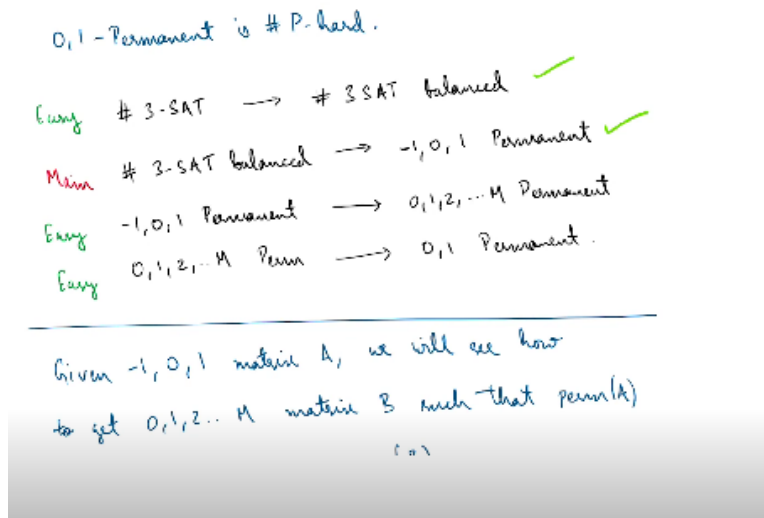


**Computational Complexity**  
**Prof. Subrahmanyam Kalyanasundaram**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Hyderabad**

**Lecture - 51**  
**Permanent is #P – Complete: Part 2**

(Refer Slide Time: 00:15)



Hello and welcome to lecture 51 of the course computational complexity. In lecture 50 we started seeing the proof that permanent is sharp P complete. So, in fact the permanent sharp P complete the first part of the proof was that permanent is in sharp P, in fact what we showed was that 0, 1 permanent was in sharp P. So, 0, 1 permanent correspond to counting the number of perfect matching's in a bipartite graph.

And then we said that we will show that 0, 1 permanent is also sharp P hard in the sense that any function in sharp P can be reduced to 0 1 permanent. And this was a rather long proof or easier rather long proof. And we said that we will follow four steps and the first two steps we completed. We reduced sharp 3 SAT to sharp 3 SAT balanced and then sharp 3 SAT are balanced to - 1 0 1 permanent.

And what remains is to show that -1, 0, 1 permanent reduces to 0, 1 permanent. So, this also follows actually two steps. We will reduce - 1, 0 1 permanent to 0 1 up to m permanent. So,

meaning it will be reduced to the problem of solving the permanent on a range of non-negative values and then we will show that that can be converted to a permanent of 0, 1 values. So, both of these are rather short. So, this particular lecture video also is going to be rather short.

**(Refer Slide Time: 02:05)**

Given -1, 0, 1 matrix A, we will see how to get 0, 1, 2... M matrix B such that  $\text{perm}(A)$  can be obtained from  $\text{perm}(B)$ .

$$\sum_{\sigma} \prod_{i=1}^n a_{i, \sigma(i)}$$

$-n! \leq \text{perm}(A) \leq n!$

Set  $M = 2n! + 1$ .

Replace each entry  $a_{ij}$  in A with  $a_{ij} \bmod M$  to get  $b_{ij}$  of B.

So, we want to reduce so the first part is to the third step that is -1, 0, 1 permanent. How do you reduce to a non negative bounded range permanent? So, given a -1, 0, 1 matrix A. We will see how to get a 0, 1, 2 up to m matrix B. So, m is some number that is depend on the dimensions of the permanent, dimensions of the matrix A. Such that the permanent of A can be obtained from the permanent of B so it will not be the same but you can get one from the other.

So, notice that a permanent is a summation of so what was permanent was? This was some nothing but summation over all permutations product over all  $i, i = 1$  to  $n$   $A_{i \sigma(i)}$ . And since we are dealing with matrices of -1, 0, 1 the products will be either 1, 0 or -1. And, how many terms are there? So, that there are n factorial permutations so n factorial terms are there and some of them could be 0. So, the maximum this can be is that all the terms turn out to be +1.

