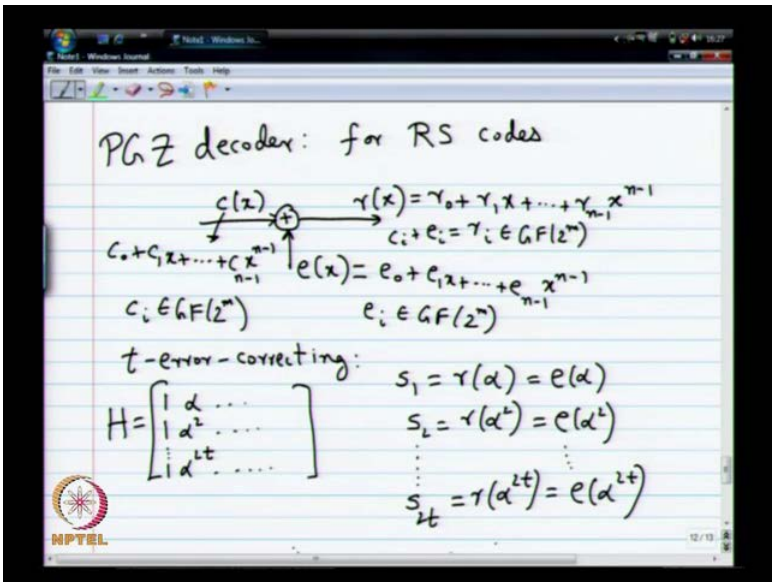
Coding Theory
Prof. Dr. Andrew Thangaraj
Department of Electronics and Communication Engineering
Indian Institute of Technology, Madras

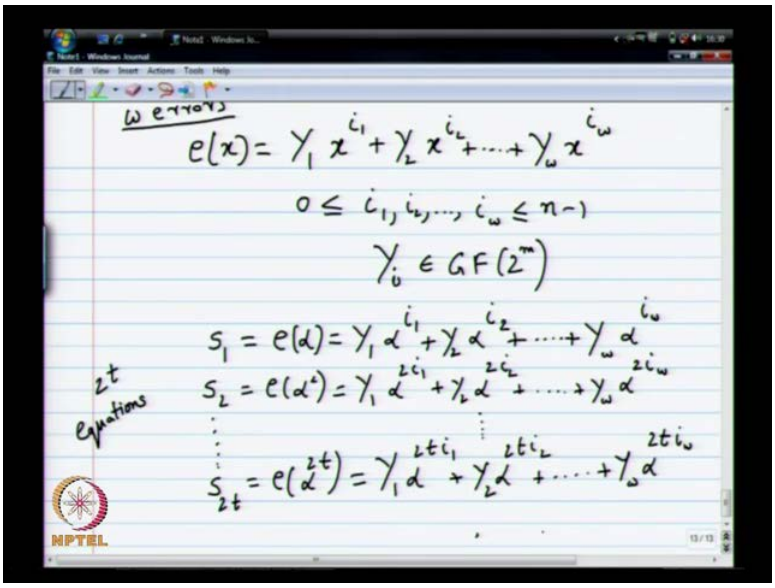
Lecture - 16
Decoding RS Codes

(Refer Slide Time: 00:14)



So, these are the equations, so let us pick up from where we left of in the previous lectures. So, we are looking at the P GZ decoder for Reed Salmon codes, so it is similar to the BCH decoder we going think of vectors as polynomials, but there difference is polynomials, now have coefficient from G F 2 power n. So, it is not a binary it is a it is going to value of field again. So, you have a slightly more complicated problem, but other than that in philosophy it is it is very similar looking equation.

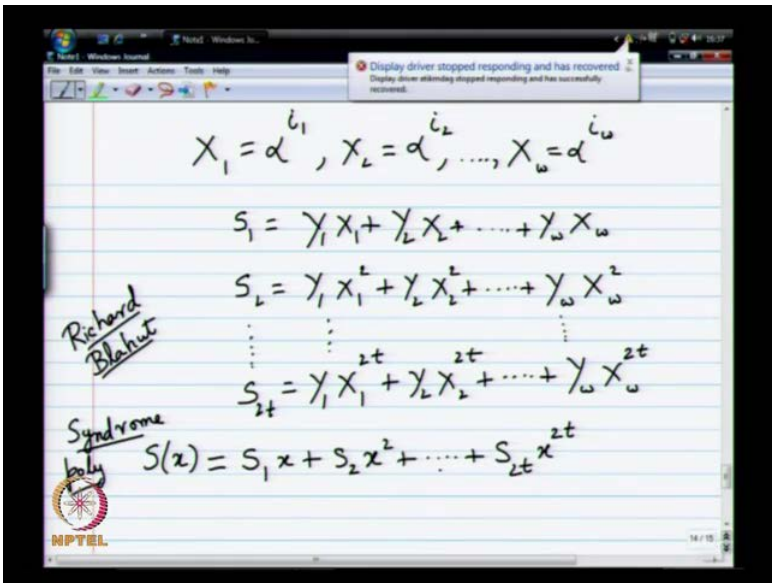
(Refer Slide Time: 00:53)



So, if you assume you are looking for the w errors then the error vector error polynomial e of x can be written in this form coefficient y 1 through y w and expedience i 1 through i w and you have y 1 x power i 1 plus y 2 x power i 2. So, once again we will do the similar substitution, what is the what does the substitution? We going to say x 1 equals x power no I am sorry, let me let me not do this let me write down, the equation in terms of e of alpha and etcetera, and then we will do the substitution.

