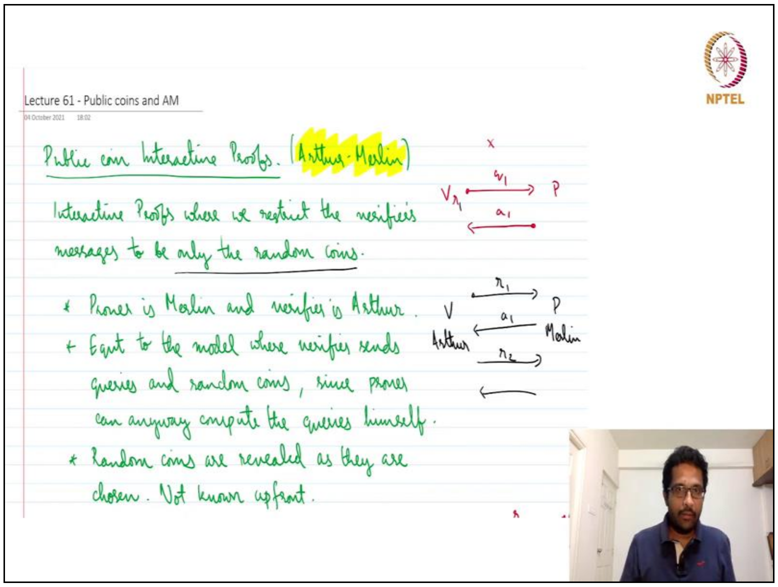
Computational Complexity
Prof. Subrahmanyam Kalyanasundaram
Department of Computer Science and Engineering
Indian Institute of Technology, Hyderabad

Lecture -61
Public Coin Interactive Proofs and AM_MA

(Refer Slide Time: 00:15)



Lecture 61 - Public coins and AM

04 October 2021 18:02

Public coin Interactive Proofs. (Arthur-Merlin)

Interactive Proofs where we restrict the verifier's messages to be only the random coins.

- Prover is Merlin and verifier is Arthur.
- Equt to the model where verifier sends queries and random coins, since prover can anyway compute the queries himself.
- Random coins are revealed as they are chosen. Not known upfront.

Hello and welcome to lecture 61 of the course computational complexity. In the in the past couple of lectures we have been seeing the power of interaction instead of getting a static proof from a from a prover what could what more could we accomplish if we were able to interact with the prover and we saw graph non-isomorphism we saw that it had an interactive proof. But the proof crucially used the fact that the random coins were withheld from the prover.

We also saw the proof for sharp 3 SAT in interactive proof of sharp 3 SAT where in fact the all the randomness was made open to the prover. So, we want that which was a public coin protocol the randomness being revealed to the proverb. So, we want to understand what is the power when the randomness has to be made public or randomness has to be announced to the prover. So, it is to think of it as a restriction.

Because in interactive proofs does not by itself require the randomness to be made open to the prover but if you make it open to the prover perhaps you cannot do some things that you could have otherwise done like in like we did in the case of graph non-isomorphism. So, with this restriction of having to compulsorily announce to the prover the the random coins what could we achieved. So, this is what we will see in this lecture.

This public coin interactive proofs and this is commonly known as Arthur Merlin proofs Arthur stands for king Arthur who had a wizard called Merlin in his in his court and Merlin is like this wizard he knew he is all powerful he even knew what Arthur may possibly ask and just like the proverb being all powerful. And this terminology Arthur Merlin will be used only in the case of public coin groups.

So, we may we may think of the interactive proofs or the public on interactive groups or the Arthur Merlin proofs as one where the verifier has to compulsorily announce the random coins. So, let us say we enforce this what did we have in the first model we had verifier sending a message q 1 over here we have q 1 and the prover sending a 1 as in response. And the q 1 is a function of the input x and the random coins generated for the first round say r 1.

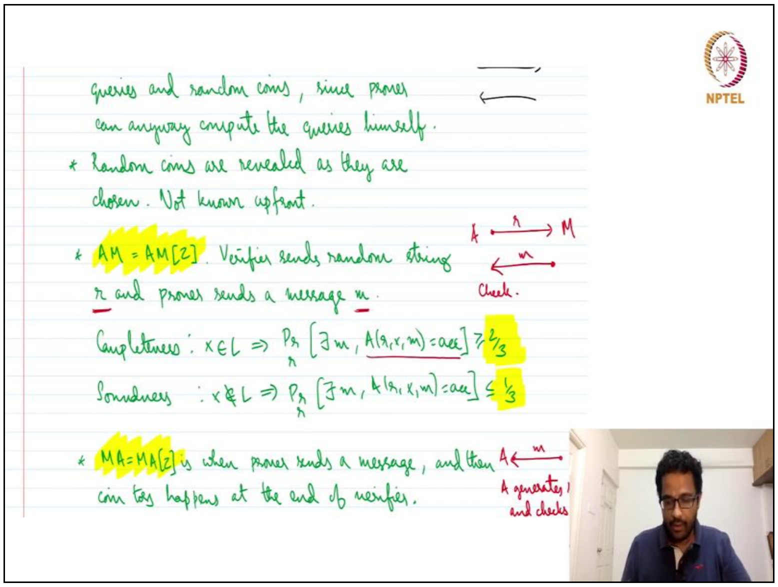
This is function of x and let us say r 1 because I AM just writing f now what is the need for the verifier to compute q 1 and sends suppose the verifier also sends r 1 along with q 1 there is no real need for the verifier to compute f because the prover can himself compute f all the prover needs is r 1 which is generated at the verifier's end but by the model we are the verifier is forced to send r 1 all the verifier needs to do is send r 1.

