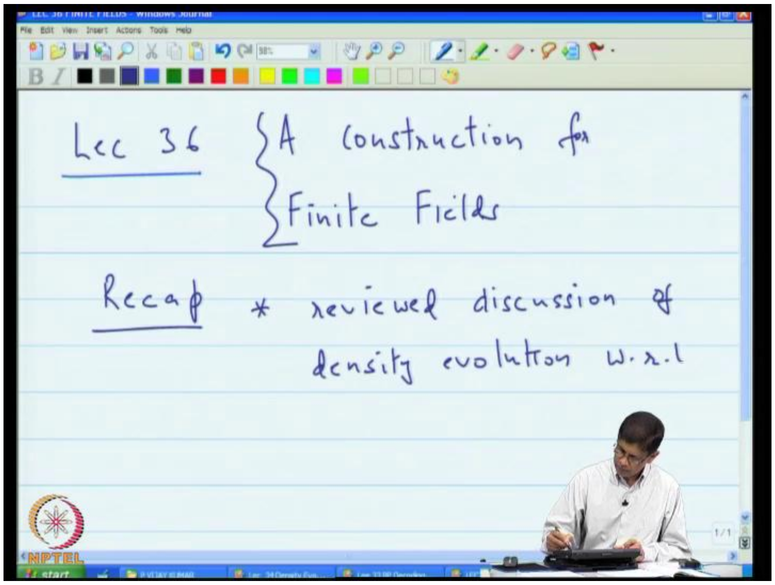
Error Correcting Codes

Prof. Dr. P Vijay Kumar
Electrical Communication Engineering
Indian Institute of Science, Bangalore

Lecture No. # 36
A Construction for Finite Fields

(Refer Slide Time: 00:30)

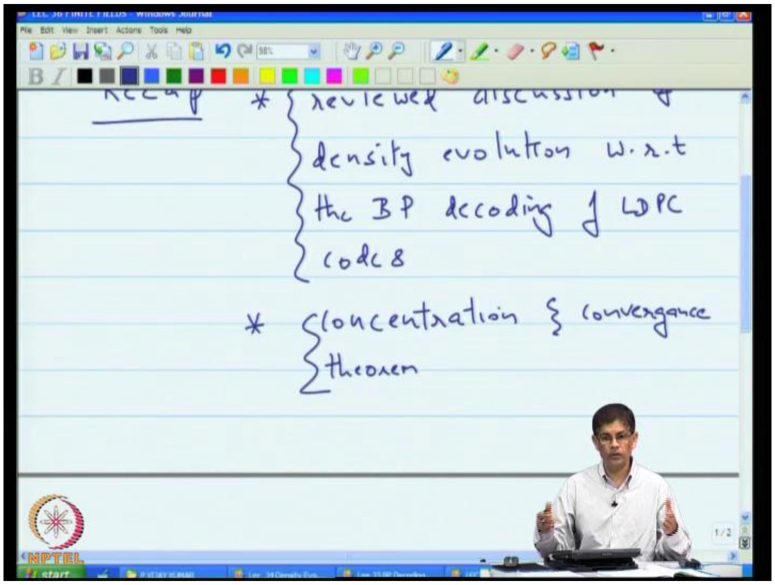


Lec 36 {A Construction for Finite Fields

Recap * reviewed discussion of density evolution w.r.t

This is lecture 36, and so when you just recap, what we did last time. I will first put it down writing, we reviewed a discussion of density evolution with respect to the belief propagation based decoding of LDPC codes.

(Refer Slide Time: 01:27)



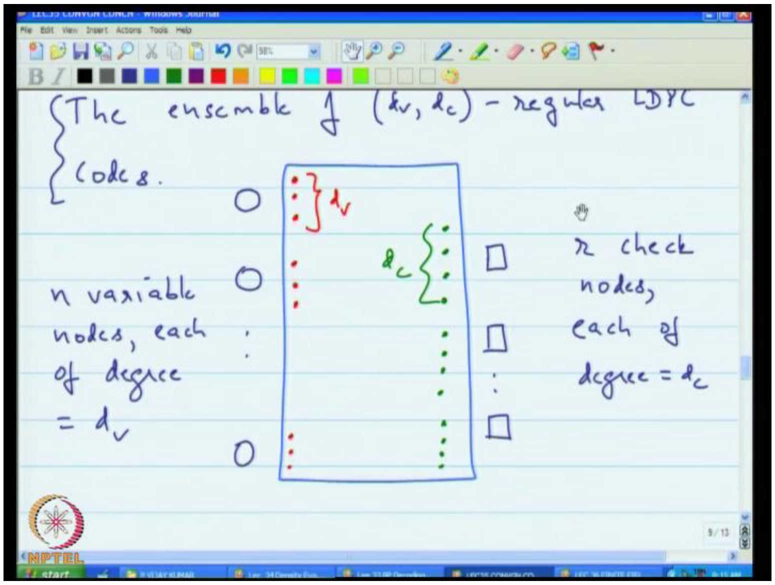
Recap

* reviewed discussion of density evolution w.r.t the BP decoding of LDPC codes

* concentration & convergence theorem

Then after that I actually stated up would I called what is called and concentration, and convergence theorem. So, wrote this theorem all about is basically says that look if did you density revolution and tree like assumption.

(Refer Slide Time: 02:20)



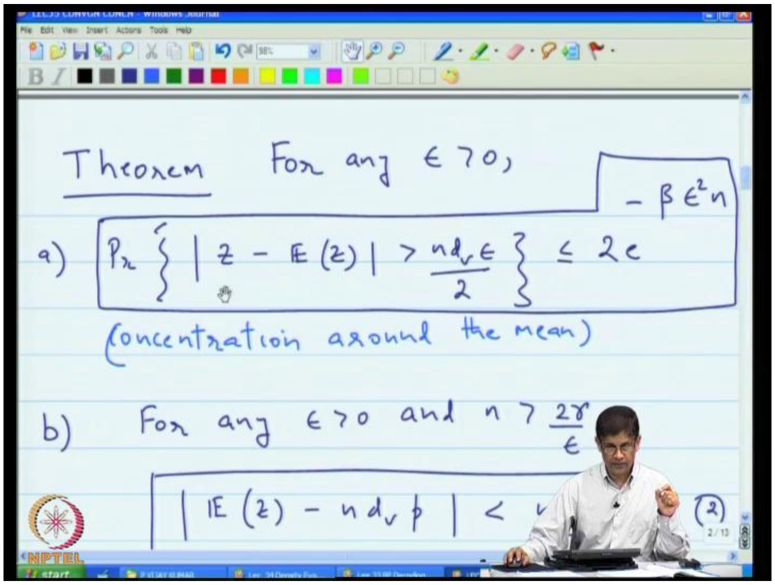
The ensemble of (d_v, d_c) - regular LDPC codes.

n variable nodes, each of degree $= d_v$

r check nodes, each of degree $= d_c$

But would not tree like in this theorem is well it terms to ratio, you how is it not lose, because with high probability. You are going to perform guessed as good as you did in the tree like is. So, lining do the following. Since, I want to do more or less complete proof that I started out in this theorem. Now, I am going to take the advantage of our technology, because our technology a loves me to go back to the writing of the previous lecture.

(Refer Slide Time: 02:41)



Theorem For any $\epsilon > 0$,

a) $\boxed{P_r \left\{ \left| Z - \mathbb{E}(Z) \right| > \frac{n d_v \epsilon}{2} \right\} \leq 2 e^{-\beta \epsilon^2 n}}$

(concentration around the mean)

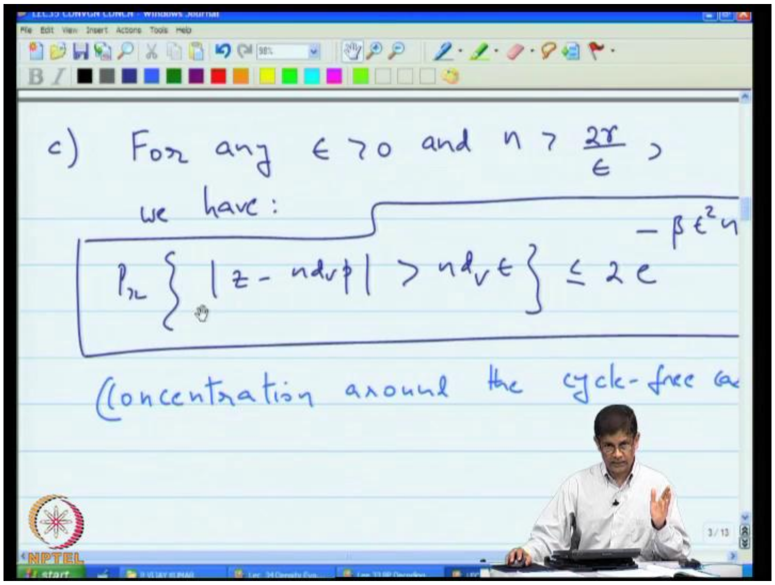
b) For any $\epsilon > 0$ and $n > \frac{2\gamma}{\epsilon}$

$\left| \mathbb{E}(Z) - n d_v p \right| <$

(2)

And I am going to use that complete the proof, so let us take the look at the statement of the theorem again. So the thermos as that look the difference between the number of messages passed in the during the l th iteration along from along all the edges going from a variable to check note in the l th iteration the probability there it d v x significantly from the mean is small now this probability is completed. Over all channel realizations an overall selections of d v d c regular graphs and I explain that last time. The second part actually says that the difference between the average over the sum sample of channel realization in d v d c regular graphs the deviations of this from the expected value of the number of incorrect messages. In the tree like case is small provided in make in the block link large enough and if put to together if you find that the probability. It else that the probability that if you could be graph it random that the number of incorrect messages there are passed during the elite iteration.