So, which is n factorial and the smallest that this could be is that all the terms turn out to be -1 which is - n factorial. So, permanent of 0, 1 -1, 0 1 matrix A is going to be bounded between - n factorial and + n factorial. So, what we will do is to shift this to a completely positive domain.

So, what we will do is to? So, right now we have this situation. The values could be anywhere from 0 to  $-n$  factorial to  $+n$  factorial. It could be anywhere in between.

So, what we will do is to shift this entire thing to the we will shift it that, maybe I will use a different colour, we will shift it so that the 0 goes to so 0 to  $n$  factorial remain at the same place but  $-n$  factorial and these values get shifted. So,  $-n$  factorial will actually become  $2n$  factorial, so, using modular arithmetic. So, it will be the point here is that the green values are all non-negative, are all non-negative.

So, we will use modular arithmetic to move to this domain. So, what we do is to? Set  $M$  to be twice  $n$  factorial + 1. So, in the mod  $m$  domain everything is between starting from 0, 1, 2, 3 up to  $2n$  factorial. That is  $2n + 2n$  factorial + 1 again becomes 0 mod  $m$ .

**(Refer Slide Time: 05:30)**

$$\begin{array}{l}
 \text{So} \quad 1 \rightarrow 1 \\
 \quad \quad 0 \rightarrow 0 \\
 \quad \quad -1 \rightarrow M-1.
 \end{array}$$

We can compute  $\text{Perm}(B) \bmod M$

$$0 \leq \text{Perm}(B) \bmod M \leq 2n!$$

If  $\text{Perm}(B) \bmod M \leq n!$ ,

then  $\text{Perm}(A) = \text{Perm}(B) \bmod M.$

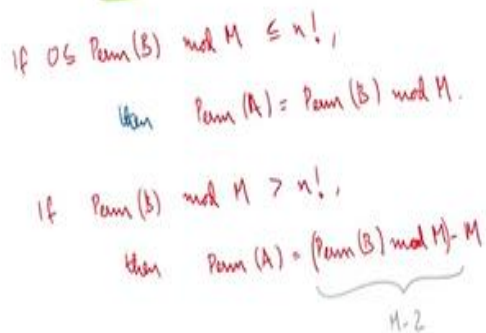
---

$n! > n!$

So, we look at each entry of  $A$  the matrix  $a$  and replace it with the equivalent mod  $m$  value of to get  $B$ . So, 0 and 1 so  $a$  has 3 types of entries 0, 1 and  $-1$ , so 0 and 1 just remain 0 and 1. However  $-1$  becomes  $m - 1$  in the modulo  $m$  setting.  $m - 1$  is actually  $2n$  factorial. So, now we compute the permanent of  $B$  where everything happens modulo  $m$ , everything so all multiplications additions everything happens in the modulo  $m$  word.

So, since everything happens in the model of  $m$  at the end, we will get some number which could be anywhere from  $0$  to  $m - 1$ , which is  $0$  to  $2^n$  factorial. So, that is how we get this inequality.

**(Refer Slide Time: 06:18)**



If  $0 \leq \text{Perm}(B) \bmod M \leq n!$ ,  
 then  $\text{Perm}(A) = \text{Perm}(B) \bmod M$ .  
 If  $\text{Perm}(B) \bmod M > n!$ ,  
 then  $\text{Perm}(A) = (\text{Perm}(B) \bmod M) - M$   
 $M-2$



And if the value is anything between  $0$  and  $n$  factorial, if the so in fact let me just say this if the value is between  $0$  and  $n$  factorial, then it means that the permanent of  $A$  it is actually the permanent of  $A$ . Because, that is how it is going to be. If it is  $0$  and  $n$  factorial that is how we would have got there. However, if the; permanent of  $B$  modulo  $m$  was greater than  $n$  factorial. Meaning, it is anywhere from  $n$  factorial +  $1$  to  $2^n$  factorial or  $n \cdot 2^m - 1$ .

