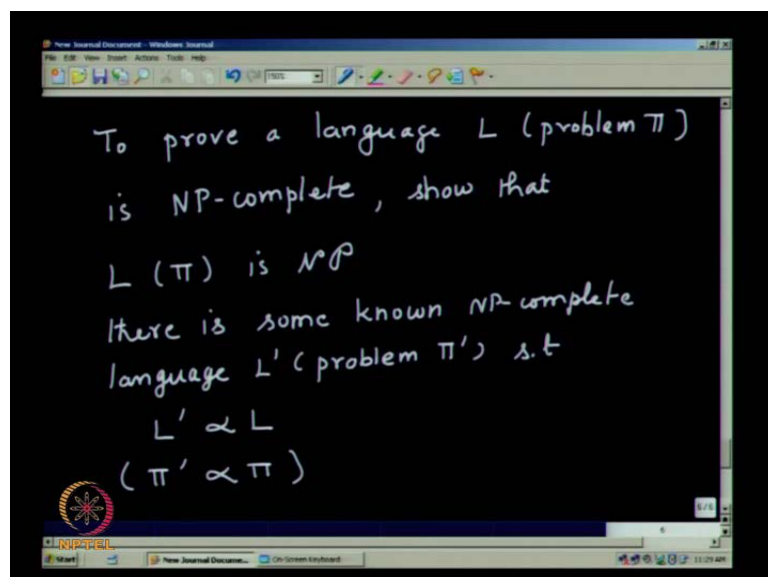
So, suppose this is the class, you are considering the class NP and this is the class L_1 and L_2 are in this L_1 is in NP complete and if you can reduce L_1 to L_2 then L_2 is also NP complete. How do you prove this? Now, I know that L_1 is NP complete I want to prove L_2 is NP complete.

(Refer Slide Time: 16:41)



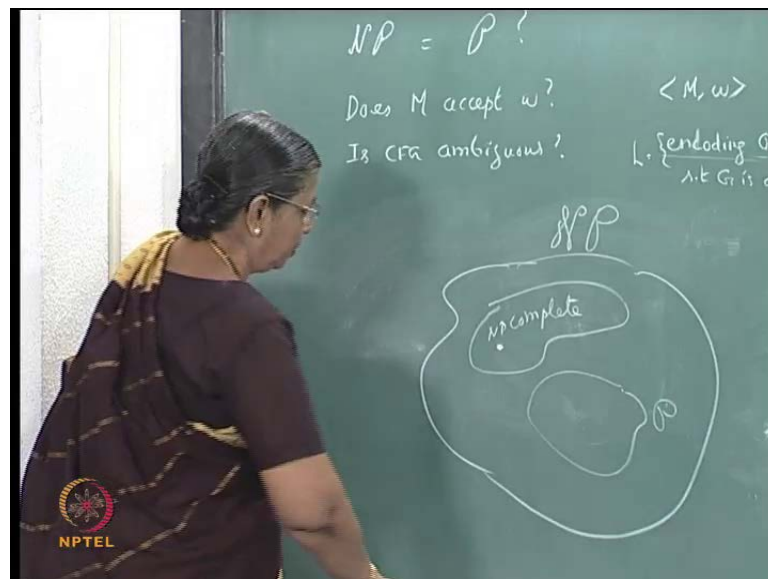
Now, there are two conditions which are to be satisfied. What are the two conditions? You have to show that L_2 belongs to NP first condition, but that is given L_1 and L_2 is in NP. So, this is satisfied, the second condition any L' belonging to NP for any L' belonging to NP, L' is polynomially transformable to L_2 this is what we have to prove, but L_1 is a NP complete, we already know L_1 is NP complete. So, L' if you take it is polynomially transformable to L_1 and it is given that L_1 is polynomially transformable to L_2 so, by transitivity you get this. So, the second condition is also satisfied.

(Refer Slide Time: 18:18)



So, that this lemma now, what you have to do you is given a language L or a problem π a new problem π then, you want to show it is NP complete. How do you show that first of all you show L is in NP or corresponding problem. We talk about π is in NP there is some known NP complete language L dash such that L dash can be reduced to L in polynomial time. You can talk about in the as problema problem π is said to be NP complete, if π is in NP and there is some known NP complete problem π dash just that π dash is polynomial reducible to π .

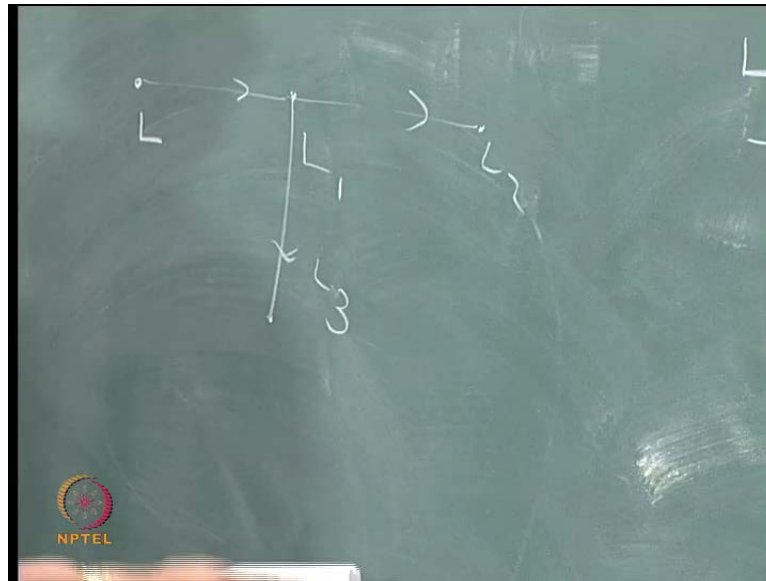
(Refer Slide Time: 19:17)



So, the class is like this NP is this class and P is like this NP complete problems current thing looks like this. Whether this is proper inclusion or not we do not know it is still an open problem.

So these problems are such that even for one problem, if you give a polynomial time algorithm deterministic polynomial time algorithm everything collapses P becomes equal to NP, even if you are able to give a solution deterministic polynomial time algorithm for one of this then, NP becomes equal to P .

(Refer Slide Time: 20:22)



Now, if you know one problem to be NP complete, other problems you can show to be NP complete by some other problem by reducing this to this. If you know one problem to be NP complete you can reduce polynomial time reduced to another new problem and new problem is NP complete. Then once you know this you can reduce it to L2 you can reduce it to L3 and so on.

