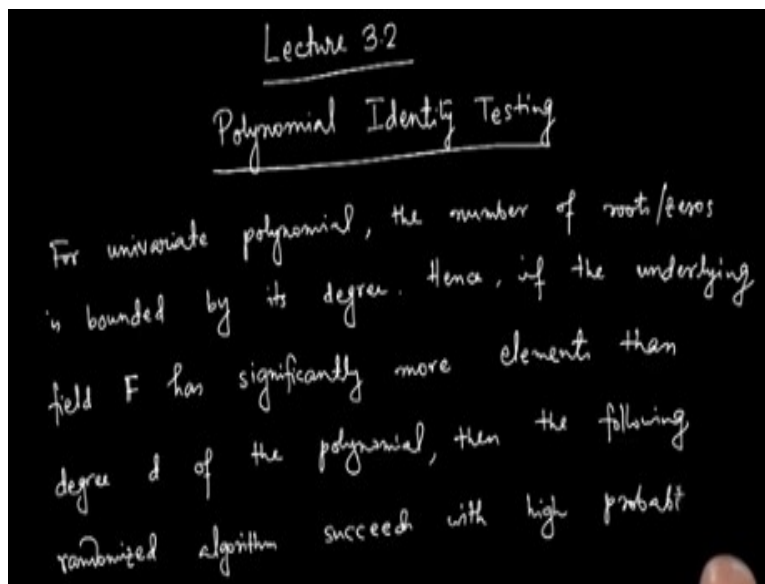


**Selected Topics in Algorithm**  
**Prof. Palash Dey**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Module No # 03**  
**Lecture No # 12**  
**Polynomial Identity Testing**

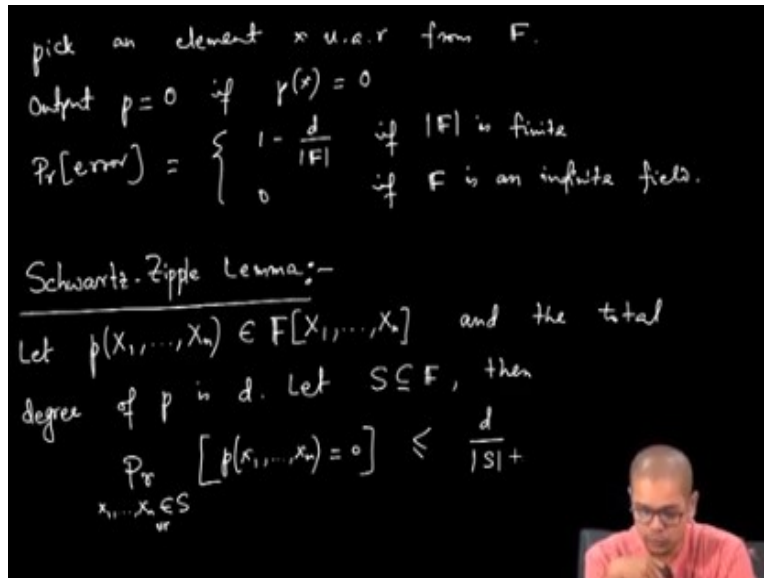
In the last lecture we have started studying randomized algorithms and we it is a first problem we started to look at the polynomial identity testing problem so let us continue that.

**(Refer Slide Time: 00:43)**



This is lecture 3.2 polynomial identity testing and from last time we observed that for univariate polynomial the number of roots or zeros is bounded by its degree. Hence if the underlying field if so what is the underlying field from where the coefficients come? That is the underlying field and if the underlying field has significantly more elements than degree  $d$  of the polynomial. Then the following randomized algorithm succeeds with high probability.

