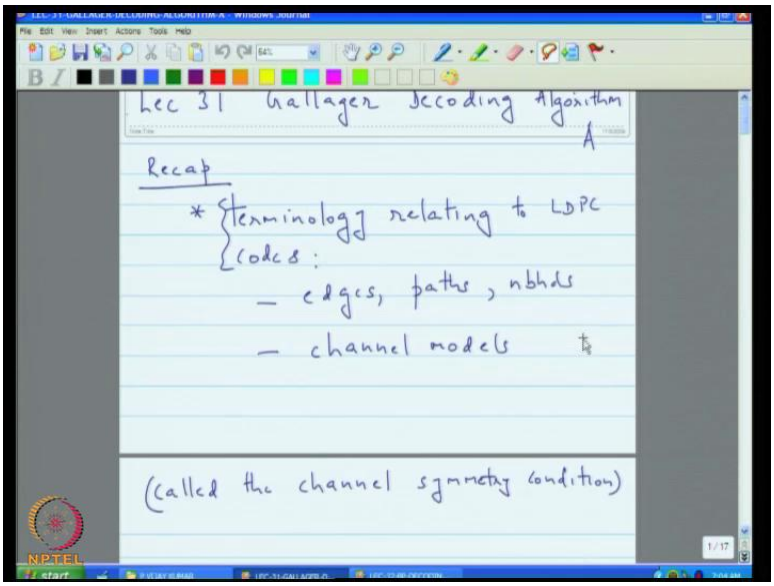
Error Correcting Codes
Prof. Dr. P. Vijay Kumar
Electrical Communication Engineering
Indian Institute of Science, Bangalore

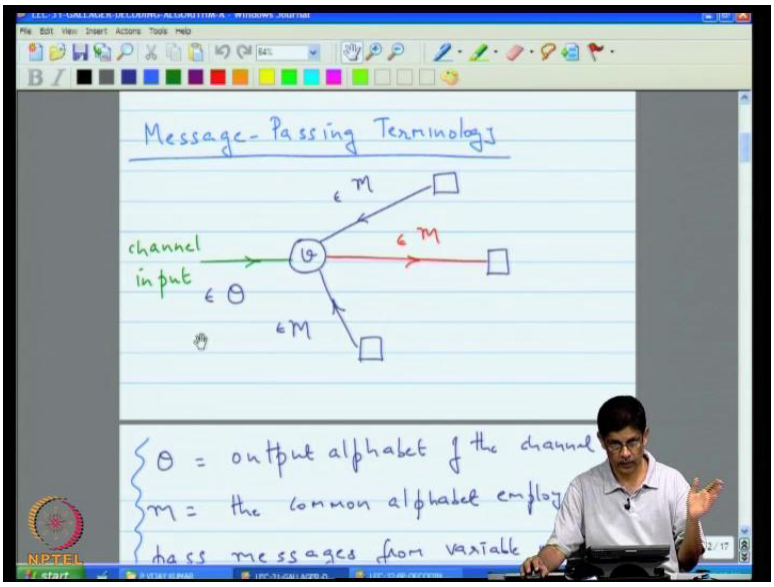
Lecture No. # 32
BP Decoding of LDPC Codes

(Refer Slide Time: 01:00)



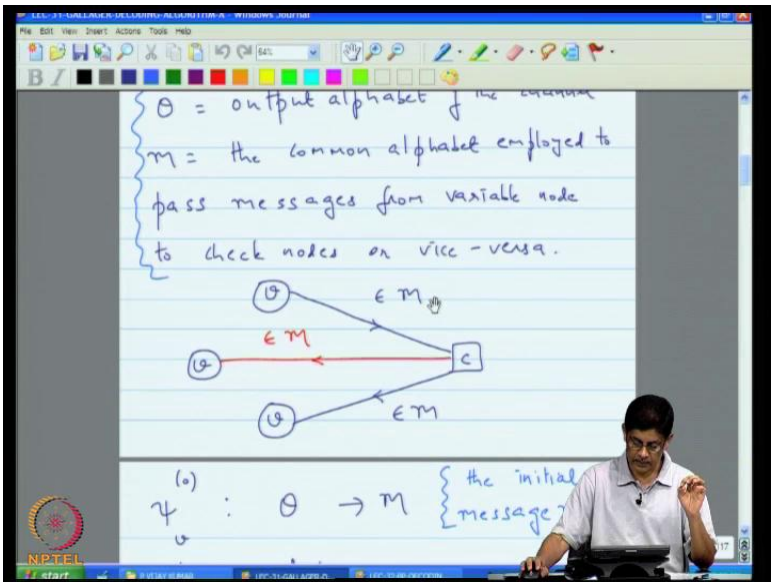
Good afternoon, welcome back; this is are thirty second lecture, and as always let me begin with recap of what we did last time. So last time the title of the lecture was Gallager decoding algorithm A. And I begin, so we are going to LDPC code.

(Refer Slide Time: 00:44)



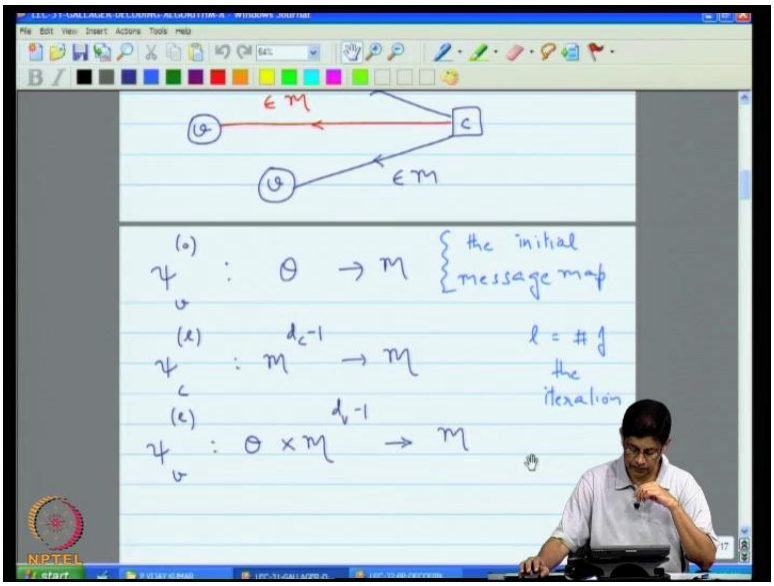
We are going to see how one can decode them by passing messages on the tanner graph that is associated in LDPC code. So we talked about the tanner graph earlier. So in this lecture, in the last lecture we begin by introducing message passing terminology and here we said that o is the output alphabet of the channel; that is the alphabet whatever the channel provides you whatever alphabet it uses that is o. And then for the messages, that are passed back and forth along the age is in the tanner graph there is, a common simple there is script them and that is the message alphabet.

(Refer Slide Time: 01:19)



And is in the base alphabets are subset of the real numbers, and similarly at the check node there are incoming messages that come from the very been nodes and in outgoing message.

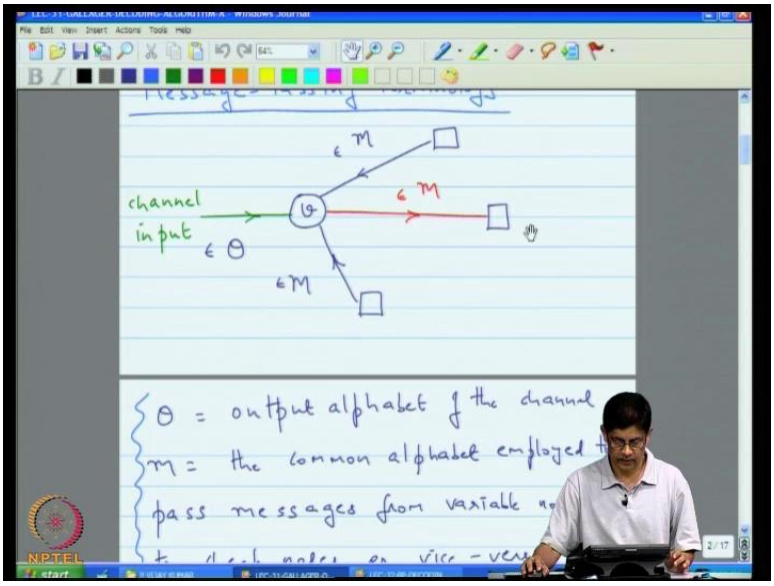
(Refer Slide Time: 01:33)