Because x is also known to the prover and ones the verifier sends r 1 the prover also knows r 1 and the prover may as well compute f and then sends the response. And similarly in round 2 maybe or like then sends a response and then instead of q 2 again the verifier may just send r 2 the next set of random bits that were that he has generated. The point here is that there is no nothing lost by restricting the prover or restricting the verifier to only send the random coins.

Because any function that he intended to compute could be computed by the prover himself. So, in this model the verifier will only be sending the random coins the prover is called just as I said before the prover is called Merlin and the verifier is called Arthur. So, this is as I said it is equivalent to the model where verifier only sends the random coins. We will restrict the verifier to only send random coins.

But this is equivalent to the situation where the verifier sends queries and random coins because prover can anyway compute the queries.

(Refer Slide Time: 04:49)



queries and random coins, since prover can anyway compute the queries himself.

* Random coins are revealed as they are chosen. Not known upfront.

* AM = AM[2]. Verifier sends random string $\underline{r}$ and prover sends a message $\underline{m}$.

$A \xrightarrow{r} M$

$\xleftarrow{m}$

Check.

Completeness : $x \in L \Rightarrow \Pr_{r}[\exists m, \underline{A(q, r, m) = acc}] \geq 2/3$

Soundness : $x \notin L \Rightarrow \Pr_{r}[\exists m, A(q, x, m) = acc] \leq 1/3$

* MA = MA[2] is when prover sends a message, and then coin toss happens at the end of verifier.

$A \xleftarrow{m}$

A generates r and checks

And the key thing is that the random coins are revealed only as they are generated. If you think of the sharp 3 SAT proof the prover was sending the verifier was sending the random coins but if the verifier sent all the randomness at the beginning he lets say the verifier generated all the randomness at the beginning and sent to the prover. Then the prover could possibly cheat by looking at the entire set of random coins and then engineering a function at each step.

Because he knows that what is going to come in the future but what really helped was the fact that every randomness was generated at the time the prover does not know what to expect in the future and this was used. So, just like that we will we will insist that the random coins are revealed as and when they are chosen. The verifier will require randomness for a particular round he will generate it and then send it the word does not know what random coins are going to be generated in the future.

They are not known up front the class M is stands for Arthur Merlin proves. And M without qualifying the number of rounds stands for M with 2 rounds meaning M Arthur speaks first the verifier speaks first and then Merlin speaks. Arthur sends the randomness r and verifier and the prover sends the message M the Merlin sends the message M m stands for AM with 2 rounds.

So, this is a bit inconsistent with what we said for IP we said that when we do not qualify the number of rounds for IP it stands for polynomial mini rounds but in the case of AM it is it stands

for just 2 rounds. Let us try to look at the completeness and soundness when x is in the language completeness a random string is sent and the prover if x is in the language prover should be able to pick a message such that the verifier should be able to verify the message r the message M the random string r and his input x and it should be accepted with probability at least 2 thirds.

So, a is a function of at the very first end capital A, r is a random coins x is the input M is the message from the prover. If x is in the language prover should be able to pick out an message M such that the probability of it getting accepted is or rather the r is already chosen for 2 thirds of the choices of r at least 2 thirds of the choices of r the verifier the prover should be able to pick out an n. In some cases there may not exist AM but that is for as long as majority of the cases or 2 thirds of the cases the prover can pick out an m.

And the soundness when x is not in L for the majority of cases for 2 thirds of the cases the prover should not be able to pick out such an n or in fact the probability that the prover can pick out an M that leads to acceptance is at most one thirds. So, notice that we have the existential quantifier for the soundness also this is not a typo it is the existential quantifier because verifier sends the randomness and the prover what is the probability that the prover can pick out a message M that leads to acceptance.

So, this is the same in the case of sound completeness and soundness. This is the only case where AM is only case where we will we will we will be having this direction in both cases just just a pictorial depiction of the protocol here Arthur sends a random string M sends a message and then it is checked. Similarly like AM we could define a class called MA and MA is also MA with 2 rounds when we do not qualify how many rounds it is MA is also MA with 2 rounds.

And this happens as you may guess MA stands for Merlin sends the message first so I have drawn it here. So, Arthur generates and then Arthur generates a random string and then verifies and this random string Arthur could possibly send it to Merlin but then there is nothing to be accomplished by sending it to Merlin because there is no nothing more to be heard from Merlin it is just in fact MA of 2 is just one round in one round of communication but the second round are the generates r the random bits and then does the verification. So Merlin sends the message Arther generates the randomness and verifies.

So, completeness when x is in the language there should exist a message M that the prover can send such that for most random coins picked out by the verifier should lead to acceptance. And soundness when x is not in the language whatever for whatever a message picture picked out by the prover is not going to be accepted beyond a probability one third. The completeness there should be a message with prover that is accepted with probability at least 2 thirds soundness whatever message is chosen by the prover it is accepted with probability at most at most one-third.

Here we have again their x’s and for all MA also without qualifiers indicates MA with 2 rounds which is what I described just now. And it is convenient to think of MA as just like NP then everything is like NP where it is just like Merlin sends a message or a certificate that needs to be verified. Just that the verifier machine is a probabilistic machine instead of a deterministic machine it is a randomized machine.

