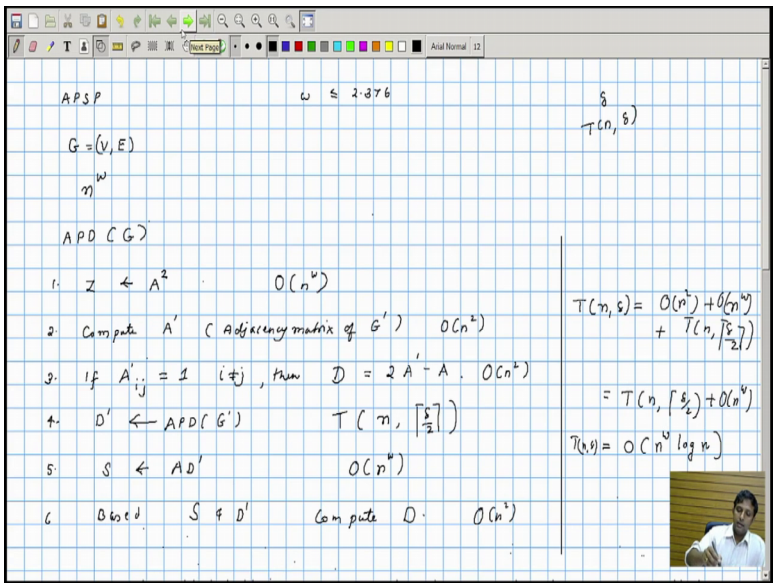
Randomized Algorithms
Prof. Benny George Kenkireth
Department of Computer Science & Engineering
Indian Institute of Technology, Guwahati

Lecture - 27
All pair shortest path-II

(Refer Slide Time: 00:28)



We were learning about the All pair shortest path point where in the input has a graph and we want to compute the shortest distance given any two pairs points and we want to do this for all points and we want to do it in sub cubic time. We assumed that omega is the exponent of matrix multiplication which means the fastest algorithm can do it in n to the power of beta. So, based on that currently omega is known to be less than 2.376 and based on matrix multiplication we want to compute all pair shortest path.

And what we have achieved so far is we looked at all pair distance problem and we developed an algorithm to solves a deterministic algorithm which can compute the distances between any two pair of paths. And the method was you will first compute Z which is the square of the adjacency matrix of G. And then compute the adjacency matrix of G prime where G prime is square of G ok.

And this could be done by looking at Z and the adjacency matrix of A and if A prime is the adjacency matrix of the complete graph, then from that we will recover D. So, if A prime i comma j is equal to 1, for all i not equal to j; then we argued that the distance

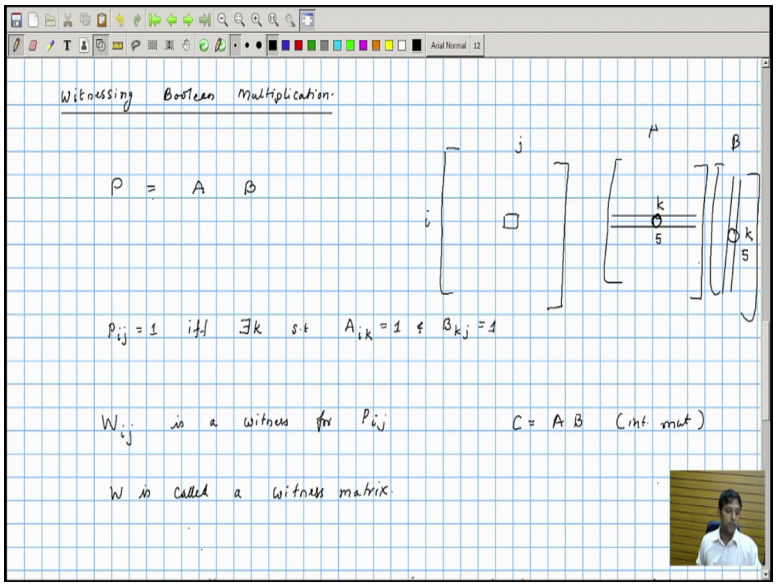
matrix will be equal to twice A prime minus A. If this is not then we have to do further computations recursively; so if graph G, then we will compute the all pair distance for G prime; we make a recursive coming this is let us say D prime. We compute S as A D prime and based on S and D prime, compute D found the distance between any two pair of paths.

And this algorithm can be analyzed easily; the first step requires order n power omega because it is a matrix multiplication. The second step looks at all entries in both Z and A; so that would take O n square. The third step would also take O n square; the fourth step it will take time proportional to the diameter of the graph. If the diameter was delta and if the takes T n delta; G prime is a graph whose diameter is at most half of the original diameter.

So, this step would take recursively T n delta by 2 sealing of this; this is another matrix multiplication; so this will take O n to the power omega. And once S and D prime are there you can easily compute D and that you take O n square. So, the entire relation can be rewritten as and the recurrence relation or the time taken and the computed as T n delta that is equal to O n square plus 2 matrix multiplication. So, we can say plus n to the power of omega O n to the power omega plus T and delta by 2 and omega certainly is greater than or equal to 2.