So, basically the equation we have we have 2 t equations right? And how many variables that is not w so y is there 2 w variables that is that is so let us see so. How do these how do these variables look its important s 1 is going to be e of alpha which is y 1 alpha power i 1 that y 2 alpha power i 2, so on till y w alpha power, s 2 is e is of a square. This is y 1 alpha part 2 i 1 y 2 alpha part 2 y 2 alpha power 2 i w all the way down to s 2 t which is e evaluated at y 2 alpha power 2 t i 2 so on till y w alpha power 2 t i w. So, these are the equations very similar to before we have a alpha power i 1 and then the additional term is i 1 the constant appearing in front P C H you would not had that so we same substitute as before.

(Refer Slide Time: 03:35)



We let x 1 to be alpha power i 1 x 2 to be alpha power i 2 so on till x w to be alpha power i w. So, I pulled a bit of stunt here and I have introduced a new variable without telling you what the variable is and we do not know ahead of time, what that is I have put that just nobody asked my asked me that question. So, not I was reminded to do that what is that extra variable that I have introduced which I do not know w right it is crucial w is do not know also, I will just introduced it but let us not worry about it, we can fix w later w can be at most t. So, t is a small number so we are to scared about it so we will worry about that later.

So, once you do it this equation become s 1 equals y 1 x 1 plus y 2 x 2 plus so on till y w x w s 2 equals y 1 x 1 square plus y 2 x 2 square so on till y w s w square all the way down to s 2 t which is y 1 x 1 power 2 t y 2 x 2 power 2 t, so on till y w s w 2 t. I know many of you are tempted to say omega it looks very much like omega so it is not omega it is w we are electrical engineers we have a special affiliation to make these are the these are the equations, and some looking at the B C H example being motivated by the B C H example we are going to make some substitution and transform it simpler set of equations.

Finally, try to solve it that what get one equation whose roots will give me the solution that is the idea behind the all these things before I go into that I want to give you a brief glimpse as why this solution is very, very complicated and the B C H K equation look

very simple and the solution any way we are doing a exhaustive search why is exhaustive search very easy in this case,

Student: ((Refer Time: 06:07))

Yeah, if you see try the number of exhaustive searches you have to do is just becomes too many, number of trials you have to make is too many because you have x 1 through x w which are w positions out of n possibilities. So, n choose w is going to be a large number. So, we are thinking of n being in the range of two thousand etcetera thousands even if the w is 20, two thousand choose 20 is how big it is very big right. So, there are some simple bounds you can do by k, so you can do some bounds and evaluate what that is it is very large number two thousand choose twenty is a really, really large number or two many possibilities. So, you cannot try everything out.

So, ultimately we will get one equation for which you can do a exhaustive search that only one type of search that is not too many. So, here so many equations and just it is mind boggling to try and solve it so it is too many cases, so you have to do a series of substitutions and make it smart do it smartly so that you get a simpler solution, simpler equation for which you can maybe do a exhaustive search. So, that what we will do and there is a there is a trick to this and it is no way to easily motivate that trick.

So, I am going to be simply give you that give you that trick and then we will see we will see you have a interesting way of motivating it. So, far I have not found out very, very smart way of motivating it at least some slightly smarter, so maybe find something that is interesting. So, you start of first by defining as syndrome polynomial so say s of x there are various ways of describing this and it fact in books, there will be several different ways the method that I am following here is closely followed by the book and by the Richard Blahut.

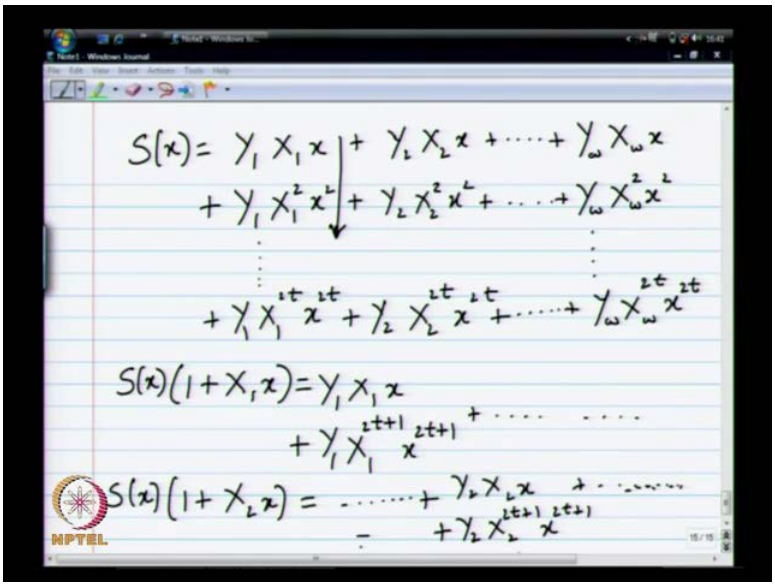
So, I am basically following this method, there are various other ways of describing it is it is also an very old algorithm this is been quite a while. So, you first start by defining syndrome polynomial, which I believe as a s 1 x plus s 2 x square so on till s 2 t x power 2 t let me make sure that I have all correctly done, this is the syndrome polynomial you should wonder what is the small x, small x is some x, so it is not very easy to grow out what it means. And we will finally, see that that has that has very nice interpretation.