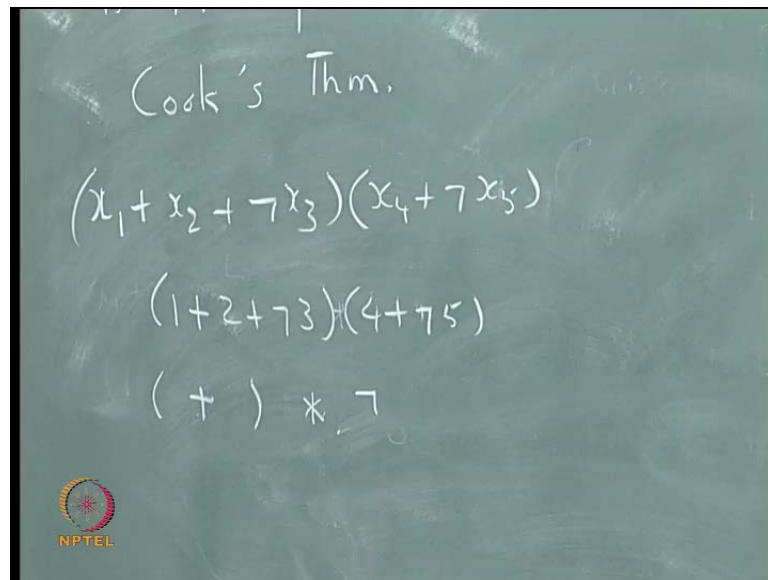
But first one problem you have to show up to be NP complete, that is the Boolean satisfiability problem.

(Refer Slide Time: 21:18)

The problem of determining whether a Boolean expression is satisfiable is NP complete.
Cook's Thm.

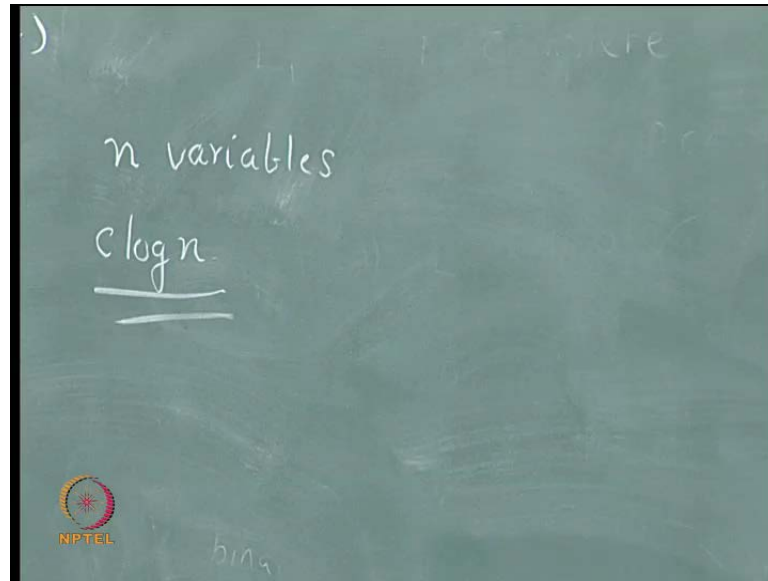
So, we will show that Boolean satisfiability is NP complete or this what you want to show. The problem of determining whether a Boolean expression is satisfiable is NP complete, this is known as Cook's theorem. So, we will consider the proof for this now so, we will consider how to prove that.

(Refer Slide Time: 22:42)



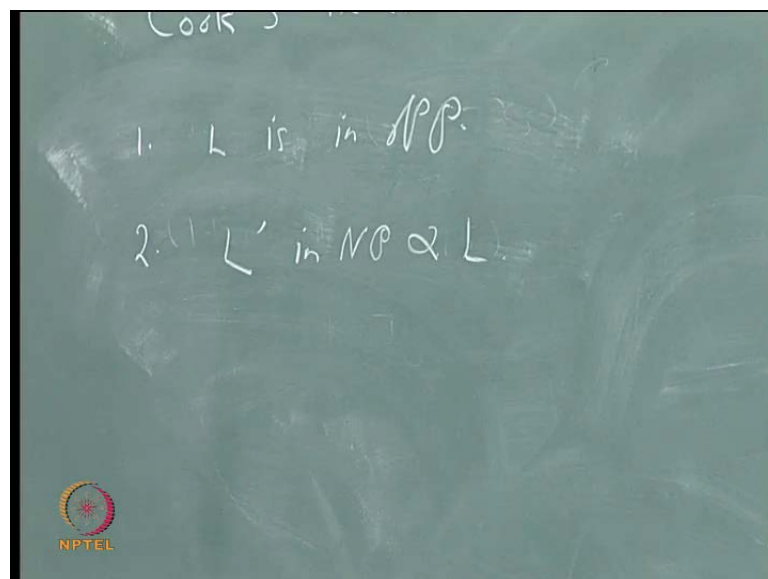
Now, in order to show that Boolean satisfiability is NP complete, first of all let us consider the representation of it. How do you represent the Boolean expression? As I told you can use something like say x_1 plus x_2 plus not x_3 into x_4 plus not x_5 something like that as 1 plus 2 plus not 3, 4 plus not 5. The symbols you use are left parentheses plus parentheses you may also use star here star is omitted for and you use star for or you use plus and then the not symbol and the variables are represented by decimal numbers.

(Refer Slide Time: 23:29)



Now, if you have variables to represent each one of them in decimal or something like that. You require something like $c \log n$ bits, but let us not bother about this factor, because ultimately when you have a polynomial time multiplying by $\log n$ is not going to affect the polynomial or the non polynomial time of it. So, let us not worry about that assume that every variable is represented as one symbol like this.

(Refer Slide Time: 24:21)

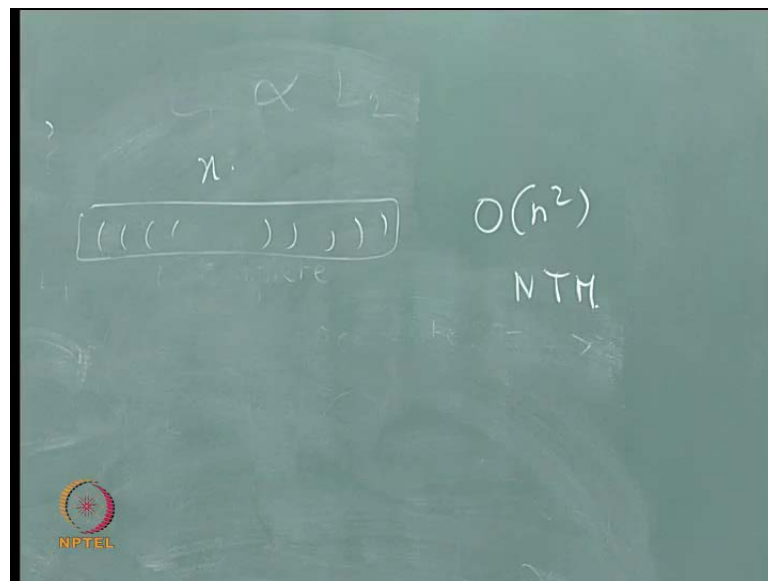


Now, there are two aspects to proving something is NP complete you have to prove that L is in NP and for any language L in NP you can transform it to L' such that L is in NP iff L' is in NP. Now, how do

you show that first this is in NP can you have a non-deterministic Turing machine which will take a Boolean expression as input and say whether it is satisfiable or not in polynomial time. You can have a non deterministic Turing machine, which will take as inputs. The given Boolean expression it will non deterministically guess an assignment, if there are n variables there are $2^{\text{power } n}$ possible assignments if you use a deterministic Turing machine one by one you have to try the $2^{\text{power } n}$ assignments.