In general, if you consider the maps each you can regard the operation that is conducted at each node as a map. So for example, initially the variable node a map just simply a map that carries an simple from the output alphabet on to the message alphabet. In subsequent iteration, there are

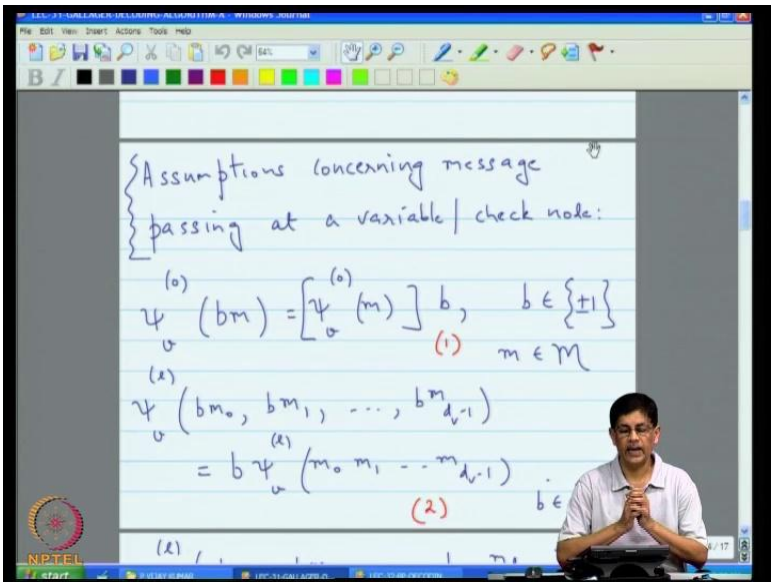
inputs from the check nodes in those situation work the very been output out is a functional not just a channel output, but also the messages there are incoming from the other check nodes. At a check node we just have incoming messages and map from incoming to outgoing messages.

(Refer Slide Time: 03:00)



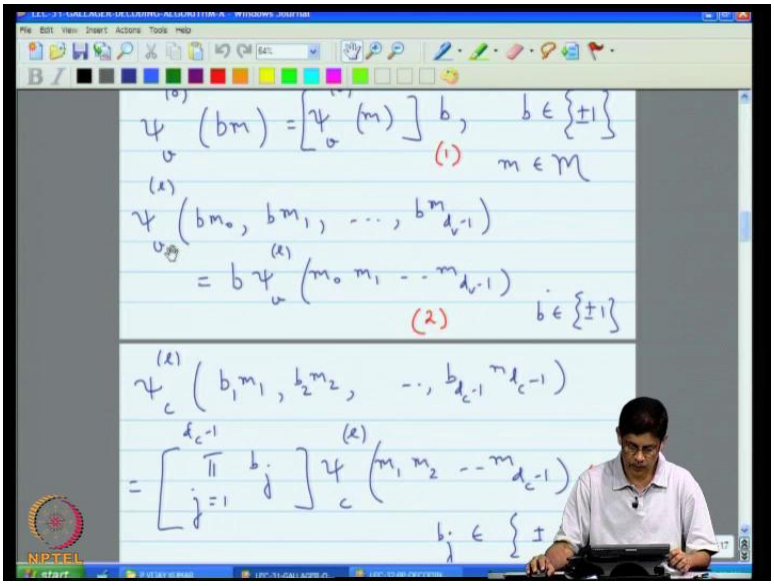
Now in our notation will put a reserve the superscript for the number of iteration. So, the zero iteration, you have messages that go, we have a map that carries out a maps from the out channel output from the messages and thereafter from we have the maps here. And just remind you quickly that the way are iteration go, we initialize some message from variable to check node and that point will start iteration. So the first iteration begin some check node goes to the variable node and comes back. The second iteration thus the same, so the iteration originate in the sense at check nodes.

(Refer Slide Time: 03:25)



There is a zero th iteration in which a message. So that is terminology and we are going to analyses the performance of these decoding algorithms where we are going to actually analyses the performance of class of decoding algorithm.

(Refer Slide Time: 04:00)

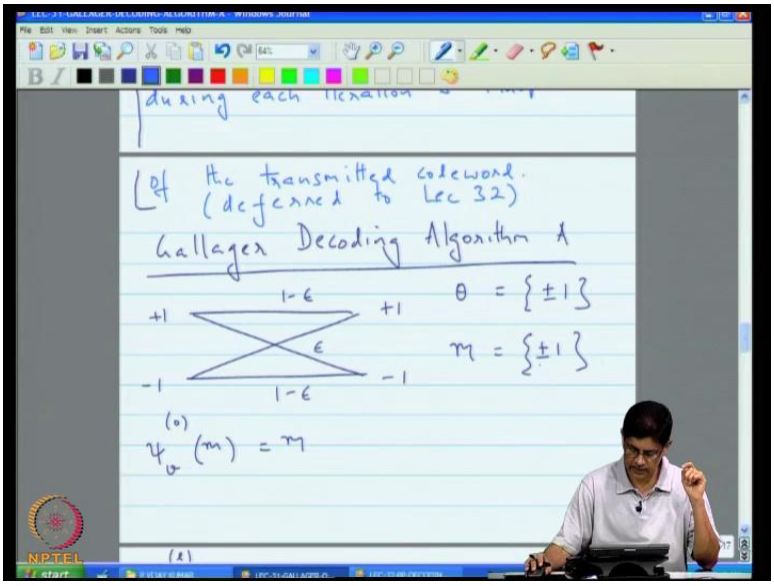


Now these decoding algorithm of certain features in common. Actually the require to making analyses retractable and one of the requirements is that supposing there incoming message from

the channel in b times n in your outgoing message is what to a been. In absence of b times b itself, where b is the plus minus 1, simple. Similarly, at which variable node in the general case if all the messages there are incoming including the one that incoming the channel output are all the scale fact to b then the output also, response scale for the fact b. At the check node if the incoming messages are scale by different constants b i then the outgoing messages is scale by the product of the scale factors.

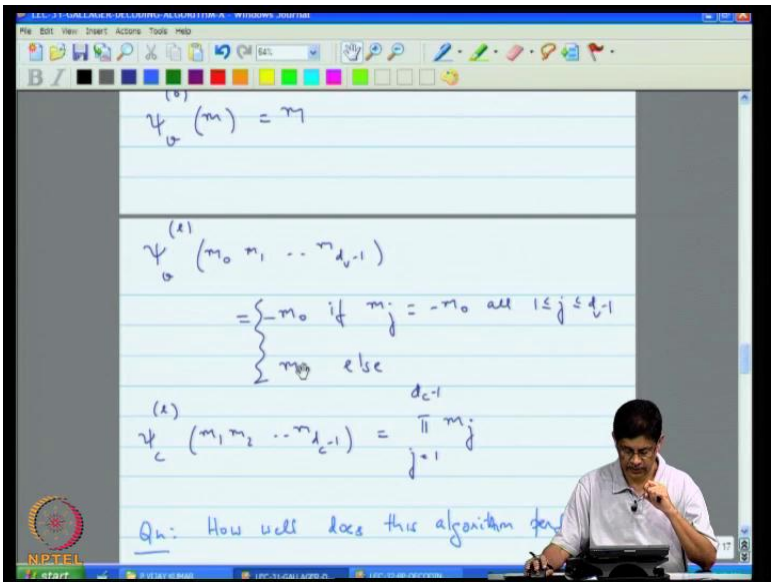
So these are known as the variable and check node symmetric conditions, if you got that word in last time select symmetry. Then, in middle of the lecture have made a statement that we will not proceed to show the number of incorrect messages is past a along the edges of the tanner graph during each iteration independent of the transmitted code word, but actually what we did was differ that lets differ that to let say sequent lecture. When just make a motto fit here that this was differed to lecture thirty two all right.

(Refer Slide Time: 05:00)



And then after that I started a discussing Galleger decoding algorithm A. Galleger decoding algorithm A, so is that initially the message that past on that variable node is simply whatever comes in from the channel subsequently passes on whatever it receives from the channel unless it's over ruled anonymously by all the other messages that is explain by this.