So, n to the power of omega subsumes O n squares. So, this T n delta by 2 plus O n to the power omega and so the overall running time would be is and say T n delta is going to be O n to the power omega log n ok. So, that is the running time of the algorithm that computes the distances between every pair G. Now, based on this algorithm we are now going to develop a randomized algorithm which will compute the shortest distance path between any two pair of paths.

(Refer Slide Time: 05:44)



So, in order to do this we will look at a related problem called as witnessing Boolean multiplication. So, first we will understand this problem and then we will think about the relevance of this problem to all pair shortest paths. So, let us look at a matrix P which is a product of two Boolean matrices A and B. So, if you look at the i jth entry of P; this entry is going to be 1 if and only if there is an entry in A and an entry in B which multiplies it will be C 1.

In other words P i j is equal to 1 if and only if there exists k such that A i k is equal to 1 and B k j is equal to 1. So, if you look at the ith row of A and jth column of B and multiply them out; what you get is the i jth entry in P and this multiplication is Boolean multiplication ok. So, this is going to this multiplication is going to give you 1, if and only if at the kth position of this row and the kth position is to column; you have 1. And such a k we will call it as a witness for P i j equals 1 ok. So, if this position was 5 and we will say 5 as a witness for P i j.

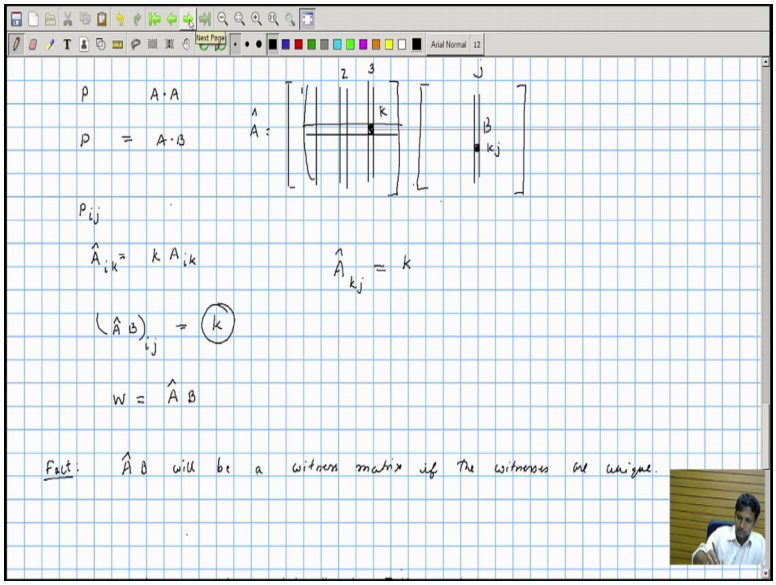
But there is no witness then you will say with the witness is 0; a few index the rows and columns by 1 to n; then if there is an index that is denoted by a number from 1 to n. If there are no if there is a witness it is indicated by a number between 1 and n, if there are no witnesses that is indicated by 0. So, such a matrix consider a matrix W such that the i jth entry is a witness for P i j ok. So, P i j could be 1 in that case W i j would be a positive

not a positive integer; if P i j is 0 the W i j would be 0 such a matrix is called as a witness matrix W is called a witness matrix.

So, in every entry in W; the i jth entry in W you will have a number and that number indicates which positions in A and which positions in B are to be in multiplied. There are n positions in A, where which you could multiply with n positions in B so that you will get 1. Out of this the correct position there might be many such, but each correct positions called a witness and a matrix which carries all this information is called as the witness matrix.

Note that if you know the witness matrix then you can quickly compute the product because if the witness is a 0 value, the value of W i j is 0 and in order to products will be 0. And if it is nonzero then you can look at that particular position and compute the product and product is going to be 1. And if you just multiply the matrices A and B; instead of doing Boolean multiplications, if you just multiply them about as integers then the matrix that you get it is C is the multiplication, the integer multiplication C i j will basically denote the number of witnesses.

(Refer Slide Time: 10:35)



Now, you look at this matrix P obtained multiply A with itself. So, suppose A as the adjacency matrix or some particular graph and P equals A square. So, if you multiply A and A as Boolean numbers, as if you carry out the Boolean multiplication of these

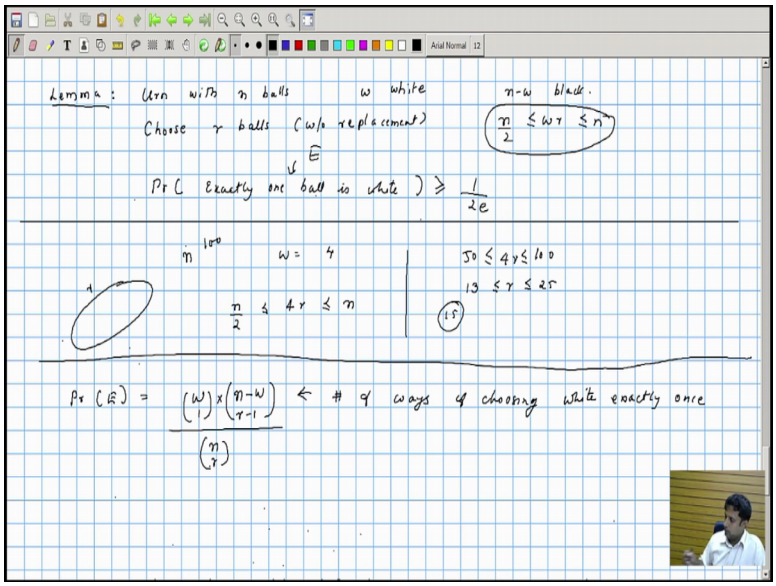
matrices A and A; P i j is 1; if and only if there is a path of length 2 between i and j in the graph.