But if you use a non deterministic Turing machine non deterministically you can guess a value for all each of the variables that is you can non deterministically guess an assignment after guessing that assignment you have to evaluate that expression. How much time it will take to evaluate that expression can it be done in polynomial time? It can be done in polynomial time, because it depends on the parsing algorithm you have for a context free grammar can generate all Boolean expressions and how much time that parsing algorithm will have and so on. Or otherwise even look at it as a given string is of length n .

(Refer Slide Time: 26:05)

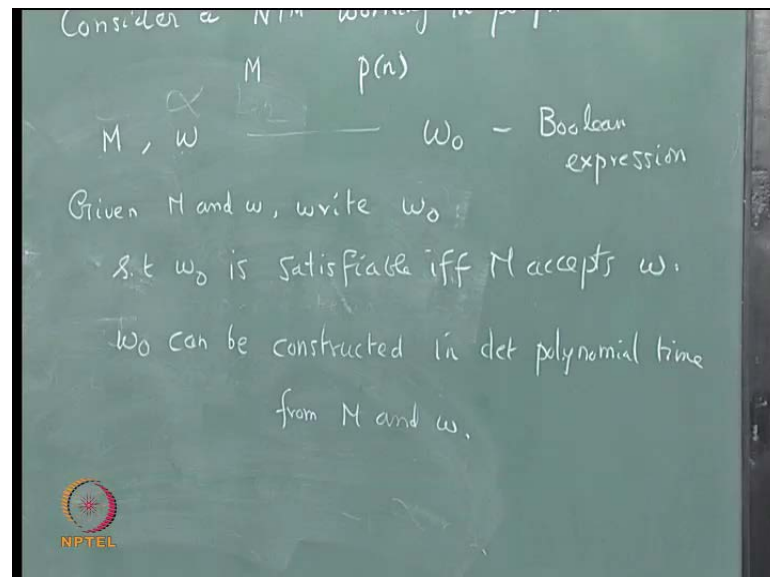


The Boolean expression we are considering in the terms of input isn't it. Input is of length n at the most you can have sort of a order n parentheses nested parentheses you can have. So, make one pass evaluate all the inner most things will be evaluated make another pass evaluate and so on.

In one pass will take order in time at the most you have to make passes. So, in order n^2 time anyway you will be able to evaluate. Once you are able to guess an assignment evaluation of the expression will take order n^2 times. Some shifting this way that way all those things will be there that does not matter our aim is whether, it is a polynomial or not the constants do not matter so much at this stage.

So, in order n^2 time you can have a non-deterministic Turing machine which will evaluate the Boolean expression and say whether it is satisfiable if it reduces to 1 it is satisfiable, if it does not reduce to 0 if it reduces to 0.

(Refer Slide Time: 27:52)

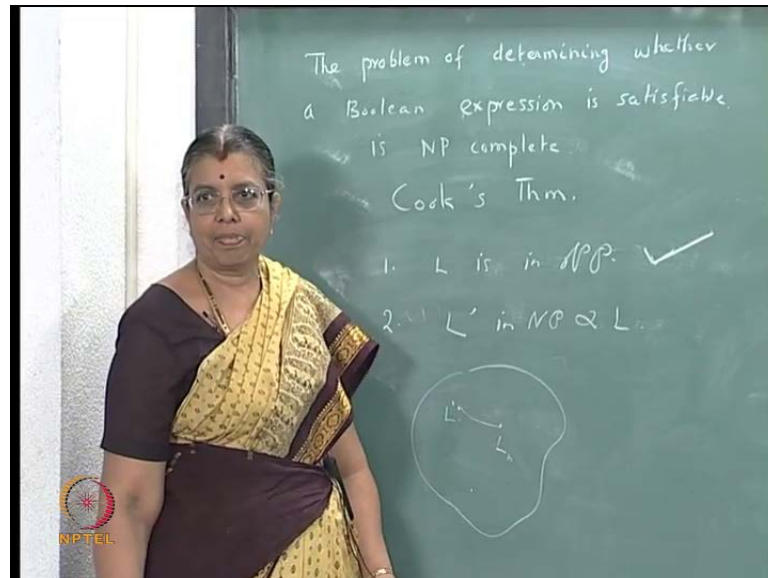


So, L is in NP this is very clear. The second is any Turing machine any non-deterministic any language L accepted by a non-deterministic Turing machine is polynomially transformable to L this is the proof. What we do is considering a non-deterministic Turing machine working in polynomial time. So, there is a Turing machine M for which the time complexity is a polynomial $p(n)$.

Now, given M and input w , M is a Turing non-deterministic Turing machine which will accept w in polynomial time accept or not. So, given M and w you construct a Boolean expression w_0 this is the Boolean expression which will be satisfied, this w_0 will be satisfied if and only if M accepts w given M and w you write an expression w_0 a Boolean expression w_0 such that w_0 is satisfiable if and only if M accepts w given M and w write w_0 form an expression w_0 such that, w_0 is satisfiable if and only if M accepts w .

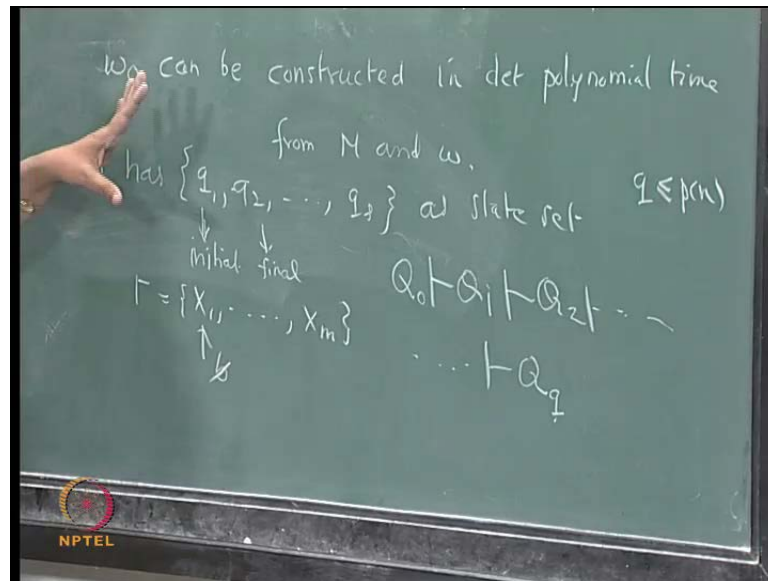
But the point is given M and w to construct w_0 it takes only polynomial amount of time there is a deterministic polynomial time algorithm which will construct w_0 given M and w . So, there is w_0 can be constructed in polynomial time from M and w . This is the main point w_0 can be constructed in deterministic polynomial time from M and w .