So, let us let us look at this polynomial little bit closely, so s of x remember it is s 1 x plus s 2 x square plus x 2 x square plus 1 right.

Student: ((Refer Time: 09:55))

So, I am sorry should I start with 0 or 1 yeah I am going to start with 1 so 1 x is fine that is what I check also it is correct, java has some problems it is something restarted so this is right.

(Refer Slide Time: 10:25)



So, what happens to s of x if you look at the little bit differently is you get y 1 x 1 x plus I will write next term here y 1 x 1 square. In fact the first term will be what y 2 that is 2 x plus so on till y w s w then x 1 square plus y 2 x 2 square x square so on, till y w x w square, square all the way down to plus y 1 x 1 power 2 t x power 2 t x 2 power 2 t x power 2 t y w x w x power 2 t.

Remember all these things have being added right that is the definition of s of x is that all right. So, ultimately the goal is we want to get rid of all this non-linear equations and go to linear equations right because the only thing we can really solve is linear equations. That is basic idea behind the whole simplification, so looking at this complicated non-linear type of equation and we want to get linear equations out of it is there a change of variables can we change things around so that we can get nice linear equations, which we can solve that is the idea.

So, to do that you make this observation if I take s of x and multiply by 1 plus x 1 x so I have written down the s of x so in this form I am going to multiply it with 1 plus x 1 x. So, the reason why I am doing is if you look down this column if you look down this column when computer decides to show it to you, if look down this column you notice you have some kind of a geometric progression y 1 comes out, then you have the geometric projection with the ratio with a being x 1 x. Eventually it is going to be some something like 1 by in e plus c 1 x something like that right.

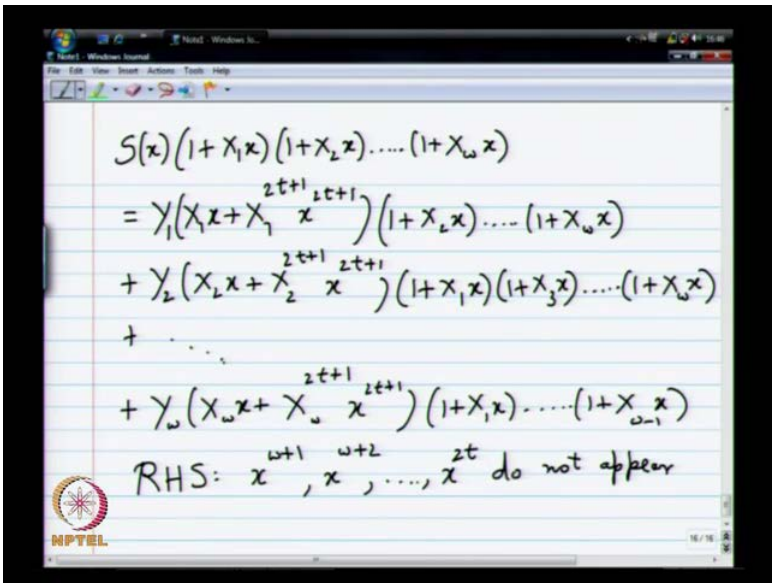
Of course, there are some I am describing it, but I am it is eventually going to do that so when I do multiply by 1 plus x 1 x i expect lot of cancelation that is the idea and multiply by s of x into 1 plus x 1 x i expect a lot of cancelation in this column in other columns there will be no other cancelation in this column I expect a lot of cancelation. So, if I do that let me write down the only the first columns I will forget about the other columns, what will happen?

In the first column you will get y 1 x 1 square c 1 x I am sorry y 1 x 1 x plus y 1 x 1 power 2 t plus 1 x power 2 t plus 1 all other terms will get cancelled out because the way multiplying it this only in the first columns, what will happen in the other columns.

Student: ((Refer Time: 14:14))

You will have other thing all the things will be there is that right so then the other columns if I do the same trick with second column, we multiply with 1 2 plus x 2 x what will happen first columns will have all kinds of stuff, then the second column will have what y 2 x and then y 2 x 2 power 2 t plus 1 x power 2 t plus 1. And then all kind of stuff will be other columns. So, if I keep multiplying by 1 plus x 1 x I am causing a lot of cancellation in which column so what will happen if I do this?

(Refer Slide Time: 15:12)



What will happen if I take s of x and multiply by 1 plus x 1 x times 1 plus x 2 x so on till 1 plus x w x, what will happen? Sorry.