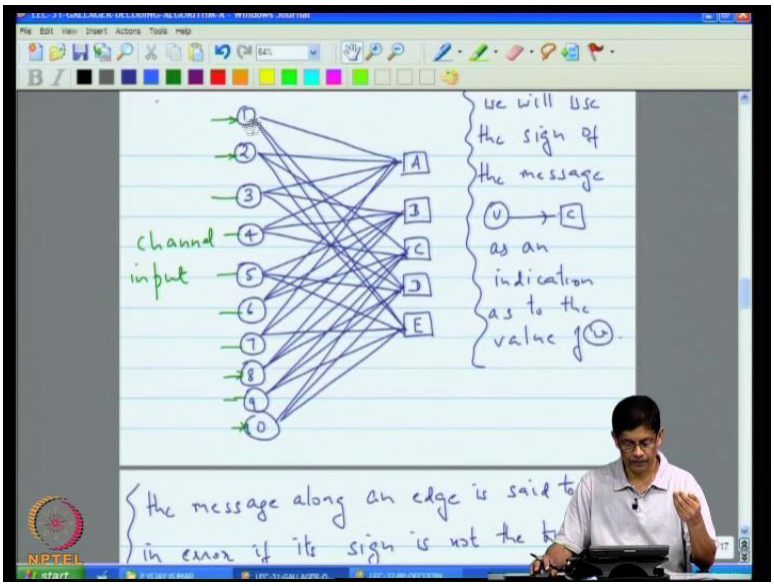
(Refer Slide Time: 06:44)



If the incoming m zero then it is minus m zero if only if all the other m j disagree and say that it is minus m zero otherwise it is m zero and it check node is simply the product the incoming messages. The Galleger algorithm resumes that were dealing with bandwidth metric channel and therefore channel output alphabet x plus minus one and you can see from the way this operation the define that the message alphabet is also plus minus one. So now this point we understand the decoding algorithm one question is, I understanding the passing message how do actually stop the algorithm and how do you make decision. What you actually do is, you can stop after perhaps number of iteration lets the start after twenty iteration and that point what do is an examine the message is that are outgoing along as these edges, leading from a variable node to check node and a check of sign of the messages.

Now these messages are the plus or minus one in the case of the Galleger decoding algorithm. If now keep another think in mind, although they are not actually proving that to be shown it is the case that the performance analysis in term of number of errors made in the decoding algorithm is actually independent of the transmitted code word. So for the sake of convenience, what we will actually do is will assume.

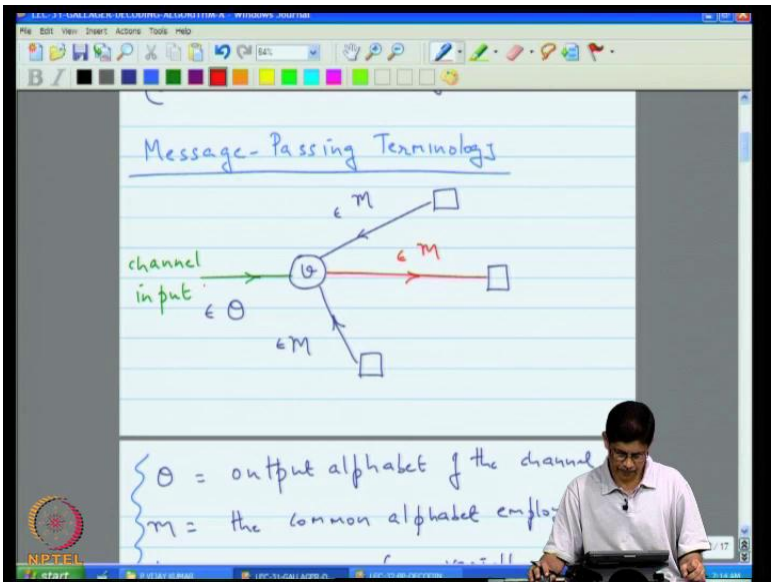
(Refer Slide Time: 08:10)



There are one code word actually transmitted here, giving the there are one code word was transmitted will look at the stana graph and it is a message that going and the from a variable node is check node. You should treat this message as an indication of what this node believe it is value to be. So, since we are assuming that all these values are actually plus 1. So, all one code word, I mean the all one code word with reference to the alphabet which is plus minus 1.

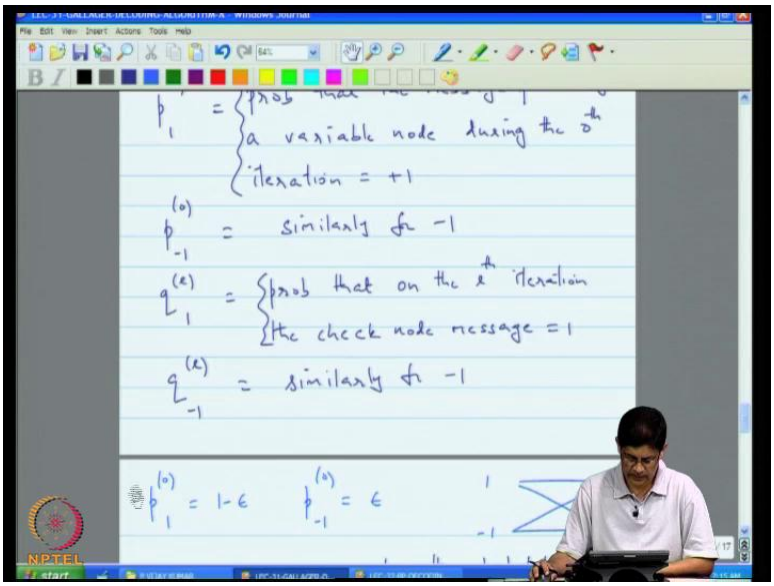
If you look if message on a edge and it is maketive, then that is in decisive in true value, because we already more the true value is 1. So, performance analysis resume that all one code word was transmitted. So, that is what you mean by name correctness, so when speak of an incorrectness is being sent over the stana graph, what we mean is that sign of the message that is transmitted along an age in the stana graph disagree with the value plus one and code in the which means the basically. So, how does it algorithm perform? We will evaluate performance by carrying out density evolution. This is the little bit mass fancy at term the minute for present all that mean is that we will estimate the number of incorrect messages for in each iteration, and will do the iterated fashion.

(Refer Slide Time: 10:00)



This is west to peep a resuming and in enforces a by writing a syndrive will resume that the all one code word the actually transmitted. Now, initially in the initial iteration when we actually have smuggling back here, initially a message there actually goes out from the variable node, and all that the variable node does we have disappointed just simply passes on whatever treasure from the channel. Now, how correct or incorrect is there, the channel begin bangle symmetric the probability there it actually, such an incorrect message. There is fields in incorrect message to the node is 1 minus epsilon, it is a epsilon sorry. So, the probability of an incorrect outgoing message is one if epsilon enough correct is 1 minus epsilon, so that in sense the density evolution process.

(Refer Slide Time: 10:45)

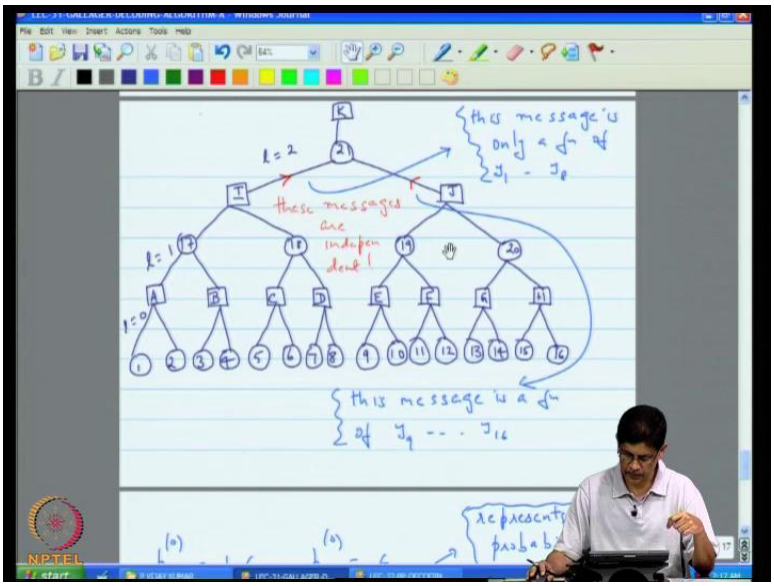


So, p 0 is, p we denote p is following terminology p 0 1 means the probability that the message pass by variable node during the zeroth iteration is 1 and similar for this. And you can see that, because done the symmetric channel, this is the channel output the team management going to be epsilon. Because we know that the actually transmitted code word is a 1. Now, in look to this won the word, how can you do not have any this stands for utilization.

This stands for the value of the code symbol, how can you do not have any notation that indicates the particular node; that is a passing message in the turn a graph. How can a notation does not reflect which node and transmitting out of… An region for that because is symmetric, the probability will be the same, because every node is operating and identical is the constants, because the input probability are epsilon 1 minus epsilon for other 1 minus epsilon for all though very been nodes.