Now, let us consider one interesting case where two matrices are such that there is a unique witness for every entry. So, you have these two matrices A and B and then you multiply them do Boolean multiplication obtain the product P. If you look at P i j suppose every i and j has a unique witness. In this case we will argue that the witnesses are we can easily compute the witness matrix ok; the way to do this would be you can verify this fact.

So,. So, define A tilde i k as k times A i k; in other words look at the matrix A; the first column you multiply with 1, the second column you multiplied by 2, the third column will multiplied by 3 and the matrix resultant matrix is what we call as A tilde. Now, if you multiply A tilde with B let us look at the i jth entry. So, this when you multiply with the matrix B; suppose you look at the i jth entry, now i jth entry is obtained by multiplying the ith row with the jth column. Now since the witnesses unique there is some particular position here unique position k such that this k when multiplied by B k j will give you 1.

Since there is a unique witness when you multiply; these the k jth entry of A tilde k j will be equal to k. And therefore, A tilde B will be; so, for there is in the i jth entry will be equal to k and k is a exactly the witness. So, if you take W is equal to A tilde times B; this W will be a witness matrix ok. So, we will write it as a fact; A tilde B will be witness matrix; if the witnesses are unique ok. So, we have solved one particular case of computing Boolean product witnessing matrices ok. So, such a matrix would be called as a Boolean product witnessing matrix and those matrices can be computed if witnesses are unique.

(Refer Slide Time: 14:27)



Now we want to bother about the case with the multiple witnesses and this is precisely where randomness would come in handy; so, we will first state a lemma which will help us in this analyzing the randomized algorithm. So, imagine that there is a urn with n balls; out of which w are white and the n minus w are it is a black ok. If you choose r balls at random without replacement and all sources are equally likely. And this r as special value such that w times r lies between n by 2 and n; this is the case and probability that exactly one ball was white, this event happens with probability greater than 1 by 2 e.

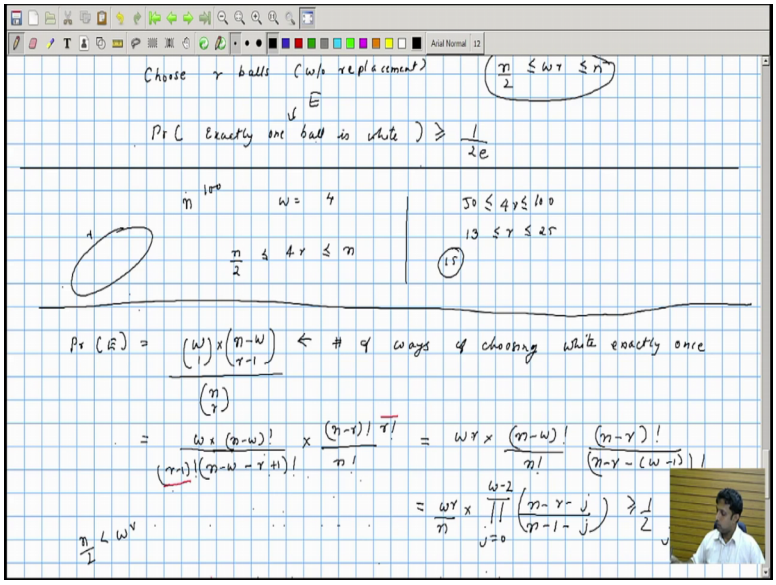
We have chosen a set containing r balls and if this r satisfies this particular equation, then with probability greater than 1 by 2 e; there will be exactly one white ball in this collection ok. So, suppose the number of white balls were 4 and the number of balls were 100; if you choose between if you choose r balls. So, r has to satisfy the following equation n by 2 should be less than 4 r and less than n; so here 4 r should lie between 50 and 100; in other words r should lie between 13 and 25.

So, let us say you pick 15 balls. So, there were 4 white balls and if you are picking something like 15 balls; then there is at least 1 by 2 over e probability that you will choose exactly one white ball. We will prove this theorem the proof is fairly simple; it is just a counting the total number of ways in which you can pick r balls such that exactly one ball is white; that divided by the total number of ways in which r balls could be

picked. So, if you call this event as e; probability of e is equal to number of ways in which you can choose exactly one white part.

So, that w you choose 1 this number of ways in white balls should be picked and the remaining balls would be picked in they have they all have to be black. So, n minus w choose r minus 1 is the total number of ways white exactly once. And this should be divided by the total number of ways of choosing r balls; that would be n choose r and this probability we need to show that it is greater than 1 by 2 or itself slightly; involved calculation.