Student: ((Refer Time: 15:34))

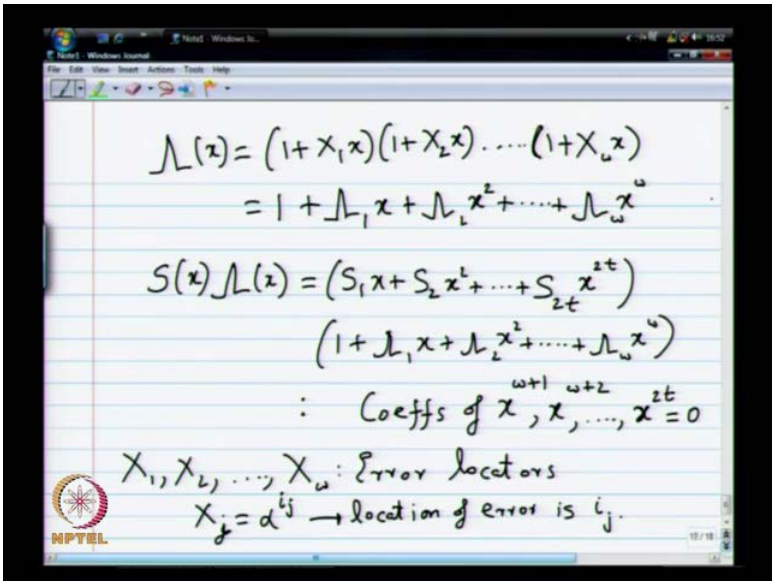
Let me write it down you have y 1 times x 1 x plus x 1 2 t plus 1 x power 2 t plus 1 x power 2 t plus 1 multiplied by 1 plus 1 plus x 2 x. So, until 1 plus x w x and then what will happen to the second column y 2 x 2 x plus x 2 plus 2 t plus 1. Anyway the first term I read about this cancellation, I was really excited I do not know you guys are really excited are not, but just it is very interesting stuff you know it is not one of those things which we will see in circuit theory. So, you get this.

Likewise each column will have some term like that and then if you want I can write the last thing once again, here I would get 1 plus x 1 x so on till 1 plus x w minus 1, scratching the beards thinking more deeply about the problem. So, have I accomplished anything other than that it is a basic simple algebra, as anything being accomplished is do you observe anything on the right hand side. There are several power of x that show up in right hand side I am actually interested in the power of x that do not show up on the right hand side, what powers of x are not there in the right hand side.

Of course constant is not there the constant is not there in left hand side also 2 t from where w plus 1 to 2 t, right? There is no term so on the R H S there are some terms that

they do not appear x power w plus 1 x power w plus 2 so on till x power 2 t do not appear, that's great seems like positive step do they appear on the left hand side. Yeah they do appear so you could equate them to 0 and that will give you slightly different kind of equations. So, the question they give linear equation say I know s of x i know all the calculation of s of x, but on the right hand side and the multiplying the s of x i have series of terms how can I how can I get linear equation, very simple trick actually it is not too difficult it is not even a trick.

(Refer Slide Time: 19:41)



So, what do you do is you define which I will can lambda of x to be equal to 1 plus x 1 x 1 plus x 2 x 1 plus oh my god this is really should probably restart or something 1 plus x w x I do not know what this coefficient are, but let us say when I multiply the mouth and add it all up I will finally, get some polynomial of degree what of degree w. And those polynomials will have some coefficient for instance first qualification will be one for sure and what else maybe it is lambda 1 x I do not know what it is might be some lambda 1 x and then lambda 2 x square so on till lambda w x power w. Now, what do I know s of x if I multiply by lambda of x what is going to happen?

When I multiply s of x by lambda of x what is going to happen a lot of things will happen, but what cannot happen on the right hand side, I cannot have any coefficient with powers w plus 1 2. So, this will give you some polynomial, but it will be such that

what is this polynomial, let me write it down i x plus x 2 x square plus go on till s 2 t x power 2 t times 1 plus lambda 1 x plus lambda 2 x square so on till lambda w x power w.

I know the s s 1 through to s 2 t I know I do not know the lambda, lambda 1 through lambda w I do not know, but what will happen when I multiply these 2 polynomials.

Student: ((Refer Time: 22:09))

So, coefficients of coefficients of x power w plus 1, x power w plus 2 so on till is going to die x power 2 t equals what now, let me I have this linear equations yeah leave me linear equations in the lambdas. So, I can solve from the lambdas then how do I go to lambda to the excess, how do I do it? I have to find the roots of lambda of x so that why I am exhaustive search will come, so how are x xi related to the lambda is you make a polynomial lambdas find out the roots, x i will be the inverse of the roots. So, that is simple relation you can see here I will talk more about it as we go along, but anyway that is idea.

