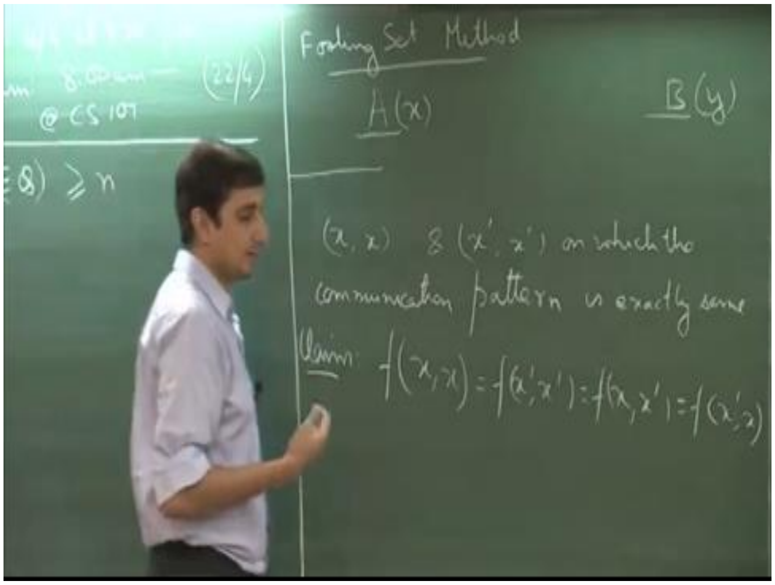
Computational Complexity Theory
Prof. Raghunath Tewari
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture -39
Introduction

(Refer Slide Time: 00:17)


8:00pm
@ CS 101
(22/4)
(EQ) ≥ n
Fooling Set Method
A(x)
B(y)
(x, x) & (x', x') on which the communication pattern is exactly same
Claim: f(x, x) = f(x', x') = f(x, x') = f(x', x)

So, as I discussed last time that the complexity the communication complexity of this equality problem is lower bounded by n. So, let us see one very simple counting based approach this is also known as the fooling set method. So, we have a selective we have these two guys we have Alice and we have Bob. And they want to decide given two strings. So, Alice has x and Bob has y. They want to check if these two strings are equal or not.

So, I claim that any protocol between these two persons; will take at least n bits so that is what this theorem says. So, suppose we have two pairs of strings, let us say x, x and x prime, x prime on which the communication pattern is exactly the same. So, in other words given both these pairs of inputs respectively to Alice and Bob, I mean the sequence of bits that they communicate between them is basically the same.

So, even on x, x if the first bit that Alice communicates to Bob is b 1 the second width which Bob communicates to Alice is b 2. And so on then on the input x prime, x prime also that same sequence is communicated between these two persons. So, then what can we say? So, then the claim is that suppose if these is the case then the claim is that for any functions; here abstractly looking at some function forget about the equality problem for now.

Let us say that Alice and Bob wants to decide some function f and they are given some pairs of strings; and if on the pair x, x and x prime, x prime they have the same communication pattern. Then the claim is that f of x, x is equal to f of x prime, x prime is equal to f of x, x prime which is equal to f of x prime, x. So, no matter which pair you choose the value of the function should be identical and why is this the case?

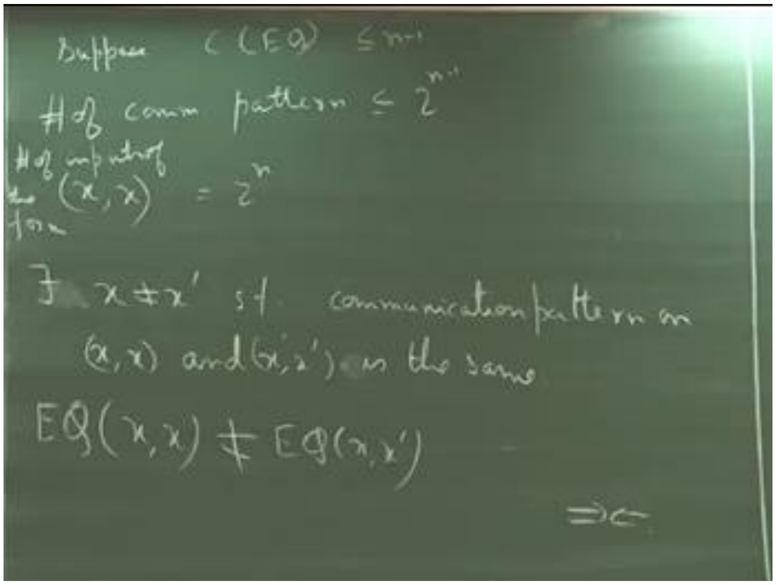
Again it is a very easy inductive argument I would not give the inductive proof but let us look at the idea behind it. So, suppose Alice has x and he communicates a bit x 1. So, by our assumption we know that irrespective of Alice having the string x or x prime he does the same thing. I mean Alice does not know what Bob has. So, Alice has x let us say and he communicates the bit b 1. And it would have been the same bit had he had if Alice had x prime also by assumption.

So, now let us move on to Bob. So, Bob gets this bit b 1 irrespective of whatever string x or x prime that he has. And Bob strategy is again the same irrespective of the string that he has also. So, he gets this fixed bit b 1 and then because the communication pattern is the same for Bob as well. So, this next bit b 2 that Bob sends to Alice will again be the same because his strategy does not change on the string x or x 1.