(Refer Slide Time: 18:40)

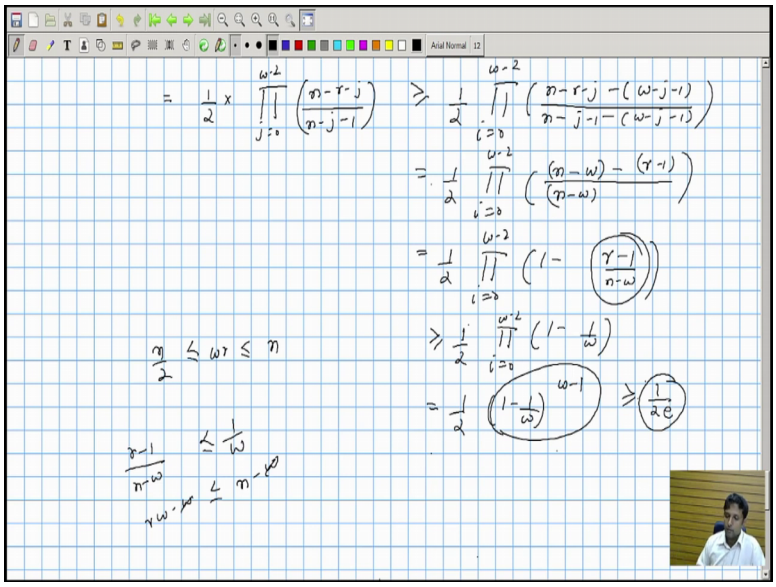


So, w choose not as w into n minus w factorial divided by n minus w minus r plus 1 factorial into n factorial minus r factorial r factorial ok. So, this is equal to; so there is an r minus. So, n 2 is n minus w you choose r minus w is n minus w factorial by n minus w minus r correspond into r minus 1 factorial. This will give us w into r minus 1 factorial and r factorial cancels out giving r and the remaining we can write it as n minus w factorial divided by n factorial. This is going to contain something like w terms; w minus 1 and then n minus r factorial divided by n minus r; minus w minus 1 factorial that is also containing of a w terms.

And this can be even rewritten as w r by n into product j going from 0 to w minus 2; n minus r minus j divided by n minus 1 minus j ok. So, this is a product of w minus 2 terms and those W minus 2 terms we will bound it by some particular quantity and it is a

product of W minus 2 terms that is going to go towards 1 by e. And w r by n because n by 2 is less than w r; w r by 2 is going to be greater than half into this particular product, j going from 0 out of w minus 2 n minus r minus j divided by n minus 1 minus j.

(Refer Slide Time: 21:25)



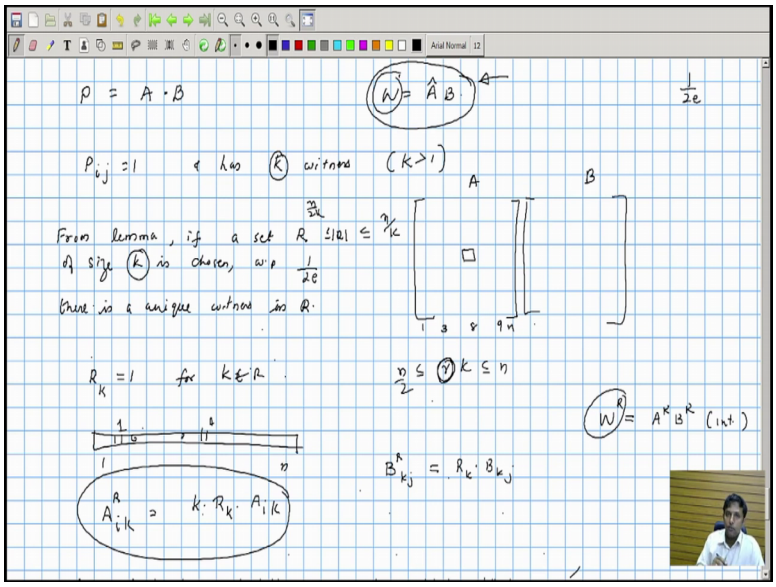
So, the expression that we have this half into some product involving w minus 1 term j going from 0 to w minus 2; n minus r minus j divided by n minus j minus 1 ok. So numerator and denominator which you subtract some equal quantity from that; this quantity would still be greater. So, this is greater than half into product over w minus 2 terms n minus r minus j minus w minus j minus 1.

So, w minus j minus 1 to subtract both denominator and numerator n minus j minus 1 minus w minus j minus 1 ok; so that is going to be equal to half into product i going from 0 over to w minus 2; n minus w minus r minus 1 divided by denominators would be n minus w. So, this is going to be half into product i going from 0 to w minus 2; 1 minus r minus 1 by n minus w. We had this inequality that W r lies between n by 2 and n ok. So, r minus 1 by n minus w is going to be less than 1 by W that is clear because this just means r w minus w is greater than or equal to n minus w this is true ok.

So, this quantity here is been be less than 1 minus w; you may subtracting in order that inequality reverses. So, this may be greater than or equal to half into product pi i equals to be 0 pi i equals to 0 to w minus 2; 1 minus 1 by w and that is half into 1 minus 1 by w raised to the w minus 1 and this expression we say that it is always greater than 1 over e.