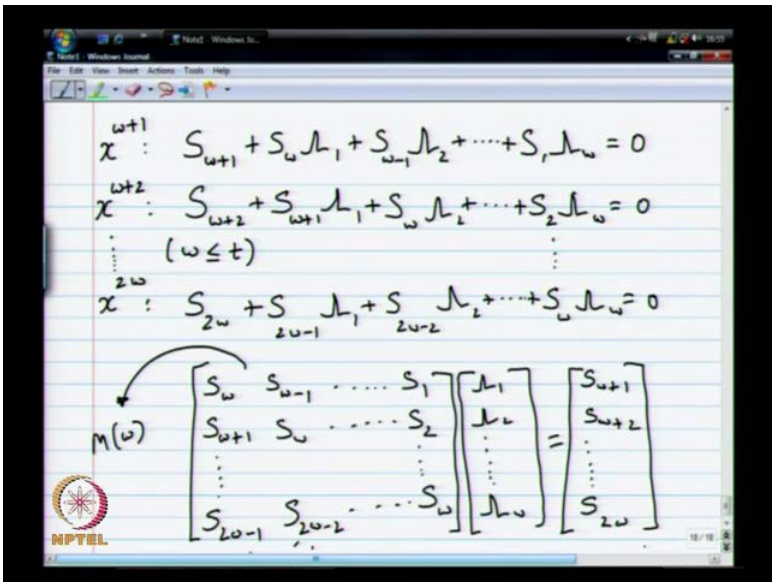
So, what I am pointing out is you can from the x 1 x 2 x omega you can find lambda of x that is the very easy operation, what I am trying to say is from lambda of x also you can find the x 1 x 2 x omega how do you do that you find the roots of the lambda of x, and then take the inverse of those things those will be the exhaustive search. So, this is the this is the basic principle of the decoder get out this linear equations write them out solve them you get a polynomial solve those polynomial, as they define the roots of the polynomial you get the invert the you get the excess, which tell you where there is the basic idea.

So, these x i have a name this x 1 through the x omega they are called error locators, why are they called error locators? Remember each of the x i is basically alpha power when x j alpha power i k, so this tells you the location of the error. So, this is the method this slide sort of speak captures the method for finding the error locators. So, you find first the syndrome polynomial, which is the very easy thing find then you define another polynomial is these lambdas, the polynomial should be such that when you multiply with s of x we should not get any coefficients.

I mean coefficients for the power w plus 1 2 t should be 0, so once you do that you can you can solve for the error locations that is the idea. So, you can now go through and list

out the coefficients of w plus 1, you will see and you will get linear equations I am going to write that down explicitly in the next slide.

(Refer Slide Time: 25:51)



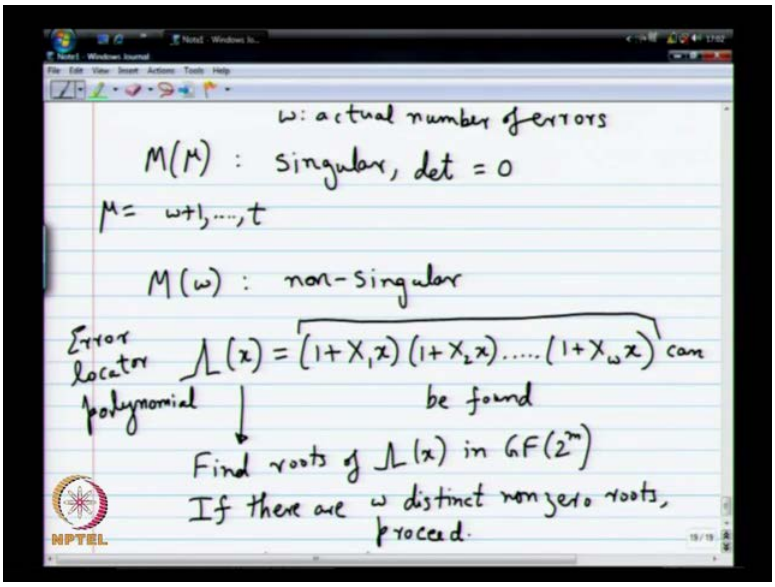
If you do x power w plus 1 you will get the following, this is what you will get for x power w plus 1 you can go back and check this, this is not to difficult w plus 2 you will get. So, all the way down to I will write x power 2 w and we will assume that less than or equal to d I will write x power 2 w will be s 2 w plus s 2 w minus 1 lambda 1 that is s w 2 minus 2 lambda 2, this all the way to s w that equal to 0.

So, you can also write this in terms of matrix should look like this s 1 s w plus 1, s w all the way down to s 2, this way you go all the way s 2 w minus 1, s 2 w minus 2 all the way down to s w multiply this with lambda 1, lambda 2 down to lambda w it should get s w plus 1 s w plus 2 all the way down to s 2 w. So, I will call this matrix as let say some m of w, I do not know if it is 2 I think it is, so if you have let say determinant of m of w being non zero. Then what does it mean? You have a unique you have unique solution and you get a unique answer determinant is 0, then something is wrong, so you got into one of those indeterminate situations with boundary distance equal, that what it means. But there is a interpretation for determinant being 0.

So, I want to so I want to talk about it little bit so you remember what are the things, we could not do was find w right we did not know w ahead of time right in this method strongly uses w, right? You equate the coefficient from w plus 1 so w plus 1 so induces

w a lot. So, the way to get on that is to use this property of m of w, what you can show it they will not prove here, can look at up in the books what you can show is…

(Refer Slide Time: 29:49)



m of mu for some mu say mu equals w, w plus 1 w all the way till t, what is m of mu if I say even you can go back and instead w you put mu. So, instead of w here you put mu that the using a notation here, so what I mean suppose say let us say w is a actual number suppose I your channel I number of in the actual realization the actual number of errors that happened is w you do not know w, w is the number of errors that actually happen.

Now, I am going to look at the matrix m of mu and I will let mu be I do not know w so I will say how to find w using this method m of mu it turns out for all these m's it is singular, what do you mean by singular? Determent is 0 equals 0 m of w on the other hand is guaranteed to be non singular,

Student: ((Refer Time: 31:20)

Sorry w this one sorry I will different way of writing sorry, obviously this is not a so m of w if w is the actual number of errors then m of w is guaranteed to be non singular. So, this equation will have a unique solution it has to right in a way w errors actually occurred and guessed w correctly you should get one unique answer, we have no problem with that w is less than t remember I definitely get one unique answer there is no problem.