(Refer Slide Time: 03:57)



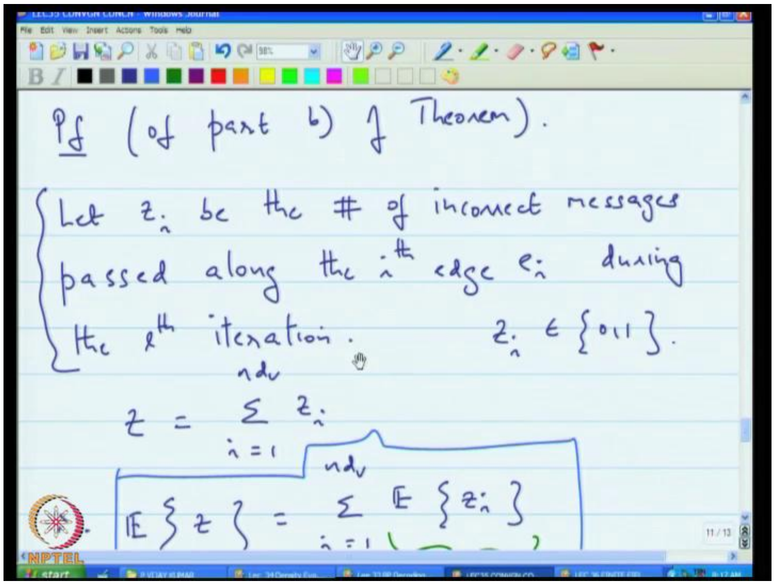
c) For any $\epsilon > 0$ and $n > \frac{2\gamma}{\epsilon}$, we have:

$$\boxed{P_r\left\{ |z - n d_v p| > n d_v \epsilon \right\} \leq 2e^{-\beta \epsilon^2 n}}$$

(Concentration around the cycle-free ca

Along the edges from the variable to the check node the probability that that d v x significantly from the average are or from the number that expected number that would be passed in the tree like case is small; that means that you actually comes from believe propagation. So that in a since that on all work on believe propagation was not in vain. Because it has meaning when apply to a graph that expected random, which may not necessarily have a tree neibourhood. Now, also said that would be going to do when you proof this part and then I am not going to proof it is happens to be some outline the, but it will put these together to actually control this so we will the process of proving part b.

(Refer Slide Time: 05:00)



Pf (of part b) of Theorem).

Let z_i be the # of incorrect messages passed along the i^{th} edge e_i during the ℓ^{th} iteration. $z_i \in \{0,1\}$.

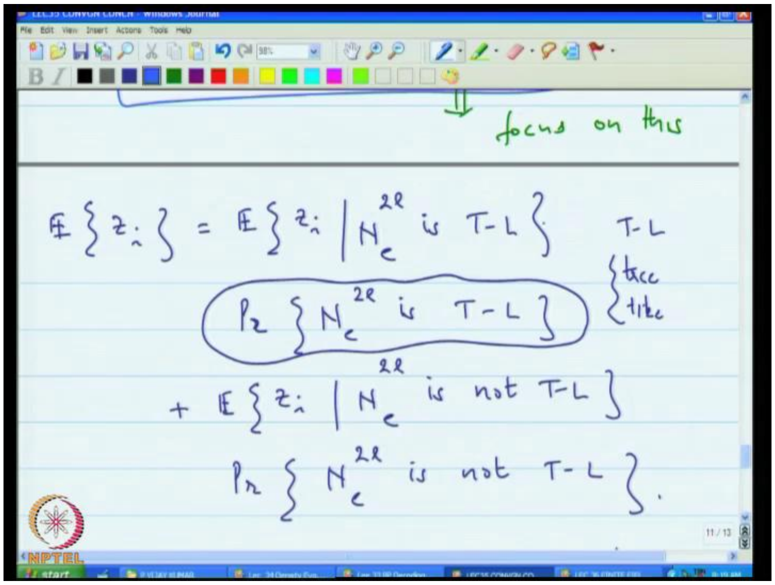
$$z = \sum_{i=1}^{ndv} z_i$$

$$\mathbb{E}\{z\} = \sum_{i=1}^{ndv} E\{z_i\}$$

And I said that look let z i z is about the number of incorrect messages passed along the i th age e i during the l th iteration. And here then since there are ndv edges that go from variable to check node the total number incorrect messages in of course the sum of the number of messages.

Along each of the ndv edges and this is the zero one function because e then edge is carrying an incorrect message are this is not ok and then we take a expectation on both sides. And then the executive values of this is nothing but the probability that this particular the message on this is actually incorrect. So how do you compute that well we again take compute this probability but breaking at on using conditional so this probability condition upon the neibourhood history like is that which is not now adjustment of the make other point.

(Refer Slide Time: 06:43)



focus on this

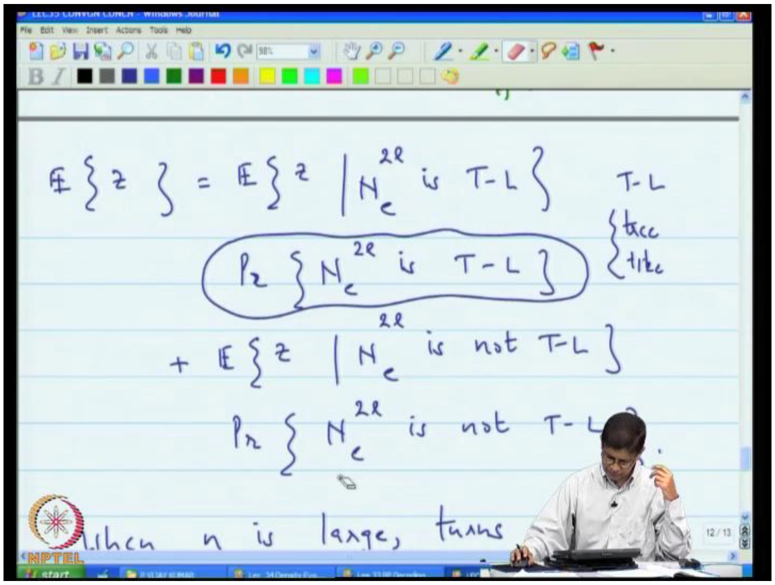
$$\mathbb{E}\{z_i\} = \mathbb{E}\{z_i \mid N_e^{2l} \text{ is T-L}\} \; \boxed{Pr\{N_e^{2l} \text{ is T-L}\}}$$

T-L {tree like

$$+ \; \mathbb{E}\{z_i \mid N_e^{2l} \text{ is not T-L}\} \; Pr\{N_e^{2l} \text{ is not T-L}\}.$$

Here is that this think here that this quantity here is by the by is miss this conditioning is in sets of number z is up i, they something I in needs to pap mention here, which is that look because of symmetry this is the same in immature, which particular edge you consider. So, this is actually equal to n d v times the expected values of z 1 in a particular edge. Lets is there z is one and I just make a note this is by symmetry, the symmetry effort a symmetry of the tanner graph. I mean we take at look a tanner graph all a density evolution really depends only upon the degree of the nodes. Since hence all of the nodes have same degree you did expect that the number of incorrect messages is the same, and that is the reason where would have that this number is a independent of the particular think here.

(Refer Slide Time: 07:45)



$$\mathbb{E}\{z\} = \mathbb{E}\{z \mid N_e^{2l} \text{ is T-L}\} \; \boxed{\Pr\{N_e^{2l} \text{ is T-L}\}}$$

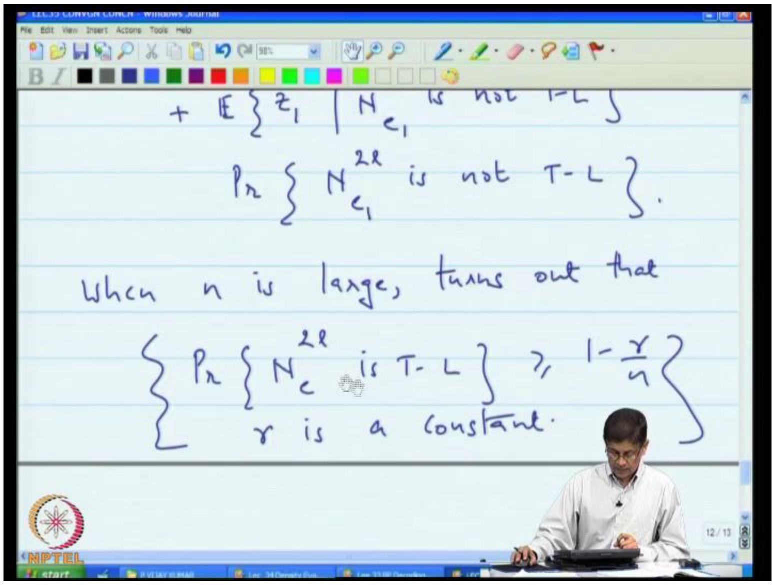
$$+ \; \mathbb{E}\{z \mid N_e^{2l} \text{ is not T-L}\} \; \Pr\{N_e^{2l} \text{ is not T-L}\}.$$

T-L {tree like

When n is large, turns

Now, in this letch actually compute given that there is the same for all i, it is perhaps clear if I say that would I am now doing is focusing on one particular edge which z 1. Now interested knowing what is the probability that the neibourhood of that particular edge even is tree like and this think here probability that particular message is incorrect given the neighborhood to that to like this comes from density evolution is entire quantity here is nothing but our p, so now with all of this information and also and the other quantity.

(Refer Slide Time: 08:57)



$$+ \; \mathbb{E}\{z_1 \mid N_{e_1} \text{ is not T-L}\}$$

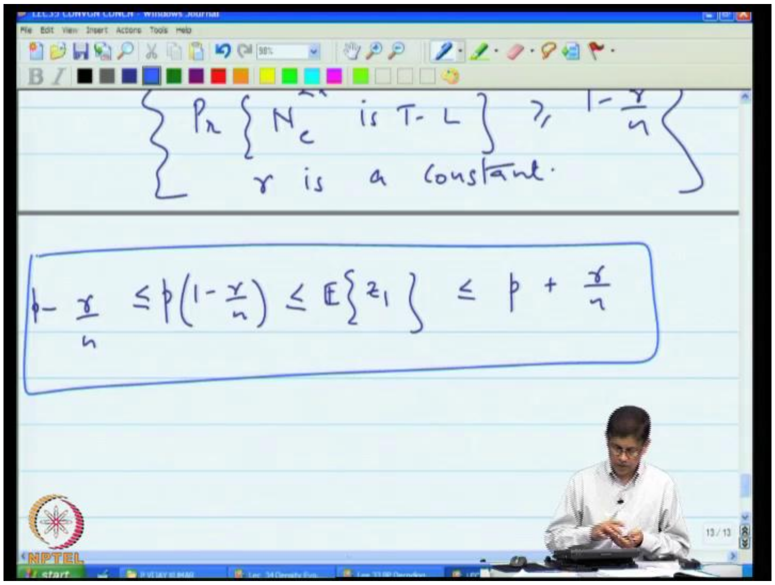
$$\Pr\{N_{e_1}^{2l} \text{ is not T-L}\}.$$

When n is large, turns out that

$$\left\{ \begin{array}{l} \Pr\{N_e^{2l} \text{ is T-L}\} \geq 1 - \frac{\gamma}{n} \\ \gamma \text{ is a constant.} \end{array} \right\}$$

I mention to kind of the last lecture that when n is large terms of the probability that if fix L, and let go out of infinity the probability that the neighborhood to the to like is greater than or equal to 1 minus gamma by n. Now, it actually is that to say that therefore the expected value of z 1.