So, this is greater than 1 by 2 over e. So, what this means is if you choose r balls without replacement from a collection of n balls; out of which W were white and if it satisfies this particular relation, then the probability 1 by 2 e; exactly one ball is white. Now if you repeat this log n times or suitable number of times; then you can ensure that at least one of those trials will result in a pick of r balls, where exactly one of them is white. So, let us see how do we use this particular lemma.

(Refer Slide Time: 24:28)



So, we had this particular product P is equal to A comma B; A times B this is the Boolean product. And we know that if all entries of P had unique witness elements; then they can easily be computed because the witness matrix can be written as A tilde B. Imagine that there is an i jth entry; so P i j this 1 and has k witnesses. We can assume that k is greater than 1 k is at least 2; this is something you can assume. Because all the elements which are exactly one witness can be calculated by this; so compute this and check for the entries from that we can from this witness matrix, we will figure out all the entries which is exactly one witness more than one it might not correctly identified ok.

So, we can look at only the remaining elements for the remaining elements look at any other element which is more than one witness. Now what we will do is the following we had these matrices A and B; we will choose some random subsets of A and B. So, let us say out of these 1 to n columns; we will choose some of them and the rest we will make it as 0. So, if I take let us say 1 3 8 and 9 and rest everything has made 0.

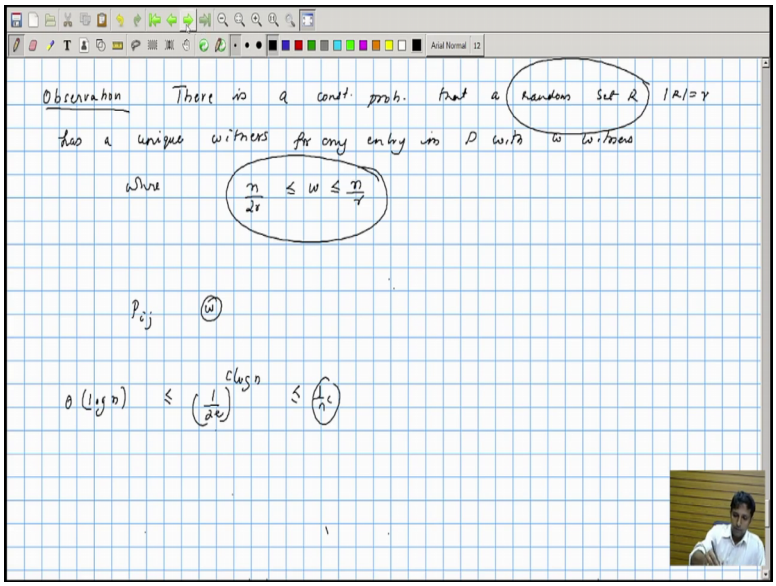
Now, will this matrix have unique witnesses; our previous lemma says that in any witness that was originally there might be k witnesses, but if we choose r and the number of 11 number of rows that we pick from A and the number of columns we pick from B; that number r is chosen in such a way that r times k lies between n by 2 and n, then we know that with probability 1 by 2 e there will be a unique witness and if there is a unique witness we can easily identify it.

So, more completely from our lemma; if a set R of size k is chosen with probability 1 by 2 e; with a with probability at least 1 by 2 e, there is a unique witness in R ok; there might be many witnesses for a particular entry. But if the particular entry has k witness and if we choose a set R; whose size R lies between n by 2 k and n by k, then amongst the set with probability 1 by 2 e; there is a unique witness ok. And how do we find that witness? We can think of this incidence matrix; so R k is equal to 1 for k belonging to R.

So, you have some particular set; if all this questions 1 to n whatever was chosen in r those you set to one and the others you set to 0. And now if we look at the matrix A ok; so you can look at the matrix obtained from A named as A R and A R is equal to k times R k times A i k. So, the i kth entry of A R; so just set like this the i kth entry of A R is said to be k into R k times A i k; this is similar to the witness matrix construction when there was unique matrices ok. You can check that suppose define another matrix B R, which is choosing the corresponding columns in B.

So, B k j will be equal to R k into B k j. So, if you look at these matrices and if you look at the matrix W R which is equal to A R into B R and this B integer multiplication, this W R will contain witnesses for all those i j's which has a unique witness in R.

(Refer Slide Time: 30:00)

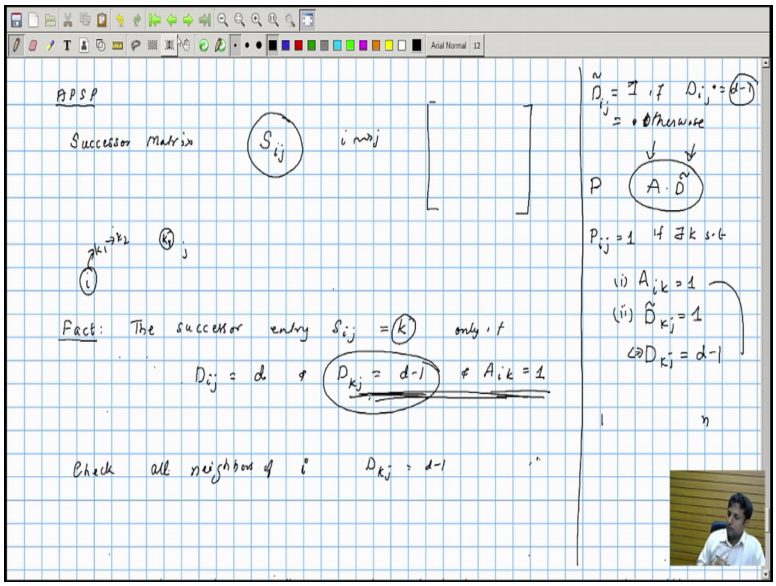


Or we can summarize witness by the following the observation; there is a constant probability that a random set R of size smaller has a unique witness for an entry in P with w witnesses; where n by 2 r is less than w is less than n by r.

