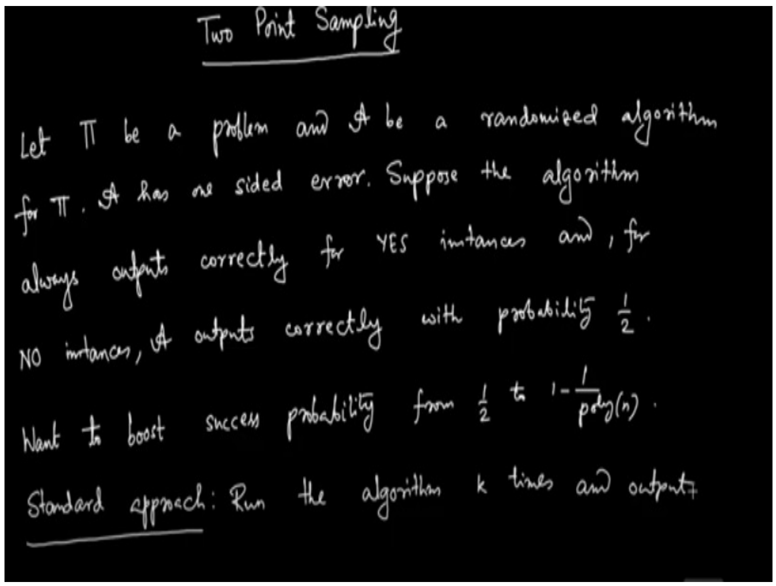
Selected Topics in Algorithm
Prof. Palash Dey
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Module No # 04
Lecture No # 19
Two Point Sampling

Welcome so in the last couple of lectures we have been studying concentration bounds and their applications. So today we will continue that and our topic is two point sampling.

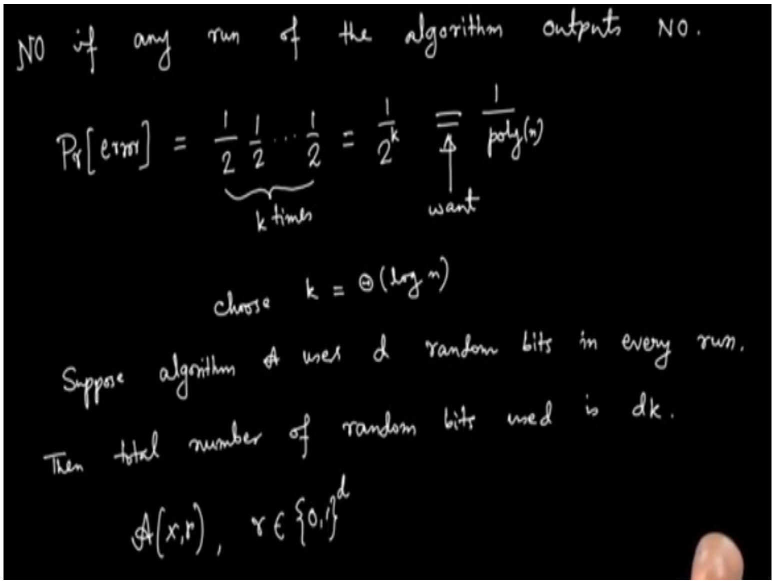
(Refer Slide Time: 00:041)



So here is the setup let pi be a problem and A be a randomized algorithm for pi. A has one sided error so it is an algorithm like for bit or for mean cut and this sort of algorithm it is not a quick sort kind of algorithm. It is a Monte Carlo type of randomized algorithm it makes error but it has one-sided error. So suppose that means the algorithm always outputs correctly for YES instances and, for NO instances, A, outputs correctly with probability say 1/2.

Now what we want is? We want to boost the success probability from half to say 1 over polynomial in n. So want to boost success probability from half to say 1 by some polynomial in n 1 -1 by polynomial in n. Now the standard technique is by repetition so standard approach run the algorithm k times and output NO.

(Refer Slide Time: 05:24)