Like in the case of interactive proofs we can assume that it is perfect completeness or we can get perfect completeness meaning the 2 thirds can be pushed to exactly equal to one. And it can also be shown this we will not prove we will not prove in this course we will not prove this although it is not that difficult to show. So, constant round public coin interactive proves constant round public on interactive proofs are either MA or AM.

So, if you had more rounds let us say AM with a constant number of rounds where AM with k rounds this can be reduced to AM with 2 rounds which is equal to AM. This can be reduced to AM with 2 rounds which is same as AM and even if you start with MA you can think of there are the true systems that are denoted MA M meaning Merlin sends a message Arthur generates a random bit then again Merlin sends a message or MA-MA like all of this will reduce to will reduce to AM.

The other thing that can happen with constant round interactive proofs public coin interactive proof is that we just have MA which is just 2 rounds Merlin sends and aster verifies. So, the point here is that constant round public coin interactive proof systems there are only 2 classes MA or AM both with 2 rounds what we just described about. In fact it may be worth to just notice the contrast between the completeness and soundness of MA and AM just now.

In the case of AM we have the probabilities outside that there x is quantified inside in both cases 2 thirds one thirds in the case of MA the probability the quantifier is outside and probability is inside. Because the order of communicating is different the order of communicating is different because in the case of Merlin Arthur the Merlin chooses first and then Arthur has to respond with randomness.

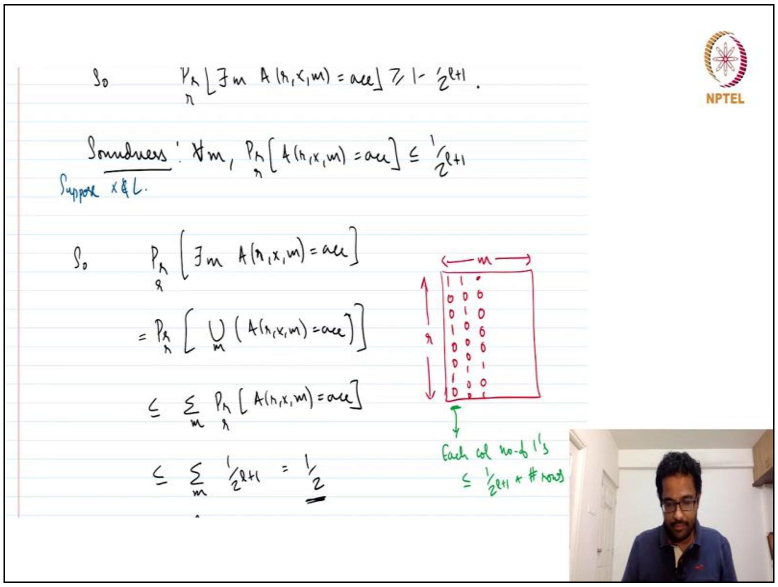
And in fact there is a way to denote this also in the case of Arthur Merlin proofs it is like Arthur sends random coins and then Merlin has to like existential quantifier for Merlin and then again Arthur has to send some random coins and so on. You can view it as a tree in fact **(())(14:04)** has this picture that you can have a look Arthur will send a random coin each round and Merlin has to pick out its like an existential quantifier.

It is kind of like M is like a member of the polynomial hierarchy where instead of the for all quantifier we have the random probability probability thing. And ones again constant k boils down to either AM or MA. So, in fact this proof we will highlight we will see a we will see the proof AM k is equal to AM. We saw AM we saw MA both being public coin protocols and we will see that MA will see now that MA is contained in AM.

You may guess that this is indeed the case or rather it is intuitive to guess that this is indeed the case because in the case of MA the prover has to pick out a message before seeing the randomness in the case of MA he can he gets to see the randomness and then pick out the message the prover has more information in the case of AM and presumably he can convince more things with that information.

So, MA is actually contained in AM when the prover is not able to see the randomness or the approver is able to see the randomness. Thirdly he can do whatever he could do even otherwise when he did not see the randomness.

(Refer Slide Time: 15:45)



So $\Pr_{r}[\exists m \; A(r,x,m) = acc] \geq 1 - \frac{1}{2^{l+1}}$.

Soundness: $\forall m, \Pr_{r}[A(r,x,m) = acc] \leq \frac{1}{2^{l+1}}$

Suppose $x \notin L$.

So $\Pr_{r}[\exists m \; A(r,x,m) = acc]$

$= \Pr_{r}[\bigcup_{m} (A(r,x,m) = acc)]$

$\leq \sum_{m} \Pr_{r}[A(r,x,m) = acc]$

$\leq \sum_{m} \frac{1}{2^{l+1}} = \frac{1}{2}$

Each col no. of 1's $\leq \frac{1}{2^{l+1}} * \#$ rows

Let us see the proof of this MA is contained in a suppose as always we pick out L an arbitrary language in may and we will show that it can it is contained in AM l is in MA which means L has an MA proof system we will see how to modify this to get an AM proof the completeness and soundness for the MA prove system is that x is in L then there x is a message that Merlin should send such that the probability of accepting the message is at least 2 thirds.

Soundness means x is not in n for any message that is being sent by Merlin the probability that Arthur accepts it is at most one third. And we can amplify this 2 thirds one thirds we already said we can attain perfect completeness but just like what we did in BPP we could amplify it to extremely close to 1 and extremely close to 0. 1 - 1 divided by 2 power l + 1 and 1 divided by 2 power l + 1 where L is chosen to be the length of the message sent by Merlin.