So, you look at any particular entry in P i j which is w witnesses a random set of size r which satisfies this particular relationship will have a unique witness with a probability equal to 1 over 2 e; which is a constant probability. Now if you repeat this for log n steps O of log n steps; then the probability that you do not get a unique witness in some particular random set; that is going to happen with probability less than 1 by 2 e raised to log n which will be less than 1 by n.

So, that is that is a you can repeat the algorithm some number of times if you want it to be 1 by n square, you can run it c log n times. So, repeatedly run the algorithm; form keep on repeatedly choosing random sets of size r, one of those random subsets will contain a unique witness. And if there is a unique witness immediately our earlier observation will tell us that the unique witness can be identified by computing A tilde B.

(Refer Slide Time: 32:37)



So, what we have achieved so far us if there is a unique witness, we can identify that. Even if there are multiple witness all those multiple witnesses can be identified; I mean all I mean amongst the multiple witnesses one witness can be identified by randomly choosing subsets of 1 to n. So, now if you have solved this particular problem we will see how we can determine the all pair shortest paths using this particular algorithm.

So, what we are interested in is given in a particular i j; we need to compute the shortest path between those points. What we will see is if we know the length of the shortest path, then it is easy to find the path itself you will see how this is done. So, we will need something called as the successor matrix; let us call the successor matrix as S and then S i j will be the successor of i and the path from i to j.

So, i to j there is a shortest path; in this shortest path what is the element that follow immediately comes after i? That is one as a successor let us; so this information stored for all possible i and j will be called as a successor matrix. So, if you are given the successor matrix from the successor matrix one can easily compute the path. For example, if you want to go from i to j go to the successor matrix look at the i jth entry that will give you k 1.

And now look at the successor matrix for the entry k 1 j that will give you k 2 and at some point this will give you k r such that k r k j is connected by an edge ok; so that would be the complete path. So, if you know the successor matrix from that one can

decipher what is the shortest path and this deciphering takes time proportional to the length of the path. If the path is long and of course, describing that path takes long time, but the point is the path can be described in time proportional to the linearly proportional to the length of the path.

Now, how do we compute this particular successor matrix? So, it is in computing the successor matrix that the witness matrix problem was going to help us. So, let us see what will try to understand what is the successor of i j and the what relationship does it have to the distance matrix ok. So, this is the crucial fact that we will be using the successor entry S i j is equal to k only if distance between i and j this D i j is equal to small d; so some particular d.

And D k j is equal to d minus 1 and A i k should be equal to 1 ok; look at the successor entry corresponding to i j. If it is k and; that means, k has to be a neighbor of i and the distance from k to j should be equal to D minus 1. If these two conditions are satisfied; then k is a valid successor entry that would be multiple such k, but we are interested in just finding one of them.

So, if we can find such an entry such that it is a neighbor and its distance is D minus 1; then we can compute, the successor matrix. Well we can look at all possible neighbors of i so that would be the naive algorithm check all neighbors of i ok. And whichever is connected to i and is of and distance k j; if it is equal to D minus 1 you can include that are successor.

But this requires you need to compute S i j for n square entries. So, each of these if it takes linear amount of time; the total complexity is going to be n cube. So, we cannot really check all possible neighbors we need to find some way out. Basically what this mean is the following; this is like a matrix multiplication A i k and D k j must multiply and give you 1 or should give a nonzero entry.

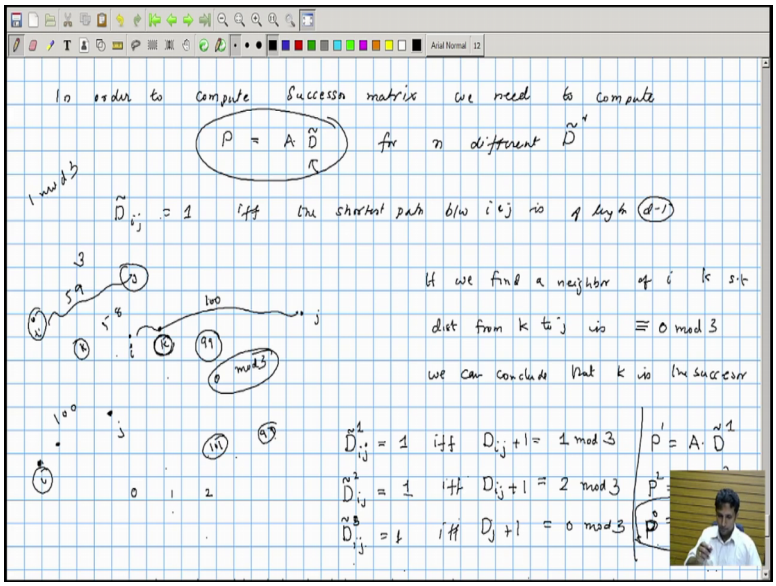
So, let us consider a matrix D tilde which is equal to I mean D tilde i j is equal to 1 if and only if D i j is equal to D minus 1. In other words all pairs of points which are separated by a distance D minus 1 gets a 1 and the others gets 0; 0 otherwise. And if you multiply two such matrix matrices and then if you get a 1; that means, both these conditions are met A i j is equal to 1 and B k j is equal to d minus 1.