(Refer Slide Time: 30:59)



So, if you do that what you are showing is any L in NP this is some language a non deterministic Turing you can convert to this Boolean satisfiability. If I put it as L_0 in polynomial time. So, if you prove this then that means, we are showing that Boolean satisfiability is NP complete.

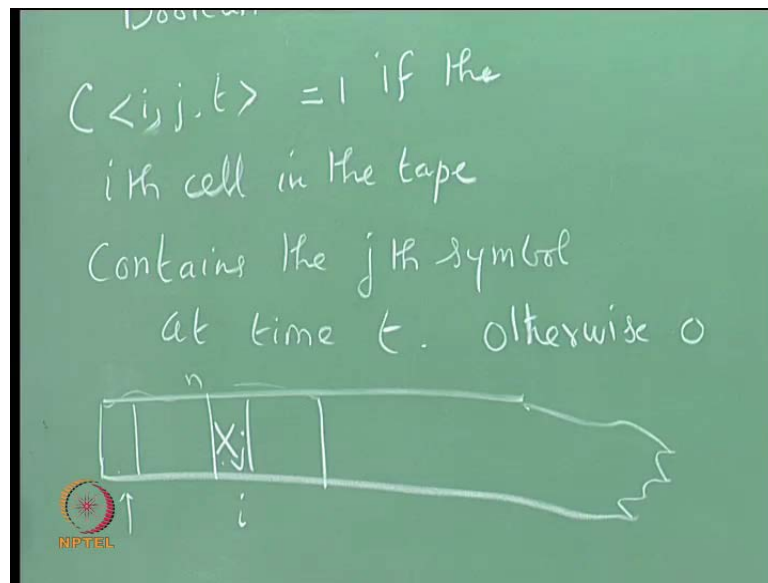
(Refer Slide Time: 31:44)



Now, we know how do we go about constructing w_0 from M and w where are some assumptions you have to make assumptions maybe I will write here itself M has states q_1 and q_2, q_3 this is the stateset of states and this the initial state and this is the final state without loss of generality you can assume that then the alphabet Γ is X_1, X_2, \dots, X_m , M symbols are there in the tape alphabet and the first symbol you can take as the blank symbol one of them you have to take as blank symbol does not matter which one.

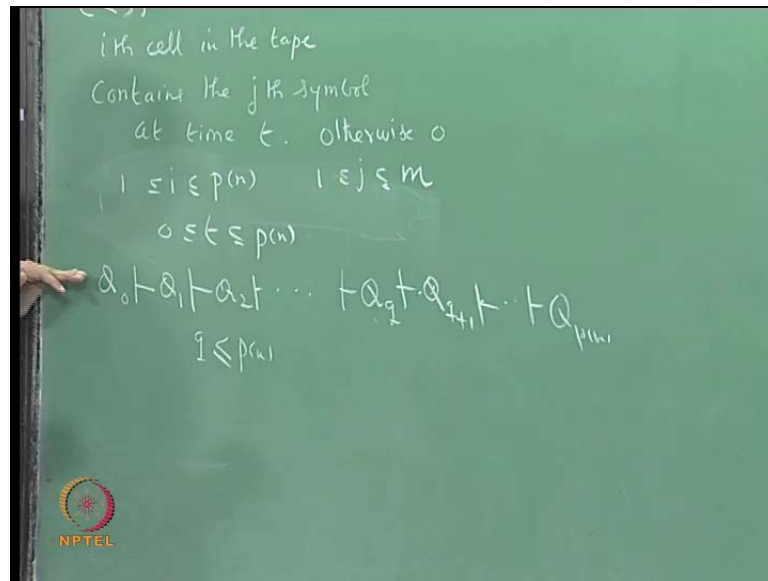
So, the initial ID of the Turing machine let us say some Q_0 then the next ID will be Next ID will be Q_2 and so on. After some after some steps at Q_q it will accept or reject. What is this Q_q is less than or equal to p of n maximum number of steps will be p of n within that step it will accept. So, q is less than or equal to p of n these are some assumptions we make one more, two more things we have to take into account that I will mention.

(Refer Slide Time: 33:42)



Now, in order to find the expression w_0 , we have to use some Boolean variables. What are those variables? You have a set of variables of the form $C_{i,j,t}$ a collection of variables of the form $C_{i,j,t}$ and what is the meaning of this variable is $C_{i,j,t}$ is equal to 1 if the ith cell in the tape contains the jth symbol at time t. The tape will be like this, the input is of a length n initially it starts you will be starting at this point initially initial state will be q_1 , if the ith cell contains the jth symbol at time t then, $C_{i,j,t}$ will be equal to 1 otherwise 0. Now, what is the maximum number of cells you will require? The machine starts here and it has to halt within $p \cdot n$ steps. So, at the most it will need up to $p \cdot n$ cells even, if it moves just forward it will be going up to the $p \cdot n$ cell.

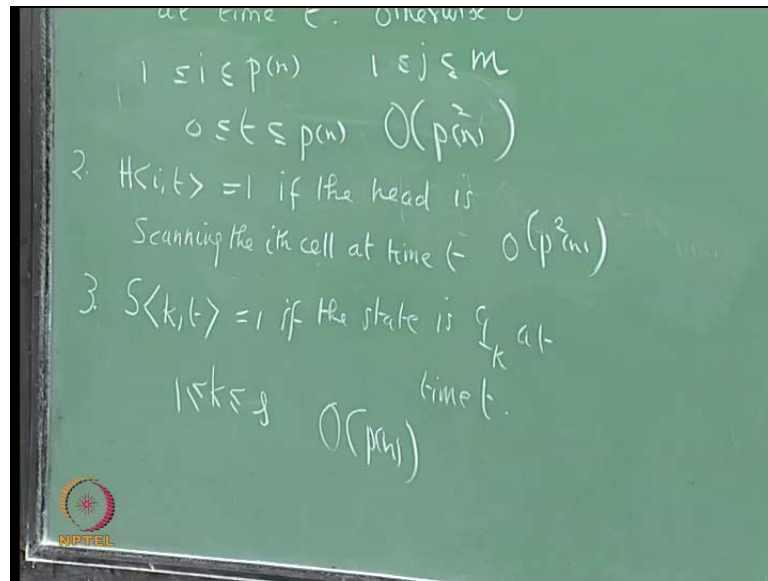
(Refer Slide Time: 35:47)



So, what is the range for i ? From the first cell it can go up to the p th cell it will not use more than that, because the time complexity is p of n . What is the range for j ? j can be anyone of the M symbols x_1, x_2, \dots, x_M , we have defined. So, it can be any one of the M symbols. So, the range of j will be 1 to M . What is the range for t ? Initially t is equal to 0. Initially you start at time t is equal to 0 and you can go up to time p of n . There is a small thing you have to note here from ID q . You go to q_1 , you go to q_2 and after some step it stops that q will be less than or equal to p of n . If it is less than p of n we want all the IDs to go up to p of n steps, we do not want to distinguish between something which is less than p of n and equal to p of n . So, the other IDs see here all these are taken identical to $Q_{p(n)}$. Next step it is also remaining the same no moves so that, we assume that everything takes p of n steps.