This will come a bit later I will highlight it again why we chose this probability. Let us see completeness. We have this when x is in the language suppose x is in the language this means there x is an M such that probability of acceptance is at least 2-thirds. Now let us try to draw this matrix as I have in the right side where rows denote are indexed by random coins and columns are indexed by messages that are sent by Merlin.

So, what does it say it says that there is a column that has a big fraction of ones because the completeness is there excess M such that the probability of acceptance is higher we said it is 2 thirds but then we said we will we are going to boost it to 1 - 1 divided by 2 power l + 1. This means there is a row there is a column sorry such that this column this column has 1 - 1 by 2 power l + 1 fraction of ones which means large fraction of entries in this column are ones.

Maybe I will just highlight this in this column a majority a large fraction are ones. Now let us look at the completeness condition of AM where the randomness is sent and then for which values of r can Merlin pick out a message that will lead to acceptance. And let us say this before that let us say this column which had at least this many ones let us call this column M star which is what I have written here.

So, the point is that now if you choose a randomness first now Merlin has to pick out some message that will lead to acceptance Merlin already knows the randomness. The question is ones he chooses a randomness will Merlin be able to pick out M. We know that already in this in this column a huge fraction are ones which means that if these for these entries these rows which where this column has ones.

As long as a column has any one as long as a row has any one that that random choice of r is good but already we know that a majority of random the choices of r are good because there is one column that has a huge number of ones. So, in fact the same M star will work for most of the for almost any r the same M star Merlin does not does not even you need to think the Merlin could just send M star and that will work for almost all of the r’s because M star itself works for a huge fraction of the inputs that is the completeness of the problem.

You can basically you can take the existential quantifier inside the probability in other words we are saying that the completeness condition for AM happens to be implied by the completeness condition for M. And now let us see the soundness the soundness is a bit more involved only slightly more involved soundness condition for MA is that for all M suppose x is not in L suppose x is not in l then for all M the probability that it gets accepted is at most one by 2 power l + 1.

Let us see pictorially what this means we again have the same matrix M and r. So now you can as you can see there are more zeros than ones because x is not in l the probability of acceptance at most one by 2 power l + 1. This means that for each column the number of ones is at most the number of ones is at most each column number of ones is at most 1 by 2 power l + 1 multiplied by number of rows.

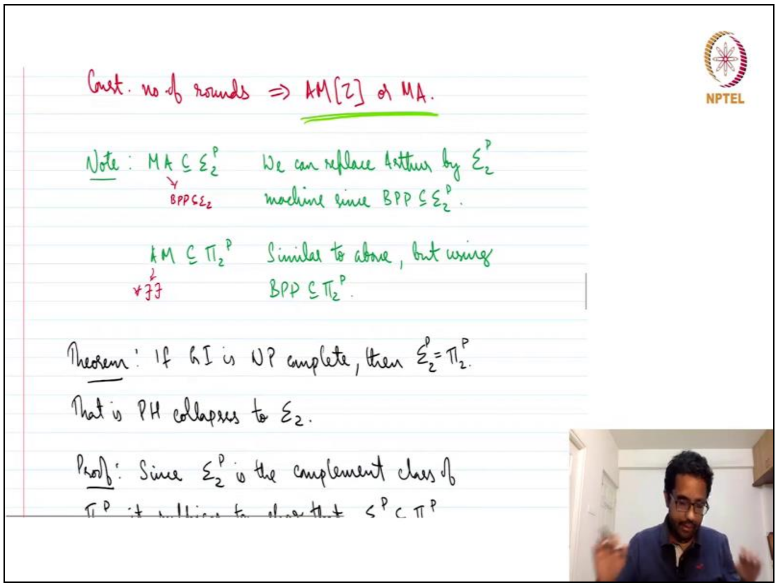
Because we know that the probabilities that was this what is the total number of ones in the matrix each column has this many this many ones this is equal to total number of ones is at most this quantity which is 1 by 2 power l + 1 into number of rows multiplied by number of rows multiplied by number of columns. But how many columns are there remember we said that the length of message that Merlin sends is equal to l and assuming 01.

I have been assuming 01 although I did not make it explicit this means the number of columns is actually equal to 2 power l this means that this is equal to the 2 power it is like 2 power l divided by 2 power l + 1 into number of rows which is half in half multiplied by number of rows. So, the total number of one’s is at most half times the number of rows this means that the total number of ones in this matrix is at most half times the number of rows which means that there are half there are the number of one’s is itself half the number of rows.

Which means at least half rows are all zeros because the best you can distribute the ones is you can put exactly one in each of the row but you can only put you only have many ones let us say this is this matrix says 100 rows you only have fifty one you can put each one for the first 50 rows and the remaining 50 rows do not have any ones which means for half the rows there are no one’s at all the half the rows are all zeros at least half the rows.

This means that this is what this means that what is the probability. So, if the random choice of r is for those half where there is no which correspond to all zero rows then Merlin will not be able to send out an M because the all those rows are entirely zeros. With probability at least half or at most half or with property at most half I am sorry with probability at least half Merlin has no choice no way to convince a verifier which means the probability of acceptance is going to be at most half.

(Refer Slide Time: 24:25)



Const. no of rounds $\Rightarrow$ AM[2] or MA.

Note : MA $\subseteq \Sigma_2^P$ We can replace Arthur by Σ_2^P machine since BPP $\subseteq \Sigma_2^P$.