Look at a times D tilde and look at the i jth entry ok. So, if you call this as the matrix P; P i j is equal to 1 if and only if there exists a k such that two conditions has to be it. First A i k should be equal to 1 and second condition D tilde k j should be equal to 1, but D tilde k j is equal to 1 only if this is equivalent to D k j equals d minus 1.

So, this is precisely the condition that is required it. So, if this matrix product may comes if P i j equals 1; then it essentially says that this condition has been checked. So, how do we check of P i j equals 1 ok? That is where we will use the witness matrix we will compute the witness matrix for a and D tilde. Once we compute the witness matrix for A tilde a D tilde using our previous algorithm, we can completely figure out what is the successor matrix.

But again we need to construct these witness matrices for every value of d. So, d could vary from 1 to n and there are too many of them to be compute. What we will see is that why have a clever observation instead of computing n different matrices of the form D tilde; we will just compute 3 matrices.

(Refer Slide Time: 40:44)



So, let us see there we are at the (Refer Time: 40:48). So, in order to compute successor matrix; we need to compute P equals A into D tilde for n different D tildes ok. So, here D tilde is a matrix whose i jth entry is equal to 1; if and only if the shortest path between i and j is of length d minus 1. So, for each such length there was a different D tilde; we should call it as D tilde, r there r varies from one to D to n minus 1 ok. So, if we compute

these products; from those products we can compute the successor matrix. But in order to compute those products we will basically compute their witness matrices; witness matrices can be quickly computed that is what we learnt earlier.

Now, but there are too many witness matrices to be computed instead of computing n of that we will reduce problem to computing just 3 witness matrices. So, do we really need to know this for all values of d? So, let us look at the following problem. So, here is a vertex i and here is a vertex j and we know that the distance between them is it is a 100. We want to know if there is a vertex k; there is a neighbor k such that the distance from k to j is 99.

We find a vertex whose distance from whose distance to j is 99; then we and they are connected to i then we know that the successor is k. But do we need to know this that it is 99; as long as we know that it is 0 mod 3, we are on good ground ok. So, if we find a neighbor of i and the column neighbor as k such that distance; it is the shortest distance from k to j is congruent to 0 mod 3.

We can conclude that k why is this so? If you compute the distance and compute the mod 3 value for that; if it is 1, then it has to be either 100 or 100 and 3 and so on or 97 and so on and none of those elements can be neighbors of i. So, the distance from the shortest distance from the neighbors of i to j has to lie between 101 and 99.

And second if you look at any vertex and look at any of its neighbors all the neighbors will have; you need to compute the distance from those neighbors to j that is going to vary by at most 1; to be plus or minus 1 or 0; so, there are only three possibilities. So, if you could identify the distance mod 3 that is sufficient ok. So, instead of computing D tilde for all the possible distances; we need to compute D tilde only for three values namely what we need to look at the distance matrix and look at the distances mod 3. And as long as the modulus value 0 1 and 2 these are the only information that is required ok.

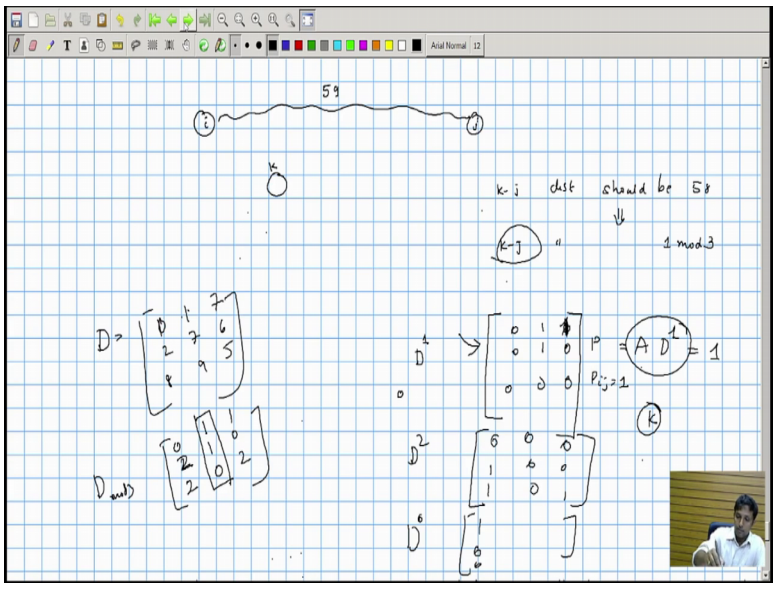
So, we can define 3 matrices called let us say D tilde 1 such that you can define 3 matrices let us call it as D 1; D tilde 1 and this is equal to 1 if and only if. So, look at the i jth entry the i jth entry is 1 if and only if the i jth entry of D plus 1 is equal to 1 mod 3 and D tilde at 2 i j is going to be 1; if and only if D i j plus 1 is equal to 2 mod 3 and D tilde 0 or tilde 3 i j is going to be 1 if and only if D i j plus 1 is equal to 0 mod 3 ok.