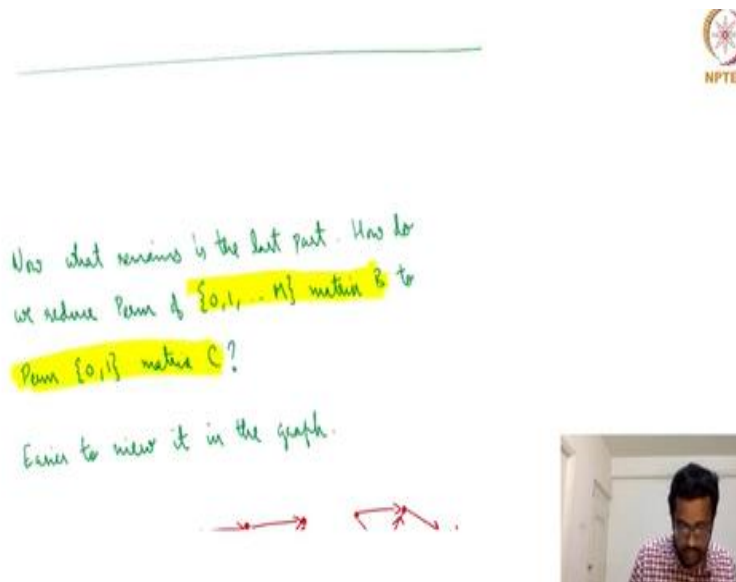
That means that it was actually in the negative range. And it was because we applied mod  $m$  it came to the positive value, so this means that the permanent of  $A$  is you take the permanent of  $B$  modulo  $m$  whatever value that is and you subtract  $m$  from there. Because, it if for instance if it is, if the permanent of  $B$  mod  $m$  if this was, let us say, if this was for instance if this was, suppose this was let us say  $2^m$  or this will be something between  $0$  and  $n - 1$ .

Let us say suppose is  $m - 2$ , so then this corresponds to this means that permanent of  $A$  is  $-2$ . If this is, let us say just  $m + 1$  what I want to say is if this is  $n$  factorial +  $1$ . This means, this  $-m$  is  $2^n$  factorial +  $1$ , this will be  $-n$  factorial. So, like that there is a correspondence between all the values of permanent  $B$  mod  $m$  and permanent  $A$ . So, you just compute permanent  $B$  mod  $m$  and you can compute permanent  $A$  using.

So, that is how we reduce a permanent of a 0 1 - 1 matrix to a permanent of a matrix that has values in the range 0, 1, 2, 3 up to capital m. In fact, in fact, we have in fact the values will be up to m - 1 and we are actually doing module m - 1. So, in fact this is I could actually say this is true but it is fine 0 1 to m is actually a sub, is actually a superset of this. In fact, the matrix has only three values 1 0 and - m - 1.

It is not even the entire range, but the permanent could be anywhere in these ranges. So, that is how we complete this part - 1, 0 1 permanent reduces to 0, 1 2 up to m permanent where it is bounded positive values. So, now what remains is the last part? If you are given a set of bounded positive values a matrix that contain mounted positive values. How do we reduce this to a 0, 1 matrix such that the permanents are the same.

**(Refer Slide Time: 10:00)**





Handwritten notes in green ink:

Now what remains is the last part. How do we reduce Perm of  $\{0, 1, \dots, m\}$  matrix B to Perm  $\{0, 1\}$  matrix C?

Easier to view it in the graph.

Two red arrows pointing right, followed by a red arrow pointing left.