**(Refer Slide Time: 04:08)**

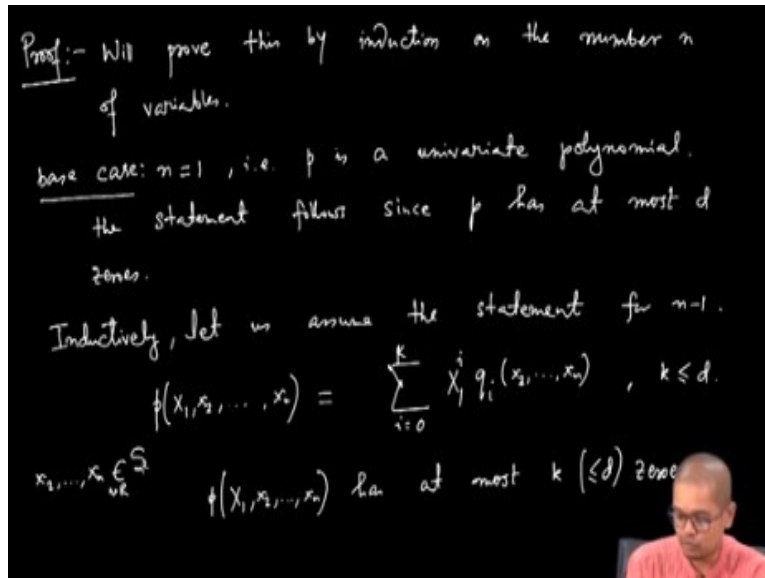


What is the randomized algorithm? Pick an element  $x$  uniformly at a random from the underlying field. And output the polynomial  $p$  to be 0 if  $p(x)=0$ . So the success probability or the error probability of error is the degree is  $d$  then this a non-zero polynomial of degree  $d$  it can have  $d$  roots. So if the uniformly picked element will be one of its root and it can have at most  $d$  roots then just this algorithm makes an error otherwise this algorithm succeeds this is if  $F$  is a finite field.

And this algorithm always succeeds if  $F$  is infinite field because an element  $X$  picked uniformly at random from a field of infinite elements will be one of the finite elements this happens with probability 0. Now using Schwartz-Zippel Lemma allows us to extend this algorithm to multivariate polynomials so last time we also stated Schwartz Zippel Lemma. What does the Lemma say? Let  $p(X_1, \dots, X_n)$  be a polynomial over  $F$  in  $n$  variables.

So if third bracket  $X_1, \dots, X_n$  denotes the set of all polynomials over the field  $F$  let this be a polynomial let  $P$  belong to this and the total degree of  $p$  is  $d$ . And let  $S$  subset of  $F$ ; then probability that if I pick  $x_1, \dots, x_n$  uniformly at random from  $S$  this is uniformly randomly then this polynomial  $P$  evaluated at  $x_1, \dots, x_n$  this is 0 this probability is at most  $d$  by size of  $S$ . So first let us prove this Lemma and then we will apply this Lemma to the polynomial identity testing problem.

**(Refer Slide Time: 08:40)**



Proof so this is we will prove this will prove this by induction the number in of variables. So base case  $n = 1$  that is  $p$  is univariate polynomial now in this case because univariate polynomial has at most  $d$  Roots where  $d$  is its degree and for universe polynomial total degree and degree is the same then it follows from the so base case. So the statement follows since  $p$  has at most  $d$  zeros. So inductively let us assume the statement for  $n - 1$ .

Now what I will do is that I later let me write this polynomial  $p(X_1)$  and for other things for variables  $X_2, \dots, X_n$  I will put elements from field which is picked uniformly at random from  $S$ . So  $x_2, \dots, x_n$  they are picked uniformly randomly from  $F$  now this then because in terms of in place of variable  $X_2$  I put the element  $x_2$ . And so on so only I keep the variable  $X_1$ . So this becomes a univariate polynomial in  $X_1^i q(x_2, \dots, x_n)$ .


So in each monomial you know  $i$ -th place of  $X$  to variable  $X$ , I put  $x_2$  and so on so this how now it becomes a polynomial in  $X_1$  only and suppose the degree is at most  $k$  or degree is  $k$  of course  $k$  is less than equal to  $d$ . Now if I pick  $x_1$  uniformly at random now this polynomial  $p(x_1, x_2, \dots, x_n)$  has at most  $k$  which is less than equal to  $d$  zeros. So if I pick a  $x_1$  uniformly randomly from  $S$  so this is this I should pick from  $S$  that is what the statement is from  $S$  then it is 1 of the 0 with probability at most  $k$  by  $S$ .