BPP$\subseteq\Sigma_2$

AM $\subseteq \Pi_2^P$ Similar to above, but using BPP $\subseteq \Pi_2^P$.

$\forall\exists\exists$

Theorem : If GI is NP complete, then $\Sigma_2^P = \Pi_2^P$.

That is PH collapses to Σ_2.

Proof : Since Σ_2^P is the complement class of Π_2^P it suffices to show that $\Sigma_2^P \subseteq \Pi_2^P$

So, the same thing again here in a different way in the left side what is the probability this is the soundness condition for AM what is the probability that there x is an M that that leads to acceptance. This is like the worst cases you this is a union and you can take the union bound you can take the summation of all the probabilities summation over all M the probability that M will lead to acceptance and the probability that a specific M leads to acceptance is for a fixed sorry for the probability that for a specific M and the r gets accepted is at most 1 by 2 power l + 1.

By the soundness condition above and you sum it over all M you get half which is exactly the same computation that we did over here. This we got this 2 power l divided by 2 power l + 1. It is exactly the same proof but here it is more mathematical notation and the side I try to present it in a in a different way in a by looking at the matrix. So which means for the pro with half probability for half the choices of r half the charges of at least half the choices of r will lead to all zero rows and Merlin will have nothing to respond to that lead that could lead to an acceptance.

This means with the probability of acceptance is at most half. So, this is why we needed a boost because we use the union bound. The soundness is at most half and the completeness is at least one minus one by 2 power l + 1 there is a gap here and you may think that this is not less than one third but then I could have chosen the amplification to one divided by 2 power l + 2 in which case I would have got one fourth which is not really a big deal.

That completes the proof that MA is contained in AM which means if you have by revealing the randomness to the prover you potentially are able to the prover can convince more things to the verifier MA is contained in AM. And we can also it is not that difficult to see that we can whenever MA shows up in a as a part of a protocol we can replace it by AM and this is the proof that any constant round protocol can be reduced to a 2 round protocol.

So, if you have an AMA protocol AMA protocol this can be reduced to this MA can be replaced by AM and it this it can be replaced by a AAM protocol and AAM means it is like 2 sets of random bits and by Arthur instead you can think of it as one set of random bits and send it in one go that is actually AM. And similarly even if you have MAM where Merlin Arthur Merlin this in the first case this AM was replaced by I am sorry.

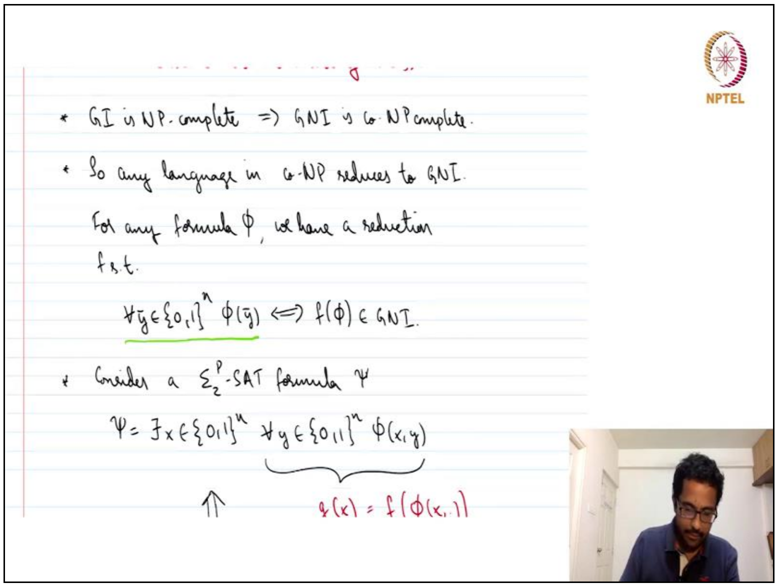
The first case this MA was replaced by this AM in the second case this MA was can be replaced by this AM and instead of merging sending 2 m 1 and m 2 2 strings one by one instead of that you can think of him as him sending a big string M 1, M 2, M concatenated or something even that is equal to AM and you can do this as long as it is a constant number of such replacement operations that is why whenever we have constant many rounds this can be replaced by a 2 round protocol either AM 2 or MA.

MA is not is only as at most as powerful as AM and we have this proof that constant round protocols are either AM or MA another thing to note is that MA is contained in sigma 2 which is which is a complexity class that does not have anything to do with interaction. Because Arthur is a BPP machine Arthur is a does random coin process and then does some verification. This bpp machine can be thought of as this BPP machine can be Arthur is a BPP machine which is contained in sigma 2.

And sigma 2 means it is a there exists a quantifier there x is for all quantifier but Merlin is also where there exists quantifier he has to send for completeness he has to send or rather he has we are testing whether he can produce a M that leads to accept. This directs us there exists for all you can merge with their excess quantifiers to get a sigma 2. And similarly BPP is also contained in pi 2 when Arthur goes first n this can be replaced by for all there exists.

And for all directions there exits can be converted into for all there exists so AM is contained in pi 2. So, MA and AM are in sigma 2 and pi 2 respectively yeah we know that MA is contained in AM.

(Refer Slide Time: 30:03)



- GI is NP-complete $\Rightarrow$ GNI is co-NP complete.
- So any language in co-NP reduces to GNI.

For any formula ϕ, we have a reduction f s.t.