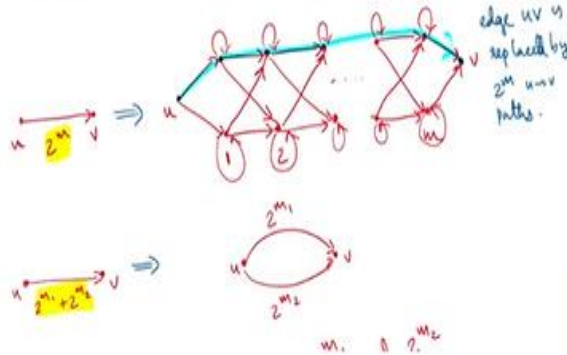



So, here the permanent needs a bit of computation but we will, here we will reduce the permanent of 0, 1 up to m matrix to another matrix C, such that the permanent of matrix C will be the same as permanent of matrix A.

**(Refer Slide Time: 10:18)**

Perm  $\{0,1\}$  matrix  $C$ !

Easier to view it in the graph.



In fact, this is slightly easier to view it in the graph setting. So, we said that the permanent corresponds to the sum of the weighted cycle covers, some of the weights of the weighted cycle covers. So, some of all the cycle covers all the weighted cycle covers where the weight of cycle cover is just the product of all the weights. So, let us see what this means? So, what we will do is, we will see how each the graph.

So, the permanent of the let us say a matrix with 0 1 up to  $m$  values corresponds to a matrix or corresponds to a graph that has edge weights 0, 1, 2, 3 up to capital  $m$ . Now we will tell we will see how each of these values are not 0 and 1, can be replaced by some gadgets or some equivalent graphs, some the parts can be replaced by equivalent graphs, which have only 0, 1 weight.

But we get the same the cycle covers will the weight of the cycle covers will be unchanged. Let us see why or how? So, suppose, so first let us see, there is a edge of weight  $2^m$ , so it means any edge need not be of this weight it could be it may not be of did not have its weight as power of 2, but let us as a first step let us see an edge of a  $2^m$ . So, now we can replace that edge with this kind of network.

So, this may look familiar to you in fact we used the same kind of, you we use the same gadget in the proof where we saw that if we are able to count the number of cycles in a graph in

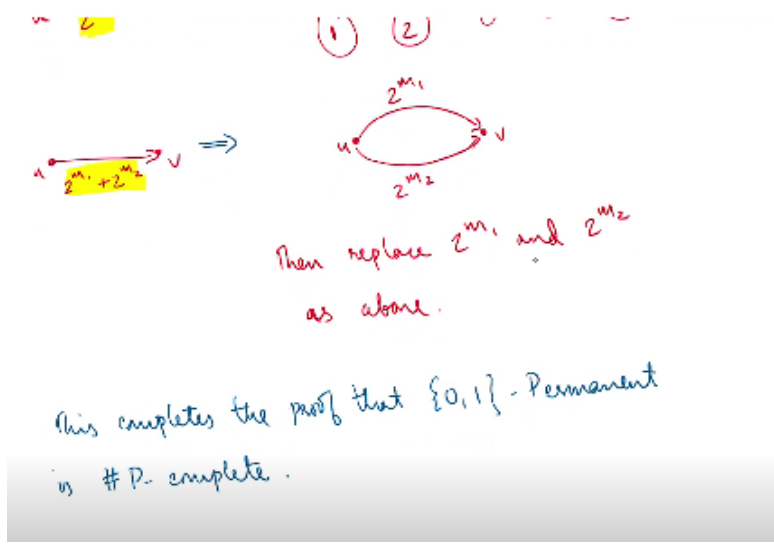
polynomial time. Then we can decide whether there exists a Hamiltonian cycle. So, we use the same idea so the point is that in now this the graph on the right-hand side, the network on the right-hand side, the same starts with  $u$  ends with  $v$ .