So how many ways such variables will be there? i range is from 1 to p of n , t ranges from 0 to p of n , j ranges from 1 to M , M is a constant, s is a constant number of states q_1, q_2, \dots, q_s , s is a constant. So, you have a order p^2 of n variables of this form.

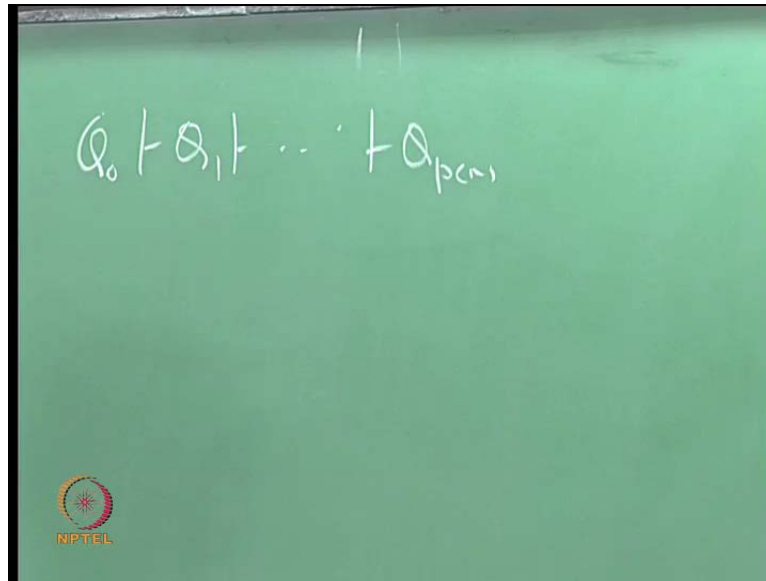
(Refer Slide Time: 38:16)



This is one set another set of variables $H_{i,t}$, $H_{i,t}$ is equal to 1 if the head is scanning the i th cell at time t . You have variables these have meaning like this $H_{i,t}$ is equal to 1 if the head is scanning the i th cell at time t . So, what is the range for i to $p(n)$ range for t 0 to $p(n)$ again order p squared n variables will be there.

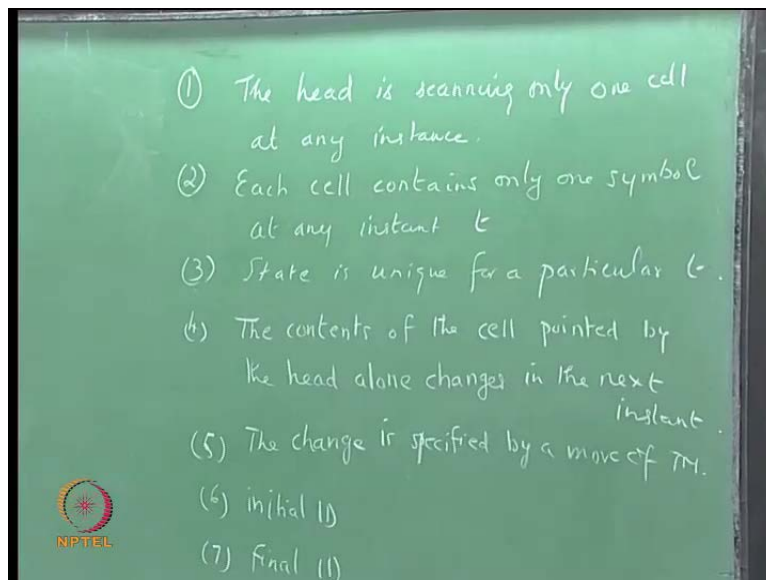
Third set of variables $S_{k,t}$ state S denoting the state this is equal to 1, if the state is q_k at time t . So, of course, will vary from 1 to S range for k is 1 to S for t , it is 0 to $p(n)$. So, here we have order of n variables now, each of this variables we assume that when you write the expression it takes only one unit or one symbol. It represent as one symbol actually since, there are order p squared n variables you have to represent them means some each one you have to represent by in a binary notation or something like that another $\log n$ factor will be there. So, we are not worried about that $\log n$ factor, because ultimately it will not affect the polynomial or the polynomial aspect of it. So, each variable is taken as one symbol for our calculation at present. Now, this expression W_0 , we have to write first given m and w you have to represent w_0 and w_0 is satisfiable if and only if it represents a sequence of moves like you know.

(Refer Slide Time: 41:16)



Which leads to acceptances q_0, q_1 etcetera up to Q . You have to write w_0 in such a way that it will become satisfiable. If and only if there is a valid sequence of ID's leading towards something.

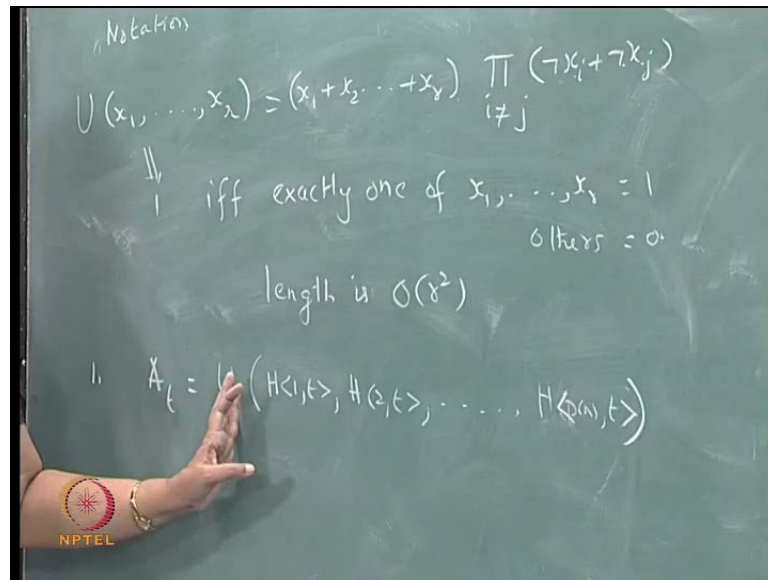
(Refer Slide Time: 41:48)



So, what are the conditions you have to look into that? These are the conditions you have to consider. The head scanning only one cell at any instance, two each cell contains only one symbol at any instant. State is unique for a particular instant t () put for a particular t there can be only one state at any instant then machine can be only in one state. The contains of

the cell pointed by the head alone changes in the next instant. The change is specified by a move of the Turing machine. You have to take care of the initial ID and you have to take care of the final ID (no audio 44:19 to 45:00).