(Refer Slide Time: 09:34)

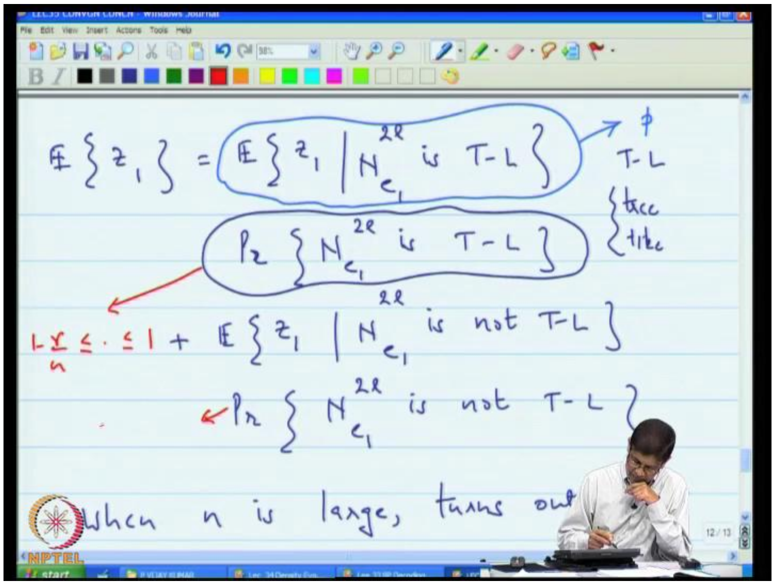


$$\left\{ P_r \left\{ \hat{N}_c \text{ is T-L} \right\} \geq 1 - \frac{\gamma}{n} \right.$$
$$\left. \gamma \text{ is a constant.} \right\}$$

$$\boxed{p - \frac{\gamma}{n} \leq p\left(1 - \frac{\gamma}{n}\right) \leq E\{z_1\} \leq p + \frac{\gamma}{n}}$$

And the one hand is less than or equal to plus gamma by n whether hand is greater than or equal to e into one minus gamma by n which in turn is greater than equal to e minus gamma by n. Solved I get this now symmetry obtaining both in up on this quantity, and now I know for instance. So put on would I know about the various quantities I know that this quantity lies between one minus gamma by n and one, I am interested in a turning the lower upper bound to this quantity. So, I want to upper bound I will replace this by one, if I want to lower bound replace it one minus gamma by n. I know that this quantity is p if I want to upper bound this is replace by one that is p.

(Refer Slide Time: 10:50)



$$E\{z_1\} = E\{z_1 \mid N_{e_1}^{2l} \text{ is T-L}\} \rightarrow p$$

T-L {tree like}

$$P_r\{N_{e_1}^{2l} \text{ is T-L}\}$$

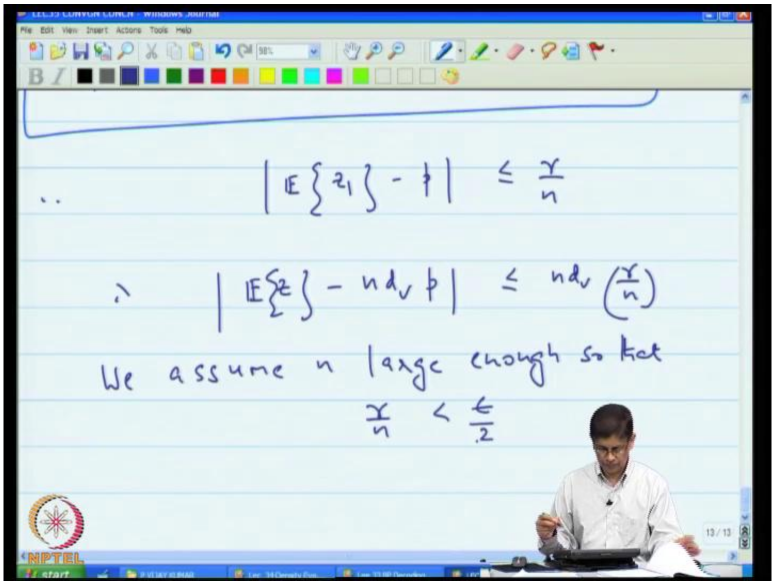
$$1-\frac{\gamma}{n} \le \cdot \le 1 \quad + E\{z_1 \mid N_{e_1}^{2l} \text{ is not T-L}\}$$

$$\leftarrow P_r\{N_{e_1}^{2l} \text{ is not T-L}\}$$

When n is large, turns out

And now we know the probability with which the neibourhood is not tree like is less than or equal to gamma by n, and since z 1 is a zero one function I can always say that this is less than equal to 1. So, then put all of this together if I want to upper bound I simply say this is p this at most one this at most gamma by n and that is I get upper bound here there is at most p plus gamma by n and whether hand . If I want to lower bound then would I do is this whole thing is negative signed truth I ignore at just together first I say that is greater than or equal to p into one minus gamma by n. But I will get this other term and so now this get this greater than or equal to p minus gamma by n.

(Refer Slide Time: 11:40)



$\therefore \quad |\mathbb{E}\{z_1\} - p| \le \frac{\gamma}{n}$

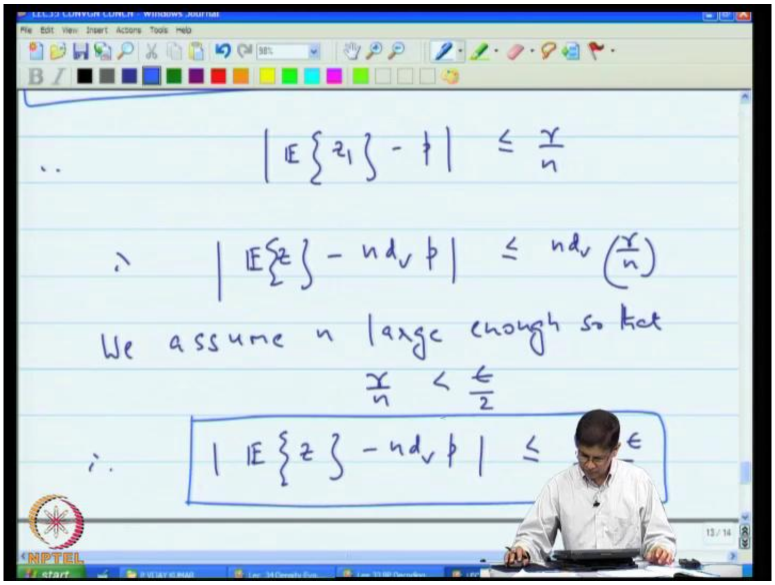
$\therefore \quad |\mathbb{E}\{z\} - n d_v p| \le n d_v \left(\frac{\gamma}{n}\right)$

We assume n large enough so that

$\frac{\gamma}{n} < \frac{\epsilon}{2}$

So from the chit follows therefore that the expected value of z 1 minus p in magnitude is less than or equal to gamma by n. Now, I know that if I want to relate to this expect value .Total number of messages that are in error a simply multiply through by n d v. Therefore the expected value of z minus n d v p is less than or equal to n d v gamma by n in, now what we do is we choose we assume are choose n large enough so that gamma by n is less than epsilon by 2.

(Refer Slide Time: 13:00)



$\therefore \quad |\mathbb{E}\{z_1\} - p| \le \frac{\gamma}{n}$

$\therefore \quad |\mathbb{E}\{z\} - n d_v p| \le n d_v \left(\frac{\gamma}{n}\right)$

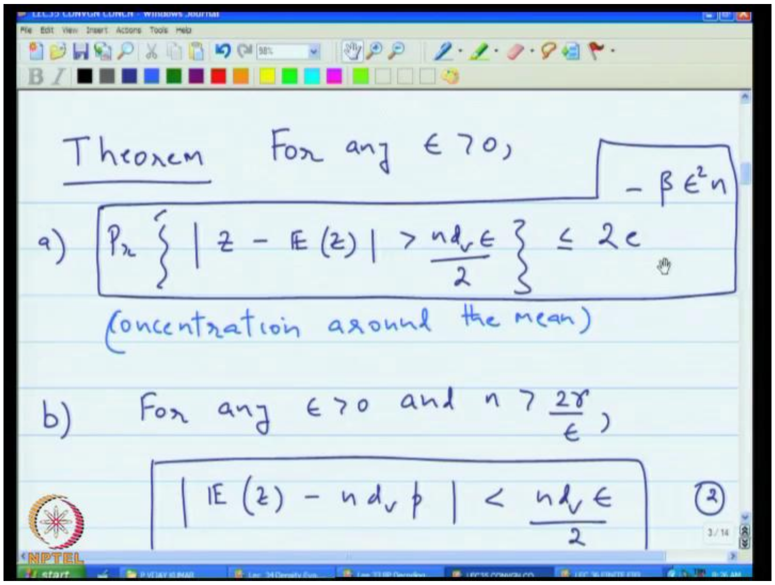
We assume n large enough so that

$\frac{\gamma}{n} < \frac{\epsilon}{2}$

$\therefore \quad \boxed{|\mathbb{E}\{z\} - n d_v p| \le \quad \epsilon}$

And with that therefore the expected value of therefore the expected value of z minus ndvp in magnitude is less than or equal to ndv epsilon by 2. So, that was art p was the theorem as you can see here, so we actually proof part two part one use a meltingly theory. What did basically does this it says look p this is an expectation difference between the random variable an expectation.