And now Alice gets back the bit b 2, so here Alice has access to b 1, b 2 and his own string x. So, I mean he will basically send the same bit b 3 respective of x or x prime. So, this inductive argument shows that the final bit that is getting outputted by on any pair of these inputs will basically be the same. So, this is a strong assumption. I mean I am not saying that this is not a strong assumption;

Because for the communication pattern to be the same what we are saying is that every bit that is communicated in a particular round has to be the same. So, what can we say now? So, let us look at its come back to the proof.

(Refer Slide Time: 06:21)



Suppose $C(EQ) \le n-1$

# of comm pattern $\le 2^{n-1}$

# of inputs of the form $(x, x) = 2^n$

$\exists\; x \neq x'$ s.t. communication pattern on (x, x) and (x', x') is the same

$EQ(x, x) \neq EQ(x, x')$

$\Rightarrow\Leftarrow$

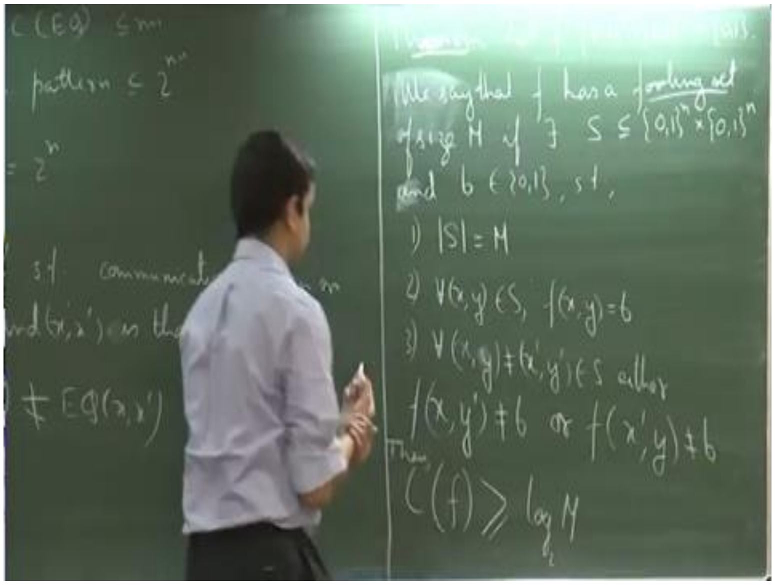
So, suppose the complexity of this equality function is less than or equal to n - 1, for the sake of contradiction. Then what can we say? So, what this statement means is basically that n - 1 bits are communicated between them. So, if n - 1 bits are communicated between them how many different communication patterns can we have? It is basically less than 2 to the power n - 1. So, the number of communication patterns is bounded by 2 to the power n - 1.

So, if the number of communication patterns are bounded by 2 to the power n – 1, so let us look at another thing how many pairs or how many inputs can you have of the form x, x? That is both the strings are the same. How many different such inputs can you have? So, the number of choices of this form is equal to 2 to the power n. So, basically the number of inputs of the form x, x is exactly 2 to the power n.

So, therefore from these two statements what we have is that there must exist distinct x and x prime as you claim. So, there exist x not equal to x prime. Such that, the communication pattern on x, x and x prime, x prime is same by simple principle, which implies that by our earlier claim that this should happen; but then this is clearly false because we know that is equality function on let us say x, x is not equal to E Q of x, x prime because we are picking unequal strings.

So, there for communication complexity so this complexity cannot be less than n, exactly n. So, I think I will discuss other way of getting lower bounds on the communication complexity also, so there is this method called tiling method, which is more general in the sense that if you get a lower bound using the tiling method; it also implies a lower bound using this fooling set method, but we will discuss it next time. So, I will just give a generalized version of what we did here.

(Refer Slide Time: 10:03)


We say that f has a fooling set of size M if ∃ S ⊆ {0,1}^n × {0,1}^n and b ∈ {0,1}, s.t.
1) |S| = M
2) ∀(x,y) ∈ S, f(x,y) = b
3) ∀(x,y) ≠ (x',y') ∈ S either f(x,y') ≠ b or f(x',y) ≠ b
Then C(f) ≥ log₂ M
C(EQ) ≤ n
pattern ≤ 2^n
= 2^n
s.t. communicat
and (x,x') in th
≠ EQ(x,x')

So, let us how do we generalize this? So, suppose we have a function f; so let f be some function from 0, 1 to the power n cross 0, 1 to the power n to 0, 1. So, we say that f has a fooling set of size M, if there exists a set of input pairs that exist some S which is a subset of 0, 1 to the power n cross 0, 1 to the power n. Such that the following is true, the first is that the cardinality of S is equal to M.

What is the second thing that we want? That on all points in x it should have the same value for some bit b. So, let me just put this here so if there exist set S and some bit b in 0, 1 such that firstly S has psi M secondly for all pairs of strings in S f has that same value. And the third condition is that, for all x, y not equal to let us say x prime, y prime in S either x, y prime, either f of x, y prime is not equal to b or f of x prime, y is not equal to b.

So, note that now we are considering the pairs x, y prime and x prime y. So, if all three of these conditions are met then we say that f as a fooling set of size M. And what the theorem says is that if f has a fooling set of size M; then the communication complexity of f, so what do you think should be? So, what is the fooling set here? What was our fooling set in this case? So, in this case our fooling set was basically all pairs of this form.

So, the pulling set the complexity is bounded by log of M, so any questions? What is i? So, where do we have an i? I log to the base two, because we are dealing with binary alphabets.