On the other hand if you guessed wrongly, but you guessed in the direction has in you as something larger than the actual w then m of mu is guaranteed to be singular. So, how do I find w using this property you start from t that is the idea you know w is less than or equal to t you start from t and find m of t so see if it is singular or not. If it is singular then number of errors that acquired as the still lesser so you go to t minus 1 t minus 2 etcetera, etcetera till you get to the first place it becomes non singular.

And then it becomes non singular you invite the matrix multiply by this at the guy and you get your polynomial lambda of x is that okay. So, this is the complete P G z decoder at least in a high level you know, how to do t g z decoder bounded distance decoder find these matrix come to a point where it is non singular then solve for that particular way to get your error locator polynomial. Does it solve all the problem? There are still something more to be done I will come to it later soon enough for now at least you know what to do.

Using this we can now find lambda of x, this lambda of x by the way it is called the error locator polynomial. So, lambda of x can be found so let us say it can be found, so once you find it, what should you do what is the next step in P G set decoder find roots of lambda of x in g f 2 power m that is important in this field not in any other fields, you find roots of lambda of x in g f 2 power m. What should happen is you should get w distinct roots non zero roots, that is very important. If you get w distinct non zero roots you proceed, otherwise you just declare something which means, otherwise if something else happens then your bounded distance decoding assumptions has been violated somewhere.

Something else is happened odd of errors happened at transmitted from somewhere, somewhere got pushed into some other situation and you think something is gone wrong. So, you can take a error, so if there are w distinct non zero roots proceeds only then distinct is true, then this is true else then something crazy has gone sums react situation has happened, and somehow some luck has found the lambda of x and which can happen right this procedure is totally meaningless when there are more than t l s, I think it can happen you might get some lambda of x, which is valid and all that, but then when you do the roots you see it is not actually valuable it is not true.

Student: ((Refer Time: 35:55))

Yeah you might get even those things, but even get repeated rows if I said that is what I said w distant non singular roots you could get repeated by which anything like that happens then something is gone some, the boundary distance assumptions has been violated on. So, if there are w distinct non zero roots proceed to the next step, what is the next step.

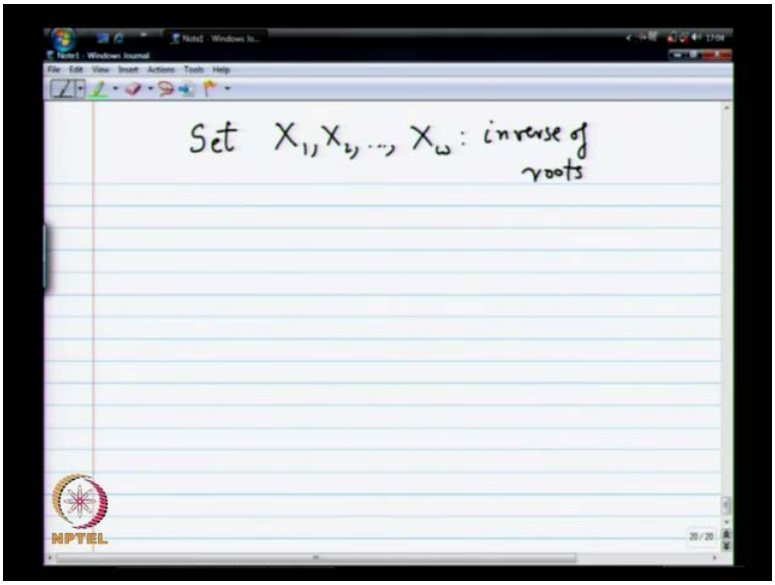
Student: ((Refer Time: 36:28))

It can also happen so in fact some what do you mean this and I didn't get your answer, what did you say.

Student: ((Refer Time: 36:36))

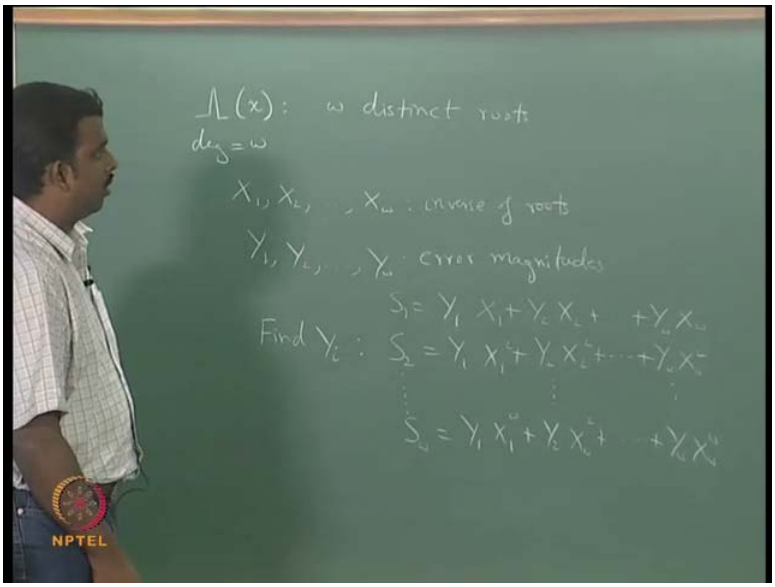
You get w distinct roots less than t error you can say that from other code for some other code word you can come all the way here codeword, you can come all the way here, but you will correct to the code word within your boundary. So, that way it is so you will go to go back to the unique codeword within your sphere of radius t around your r of s that is the definition of the problem. I am not worried about which codeword was actually transmitted, we are just doing the bounded distance decoded we want to look into t and say defined one thing and going back. So, if you find w distant roots, then I means there are only one thing that that is for sure only one code word in your sphere of radius that is true. So, battery is low I have 10 minutes 5 percent battery all right we will just stop. Whenever I decides to give up all.