(Refer Slide Time: 13:47)



Theorem For any $\epsilon > 0$,

a) $\Pr\left\{ \left| Z - \mathbb{E}(Z) \right| > \frac{n d_v \epsilon}{2} \right\} \le 2e^{-\beta \epsilon^2 n}$

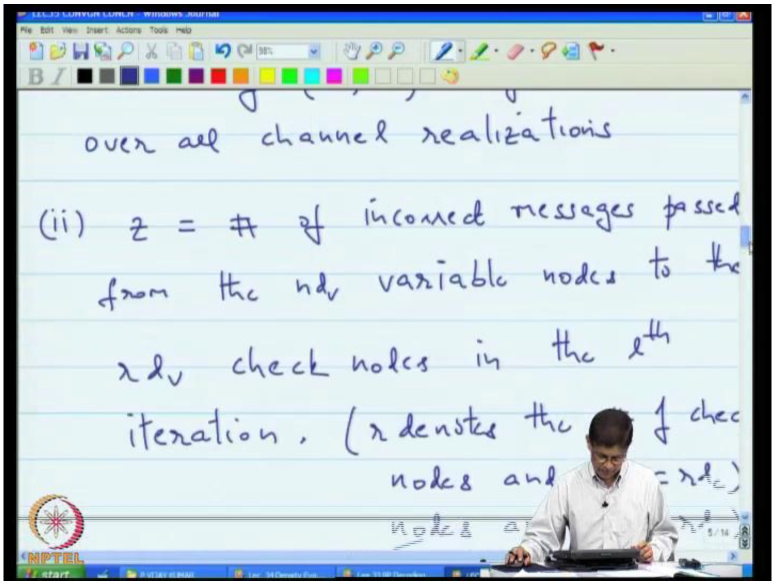
(concentration around the mean)

b) For any $\epsilon > 0$ and $n > \frac{2\gamma}{\epsilon}$,

$\left| \mathbb{E}(Z) - n d_v p \right| < \frac{n d_v \epsilon}{2}$ ②

What I can do is I can introduce sequence of a random variables, and the chain of a random variables. Such that this is the one in that chain and this is that other in the chain, and in that chain actually forms a martingale and use and in quality in one zoom as in a quality from martingale to actually derived this bound, it is not a technical. And take sub some time it is very nice result. Of course but we want actually spend the time to do that we do not alive of the time. So well I do now is I assume that assume one, so this was or result one. So, assume that we know one is true and two, and will just actually show that the two together imply part c.

(Refer Slide Time: 14:57)

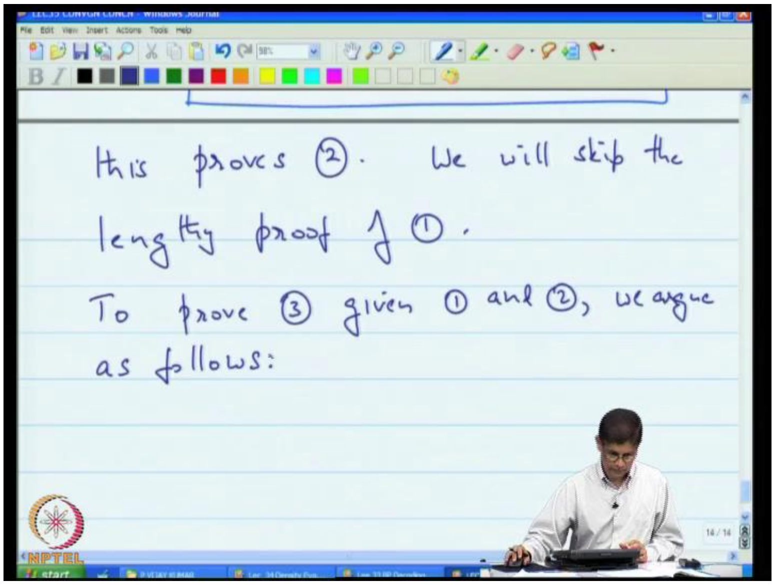


over all channel realizations

(ii) z = # of incorrect messages passed from the nd_v variable nodes to the rd_v check nodes in the ℓ^{th} iteration. (r denotes the # of chec nodes and $= rd_c$)

Part c being the theorem here. Now, if we look here you will see that this is we shown the convergence to the cycle free case, we related the average in the general case to that in the cycle free case. And we are not kind go prove this less assume that there is the concentration around the mean in the general case, and will put to together to show that the concentration around the cycle free case this proofs true.

(Refer Slide Time: 15:33)

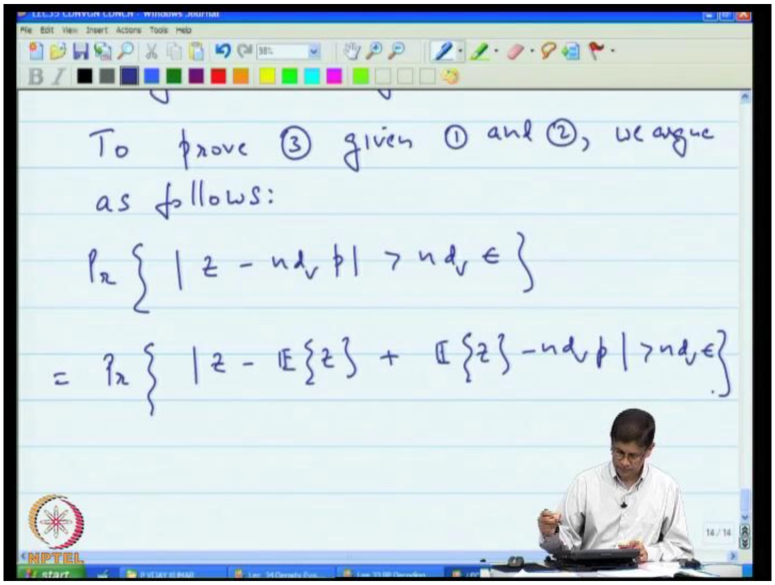


This proves ②. We will skip the lengthy proof of ①.

To prove ③ given ① and ②, we argue as follows:

This proof is true we will skip this about lengthy proof of one.

(Refer Slide Time: 16:12)



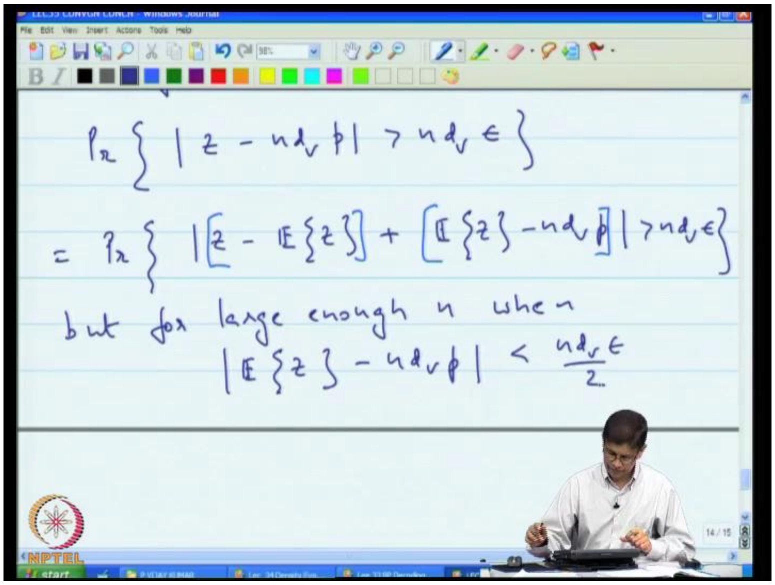
To prove ③ given ① and ②, we argue as follows:

$$\Pr\{ |z - n d_v p| > n d_v \epsilon \}$$

$$= \Pr\{ |z - \mathbb{E}\{z\} + \mathbb{E}\{z\} - n d_v p| > n d_v \epsilon \}$$

And now show three I just make the following note to proof three given 1 and 2. We are give as follows the probability that zee minus n d v p is greater than n d v epsilon is equal to the probability that zee minus that expected value of zee plus the expected value of zee minus n d v p greater than n d v epsilon.

(Refer Slide Time: 17:35)



$$\Pr\{ |z - n d_v p| > n d_v \epsilon \}$$

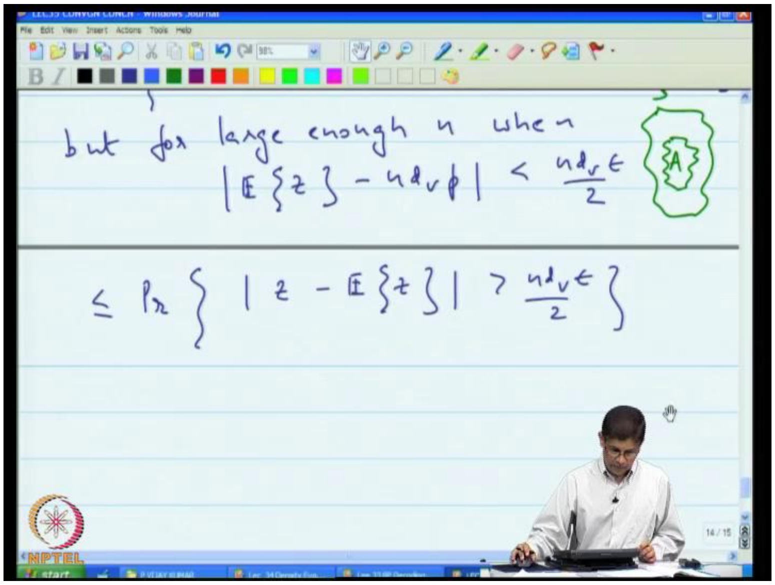
$$= \Pr\{ |[z - \mathbb{E}\{z\}] + [\mathbb{E}\{z\} - n d_v p]| > n d_v \epsilon \}$$

but for large enough n when

$$|\mathbb{E}\{z\} - n d_v p| < \frac{n d_v \epsilon}{2}$$

Now we added and subtract the expected value of z, and we have these two terms but for large enough in when the expected value of z minus n d v p in magnitude is less than n d v epsilon by two. What way in a part b we should n is a large enough this difference is going to be small so the only way that this can be large is if this is large. In other words is a, if a is the event that this actually takes place, then it must be that the event is beware this is the greater than or half of this must take place.

(Refer Slide Time: 18:47)



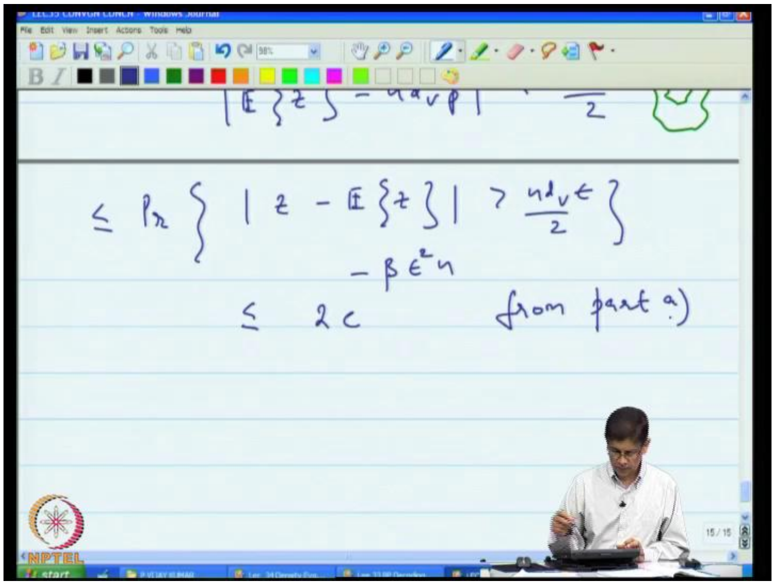
but for large enough n when

$$|\mathbb{E}\{z\} - n d_v p| < \frac{n d_v \epsilon}{2}$$

$$\leq \Pr\left\{ |z - \mathbb{E}\{z\}| > \frac{n d_v \epsilon}{2} \right\}$$

We can actually say that this is less than or equal to probability that z minus the expected value of z is greater than n d v epsilon by 2. Because this situation is something like this you have an event a, and you have an event b and sorry, they are we are on we have an event b. And we have an event a, and we interested in the probability of event a and what this actually says that since a this event given this implies the occurrence of this event it means the probability of a is upper bound it by the probability of b. And this and this, so we have this but this already have an upper bound for from the theorem z minus the expected value of z. If go back to the theorem that was the part a of the theorem. From part of the theorem we know that is the probability is small.