$\forall \bar{y} \in \{0,1\}^n \; \phi(\bar{y}) \iff f(\phi) \in GNI.$

- Consider a Σ_2^p-SAT formula Ψ

$\Psi = \exists x \in \{0,1\}^n \; \underbrace{\forall y \in \{0,1\}^n \; \phi(x,y)}_{g(x) = f(\phi(x,\cdot))}$

$\Uparrow$

So, now let us the final thing of this lecture is this is something that we had referred to when we talked about graph isomorphism. We had stated graph isomorphism as a candidate language that is NP intermediate we said that graph isomorphism we did not know of any polynomial time algorithm nor do we think that it is NP complete. This I think was lecture 22 or 23 when we talked about Laudner's theorem which discussed NP-intermediate languages.

It is as of now we do not know whether it is in P or if it is NP complete the best algorithm is like a is a quasi polynomial time algorithm quasi polynomial meaning order 2 power log n to some constant this is the this algorithm was by Bubbai maybe three four years back for graph isomorphism we still do not know whether it is polynomial time. At the same time it is unlikely to be NP complete it is believed to be not NP complete and we will see the reason why it is not NP complete in this in this theorem.

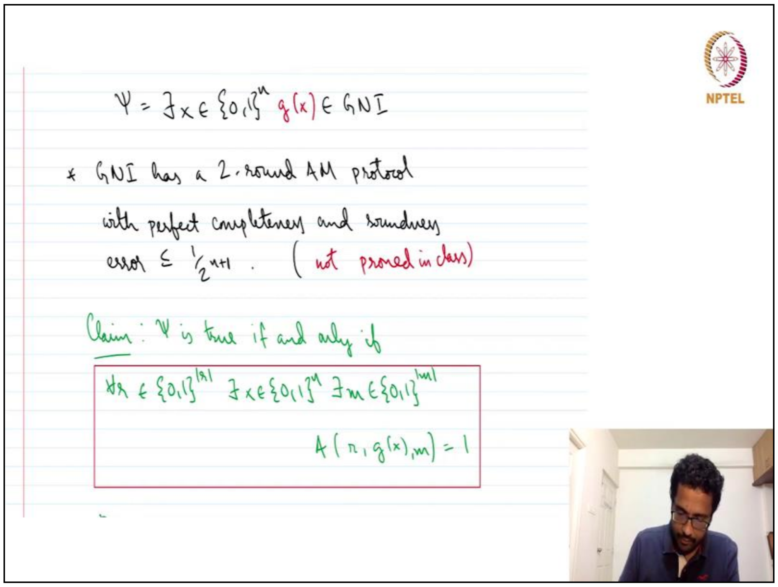
So, what the theorem states is that if graph isomorphism was NP complete then sigma 2 will be equal to pi 2 which means the entire polynomial hierarchy will collapse to sigma 2. And as I would have said when talking about polynomial hierarchy it is believed that the polynomial hierarchy is strict this theorem can be viewed as an evidence that graph isomorphism is unlikely to be NP complete.

Let us see the proof is very not very difficult to see. Since sigma 2 and pi 2 are sort of complement classes it is in order to show that sigma 2 is equal to pi 2 it is enough to show that sigma 2 is contained in Pi 2 because we have seen this trick in many other proofs like NL equal to co-NL for instance. So, we will assuming that graph isomorphism is NP complete we will show that sigma 2 is content in pi 2. we

By assumption graph isomorphism is NP complete which implies that graph non-isomorphism is co-NP complete this implies graph non isomorphism is co-NP complete this implies that any language in co-NP reduces to graph non-isomorphism which means given a formula phi this is this tautology what is the can we what do we have here, we in the left hand side we have the statement that for all y phi y is true.

I put a bar about y to denote that it is a vector for all y phi y is true this is a tautology problem which is a this is the co-NP complete problem and this can be we can reduce it to a graph non-isomorphism instance because graph non-isomorphism by assumption is co-NP complete by assumption graph isomorphism is NP complete which implies the graph non-isomorphism will be complete such that given a formula phi we can construct a graph non-isomorphism instance f phi such that phi is a tautology essence for tautology if and only if f phi is a essence of graph non-isomorphism. This is just the definition of what it means for graph non-isomorphism to be co-NP complete.

(Refer Slide Time: 34:06)



$\Psi = \exists x \in \{0,1\}^n \; g(x) \in GNI$

- GNI has a 2-round AM protocol with perfect completeness and soundness error $\le \frac{1}{2^{n+1}}$. (not proved in class)

Claim: Ψ is true if and only if

$$\boxed{\forall r \in \{0,1\}^{|r|} \; \exists x \in \{0,1\}^n \; \exists m \in \{0,1\}^{|m|} \quad A(r, g(x), m) = 1}$$

Now let us take an arbitrary language in sigma 2P. Let us take a formula psi which is a which is of this form there exists x such that for all y phi of x y is true this is a canonical sigma 2 SAT formula. Now let us see look at this the second part for all y phi of xy. This looks like a this looks like a tautology instance ones for a fixed x this this is a tautology instance. Now I can write it this as a again I can compute the reduction for this instance assuming we fix x let us say we get f of phi x and with the variable y.