So, we can compute these 3 matrices directly from D i j and you can use these matrices and compute the witnesses corresponding to this ok; we can define witness matrices. So, will look at the product P 1 is equal to A into D tilde 1; P 2 is equal to A into D tilde 2 and P 3 P 0 is equal to A tilde 2. So, we define these 3 matrices and note that if P 1 and suppose you want to know whether there is a path between i and j; suppose we suppose somebody tells you that from i to j the distance is 100 how do you find the successor of i ok?

So, since the successor has to have distance of 99 that would mean that the distance mod 3 should be 0. So, you will look at this particular matrix, this particular multiplication P 0 is equal to A into D tilde 0 and in that you look at the witness entry. So, compute the witness for this particular matrix multiplication and that witness will in fact, be the successor of i ok.

So, again if i for example, is 1 0 1; so i is some particular vertex and distance to some particular vertex j is let us say 58; the successor should be take another example; if i to j distance this 59 then the successor was that entry such that successor is that particular vertex such that the distance from k to j will be 58; k to j distance additionally should be if it is 58 it is certainly 1 mod 3 ok. So, you look at all the distances that all the i j entries such that the distance is are 1 mod 3 and amongst these you should have a witness for.

(Refer Slide Time: 49:22)



So, let us relook the entire thing once again there is some particular entry i and that is another entry j and the; you know that this length is 59; you are required to compute a successor. So, the successor is some particular entry k; what do we know about k? k j distance should be 58 that will also mean that k j distance is 1 mod 3.

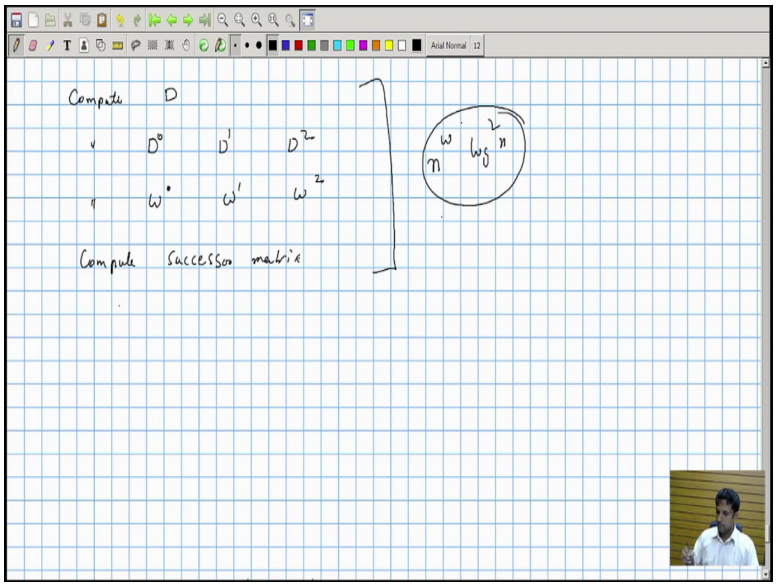
So, if you look at this matrix where all the distances this matrix if you look D 1 which records all the distances, but now mod 3 and all the entries other than the 0 i mean other than 1 are changed to 0. So, if there was if you looked at particular matrix D with values 1 to 8 ok. This was your D, look at all entries right down the mod 3 value ok. So, D mod 3 you will get some particular entries 0 2 2, 1 1 0, 1 0 2.

And D 1 is that matrix that you get by removing everything which is not 1 ok. So, all the 1's are kept as it is and everything else is replaced by 0's. So, 1 1 1; if you look at D 2 that is the matrix that you get by replacing the 2 with 1 and everything else 0s. And if you look at D 0; the 0s are replaced by 1, everything else is replaced by 0 ok.

So, k j should be 1 mod 3. So, you look at this matrix and you will compute the product A A D. So, A D 1; if this is equal to 1 what it means is there is a path means P is this product if P i j equals 1; that means, i to j i mean there is a k such that i to k there is a there is a directed. And from k to j there is a path whose length is 1 more than a multiple of 3 and that is a valid successor. So, this k can be chosen as a successor and this k is basically a witness.

So, for this particular product compute the witness using the randomized algorithm; once witnesses are found you can compute the I mean once witnesses are found compute the successor; successor can be we used to compute the shortest path between i and j. You can verify that this basically involves few matrix multiplications and success.

(Refer Slide Time: 52:52)



So, the first step would have been we had to compute the distance matrix. So, compute the distance matrix it is the first thing and then we had to compute D 0 D 1 and D 2 and then we had to compute witnesses W 0, W 1, W 2. And once this are computed, we could compute the successor matrix. So, all these steps you can do it in time n raised to w log n square. So, this is going to be the maximum time taken to perform all these operations ok. So, that is a sub cubic algorithm for all pair shortest paths we will stop here.