(Refer Slide Time: 20:43)



$|E\{z\} - n d_v p| \quad \frac{\ }{2}$

$\leq Pr\left\{ |z - E\{z\}| > \frac{n d_v \epsilon}{2} \right\}$

$\leq 2 e^{-\beta \epsilon^2 n}$ from part a)

So, this is less than or equal to two e to the minus beta epsilon squared by n from part a of the theorem. That proofs the theorem, so to summarize what we actually shown is that although belief propagation guilt in a case when you working with neibours. There are tree like all it not lose lost when you actually pick graph it random from you are in some will d v d c regular codes because you can show that with high probability. If pick for large blocking the graph it random that the number of incorrect messages passed during belief propagation decoding is going to be is going to be very closed to the number of incorrect messages passed in the tree like is, and in the tree like is you can verify that. If you going to get that number is going to be very small provided your channel is not too bad, it is the usual think that is longer than the channel is not too bad you can actually get reliable information transfer.

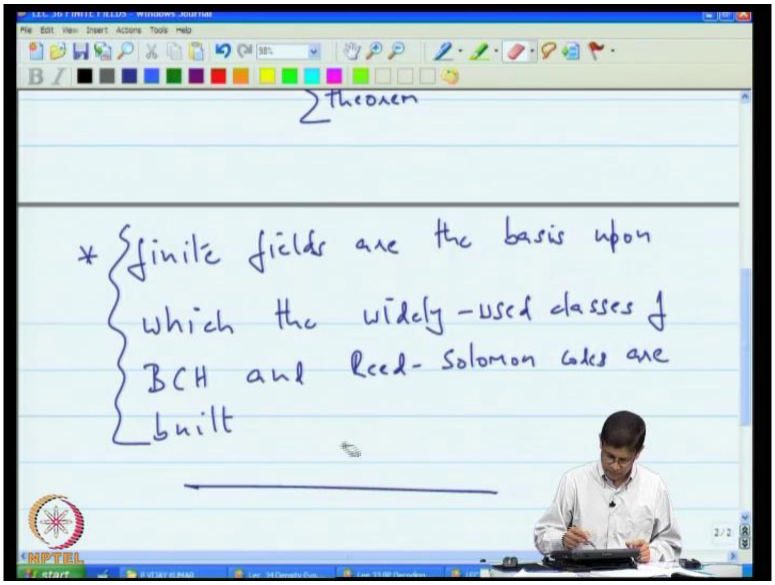
In the same thing happens over here. With that we if completed are discussion on the concentration in convergence theorem. So, now we will actually start a completely new topic and which goes back to the title of lecture 36 which is a construction a finite fields ok al right now just few words about why we are interested in finite fields. Now, we going towards in fact we going to go jump to work completely different class of codes, and these codes whether codes that where in before the recent higher level of interesting codes that are iteratively decodable, such as LDBC codes the codes have a great deals of structure, and in sense of very good codes expect. That they can be somewhat more difficult decode and not able to actually work with this soft information provided by the channel, but nevertheless in many applications they can be of the great interest particularly the classes of b c a, each Solomon codes or often the codes default codes that you would use in particular situations in fact the most widely used code in the world today is the read Solomon code, because it is found in all kinds of memory in your c d rounds. In your high definition t v, how can this story medias your read Solomon code. Because their excellent properties well matched for that medium I basically been involved in a couple of projects where the match will choice is the class of codes known is page codes, and again these are algebraic codes very different.

In nature at least in the way they evolved from this LDPC codes so they based completely on algebra. So will make a complete switch from all the from all the probabilistic arguments we making after now are in this recent discussion on LDPC codes and jump make the jump. Now, to the algebraic is now typically these codes make use of the theory of finite fields up to now finite fields are not new to us, because you works with the integer zero and one which form a field. So, that is the example of the field, that is finite however we want to work more general case of finite fields.

Now, often what you will actually see is text book will actually that the entire text book on coding theory begins perfect teaching of finite fields, now at deliberately from doing that because idea being that. Let us begin finite fields only when you needed, so up to this point in time where I need finite fields because binary codes we take a long way and binary arithmetic, but now we do needed for the class of codes. If we going to actually discuss, so that as background let me get started, so we now finite fields they two ali I will discuss in two stages.

In the first stage what will actually do this I give a construction for a large classes finite fields, and in fact in terms of at every finite fields must have such a construction. So in some sense, this construction covers all finite fields but in the beginning it is the constructions, so which leaves you one ring by will may be their other kinds of finite fields. Then will actually switch gas or will shift take a different perspective, and says less let us forget about constructions, let us try a deductive approach to finite fields each. Say I have finite field what deduce about a internal structure, and will actually join up with the construction by showing well if it is the finite field it must have a structure similar very much like that one, we had in or constructions. And therefore, so these beings to two viewpoints together, and now we you know more or less all that it about finite fields I just make a few commands.

(Refer Slide Time: 27:00)

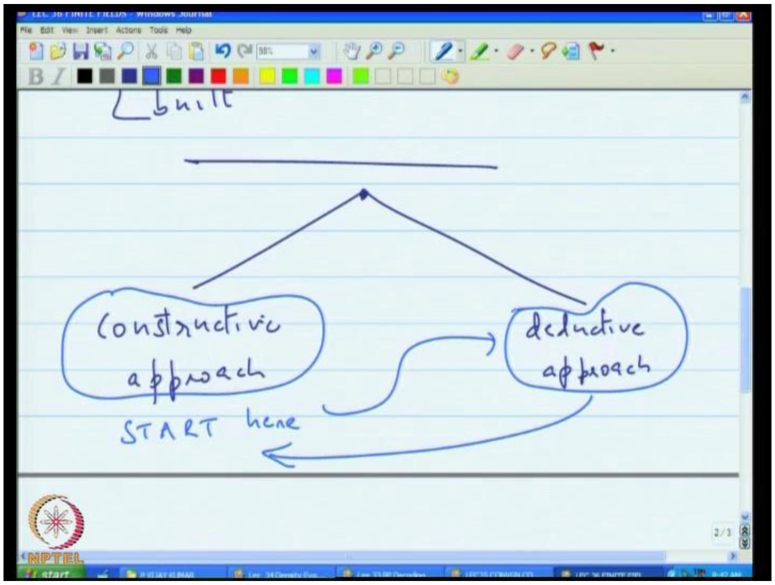


theorem

* finite fields are the basis upon which the widely-used classes of BCH and Reed-Solomon codes are built

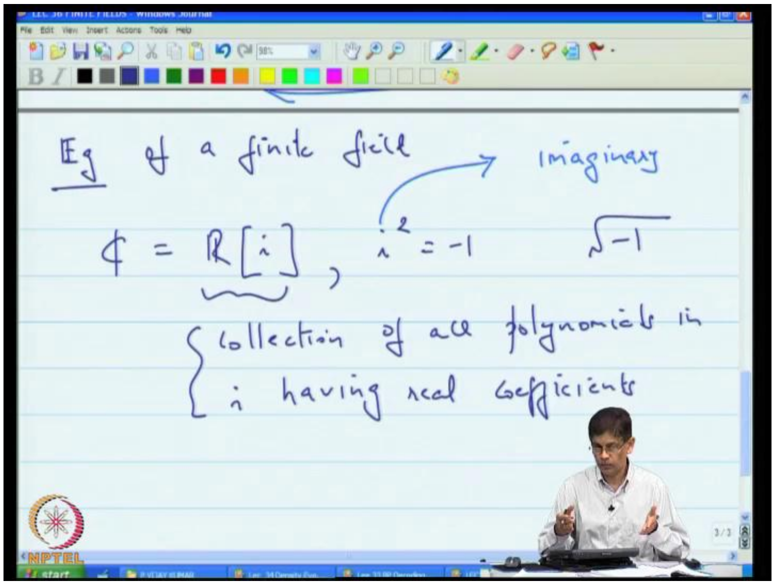
So, first of all finite fields are the basis or or r finite fields are the basis upon which the widely used classes of bch and read Solomon codes are build.

 (Refer Slide Time: 28:25)



Then, they the comment is that a discussion will begin so there is a constructive approach and then there is s deductive approach. What will actually do is will start here and then we will go on to this, and that it bring as back here and I will just explain to you. So, even within the construct approach what I like to do which I will think make for an improved understanding is to actually give a tie example.

(Refer Slide Time: 30:09)



Eg of a finite field

imaginary

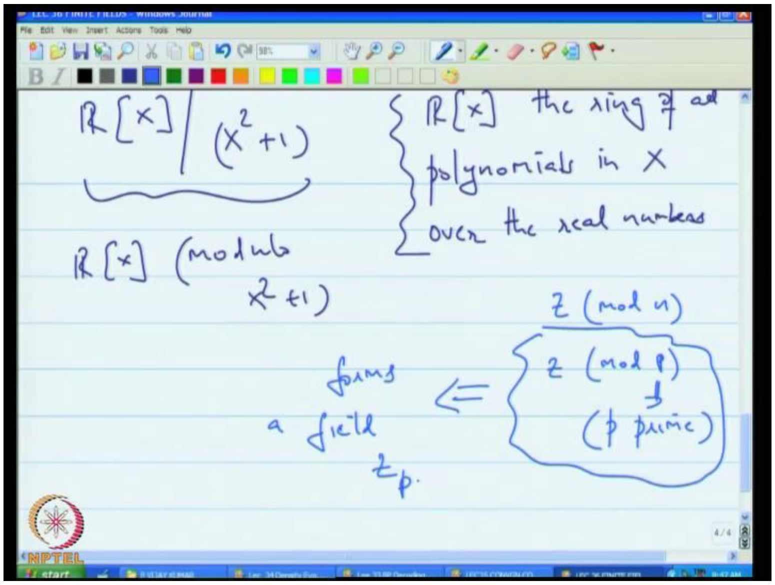
$\mathbb{C} = \underbrace{R[i]}$, $i^2 = -1$ $\sqrt{-1}$

{ collection of all polynomials in i having real coefficients

Let us begin with what mate consider at tie or prototype example of a finite field, and I motivate the a discussion like this. Now, you know that with regard to real and complex number you can think of the real numbers as you can think of the real number as of the complex numbers. In this way you can actually think of it as real numbers to which you are joined an imaginary element I which happens to satisfy the condition that I squared was minus one.