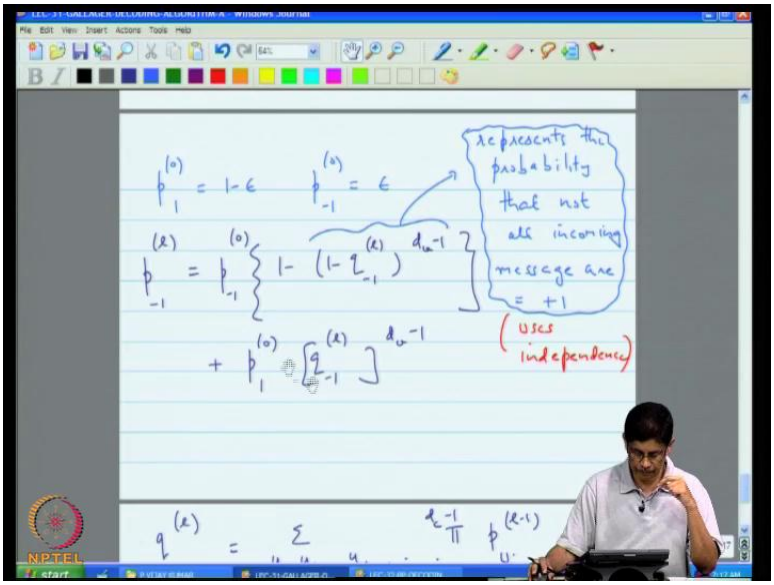
This is common, so therefore these are initial probability and the these are a used to jump start iterated process. Then subsequently what happens? So, now the notation is that king one of well is the probability then in l th iteration, the message the goes out from a check node to the very be node is the actually 1.

(Refer Slide Time: 12:45)



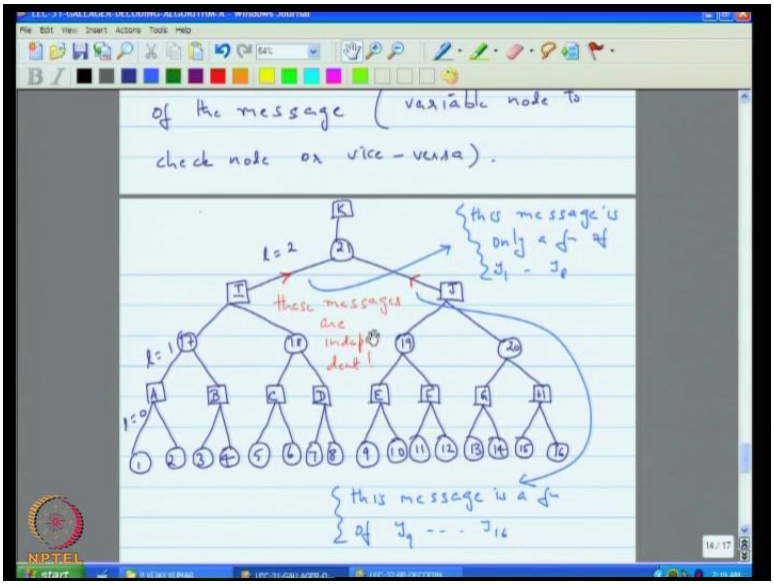
We are talking about the probability that this particular message, that the message that is outgoing from the check node is actually the plus 1 or minus 1. And similarly, for q of minus 1 then the going to be some calculations, and aboard this figure in here to explain those, but let us kept to the calculation in comeback to this graph.

(Refer Slide Time: 12:55)



What an actually said was that, let us look the probability that the message that the outgoing from am variable node is minus 1. Now, it is the minus 1, if and only if either the output from the minus one and all the other are not unanimous in the declaring it 1, which is represent by this term or it is the one and the other are unanimous in the declaring it minus one. When actually race is to the power here, I am actually using independents meaning that any, so let us take a look at the stana graph here the segment of it.

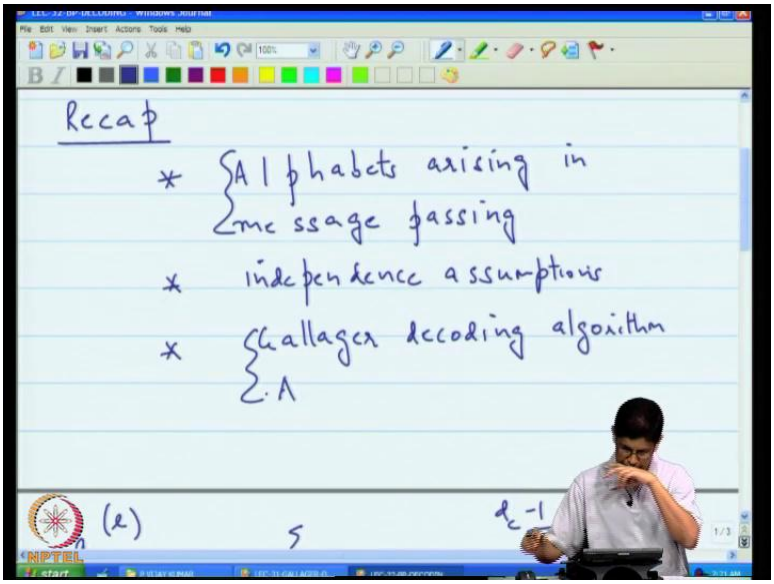
(Refer Slide Time: 14:00)



So, here this variable node is receiving a messaging from the channel; and also I am receiving from the other check node. Now, these message are either plus or minus won certain probability, and the probability depends only on the channel realization, because there is no randomness any more in the code word selection, we are assuming the code word is all one. Now, these messages are independent, because each message here is independent message wise that, here the competition tree which allows the helps as understand that. Let us say a passing message of from lets a certain variable node to a check node. This message is a function of certain receive symbols, so now let us say that this is a first iteration; see the zeroth iteration is when variable node pass message is to check nodes. On the first iteration the check node sent the message to variable node and then back to check node and so on.

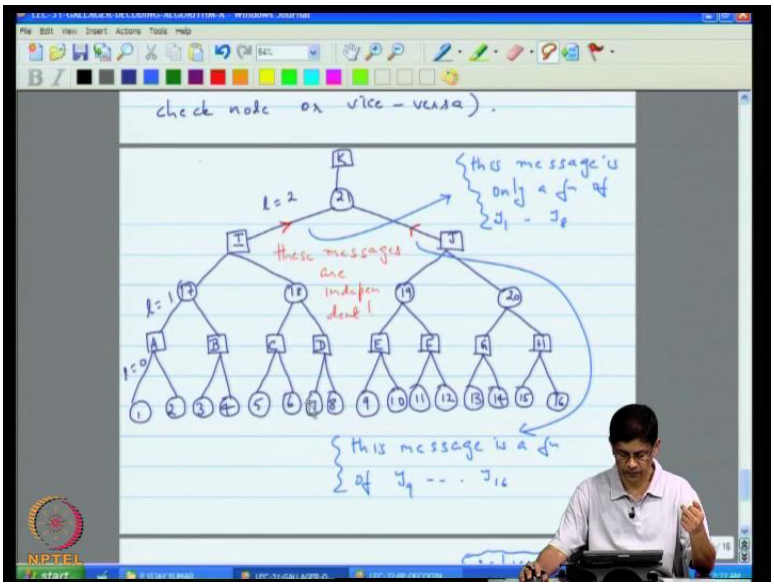
Now, when we look at the message that incoming to a variable node, like from example this one this message here is pearly a function, let us see that and the second iteration this message is pearly a function of these receive symbols. Likewise this message here is pearly a function of these receive symbols, therefore these messages are independent, and this is what justify this multiplication in the probability here. So, this was how you evolve from q minus one l to p minus one l. And I think, I am going to actually, repeat this part of the derivation again. So, let me first of all copy this page. I am cut this page because; we are going to carry out to the next lecture.