(Refer Slide Time: 45:04)



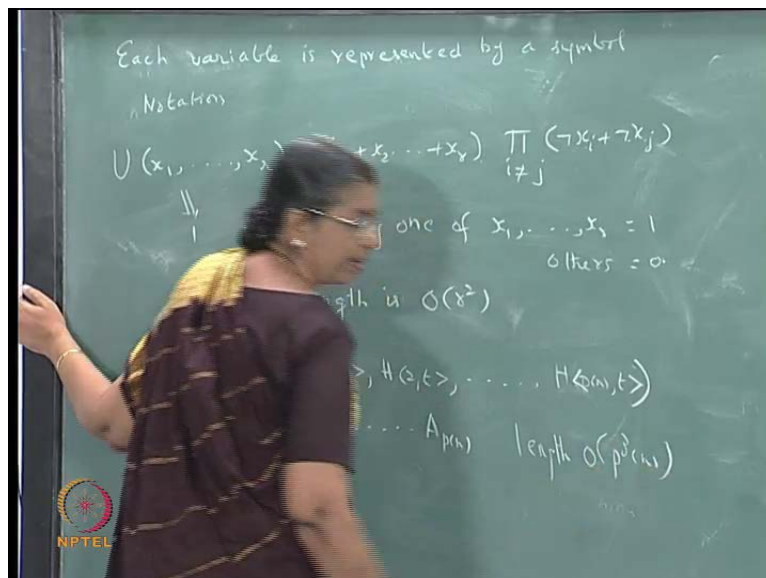
Now, we are assuming that each variable is represented by a symbol. This is an assumption we are making otherwise you have to multiply by a log n factor that is what I said. Now, let us consider for simplification we will use one more notation, an expression using Boolean variables U, x_1, x_2, \dots, x_n , this is defined like this it is $x_1 + x_2 + \dots + x_n$ and product of factors of the form $x_i + \neg x_j$ is 0 equal to j . This is U, x_1, x_2, \dots, x_n , is a Boolean expression. Which is of the form $x_1 + x_2 + \dots + x_n$ into product of factors of the form $x_i + \neg x_j$ where i is not equal to j you have all of them. So, for example, U, x_1, x_2, x_3 , will be $x_1 + x_2 + x_3 + (x_1 + \neg x_2)(x_1 + \neg x_3)(x_2 + \neg x_1)(x_2 + \neg x_3)(x_3 + \neg x_1)(x_3 + \neg x_2)$. It will be like that for n you can write like that.

Now, when we will this take the value one is true. When exactly one of them is one and all the others are 0. When exactly one of them is one it will take the value of one if none of them are one it will take the value 0, if two of them are one. So, it will take the value 0. Why if none of them is one all are 0 means this factor will be 0. So, the total expression will be 0 if two of them are ones then there will be one factor if i, j are one there will be one factor $x_i + \neg x_j$ that will take the value 0. So, the expression will be 0. So, this is equal to 1 if and only if exactly one of x_1, x_2, \dots, x_n , is equal to 1 otherwise equal to 0. Now, what

can you say about the length of this expression there are r variables what can you say about the length of this expression this will be r . How many factors will be there. n minus for one. If you take x_1 there will be a factor with x_2, x_3, \dots, x_r, r minus 1 factor then, if you take x_2 there will be factors with x_3, x_4, \dots etcetera. So, that is r minus 2 and so on. Up to one, how many factors like that it will be there 1 to r minus 1 that is r into r minus 1 by 2 factors. How many symbols it will take 1, 2, 3, 4, 5, 6, 7, some constant number. So, it will be something like r into r minus 1 by 2 into some constant k plus this one is r into r then some other constant. So, anyway the length will be order r square the length is length this order r square this is important. So, we will make use of this notation for writing the expression of those conditions. So, there are seven conditions which we have specified one by one we will write expression for them.

So, what is the first condition; The first condition is, the head is scanning only one cell at a time. So, At is the expression at time t the head is scanning only one cell. So, this can be the condition, we can write like this U of $H_1 t, H_2 t, \dots, h_p n$. What does that mean the U is this expression. So, head will be scanning only one cell at a time. So, only one of the variables has to be one rest of them has to be 0 then only this will become one.

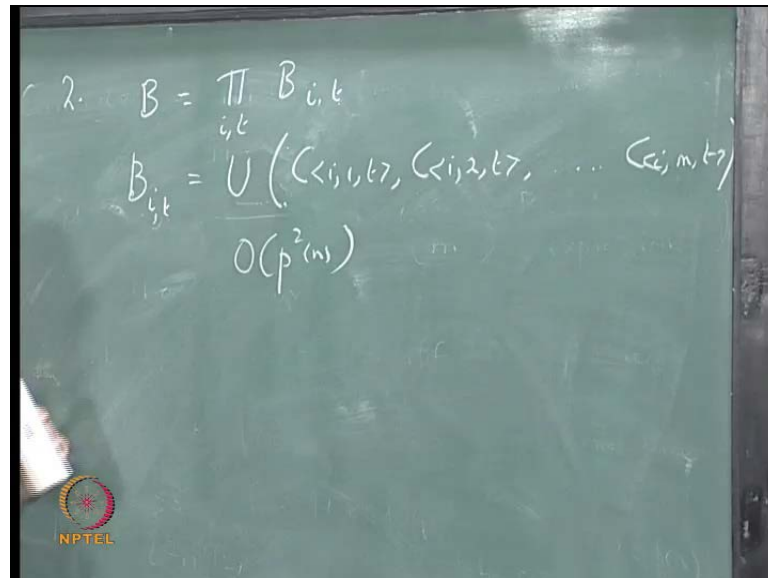
(Refer Slide Time: 51:30)



So, the whole expression is this should hold for instance t is equal to 0, 1, 2, up to $p \cdot n$. So, the expression A which satisfies the (U) condition is $A_0, A_1, A_2, \dots, A_{p \cdot n}$. Now, what can you say about the length of A , each A_t is order p squared n it here, if it is r its r

squared here it is $p \cdot n$. So, it is order p squared and you have $p \cdot n$ of them. So, the length will be length of such an expression will be order p cubed.

(Refer Slide Time: 52:34)



The second condition is each cell contains only one symbol at a time. So, you write it as $\prod_{i,t} B_{i,t}$. The expression for that will be $B_{i,t}$ is at time t only one symbol will be there that is this is U of $C_{i,1,t}$ or $C_{i,2,t}$, $C_{i,m,t}$. The i th cell can contain the first symbol or the second symbol or the m th symbol. Where the product is over i and t . Each cell can contain only one symbol at a time. So, at time instance t the i th cell can contain only symbol one or symbol two or symbol m . So, this expression is equal to 1 only one of them is one and the others are 0 isn't it the way you have written U . So, this expression make sure that at any instance each cell contains only one symbol and what can you say about the length of B , B is the expression this is a product over I and t .