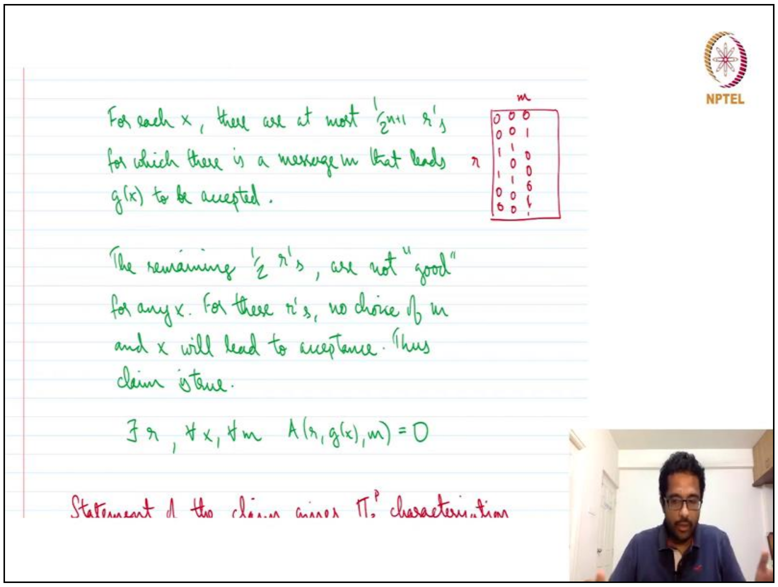
Let us say we call it g x which means this will be a graph that depends only on on the string x because that is because this formula phi depends on x and the variable was simply y, x was fixed. We get a with the same reduction above we get a graph a non-isomorphism instance called gx. Now that we have replaced this part maybe put a red bracket around this. This part with gx let us try to see what happens maybe I will make this one also red.

We are saying that psi is equivalent to their excess x such that g x is a essence of or gx is in GNI graphed non isomorphism because I can replace this for all y etcetera with gx and what we have seen? So, far it is just restatement of sorts we have not even gone to interactive proofs we are just talking about sigma 2 is contained in pi 2 and graph isomorphism and so on we are just rewriting stuff. And here is what where we what we have learnt comes into play what we have learnt in interactive proofs.

Graph non isomorphism we have seen that it has a 2 round Arthur Merlin protocol with perfect completeness and soundness error is 1 divided by 2 power n + 1 we can reduce soundness to as much as possible the sound is error to 1 divided by 2 n + 1 and we also mention that perfect completeness can be accomplished. So, i say not maybe I will say not proved but not proved in class. I mean the perfect completeness.

Soundness also it is exactly similar to BPP amplification. Let us rewrite this in another way GNI we this is all that we have known to us but let us rewrite this in another way this is i what we have here is psi maybe I will just put a red box around this as well and this psi is true if and only if there is a claim here that for all random choices are there exists x and M that x is M such that A r g x of M equal to 1 where I am just where A r g x M that this a is part of the Arthur Merlin protocol for graph non-isomorphism this is from the Arthur metal in protocol for graph non-isomorphism.

(Refer Slide Time: 38:03)



For each x, there are at most $\frac{1}{2^{n+1}}$ r's for which there is a message m that leads g(x) to be accepted.

$$\begin{array}{cc} & m \\ r & \boxed{\begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{matrix}} \end{array}$$

The remaining $\frac{1}{2}$ r's, are not "good" for any x. For these r's, no choice of m and x will lead to acceptance. Thus claim is true.

$\exists r, \forall x, \forall m \quad A(r, g(x), m) = 0$

Statement of the claim gives Π_2^P characterisation

So, let us see why this is true we want to say that given this psi let us say 1 we want to say that that is true if and only if this is true 1 and 2 are kind of equivalent. Let us let us do it in 2 parts 1 implies 2. First suppose psi is true now we have perfect completeness for graph non-isomorphism which means whenever gx is in GNI the probability that the AM proof accepts is equal to 1. The probability that Merlin can send the M is equal to 1. What is psi here?

There exists x such that gx is GNI if you rewrite there exists x such that gx is equal to GNI we can again write it as there exists x such that this is true and now like we did earlier if there exists x such that this is true we can even take the x inside the choice of x same x will work even if it is taken inside. So if we can take x inside the probability that there exists M there exists x that x x that x is M this is true is equal to 1 which means for all r there exists is x and there exists M such that this is true which is what we stated here in this box 2.

For all r there exists M and there exists x for which this is true. Now the other direction 2 implies one suppose there is a this is true that for all r there exists x and M such that A r g x M equal to 1 or in fact we will we will assume the opposite we are not going to prove 2 implies 1 rather we are going to say that not 1 implies not 2. Suppose psi is not true which means for all y of sorry for all x gx is not in graph non-isomorphism.

For all x gx is not in graph non isomorphism for all x the gx is not in graph non-isomorphism. Now soundness tells us that we assume that soundness can be reduced to one by 2 power n + 1 the probability that there exists an M since gx is not a s instance such that A r g x M can be accepted is at most one by 2 power n + 1 this is exactly the soundness condition for AM protocol. Now much like we did over here over here we did a matrix and we counted the number of accepts rejects zeros and ones much like that.