(Refer Slide Time: 16:05)



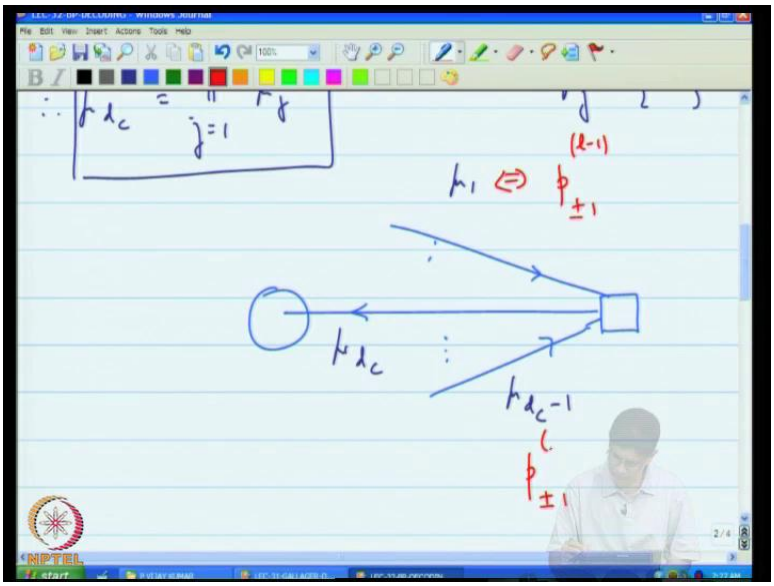
This is a recap, what be talked about is the alphabets arising in message passing. We also talked about independence assumptions, and then we behind discussing, Gallager decoding algorithm A.

(Refer Slide Time: 17:26)



Now, other fact that, I think I mention that this sometime earlier that this density evolution analysis there actually carrying out resume that your operating with stena graph, which is tree like which to depth 2 l has tree like neighbor; that is if a carrying out two iteration then to depth four it's a tree like neighbor which means, that none of this variable actually repeat. Because it perfectly possible presents of cycles example, this variable node here, who is the same is the variable node that would indicate cycle of the length eight. So, where assuming that up to depth eight, there are no up to length eight there are no cycle, and which is same is in up to depth four there is no repeat symbols. We are assuming tree like neighborhood.

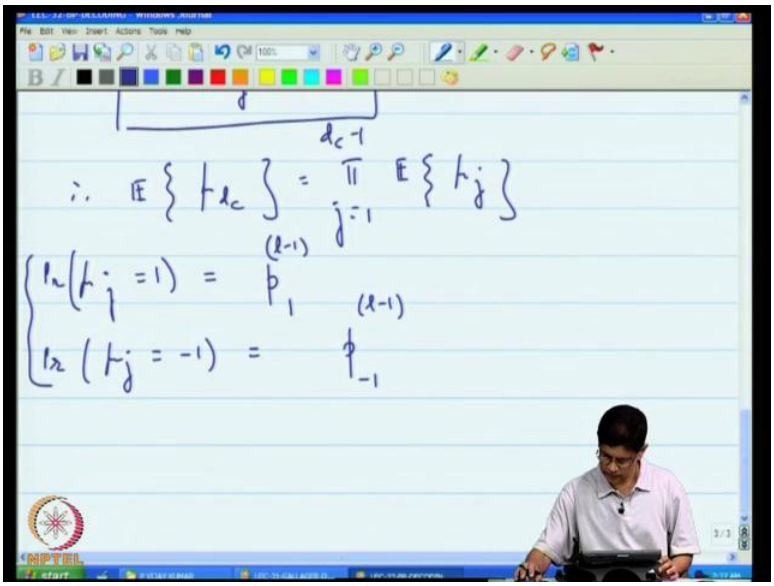
(Refer Slide Time: 18:27)

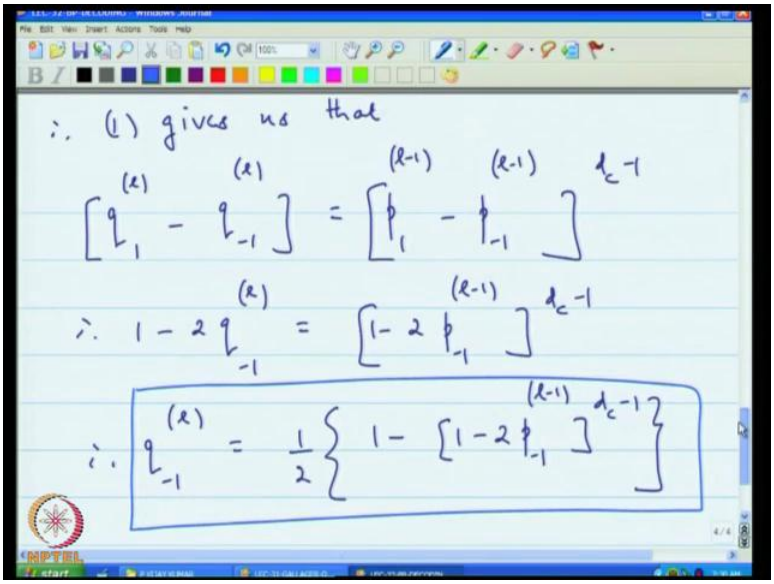


Now, we are started out with the calculation, let me just read do that I think a we may be do it know simple of as today. So we are now looking at check node, and namely introduce some notation here, let us say that the message that actually being past here is a symbol for the you one. So, may be a should change that to something else, let us assume that it is a incoming messages or let us a mu one mu dc minus one and that the outgoing message is mu dc. And we know that each of this mu is there a plus one or a minus one, we also know that Gallager decoding algorithm simply says that when you pass message is you just at check node a simply multiply the incoming messages and thus have a compute your outgoing messages.

So, what that means is that therefore mu dc is the product j equal to one to dc minus one mu j, and I want to carry this towards to the next page relax copy that. And now this are random variable, because the messages there are been passed random variables, which are functions of the receive variables, the random is ranges only because of the channel predicable channel realization tell as take expectation on both sides.

(Refer Slide Time: 21:19)





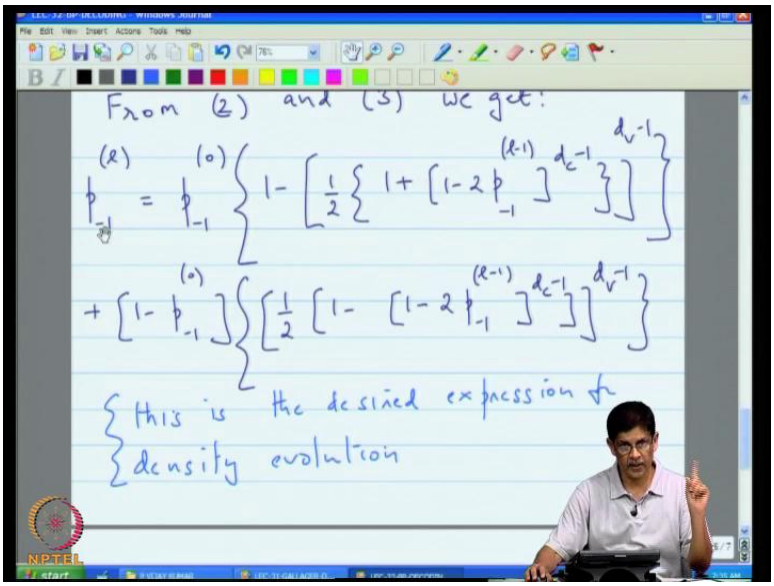
Therefore the expected value of mu dc is the product j equal to one to dc minus one expected value of mu j now the probability of mu j probability that mu j is equal to one in are notation.

We are talking about messages there are ongoing to check node is p l minus one one, and similarly the probability that mu j equal to minus one l minus one. This is the plus minus variable when you compute the expectation, all call this one. Therefore one gives us that and I give. Similarly, back here again, so this messages here are associated with probability is being l minus one be the plus or minus one. Similarly here this message of here is associated with probability q of l plus minus one, because this is density evolution giving density is of the incoming message.

You compute density the outgoing message and since iteration begin at check node see a going from the l minus one iteration to the real iteration thus the competition will doing. So, in terms of the expectation that therefore q of l one minus q of minus one l is equal to am p of one l minus one race to the power d sub c minus one. Now you race it to power, because of the independent examination and insure of multiplying j minus one terms, which have a single term because all the density along all the incoming messages are actually identical I recognizing that. Of course it shall this to that, if you add this to probability is will get a one, therefore it follow that one minus twice q minus one l is equal to one minus twice d minus one l minus one to the dc minus one therefore q minus one l is equal to one of minus two d minus one l minus one dc minus one. This is the begin of width. We can legion to the expression that we have in the last lecture, which are going to actually any copy of the page this is remove some of the material do not it k.

The actually have they will expression for q minus l of l in terms of p minus p p minus one of l minus one have a p minus one of l in term of q minus one of l put, the together. So, five call this which I call this two this is two.