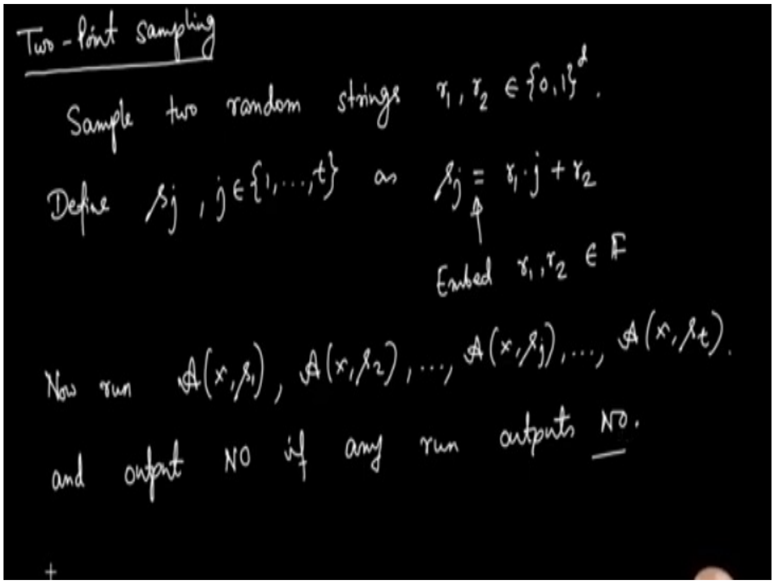


If any run of the algorithm outputs NO because when if the instance is YES then it will always output YES but for NO instances it can make error and output YES that is what we have assumed. So whenever it outputs NO that means we can say it for certain that it is the instance is indeed a NO instance. So now what is the error probability so for YES instances the error probability remains 0 it will always output YES but for NO instances the error probability will now reduce probability of error is now $1/2$ and it makes error for NO instances.

It will make an error only if it every k independent runs output wrongly so in the first run it makes error with probability half and it should make an error with in every run so this half times half this k times $1/2^k$. Now if you want to make error probability if you want there are probably to be 1 over say poly n is what we want then choose $k = \Theta(\log n)$. Now so what is the total number of random bits used?

So suppose algorithm A uses d random bits in every run then total number of random bits used is d times k using two point sampling. We will achieve this error probability of 1 over poly n by using only 2 d bits and that is the technique we will see now so what is two point sampling is? What it does is that?

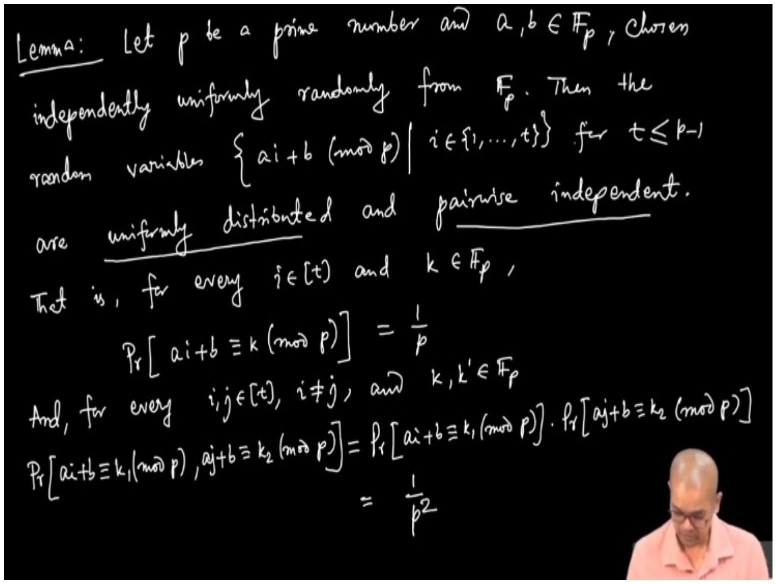
(Refer Slide Time: 09:22)



So two point sampling so we can denote the algorithm A as takes 2 inputs x and r where r is a random string 0, 1 of length d. So the so the idea of two point sampling is sample or two random strings r_1 and r_2 d bits long and again now generate some pseudo random strings. So define you know s j in say 1 to t as $s_j = r_1 j + r_2$ more formally we can assume r_1, r_2 to belong to some field.

So for this to make sense embed r_1, r_2 in some field if map each debit string to a field and this can be embedded and once you have filled you can do the multiplication and so $r_1 j$ is adding $r_1 j + r_2$. Now run A this algorithm A on input is down input x with random string $s_1, s_2, \ldots, s_t$ now run this algorithm but these are not completely independent runs because you know s_1, s_2 these are the random strings are generated using r_1 and r_2 and we run this and output NO. If any run outputs NO now let us do the error analysis but for that we need to prove a Lemma.

(Refer Slide Time: 13:36)



Let me prove that first because now you know this analysis is not applicable because you know each run is not completely independent what we will show is that they are what is called pairwise independent each i, s_j are pairwise independent. So for that let us see. So let p be a prime number and I take 2 elements $a, b \in F_p$ this is the field F_p and A, and B are chosen independently uniformly randomly from F_p think of A and B are like r_1 and r_2.