(Refer Slide Time: 37:48)



So, next step if you had w distant roots set X 1, X 2, X w to be what the inverse of the roots. So, this is important you are setting it to be inverse of the roots not the roots themselves 1 plus x 1 plus x and if you find the roots this is x i inverse, inverse of the root terminology.

(Refer Slide Time: 38:19)



So, remember lambda of x has a degree equal to w, we found w distinct w roots and we set there are locations inverse of roots we are not yet done because we haven't found the error polynomial exactly. We have found the location of the errors what have we not found so the y i's. So, the y i's are they are called magnitudes the y i's these are called error magnitudes, but once the error locations are known the error magnitude is simply it is simply a linear equation.

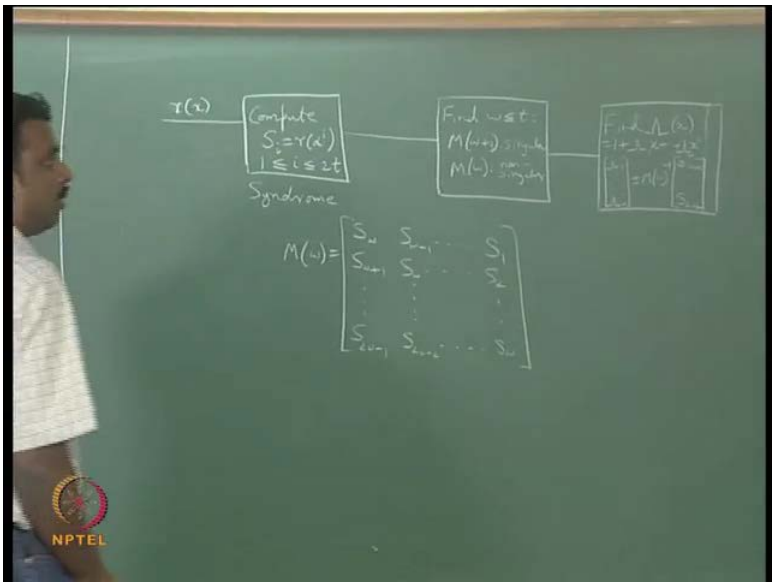
So, what you do is you look at you look at s 1 equals y 1 x 1 plus y 2 x 2 so on till y w x w take s 2 which is again y 1 x 1 square that is y 2 x 2 square all the way down to s w you can stop at s w. How do I know this matrix is invertible, this is a proper linear equation that will give me a unique solution.

Student: ((Refer Time: 39:55)

Yeah you will get random on the structure for the matrix write a matrix a and multiply by y 1 through y w you will get a random on matrix and i know x i's are distinct, clearly that

will have a non zero determined. So, I can invert it and get my i's without any problem so find.

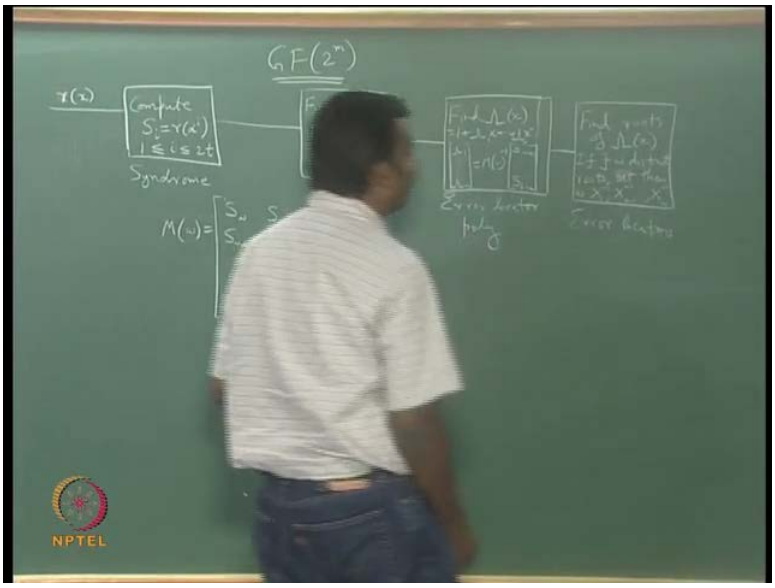
(Refer Slide Time: 40:32)



So, let us summarize next five minutes or so we will summarize the Reed Solomon decoder. So, it is complicated kind of decoding you have an r of x, first step is what is to compute S i be r of alpha power i, i going 1 to 2 t this is basically sign syndrome. So, at the output of this you will have the s i's then what should you do, find w such that m of w plus 1 is singular and m of w is non singular. And so w is obviously less than or equal to t, w plus 1 so for t it is a for t you do not do this, you get m of t to be non singular is a t error then for others, what is this m of w, m of w is basically this matrix s w, s w minus 1 all the way to s 1, all the way to s w s 1 s 2.