(Refer Slide Time: 27:02)



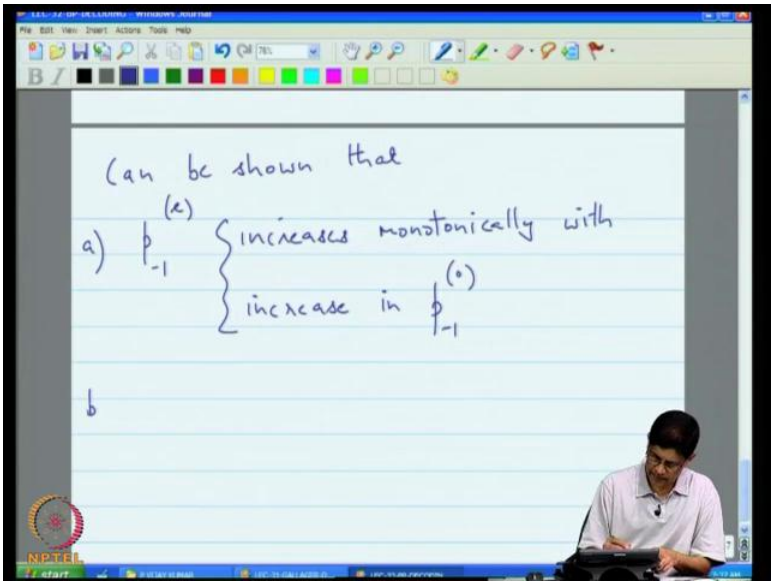
And let me call this three then from two and three from two and three, we get that p minus one of l is equal to p minus one of zero times one minus one half as one plus one minus twice p minus one l minus one to the dc minus one dv minus one plus one minus p minus one zero of one minus twice p minus one l minus one to the dc minus one to the dv minus one. I think a which is correct there something not quite right here, for that is this is half into one minus one minus two p minus one l minus one dc minus one we close this we close this use these do minus one, this is what we half.

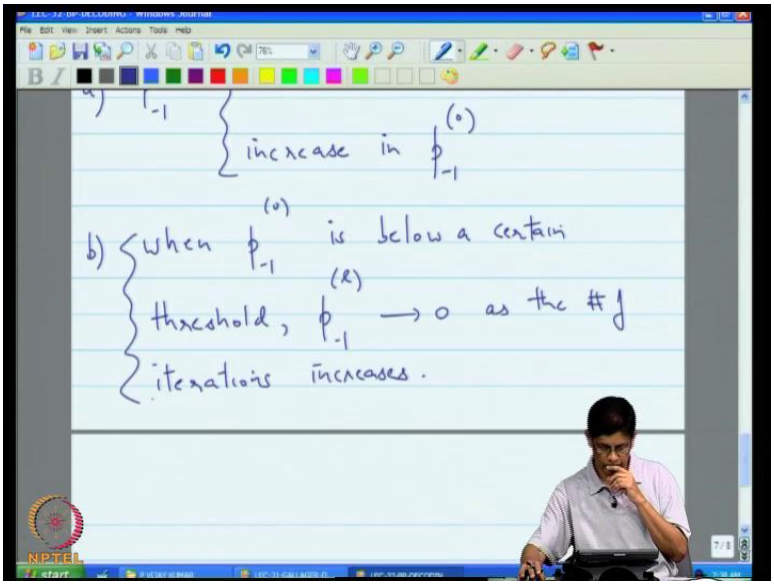
And that is work dense this is the desired density evolution expression in density evolution are a mister actually find are recursive expression for the number of incorrect messages past along.

What fill actually done is be we found out the probability there a message on the certain iteration on the l th iteration is incorrect, because minus one represent in incorrect message after all we presume that the all an code word was transmitter. These are this is the probability of incorrect message and what be do it is expression, it terms of the initial channel probabilities, which are epsilon or one minus epsilon which are none and in terms of the corresponding probability in the previous iteration that was be actually, wanted do what you can actually suspend little bit of time. You can show couple of things, you can a will basically you can actually show that these probability at any iteration increase with increase the channel cross probability that is one.

The second thing you can actually show is that as long is the channel probability is believe as certain threshold d th probability in incorrect message with increasing number of iteration is goes to zero the caveat is that.

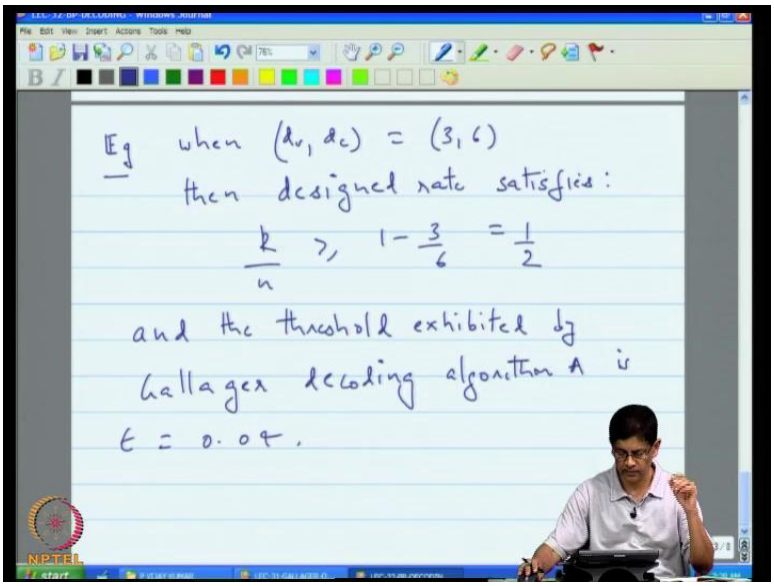
(Refer Slide Time: 31:25)

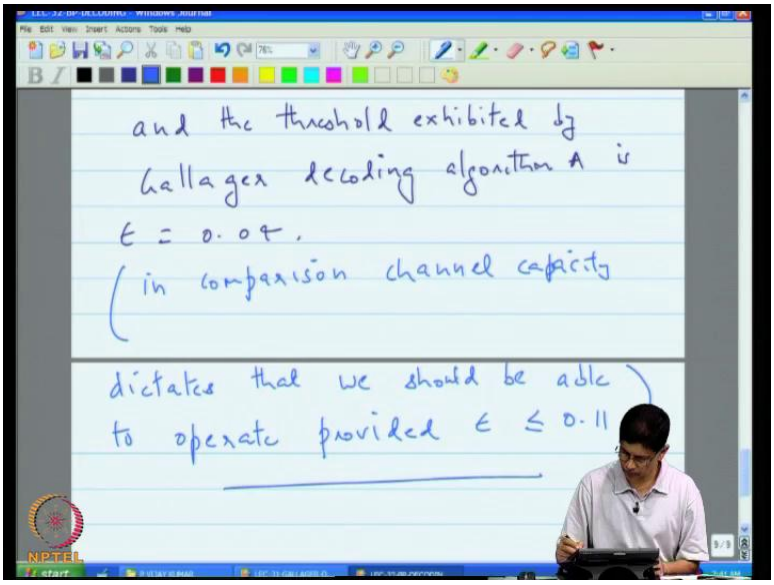




We do is that the neighborhood is tree like when we make this statement let me this put, that down can be shown that p minus one l increases monotonically that believe a set in threshold one really with increase in p minus one of zero. Let us one in p minus one zero is below certain threshold p minus one l goes to zero as the number iterations increases.

(Refer Slide Time: 33:22)



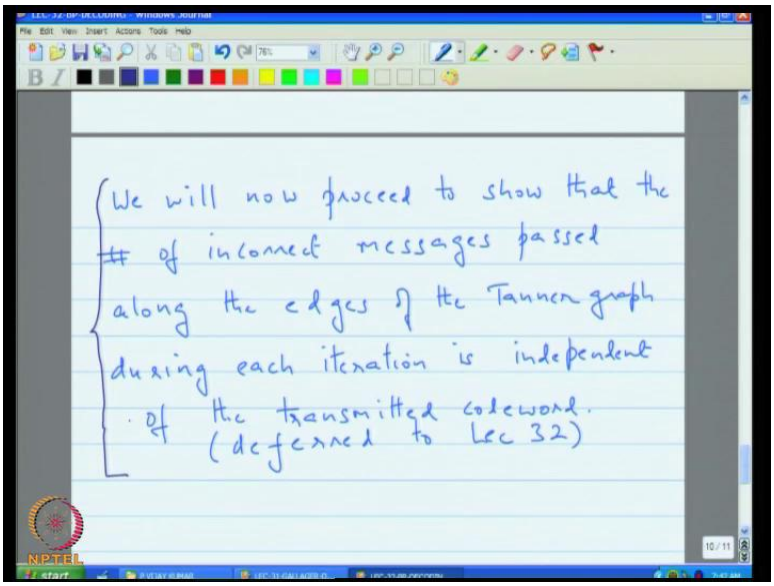


For an example when dv dc equal to three comma six then are design rate satisfies k by n is greater than are equal to one minus three by six, which is one half and the threshold observed here and the threshold exhibited by Gallager decoding algorithm a zero point is cross probability equal to 0.04, which mean that provide the cross probability is less than 0.04.