**(Refer Slide Time: 14:05)**

$$\Pr_{x_1 \in S} [f(x_1) = 0] = \Pr_{x_1 \in S} [p(x_1, \dots, x_n) = 0]$$

- $E_2$  be the event that  $f(x_1) = 0$ .
- $E_1$  be the event that  $f(x_1)$  is a non-zero polynomial.
- $f(x_1)$  will be non-zero if  $q_k(x_2, \dots, x_n) \neq 0$

$$\Pr[E_1] = \Pr[f(x_1) \neq 0] \geq \Pr[q_k(x_2, \dots, x_n) \neq 0]$$

$$\geq 1 - \frac{d-k}{n}$$


So let me write this is suppose let us call this polynomial  $F$  of  $X_1$  is a univariate polynomial and probability that  $x_1$  picked uniformly randomly from  $S$ . And it turns out to be a 0 of the polynomial  $f$  of  $x_1$  this is probability that  $x_1$  is uniformly randomly this is  $p(X_1, x_2, \dots, x_n) = 0$ . And now let us evaluate this so let us call this event  $E_2$  be the event that  $f(X_1)$  is 0 and  $E_1$  be the event that the univariate polynomial is non-zero.

Because this argument holds if  $f(X_1)$  is a non-zero polynomial if it is a 0 polynomial if  $f(X_1)$  is 0 then it has infinitely many roots all elements of  $S$  are roots. So  $E_1$  with the event that  $f(X_1)$  is a non-zero polynomial. Now  $f(X_1)$  will be a non-zero polynomial if at least 1 term containing  $X_1$  survives in  $p(X_1, \dots, X_n)$ . So  $f(X_1)$  will be non-zero if you know the first maybe this term say  $q_k(x_2, \dots, x_n)$  is non-zero.

Of course it could be non-zero if you know the first term  $q_k$  becomes 0. But other terms any terms are 5 but if  $q_k$  survives at least 1 term namely if  $q_k$  survives then of course this is  $f(X_1)$  will be non-zero. Of course there could be other ways that  $f(X_1)$  could be non-zero so what is the probability that  $f(X_1)$  is non-zero this is probability of the complement event  $E_2 \bar{E}_1$  this is  $E_1$  probability of  $E_1$ .

This is less than equal to probability that  $q_k(x_2, \dots, x_n)$  is not equal to 0. Is no sorry this is greater than equal to this is because if  $q_k(x_2, \dots, x_n)$  becomes non-zero then  $f(X_1)$  is non-zero but the

other way is may not be the true. So these are the set of events where  $f(X_1)$  is non-zero and in a subset of events  $q_k(x_2, \dots, x_n)$  is non-zero. So that is why this inequality goes this way and this probability is at least so this degree is  $k$  so this this degree the degree of  $q_k(x_2, \dots, x_n)$  recall  $q_k$  is the coefficient of  $X_1^k$ . So the degree of  $q_k(x_2, \dots, x_n)$  is at most  $d - k$  because the total degree is  $d$  so this is  $d - k$  by  $n - 1$  - this.

**(Refer Slide Time: 20:34)**

$$\begin{aligned}
 P_{x_1, \dots, x_n \in S} [p(x_1, \dots, x_n) \neq 0] &= P_r[\bar{E}_1] + P_r[E_2 | E_1] \cdot P_r[E_1] \\
 &\leq P_r[\bar{E}_1] + P_r[E_2 | E_1] \\
 &\leq \frac{d-k}{|S|} + \frac{k}{|S|} \\
 &= \frac{d}{|S|}
 \end{aligned}$$

The algorithm simply picks  $x_1, \dots, x_n$  u.a.r from a suitable  $S$  and outputs  $p(X_1, \dots, X_n) = 0$  if  $p(x_1, \dots, x_n)$

Now let us now we will compute probability of  $E_2$  so probability of  $E_2$  so let me write this way I want to compute probability that  $x_1, \dots, x_n$  picked uniformly randomly from  $p(x_1, \dots, x_n)$  not equal to 0 this is nothing but probability of  $E_2$ . And then now let me write so this is we know this is so this probabilities either  $f$  itself becomes a 0 polynomial which is probability of  $\bar{E}_1$ . That means you know this polynomial  $f(X_1)$  itself is 0 so this happens with probability of  $\bar{E}_1$ .