Where I will range from one to $p \cdot n$, t will range from 0 to $p \cdot n$. The length of this will be order m squared, because you have m variables here. So, the total this is a constant m square is a constant this is constant, but this I ranges from 1 to $p \cdot n$, t ranges from 0 to $p \cdot n$. So, the whole length will be order p squared n .

(Refer Slide Time: 55:24)

$$3. S_t = U(S_{\langle 1,t \rangle}, S_{\langle 2,t \rangle}, \dots, S_{\langle p,t \rangle})$$

$$C = S_0 S_1 \dots S_{p(n)} \quad O(p^n)$$

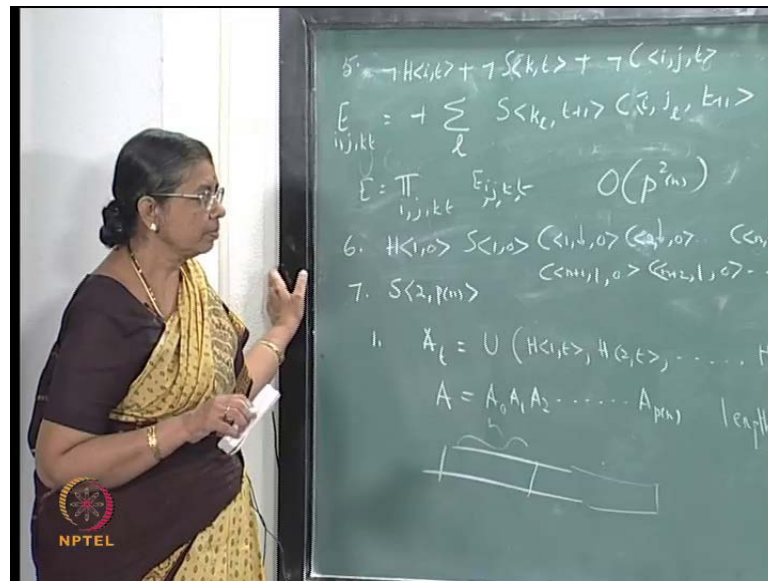
$$4. D = \prod_{i,j,t} (C_{\langle i,j,t \rangle} \equiv C_{\langle i,j,t+1 \rangle} + H(i,t))$$

$$O(p^2 n)$$

Then, the third condition. What is the third condition? The state is unique at any instance. So, S_1, S_2, \dots, S_t totally there are S states. Only one of them I can put S_t is equal to this U of this, U of this and expression C is $S_0, S_1, \dots, S_{p(n)}$ that means only one of them will be 1 others will be 0 for a particular t and you have to consider t varying from 0 to $p(n)$. The length of this is order S squared, but S is a constant right the length of this a constant but, this varies over from 0 to $p(n)$. So, the total length of this expression will be order p of n .

Then four fourth condition is only the cells scanned by the head will change the contents of the cells, scanned by the head will be changed the rest of them will remain as there isn't it. If you are if the head is scanning this one it will change this symbol, but rest of the portion it will be the same. So, that is $C_{i,j,t}$ is the same as $C_{i,j,t+1}$ or either the head is scanning the i th cell if head is not scanning the i th cell the contents of the cell i is the same at time t and the time $t+1$. This is the expression, but you have to take the product over j again j will be 1 to m i will vary from 0 to 1 to $p(n)$ t from 0 to $p(n)$ this expression will also be of length p square n .

(Refer Slide Time: 59:00)



The fifth condition is the next move is specified this is the expression D. The expression E satisfies the 5th condition. What is the 5th condition? The next move is specified by the moves of the Turing machine. So, either the head is not scanning the i th cell at time t or the state is not k at time t or the i th cell is not containing the j th symbol at time t . I want to specify the move for the case when the state is k and the i th cell head is scanning the i th cell and the contains is x_j . So, if one of this is violated, but if the head is scanning the i th cell the state is k and the i th cell contains j symbol what will be the next situation? Next situation will be state will be some k plus 1 state will change to some other state that is represented by k and head is C i th cell will contain some other symbol at time t plus 1 and the head will go to I minus 1 or I plus 1 isn't.

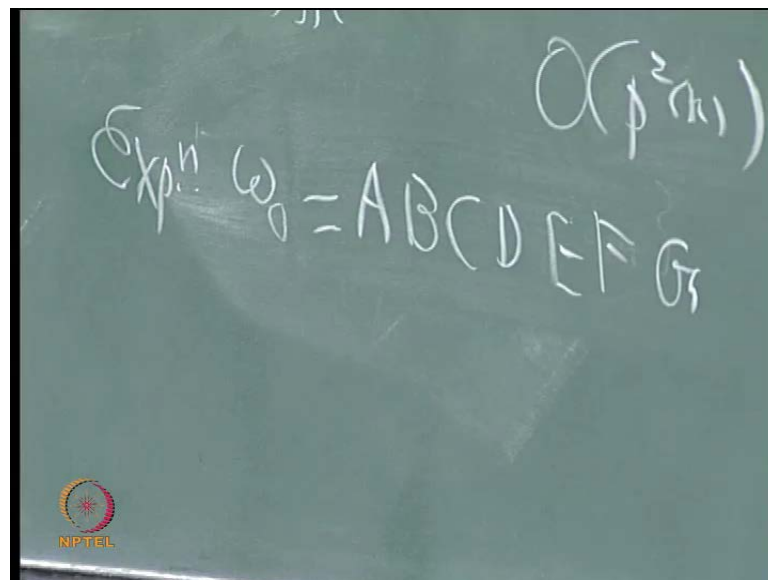
So, H i t plus 1 this will be I minus 1, if the move is left it is I plus, if the move is right actually it is a nondeterministic Turing machine. What we are considering is a nondeterministic Turing. So, next move is not unique there will be some possible choice one choice is klj there may be another choices. So, consider all possible choices write them down. So, that is why we are using sigma here not pi sigma this or this or this one of the moves it will select. So, if the head is scanning the i th cell and i th cell contains the symbol j and the state is k the next move will be given by one of them that will be possible choice each one you write otherwise, if it is not followed means head is not scanning the i th cell or the state is not k or the i th cell does not contain the j th symbol.

So, this expression tells you about the next move of the from one ID. How do you go to the next ID that is specified by this expression that is given by actually this is $E I j k t$ is equal to this and you take the product $e i I, j$, again j will vary from 1 to m k will vary from 1 to $S I$ ranges from 1 to p n t from 0 to p n . So, the length of the expression will be order p square n .

The sixth condition is initial ID. What is a initial ID? H10 time 0 the first symbol will be (Q) state is 1 $S10$ and first you $C10, c20, cn0$, this will get the input is $A1, A2$ depending upon that you will give the value here. Whichever symbol is there in the input you give then, what can you say about cn plus 10 c n plus, 20 up to cp $n0$ initially, you have the input in the first n cells and the rest cells are blank and blank is x 1 we have taken so, this will be 1 as a notation.