We will make are a free decision however, income this is the , simple decoding algorithm is an expect to much out of it just make a quick node that in comparison channel capacity dictates. We should be able to operate provide, it epsilon is less than 0.11 that finishes are analysis of glade

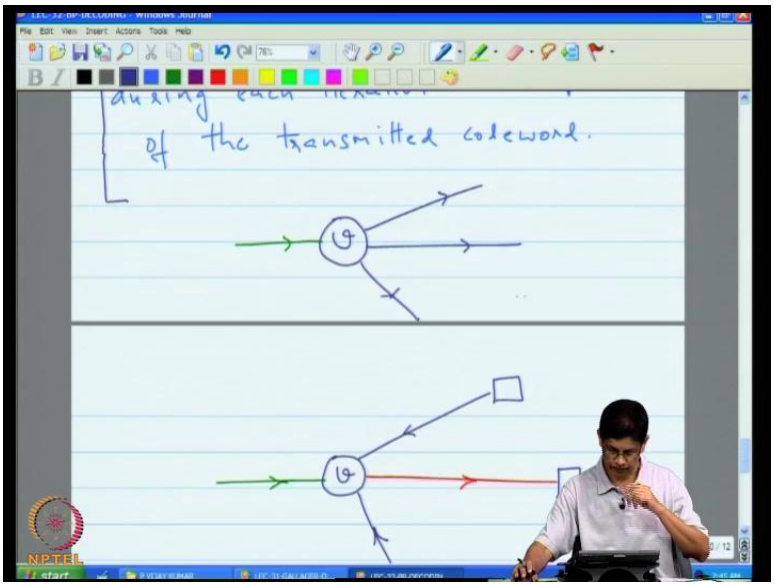
decoding algorithm A, what like to do next again go back to our last lecture and proof something, we are left un finishes last time mainly the proof of this particular statement.

(Refer Slide Time: 37:25)



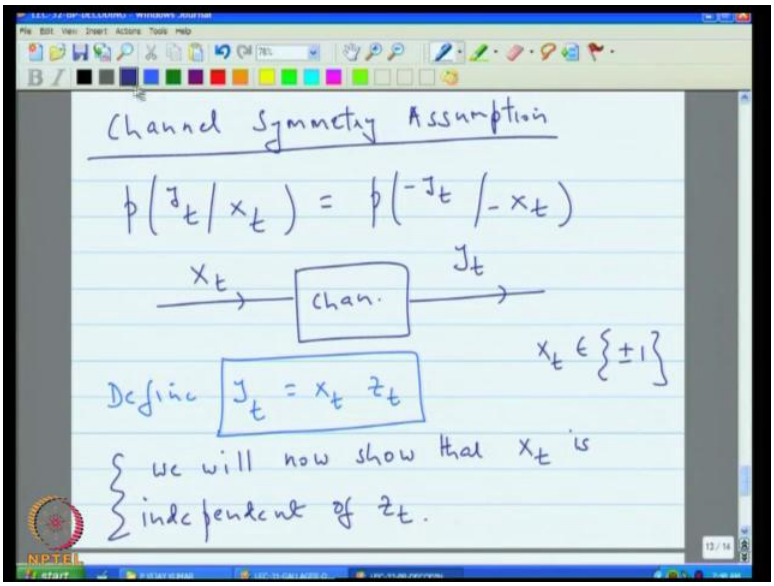
We will now proceed to show this is carried out last time, then the number of the incorrect messages past along the ages of the tanner graph during each duration is independent of the transmitted code word, this was early a differed to let us less remove this let us show, how we do that am going to actually pickup couple of picture from the last lecture.

(Refer Slide Time: 38:56)



We have the this picture here for messages is as well as this one am also going to draw one additional picture here, am going to make the saw the quick are is someone , it make it draw the quick the idea is the actually, show that let us a then the channel realization fixed and the real of the code words to varying and want to show that the number incorrect messages edge by edge iteration by iteration, when is the same therefore the without loss a generality and for sack of the convenience. We can actually resume that the all one code word this actually transmitted, but am going to make a slight, first talk a little bit about the channel.

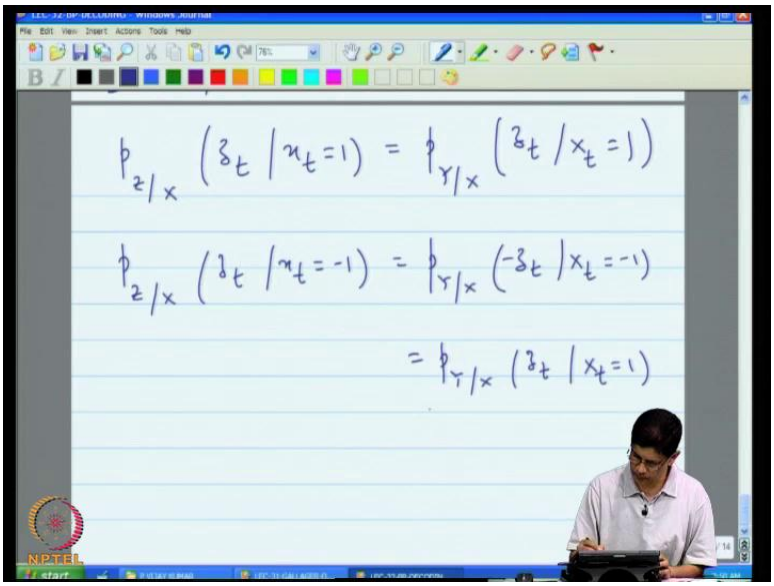
(Refer Slide Time: 41:02)

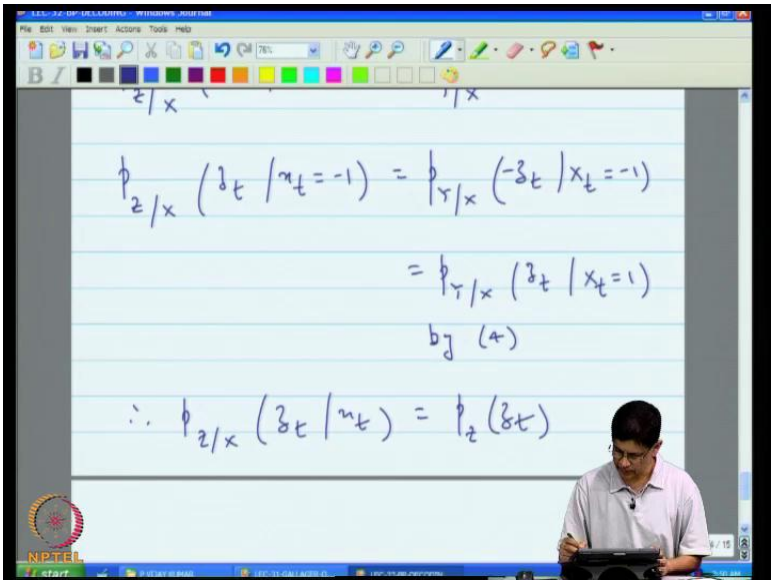


Now, we had channel, if you call early an actually talk to about the channel. We made the following examination, which I called at the time the channel symmetry examination, which basically set that the probability of yt given xt is equal to the probability of minus yt given minus xt here. An I am thinking of the following picture that is the input to the channel xt, and the output is yt, and xt here xt here is see the plus or minus one define here yt equal to xt zt.

So, other word are define zt as yt divided by zt free to do this one actually show is that, we will now show that xt is independent of zt what is happening it mean that you can actually view the output of the channel as taking something pearly comes on the channel, and multiplying by the input. So, symbol because is no coupling between, that the not dependent on and make use of this particular equation let me called at 4.