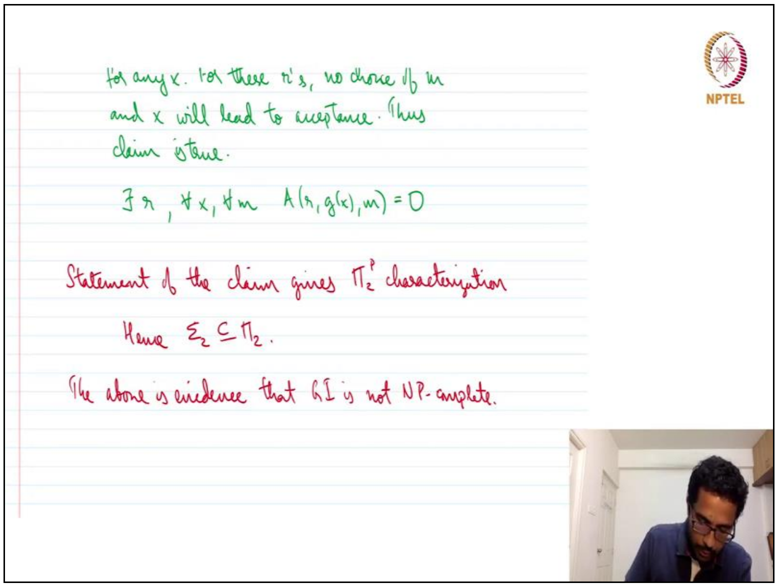
Let us see this is this is r and this is this is M there is a matrix of zeros and ones and so on. And we know that for any x for any x because for all x quantifier there are at most 1 divided by 2 power n + 1, r’s for which there is a message M that leads to gx getting accepted. This 1 indicates the acceptance of g x for that r and that M for any x there are at most 2 power n + 1 r's for which there is a message M.

So, what I want to say is that there are at most 2 power n + 1 r’s that have at least 1, 1 in its row there are at least 1, 1 in its row, so for each x that means now consider this is for a specific x. Now consider consider now another x and another x for each x there are some r's that are good which means for each x there are 1 by 2 power n + 1 rows that are good. So, what are the rows that are good for some x.

So, each row the best possible is that all the rows are spread out and there are 2 power n multiplied by 2 power and 2 power n divided by 2 power n + 1 rows which will be good for a fraction rows that will be good for some x which means that is at most half the rows which means there are at least half the rows which will not be good for any x. These are will any choice of M and x will lead to rejection or rather no choice of M and x will lead to rejection.

So, there are there are r's. So, I do not even need half the hours that all I need is there are rows which will not be accepted for any x and any M. So, there exists r says that for all x and for all MA of A r x g x M is not accepted and which is the negation of what I have written in box 2. For all r that x is for all sorry there exists r such that for all x and for all M A r g x M is equal to 0 which is what we have shown.

(Refer Slide Time: 44:28)



for any x. for these r's, no choice of m and x will lead to acceptance. Thus claim is true.

$$\exists r, \forall x, \forall m \quad A(r, g(x), m) = 0$$

Statement of the claim gives Π_2^p characterization

Hence $\Sigma_2 \subseteq \Pi_2$.

The above is evidence that GI is not NP-complete.

So, which means this is an equivalent restatement of psi, psi was to begin with psi was a sigma 2 an arbitrary language or arbitrary thing to check from sigma 2 and now we have this equivalent characterization box 2 for psi. Notice what we have here a is a deterministic polynomial time machine the randomness comes from r. Once r is fixed a is deterministic and r is some input x is some input M is some other input and we have this for all there exists there exists quantifier.

These 2 quantifiers existential quantifiers for x and M can be merged it is just like a for all r there is x, M this is true this is exactly how a pi 2 language should look like. So, state statement of the claim or the 2 statement gives a pi 2 characterization for L we started with the sigma 2 language n and we have now shown a pi 2 characterization which means sigma 2 is contained in pi 2 and the only assumption that we made was that graph isomorphism was NP complete.

This implies that graph isomorphism is NP complete implies that sigma 2 is equal to pi 2 which means polynomial hierarchy collapses down to the second level and this is an evidence or this is an indication that because we believe it will not collapse to the second level or we will not collapse at all we feel that graph isomorphism is unlikely to be NP complete and that is all that I have for you in this lecture.

Just to summarize we saw Arthur Merlin public coin interactive proofs we called it Arthur Merlin proofs. Arthur is a verifier Merlin is approver we saw the characterizations for 2 round protocols AM and MA or 2 round 2 systems AM and MA. AM stands for AM with 2 rounds MA stands for MA with 2 rounds. We saw the completeness and soundness for these 2 we saw that when we have constant number of rounds k rounds AM k is equal to AM.

The only public constant round public coin protocols are correspond to AM or MA constant round when you have no non constant let us say n rounds or n squared rounds it is it is different. We can do this replacing MA with AM only for constant many times not otherwise. Then we saw the proof that AM contains MA basically we boosted the probability of success for probability of success and reduce the probability of error completeness and soundness errors were reduced for the MA protocol.

And the completeness of MA directly implied the completeness of AM and the soundness of MA the boosted soundness was used to reason the soundness of AM as well we could replace MA by AM and that that gives the fact that any constant round protocol proof system boils down to MA or AM. Then we saw this theorem finally that graph isomorphism is NP complete implies sigma 2 is equal to pi 2. We started with arbitrary language in sigma 2 which was which was psi and then we since graphed normal isomorphism is going to be complete the latter part for all y this part could be replaced by a graph non-isomorphism instance.

And then we use the fact that we saw the 2 round AM protocol we replaced we used that to reason the equivalence between one and 2 and 2 is of the pi 2 form that implies that arbitrary language in sigma 2 can has a pi 2 characterizations which proving what we wanted. And that completes what I had for you in this lecture and there are some more interesting things about public coin protocols which I will present in the next lecture, thank you.