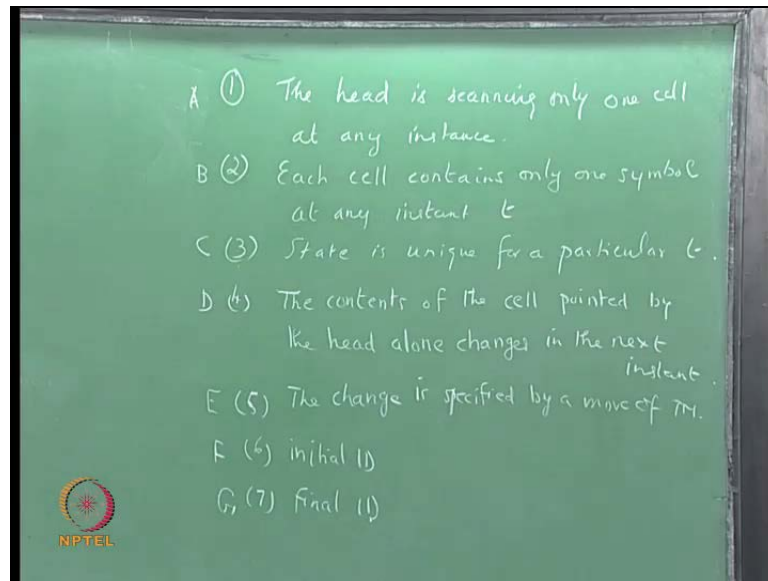
We have taken the blank to be x 1 then the final ID is just the state become two at time q 1 is taken as initial state q 2 is taken as the final state. Seventh condition is given by this expression these are all fixed length this is of length n this is only 1 **I am sorry** this is of length $P N$.

(Refer Slide Time: 1:05:11)



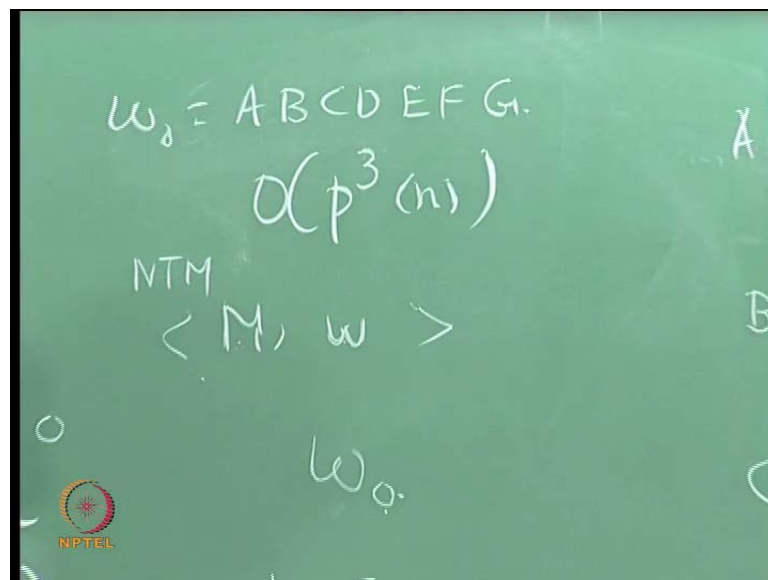
So, totally you have an expression Boolean expression w not which is equal to A, B, C, D, E , if I denote this sixth condition by F and the 7th condition by G the expression is A, B, C, D, E, F and G .

(Refer Slide Time: 1:05:52)



So, what we have done is, we have written expressions A, B, C, D, E, F, G, for satisfying the seven conditions.

(Refer Slide Time: 1:06:08)



And we consider w_0 to be equal to A, B, C, D, E, F, G. What can you say about the length of w_0 ? A is order $p^3 n$, B, C, D, E, they are $p^2 n$. I am sorry C is $p n$, B is $p^2 n$, D is $p^2 n$, E is $p^2 n$, F is $p n$, G is 1.

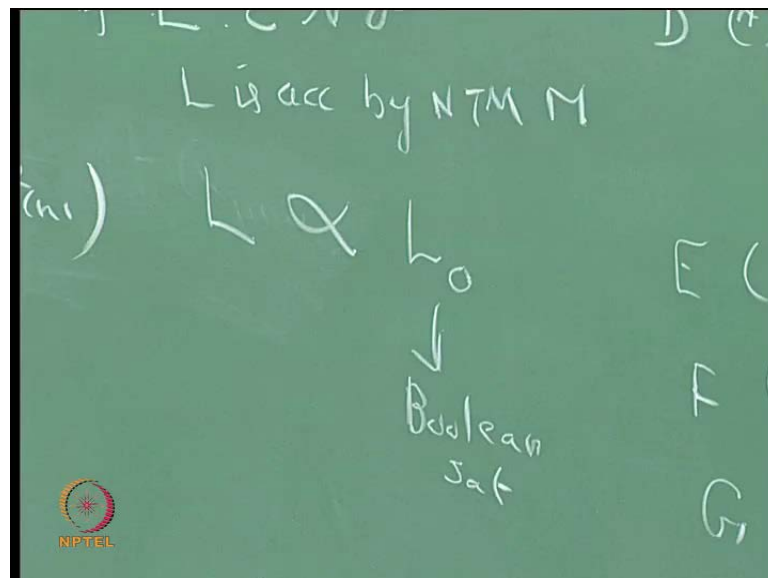
So, the total length of this is order at the most its order $p^3 n$ that is a polynomial. Here we are assuming that one variable is represented as one symbol you may have to use

some representation for represent variable in which case there will be one more logfactor. Suppose, you are having n variables you require $\log n$ bits to represent them. So, here the number of variables is order p square $n \log$ to that will be required that does not matter any one more polynomial factor will be one more expression will be there. So, given M and you can write w_0 and the length of w_0 is polynomial in n , this is the length of w and since, the length of w_0 is like that and there is you know, how to write this w_0 see there is a systematic way of writing it.

w_0 can be written down from M and w in polynomial time its length is polynomial and it can also be written down in polynomial time.

So, any nondeterministic Turing machine M if you take any nondeterministic Turing machine M you take and the input is w from this, you can write w_0 in polynomial amount of in polynomial time.

(Refer Slide Time: 1:08:32)



Deterministic polynomial time that is if L belongs to NP then, it is accepted by L is accepted by nondeterministic Turing machine M and you know that from this. We can write down w_0 such that w is satisfiable if and only if M accept w that is L is polynomial time reducible to L not L not is the Boolean satisfiability problem this is Boolean satisfiability any language L in NP can be transformed in polynomial time to L_0 so, this shows that Boolean satisfiability is NP-complete. So, we will continue in the next class lets tomorrow 11 o'clock.