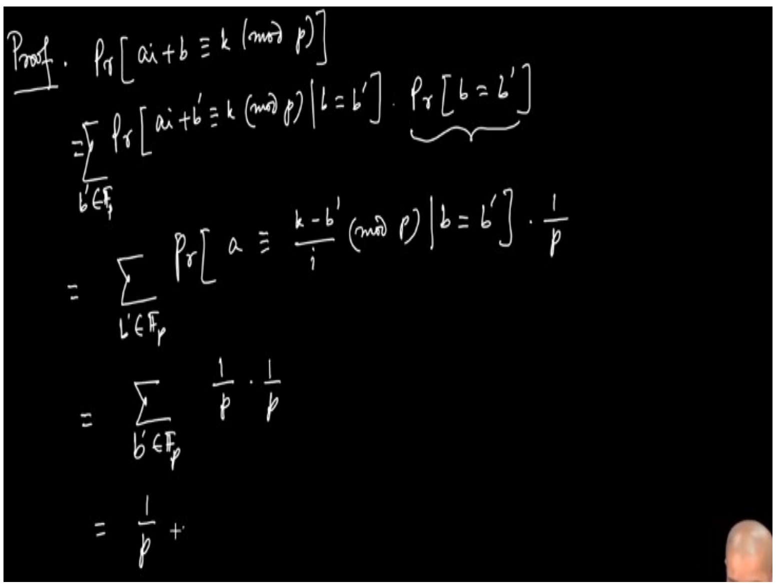
Then the claim is then the random variables so A, and B are random variables, then the random variables you know $ai+b$ and here addition multiplication everything F_p happens mod p that is how this addition and multiplication is defined in this field F_p where i varies from 1 to t. Then this random variable for t less than p -1 less than equal to, p -1 are uniformly distributed and pairwise independent that is what does this mean? Now I will write it in precise mathematics mathematical term.

What does uniformly distributed and pairwise independence mean? That is for every i in t and k in F_p we have probability that $ai+b$ is congruent to k mod p. This is the value that the i th random variable takes and the claim is this is uniformly distributed over F_p if it has p many elements and it is one of those elements namely k this probability is $\frac{1}{p}$ that is what uniform distribution mean.

And now we mathematically state what does pairwise independence mean and for every $i, j \in [t], i \neq j$ and $k, k^{'} \in F_p$ what we have is probability of $a i + b$ congruent to k_1 mod p and $a j + b$ congruent to k_2 mod p these treatments are independent that means they multiply can write it as probability $a i + b$ is congruent to k_1 mod p times probability $a j + b$ is congruent to k_2 mod p. Now each of this probability because of uniform distribution is $\frac{1}{p}$.

So this is $\frac{1}{p^2}$ so these are the claim which we will prove now and then once we after proving we will see how this helps in boosting our success probability.

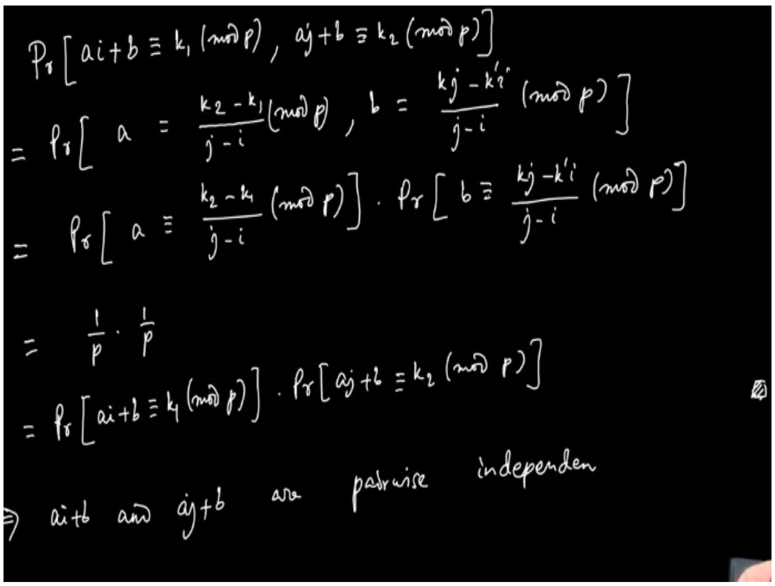
(Refer Slide Time: 19:59)



So proof first the uniform distribution we need to prove $a i + b$ is congruent to k mod p is can be written as probability we condition over b. So sum over $b^{'} \in F_p$ what value $b^{'}$ takes $a i + b$ it what value b takes k mod p given $b = b^{'}$ times probability $b = b^{'}$. Now this probability is $\frac{1}{p}$ and what is the first probability the first probability is $b^{'} \in F_p$ probability that e is congruent to $k = \frac{b^{'}}{i}$ mod p given be equal to $b^{'}$ and probability of $b = b^{'}$ is $\frac{1}{p}$.