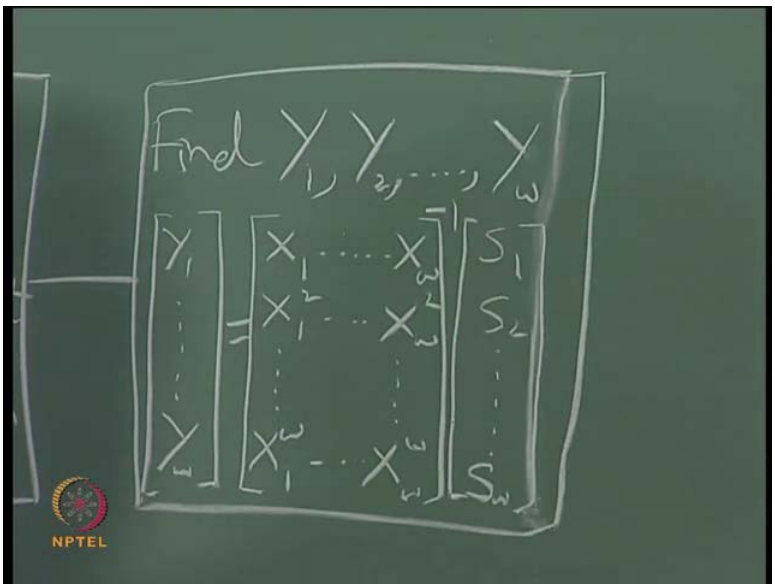
So, this is the matrix you form this matrixes determine w for which is a it is non singular w plus 1 should be singular a w strictly less, if w is equal to t so you find the w. Then what do you do, what is the next step? Yeah we have to find, find lambda of x, how do you find lambda of x just 1 plus lambda 1 x so until lambda w x for w x for w, how do you find these you have to do this equation. So, lambda 1 lambda w equals m of w inverse times s w plus 1 all the way down to s to w, so you find your error locator. So, this is basically this is some step you finding the error locator polynomial.

(Refer Slide Time: 44:20)



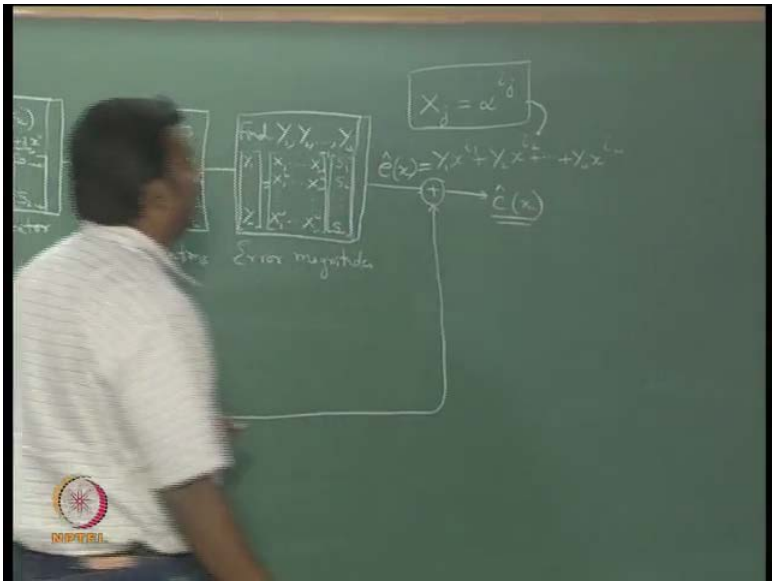
What is the next step you have to find the actual error find roots of lambda of x, if there exist w distinct roots because all of these things are in the g f 2 the b m all the operations are in the g f 2 the g m important if there exists roots set them as x 1 inverse x 2 inverse so on till x w inverse. So, in this step you find the error locations and then you solve for the error magnitudes.

(Refer Slide Time: 45:3)



Find y 1 y 2 y w so how do you find them I have an equation, we have the random on do the inverse of the random on the matrix time that once again you have to elongate the picture here. So, then what you do are you done.

(Refer Slide Time: 46:36)



These are error magnitude, so this basically defines your error, error polynomial we have to take all the way from here what are these i j's x j equals alpha power this is your c of x.

Student: ((Refer Time: 47:48))

Here for what, well the numbers are going to be huge we are working with the value of let us say 2048 and t is 40 or 30. So, if you want to get a number of possible s i itself is 2048 raise to the power 40 possible even syndrome decoder can be implement tables are tough. So, the reason why I squeezes everything into these boxes has to give me a impression this is a very small, so at least in illusion maybe not to scared of it, it is not actually very scary. Today you can implement this decoders at several giga bit second few second one or three more than one giga bit per second actually whatever the 45 and all of this, but it is a very well studied decoder. So, let us stop here.