(Refer Slide Time: 43:30)

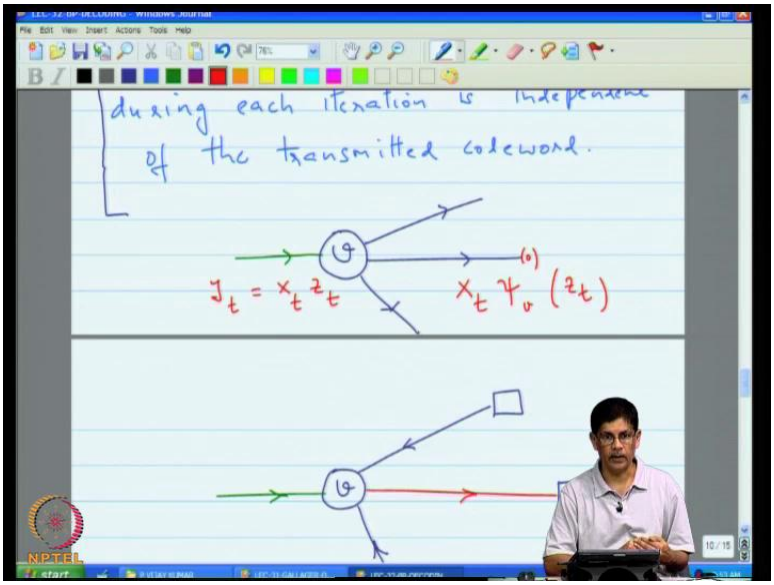




So, p of let us say p of z given x of zt given xt is the same as p of are that, we condition this upon a xt equal to one. If the probability when xt equal to one of cb equal to is zt is the same as the probability y equal to zt given xt equal to one, will right that xp of y given x of zt given xt is equal to one p of z given x zt given xt equal to minus one is p of y given x, and this time is xt is minus one this yt is is equal minus xt. This is the probability of minus zt given xt equal to minus one, but by the channel symmetric condition. This is the same as p of y given x of zt given xt equal to 1.

This is by equation four, which is of channel symmetric condition, that means is that the probability of zt does not depend upon the xt is plus or minus one. Therefore, independent therefore p of z given x zt given xt simply up p of z ct its independent of that is one thing is keep in mind then the for that, we have a very simple picture of the channel namely that what the channel does it is take whatever, the input is that is under the channel symmetric option it take whatever, the input is multiplies it is by the set in random variable zt.

(Refer Slide Time: 46:20)

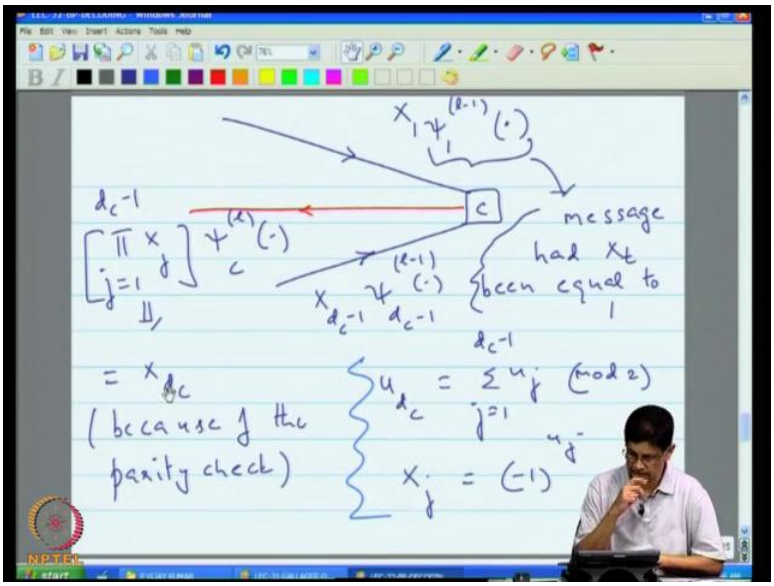


We want to actually say that the number of incorrect messages remains the same here, up consider that a yt is is your incoming he incoming message is yt, which is equal to xt into zt. Now, what is Galages let us we assume in are a very been node map, I think we define that perhaps in some point in our last lecture, that is that here, when so this called member the variable and check node symmetric condition.

So, let me underline that jumping from current pass lecture, but hot copy of this that show the message issue the matter by the variable in check node symmetric condition, one of the examination was that, if you multiply the input t by a binary plus minus one symbol that fact as the write how to the message. What that means is the here, the message that actually past here is

a is xt is xt times psi zero v of zt, that is the message that past, when the symbol is xt is xt times what it have been past had xt be is equal to one keep that when we go to a check node.

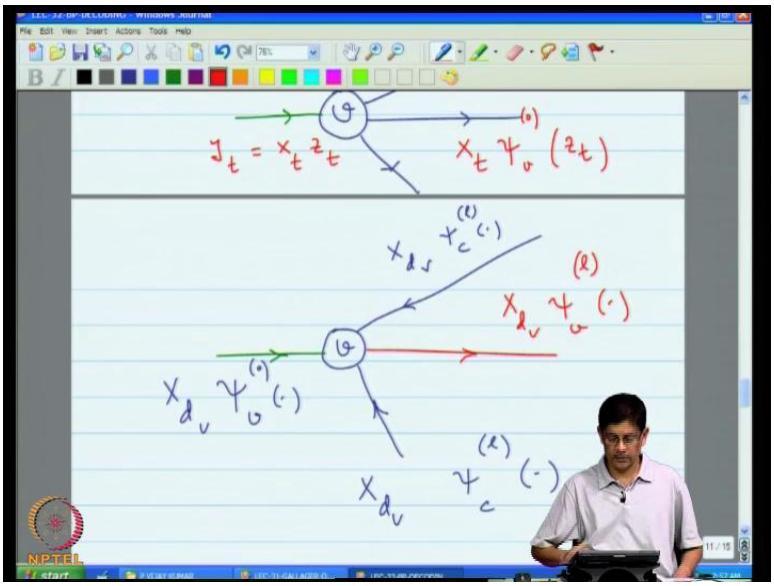
(Refer Slide Time: 48:20)



If you go to a check node keep in mind that the messages there coming in are in general xt times psi sub v of l minus one times the messages is that the would have this is message with xt equal to one had xt been equal to one, so general word happens is that this xt keeps propagating and multiplying each messages The incoming messages are multiplied like this and also palming called actually am let us say the this is x one, and then should also be this should be x dc minus one size dc minus one l minus one of whatever the message would have been in the absence. We should also been an incoming messages.

What is the check node do check node simply takes it is also the whenever the incoming messages are multiplied by set the factor it multiplies those fact as out an subsector. What comes out is the product j equal to one to dc minus one xj times the message that do a been sent out had all the message been one, but this think here this is precisely equal to x sub dc, because of the parity check that, because a parity check impose the condition that u dc was equal to u sub j j equal to one to dc minus one mod two, and your x j was minus one to the u j.

(Refer Slide Time: 51:22)



When we look at the parity condition in the plus minus one domain then the product of that causes the product actually equal x dc. So, what happening here is that if your incoming message are multiplied by the corresponding variables, then your outgoing messages are also multiplied by corresponding variable. Now, you come a here to the general case when we are looking at excuse me, what happens at variable node the incoming message here is x one times psi c l whatever it would mean. Here it is x dv minus one time size c l whatever I would have been have xt equal to one.

We know let us call this one here is x dv time, whatever the channel input message would be these are all x dc a the message is are all depended upon were there headed . This was x dc this is the x dc or dv, this is the x dv this is the x dv the outgoing message is also x dv times whatever the message would have been had x all the x is been equal to one as the result. What happens is that a message is are always x the value of the variable times whatever the messages should have been had the corresponding x b equal to one.

When we actually say incorrect your actually comparing the sign of x dv the true value x dv with sign of this message, but this like comparing these against for the this is one or minus. Therefore, for this reason the number of incorrect messages is independent of the transmitted code. We have about two minutes left lime just summarized, what we dead today basically, what idea was I

completed are competition of density evolution with respective Gallager decoding algorithm a iterative clarify a few thing which are thought were not clear last time.

We went head and proved at the statement there are at may last time that the number of incorrect messages is independent the transmitted code word in the for a free to zoom in the analysis that the transmitted code word is that fills the hold in are a development with theory from last time. What lies ahead next time what will actually do is that we actually look at a look at one decoding algorithm this is Gallager decoding algorithm a. Next time will actually look at an algorithm which is called the belief propagation algorithm, it is , but all that really doing is basically using the message passing algorithm that we develop using the gdl and the junction trees. I catch of with you and the next class, thank you.