So what that means is the collection the collection of all polynomials in i in the imaginary element, I having real coefficients. So, keep in mind this i is are is imaginary and we all but having work with it so much since your high school days. You now accepted having a very concrete existence you just think of it x is squared of minus 1 when you do not pay much a tension do it, but is fact is that really there is noses thing as square out of minus one right so how it is 1. So, I want to actually give you and all ten at give you point of the complex numbers which will be useful in our discussion and finite fields.

(Refer Slide Time: 32:30)



$\underbrace{\mathbb{R}[x] / (x^2+1)}$

$\left\{ \mathbb{R}[x] \right.$ the ring of all polynomials in x over the real numbers

$\mathbb{R}[x]$ (modulo x^2+1)

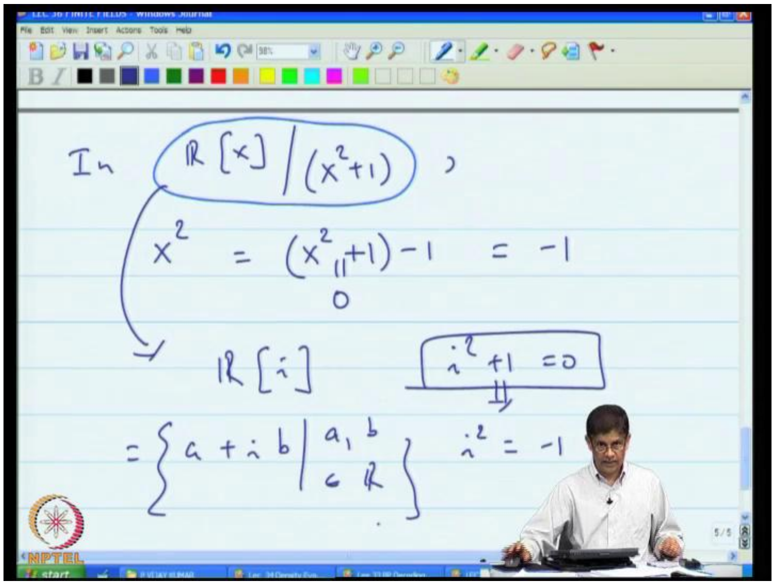
$\mathbb{Z} \pmod{n}$

forms a field $\mathbb{Z}_p$. $\Leftarrow$ $\mathbb{Z} \pmod{p}$ $\ni$ (p prime)

Consider thing of the complex numbers as follows we consider the rain of all numbers all the real numbers modulo x square plus 1. What is this mean? This means that this means that all the elements first of all this is the rain of all of all polynomials in terminate x over the real numbers and this structure is not new to us. We were actually in counted this before but what about this modulo x square plus one, so in ever we you can think you can written that what this is telling as to do so you should this as r of x. You should modulo x square plus one meaning that in all your calculations either additional multiplications. You can actually discard multiples x square plus one, so this is in alleges this is very much in alleges to when you work with in real numbers and then you go mod you go z.

But you go mod in you take the integers, when then you discard multiples of n now this one a features of this polynomial x square plus one namely that it is reduce able. It cannot be factor over the real numbers. Now, if you take this the all edges here for example if an is six that six can be factor so if you want more exact analogy. What you have to do is replace this and with prime so we look at z mod p for p a prime. So the integers modulo p so just like we just this form the field. We know that this structure forms a field and when actually called this z p, and doing a little bit in formal here I am not writing of very carefully, because ideas is to motivate. And you all ready some idea.

(Refer Slide Time: 35:25)



In $\mathbb{R}[x]/(x^2+1)$,

$$x^2 = (\underset{\overset{\shortparallel}{0}}{x^2+1}) - 1 = -1$$

$$\mathbb{R}[i] \qquad \boxed{i^2+1=0}$$

$$\Downarrow$$

$$= \{a+ib \mid a, b \in \mathbb{R}\} \qquad i^2 = -1$$

So, my point is that the complex number can also be considered to be this particular structure where is that, because think about it there is in a in R x mod x square plus 1. What is x square? Well, x squared can be expressed as x squared right plus 1 minus 1 adding and subtracting 1, but when you go modulo x square plus 1, then you disaccord this. So, these are treated has being equal to zero so this is minus one, so now this string therefore contains an elements search that is square is equal to minus 1. Now, so from a certain point of you if you want at a little bit more regulars you really should think of the complex numbers like this, there is this set of all polynomials in determinate x, where the coefficient of real expect that doing the arithmetic modulo a polynomial x squared plus 1. But that is the laborious, but I am sure that you much prefer the vary actually do it. How do they actually handle it we say well we know but that is completely provident to actually sign that rather than r of x modulo this we work with R i where i squared plus 1 is zero in other it being introduce, if we tissues element which we call I having the property there I squared plus 1 equal to 0.

So, that now we are working with polynomials with i is co efficient, so what do this polynomials look like now because i squared is equal to minus 1, you never have to consider polynomial is degree is greater than 1. Because the moment you come into degree 2, we can fold it back, because you can say alive the moment into anything which is degree two I can actually use it to come back to degree zero or zero in i. Therefore this is nothing but the collection of all elements of the form a plus ib where both a and b are actually real numbers now it terms at the finite fields. Actually we can struck it in very similar way, so the complex numbers again to recap the complex numbers you can think of as been constructed as follows you start with the real numbers. Then you take a reduce able polynomial which is x squared plus one and then you go r of x mod x squared plus one and that gives another field. So in terms of the refuse start be with the field, so terms at the refuse at start with the field.

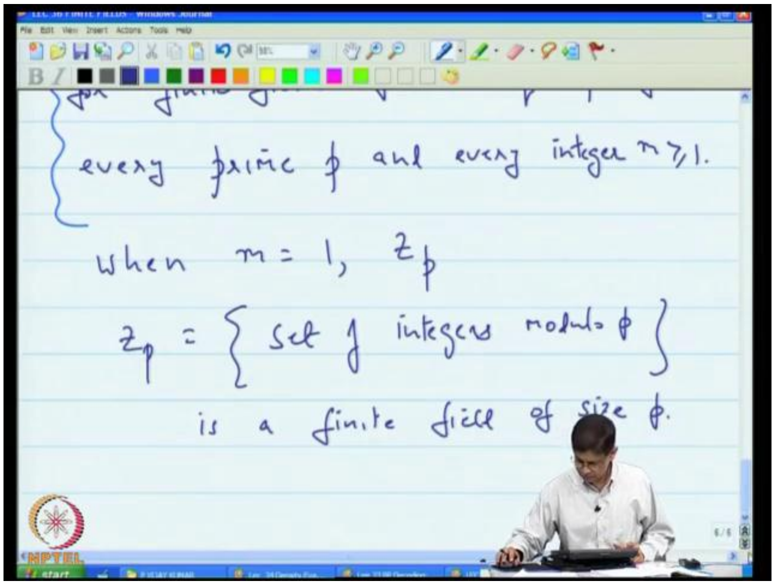
You go modulo and a divisible polynomial where what as a reducible mean it means it cannot be factor so it is analog of a prime number which cannot be factor I will actually write this done little bit more carefully. But just give we by idea so that is a first step that you go r of x mod x squared plus one, then you says that laborious and going to replace x squared plus 1 by remaginar x by remaginar element i and just go to assume i squared is equal to minus 1 which is equal into sign i is squared of the minus 1.

And now go at work with polynomial in i over r, so that is now how you actually bring in imaginary numbers so with the finite fields, we do the same thing or starting point is not the real numbers are starting point are the integers modulo p z p, the integers modulo p we know that the form of field, right. Because the way we sawed as well we saw very early on the, if we looked the integers mod n, then that is a rain and that the n is a prime. Then you actually have a field so this back to an early discussion on ring you can actually go through on your notes, and look that up perhaps.

Your starting point which was the real incase of the complex numbers is now z p, then you and hung for end we reducible polynomial over z p, and in terms of the mat the what degree you name you love this find in reducible polynomial. This is in the contrast the complex number, because in the case of the complex number, you only have any reduce able the polynomial degree two even you have any other polynomial, everything else can be fault. So, at least in the sense that well you do, but once you actually gone from the real numbers to the complex number is any other polynomial can actually be factor over the complex numbers.

In some sense the only radius able x squared plus 1, now with finite fields you actually had the integers mod p, and you take a reducible polynomial they exist for all degrees. And you go modulo that reducible polynomial, and in terms of that gives you all known finite fields all the finite fields. We that let we just start are more formal development in all start writing work are filling.

(Refer Slide Time: 41:05)



every prime p and every integer $n \geq 1$.

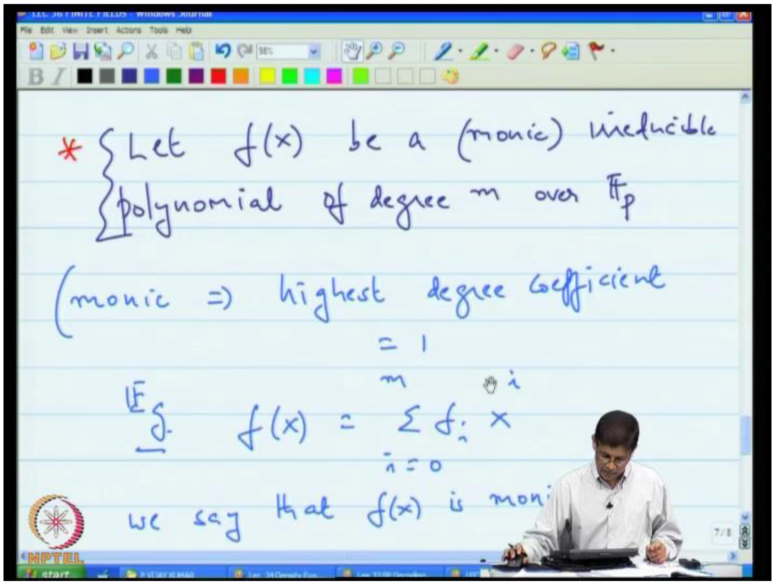
when $m = 1$, Z_p

$Z_p = \{$ set of integers modulo p $\}$

is a finite field of size p.