But look at the number of ways in which you can reach  $v$  from  $u$ , so you can see that at each there are  $m$  stages in  $m$  intermediate stages and each stage you can you have two options choose either remain on the top or go to the bottom. So, there are  $2$  power  $m$  paths in this network from  $u$  to  $v$ . So, if you replace this edge  $u$   $v$  of weight  $2$  power  $m$  with this network what happens is that any cycle that originally went through  $u$ ,  $v$  in the graph on the left-hand side.

Now there are any cycle that went through  $u$ ,  $v$ . Now there are this edge  $u$ .  $v$  is replaced by  $2$  power  $m$  possible paths from  $u$  to  $v$  and these edges these vertices intermediate vertices do not interact with anything else outside in the graph. So, any so the edge  $u$ ,  $v$  can is replaced by two power  $m$  possible paths. So, edge  $u$ ,  $v$  is replaced by  $2$  power  $m$   $u$  to  $v$  paths. So, instead of there being one cycle for which  $u$ ,  $v$  contributes to power  $m$ .

Now we have  $2$  power  $m$  different cycles each of which for which the  $u$ ,  $v$  path contributes one. So, that is how we get an equivalent representation. And here in the graph on the right-hand side all the edges have weight  $1$  and including many edges that have weight  $0$ . So, for instance this edge there is no such edge but this is like a edge of weight  $0$ .

**(Refer Slide Time: 14:23)**



So, now we have told how to, we have seen how to convert a edge with weight  $2^m$  or a power of 2 to a network to a 0 1 network with 0 1 weights. So, now what if it is not a power of 2? So, let us see it is a sum of 2, powers of 2. Let us say there is an edge with weight  $2^{m_1} + 2^{m_2}$ . What we can do is to replace? Before getting there then we may need to do one more thing because a cycle cover may not actually cover all these vertices from  $u$  to  $v$ .

Because, let us say is a cycle cover that takes this path it does not really use the bottom edges. So, what we will also need to do is to actually put self loops all over here and also in the top. So, that the edges that are not used can just participate in the cycle the vertices that are not used in cycle cover can participate using these self loops. So, now let us come back to this, what if an edge has a weight that is not a power of 2? So, let us say  $2^{m_1} + 2^{m_2}$ .

Well, what we can do is just to have see it has 2 parallel edges? And where each  $2^{m_1}$  edge of a  $2^{m_1}$  and edge of a  $2^{m_2}$  and then what we can do is to replace each of these edges with the corresponding network that we saw? So, one network which has  $m_1$  layers and one network that has  $m_2$  layers. And any number as we all know can be represented as a sum of powers of 2.

So, any positive, any non-negative weight can be represented as powers of sum of powers of 2 and consequently as a bunch of networks like this. So, that will if there is a edge of a  $w$  from  $u$  to



$v$ , then what we will do is, to replace it with a network of edges 0 and weight edges from  $u$  to  $v$ . So, that instead of there being an edge and 1 edge of weight  $w$ , now in the network there will be  $w$  possible cycle covers that take this path from  $u$  to  $v$ .

So, this is how you will of course I am just talking in the graph setting but all of this has a corresponding situation or corresponding equivalent in the matrix situation as well. So, this is how we can replace an a matrix  $b$  which has 0, 1, 2 up to  $m$  values, to a 0, 1 matrix. So, here both  $2^{\text{power } m - 1}$  and  $2^{\text{power } n - 2}$  will be replaced by 0, 1 a network that has only 0 1 weight edges. And that completes the proof.

So, that is the last part that we had left that completes the proof that 0, 1 permanent is sharp P complete. So, even permanent even restricted to 0 1 values is sharp P complete. So, this is variance theorem from 1979 that even permanent, so permanent one may think that permanent is not such a difficult problem because permanent is just corresponds to the counting of the number of matching's in a bipartite graph.

So, the decision version of the problem is easy, just like we said about the number of counting the number of cycles. However, we see here that the counting version of the problem, counting the number of perfect matches in a bipartite graph. This is sharp P complete, meaning you take any problem in sharp P then you can reduce to permanent. So, with that I can conclude this lecture and thank you.