Because b is picked uniformly randomly from F_p now $\frac{k-b'}{i}$ this is a constant and again because a, is picked uniformly randomly from F_p the probability that a, is this particular value $\frac{k-b'}{a}$, is again $\frac{1}{p}$. This is $\sum_{b' \in F_p} \frac{1}{p} \times \frac{1}{p}$ which is $\frac{1}{p}$ which concludes the proof the first part that it is uniformly distributed.

(Refer Slide Time: 22:22)

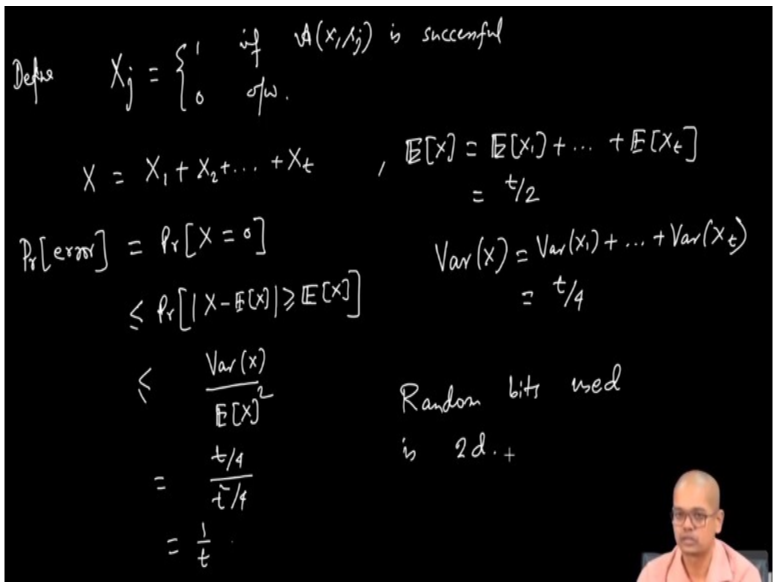


Now come to the second part that they are pairwise Independence probability that $ai+b$ is congruent to what is the notation we used k_1 and k_2 congruent to k_1 mod p and $a\,j+b$ is congruent to k_2 mod p. Now we use that F_p is a field so we can solve these 2 equations $ai+b=k_1$ and $a\,j+b=k_2$ where using treating a, and b as variables. So this is same as this probability is probability that e is what a, is $\frac{k_2-k_1}{j-i}$ mod p and b is $\frac{kj-k'i}{j-i}$ mod p.

All you need to do is to solve this two linear equations with 2 unknowns a, and b treating a, and k_1 and k_2 as constants. Now a, and b are uniform are independent they have been picked uniformly and independently. So this can be written as probability that a, is congruent to $\frac{k_2-k_1}{j-i}$ mod p times probability b is congruent to $\frac{kj-k'i}{j-i}$ mod p. Now each a and b are uniformly distributed so is $\frac{1}{p} \times \frac{1}{p}$ and this is this follows from first part that $\frac{1}{p}$ is probability that $ai+p$ is congruent to k mod p and $aj+b$.

This k_1 and k_2 mod p congruent to k_2 mod p this is using first part that no the, $ai+b$ these are this part that $ai+b$ is also uniformly distributed over F_p so this concludes the proof that means hence $ai+b$ and $aj+b$ are pairwise independent.

(Refer Slide Time: 26:25)



Now it is very easy so then define X_j to be 1 if the run of the algorithm with X and s_j is successful and 0 otherwise and define x equal to $X_1+X_2+...+X_t$. So probability of error is probability that X is 0. And what is expectation of X? Expectation of X is by linearity of expectation of $X_1+...+$ expectation of X_t and it succeeds with probability half. So suppose the input instance is a NO instance because if it is YES instance it does not make an error suppose if input distance is a NO instance so it is successful with probability half this sum is $\frac{t}{2}$.

So probably this can be less than equal to probability that X - expectation of X is greater than equal to expectation of X. Now; using Chebyshevs formula this; is $\frac{var(X)}{E[X]^2}$ now what is variance of X? Here now we use the pairwise independence property of $X_1, \ldots, X_t$. Because they are pairwise Independence they are covariance terms vanishes they are 0. So variance of X is simply variance of X_1 + variance of X_2 up to variance of X_t now variance of X_1 is a binary random variable with parameter half so each variance is $\frac{1}{4}$.

So this is $\frac{t/4}{t^2/4}$ this is $\frac{1}{t}$ so to make the error probability log n 1 over polynomial in n. All we need to do is that we sample 2 random Boolean strings and generate this n many or poly in many this pseudo random strings s_j s for you can choose t to be poly n and using this only with 2 random bits 2 random strings. We are able to achieve error probability 1 over poly n so with or let me write random bits used is 2 d it is just r_1 and not 2 so we will stop here today.