So, we will now proceed to provide a construction of for a finite fields of size q of size q equal to p to the n for every prime p, and every integer n greater than or equal to 1 then n is 1. We know that z p where z p is the set of integers modulo p, we know that this is a field is a finite field size p know that how to construct finite fields for the case when m is 1.

(Refer Slide Time: 43:05)



* Let $f(x)$ be a (monic) irreducible polynomial of degree m over $\mathbb{F}_p$

(monic ⇒ highest degree coefficient $= 1$

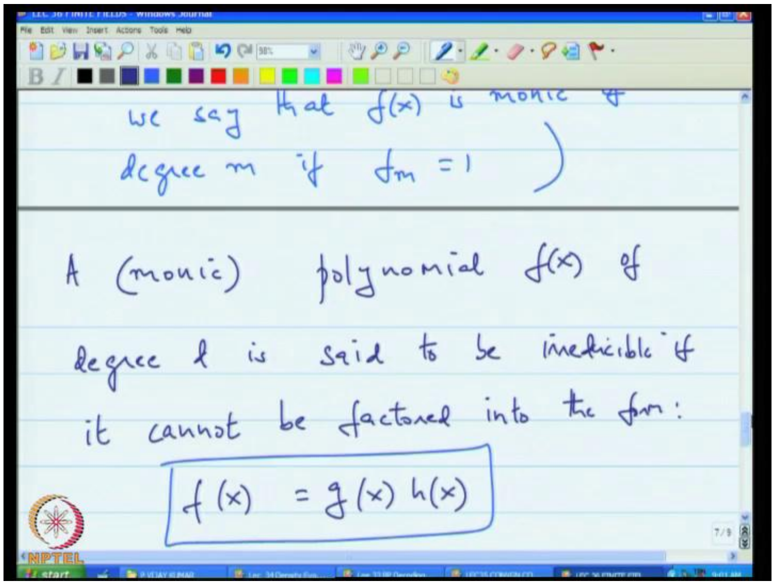
Eg. $f(x) = \sum_{i=0}^{m} f_i x^i$

we say that $f(x)$ is moni

So, let us focus, therefore on the case n is greater than or equal to 2, we focus therefore on the case when the m is greater than or equal 2, so as the starting point of this let f of x b a monic, we reducible polynomial of degree n over fp. So what is the monic, mean monic simply means monic simply means that the highest degree co efficient is equal to 1. So for example you had f of x equal to sigma f I x to the i, i is equal to zero to m. Then we say we say that f of x is of degree is monic is monic of degree m, if f sub m is equal to one. So that is what we mean by the highest degree co efficient we actually look at all these terms the highest degree terms corresponds to i equal to m, so we say there is monic of the degree m if f sub m is equal to 1.

Now the other word here is reducible. What is the reducible mean a polynomial and now just a clarification here have written monic in brackets. Here and the reason for that is that when never is speak of the reducible polynomials.

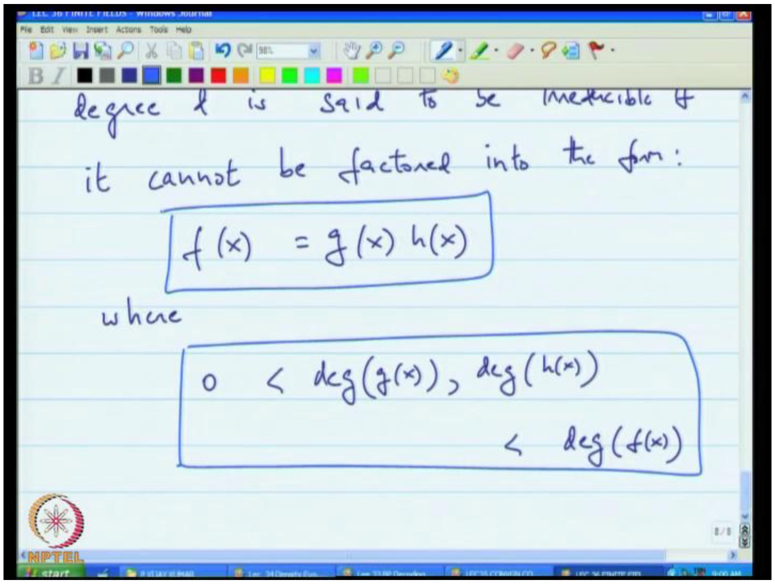
(Refer Slide Time: 46:15)



we say that $f(x)$ is monic of degree m if $f_m = 1$)

A (monic) polynomial $f(x)$ of degree ℓ is said to be irreducible if it cannot be factored into the form:

$$\boxed{f(x) = g(x)\,h(x)}$$



degree ℓ is said to be irreducible if it cannot be factored into the form:

$$\boxed{f(x) = g(x)\,h(x)}$$

where

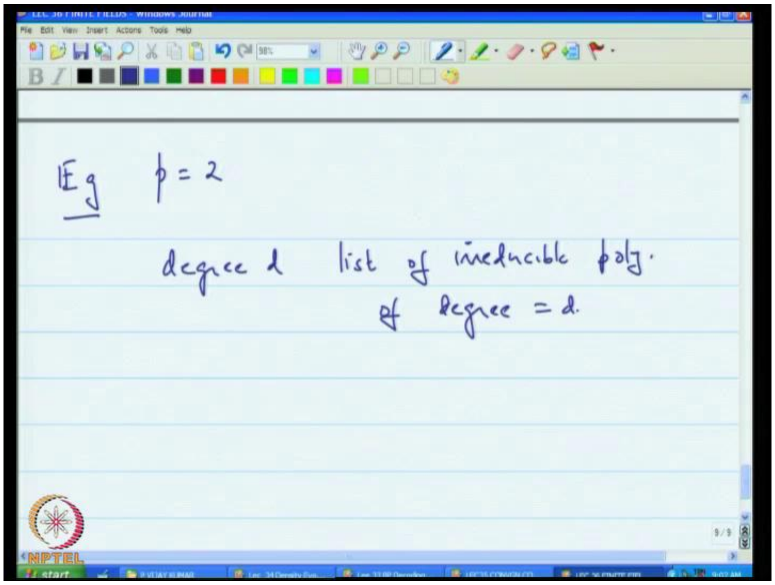
$$\boxed{0 < \deg(g(x)), \deg(h(x)) < \deg(f(x))}$$

We will automatically assume that the polynomial is actually monic. So, we will make there is assumption a polynomial so for that reason. A monic polynomial again in brackets f of x of degree, let us gives this degree of degree d is set to be is reducible.

If it cannot, if it cannot be factor into the form f of x is equal to g of x h of x, where the degrees of both g of x and h of x, so we say that is reducible. If it cannot be factor into the sum where if it is possible to express it as a product of two polynomials both of which whose degree is first of all greater than zero, and strictly less in the degree of f then it is not a reducible. Otherwise, it is so what as an a examples.

Example and by the way are not the polynomials over whenever you speak of a polynomial the polynomial is going have coefficient in a certain field, so are not is in actually in polynomials over the field fp. So perhaps I should where at that here p. Let me just add that here over f p of degree that t, right

(Refer Slide Time: 49:20)

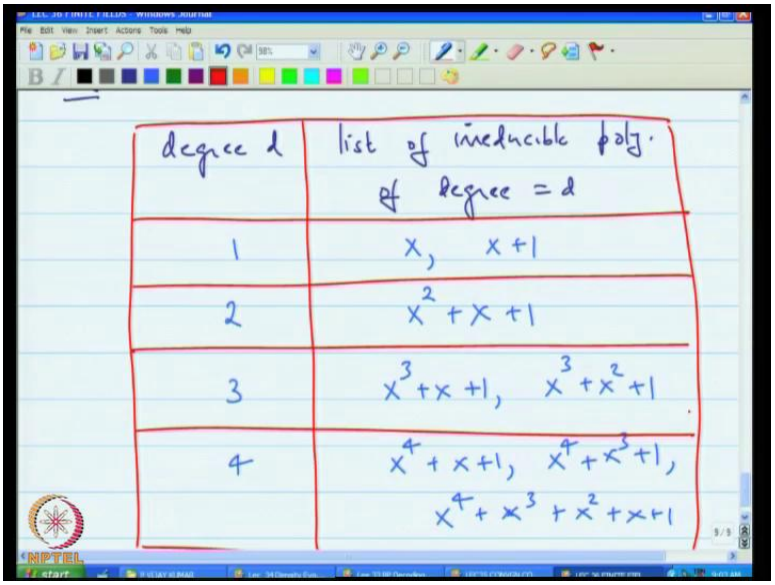

LEC 36 FINITE FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL
start

Eg $p = 2$

degree d   list of irreducible poly.
of degree = d.

So, for example, suppose you will take p is equal to 2, it turns are that here is a list of reducible polynomial is various degrees. So here is the degree and the list of reducible polynomials of degree, so let us the call this degree d, the reducible polynomials of degree equal to d.

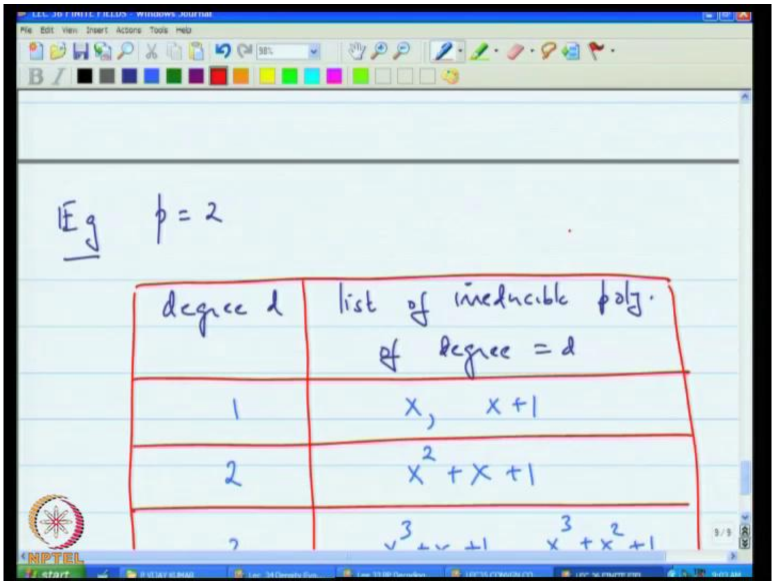
(Refer Slide Time: 49:55)



degree d	list of irreducible poly. of degree = d
1	x, $x+1$
2	x^2+x+1
3	x^3+x+1, x^3+x^2+1
4	x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$

When the degree is 1, then you have x and you have x plus 1, when the degree is 2 you have x squared plus x plus 1, when the degree is 3 you have x cubed plus x plus 1, and x cubed plus x squared plus 1, when you degree is 4 you have x 4 plus x plus 1 and x 4 plus x cubed plus 1 x 4 x cubed plus x squared plus x plus1. It also this list it also if list of all polynomials over f 2 whose degree is that specified.