Or if  $f(X_1)$  is not 0 then after putting a uniformly random  $x_1$  then it becomes 0 that is the probability of  $E_2$  given  $E_1$ . So 2 ways it could be  $f(X_1)$  is itself a 0 polynomial then of course this  $p(X_1, \dots, X_n)$  becomes 0 and even if it is non-zero then after putting a uniformly random  $x_1$  it becomes 0 that is the probability  $E_2$  given  $E_1$ . So this is and this times probability of  $E_1$  now probability of  $E_1$  is at most 1 this is  $\bar{E}_1$  plus probability of  $E_2$  given  $E_1$ .

Now this is less than equal to probability of  $\bar{E}_1$  is less than equal to  $d - k$  by size of  $S$  and probability of  $E_2$   $f$  is a univariate polynomial it has at most  $k$  roots is  $k$  by size of  $S$  this is  $d$  by

size of  $S$  which concludes the proof. So what is the randomized algorithm? The algorithm simply picks  $x_1, \dots, x_n$  uniformly at random from a suitable suitably large suitable  $S$  so for finite fields it could be the set of all elements in the field for infinite field we can take a very large  $S$ .

Simply pick  $S$  takes a uniformly at random from a suitable  $s$  and outputs  $p$  the polynomial  $p(x_1, \dots, x_n)$  this is 0 if the evaluation turns out to be 0.

(Refer Slide Time: 25:05)

$$\Pr[\text{error}] \leq \frac{d}{S}$$

$$|S| = |F|, \quad \Pr[\text{error}] \leq \frac{d}{|F|}$$
 If  $|F|$  is not too large compared to  $d$ , then  
 let us repeat the algorithm  $l$  times and output  
 $p(x_1, \dots, x_n) \neq 0$  if in any run  $p(x_1, \dots, x_n) \neq 0$ .  

$$\Pr[\text{error}] \leq \left(\frac{d}{|F|}\right)^l = e^{-l \ln \frac{|F|}{d}}$$

$$l = \ln \frac{|F|}{d} \quad \text{then} \quad \Pr[\text{error}] = O(1) +$$

And what is the probability of error is at most  $d$  by  $S$  you know which is now if you pick  $S$  equal to cardinality  $F$  for finite fields then probability of error is less than equal to  $\frac{d}{|F|}$ . So law for large fields it; is but you know if size of  $F$  is comparable to the size to  $d$  then this may not be too small and then we need a boosting. So if cordiality  $F$  is not too large compared to  $d$  then let us repeat the algorithm  $l$  times.

And output  $p(x_1, \dots, x_n)$  is not equal to 0 if in any iteration in any run  $p(x_1, \dots, x_n)$  is not equal to 0. So observe that this algorithm has 1 sided error if it outputs that the algorithm that the polynomial is not to 0 then it is true. Because then it has found a point  $(x_1, \dots, x_n)$  where the polynomial evaluates to be non-zero the polynomial cannot be a 0 polynomial. On the other hand it can only make an error if the polynomial is non-zero but every time it picked a 0. So if cardinality  $F$  is not too large then  $d$  then we need to repeat  $l$  times.

And then probability of error is that it made an error every time so this is  $d$  by cardinality if to the power  $l$  now if I pick now let me write this way this is  $e$  to the power minus  $\log$  of  $F$  by  $d$  times  $l$ . So now if we pick  $l = \frac{\ln |F|}{d}$  cardinality if by  $d$  then the error probability then probability of error is big of 1 constant less than before not big omega big off 1. so this concludes the description of the algorithm so we will continue from here next place