(Refer Slide Time: 51:12)

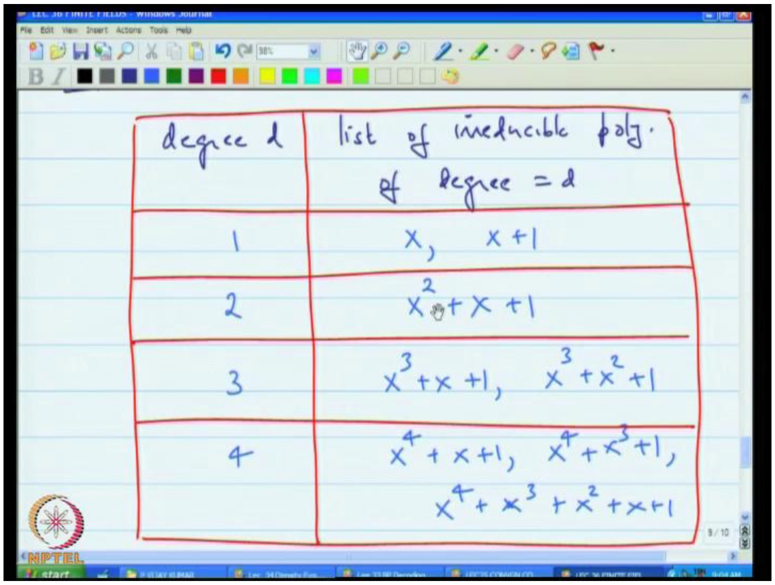


Eg $p = 2$

degree d	list of irreducible poly. of degree = d
1	x, $x+1$
2	x^2+x+1
3	x^3+x+1, x^3+x^2+1

So, these are the only reducible polynomials of these various degrees. The remember sense the setting p equal to 2, the co efficient fields is f 2 is which is 0 or one and that way all this polynomials have co efficient, which i is the 0 or 2 0 or 1. We bought an exercise one to actually verify the, these are reducible there is we take of polynomial like this, it cannot be facted in the of two polynomials whose degree is the less than 3 and greater than 0, and is not hard because you can work your way of through this list.

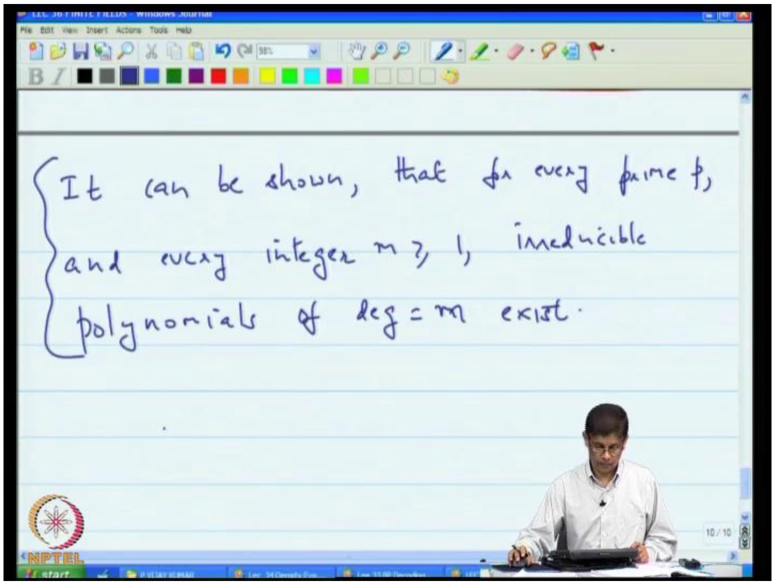
(Refer Slide Time: 51:58)


LEC 36 FINITE FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL

degree d	list of irreducible poly. of degree = d
1	x, $x+1$
2	x^2+x+1
3	x^3+x+1, x^3+x^2+1
4	x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$

It is easy to show that these their reducible then you consider all polynomial of degree 2, there actually four of them, and you can show this is the only reducible, because of can be facted in terms of these, and so you work a way of through this list. So, might be the list so that might be an interesting exercise.

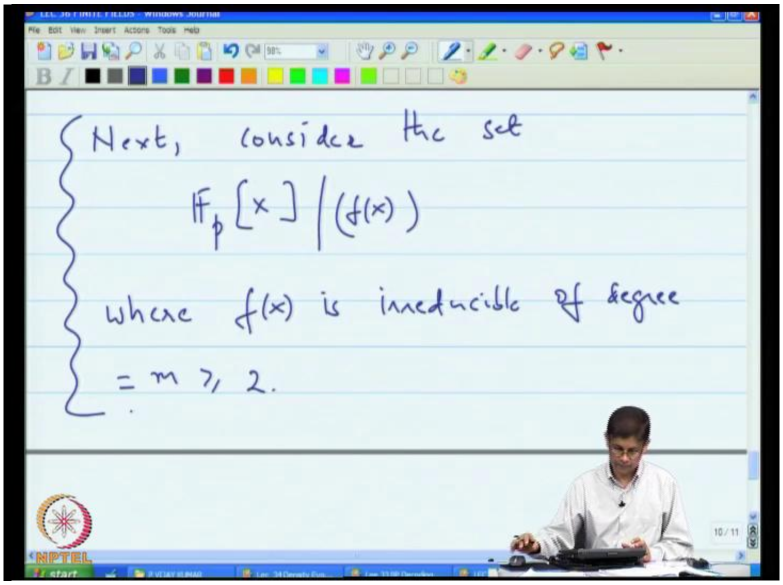
(Refer Slide Time: 52:21)



It can be shown, that for every prime p, and every integer $m \geq 1$, irreducible polynomials of deg $= m$ exist.

Just a common here, it can be shown it can be shown that for every prime p, and every integer m greater than or equal to 1 various above polynomials of degree equal to m exist.

(Refer Slide Time: 53:37)



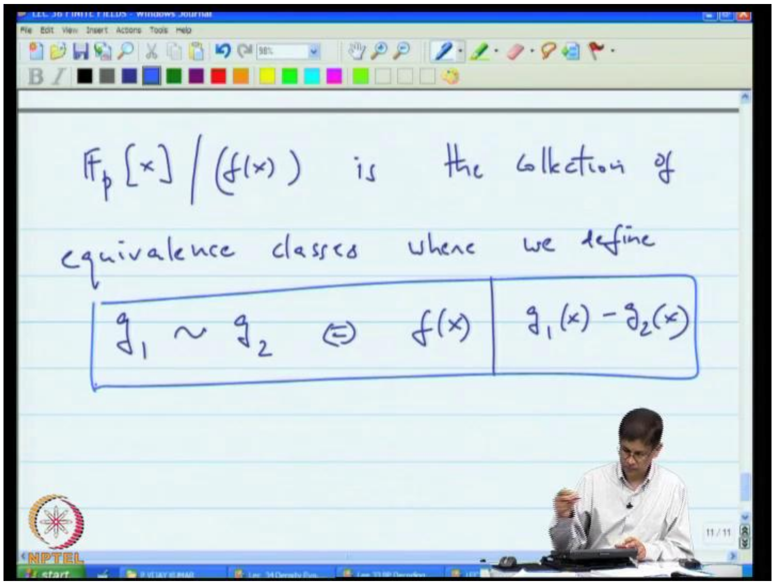
Next, consider the set

$$\mathbb{F}_p[x] / (f(x))$$

where $f(x)$ is irreducible of degree $= m \geq 2$.

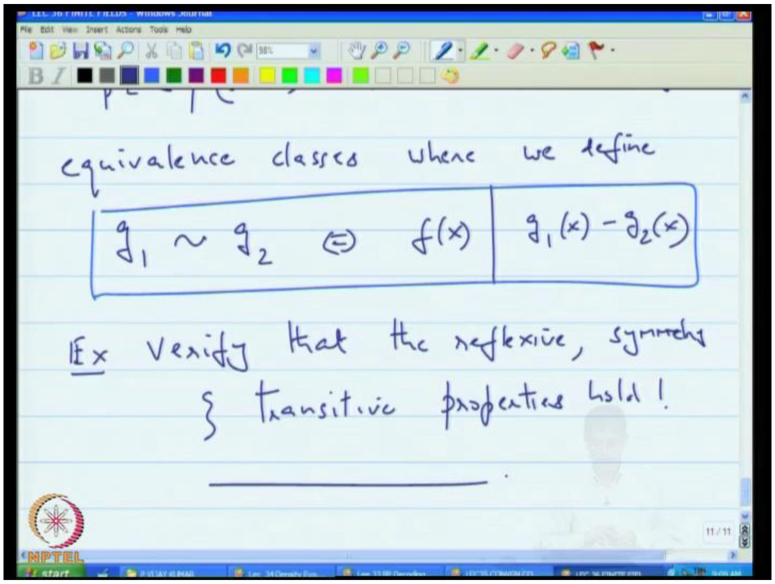
Next consider, excuse me consider the set F p x mod f of x, where f of x is irreducible of degree equal to m equal to 2.

(Refer Slide Time: 54:41)



$\mathbb{F}_p[x] / (f(x))$ is the collection of equivalence classes where we define

$$\boxed{g_1 \sim g_2 \Leftrightarrow f(x) \mid g_1(x) - g_2(x)}$$



equivalence classes where we define

$$\boxed{g_1 \sim g_2 \Leftrightarrow f(x) \mid g_1(x) - g_2(x)}$$

Ex Verify that the reflexive, symmetry & transitive properties hold!

Now what do you I mean by this, so and actually seeing before so this is the collection of equivalent classes, where we define g 1 equivalent to g 2; if and only if f of x divides g 1 of x minus g 2 of x.

Now, I leave it to exercise in verify that reflects if symmetry and it transits if properties hold I see that we almost lot of time. So, just is the pick recap I completed a discussion on the concentration and convergence theorem for LDPC codes. That we shift it girls shift your complete in new topic static talk about algebraic codes, and I started introducing finite fields and

I about to give you an example construction for finite fields which happens to be to really be exact when that sense that equivalent construct every possible finite field using this constructions, thank you and will see you next class.