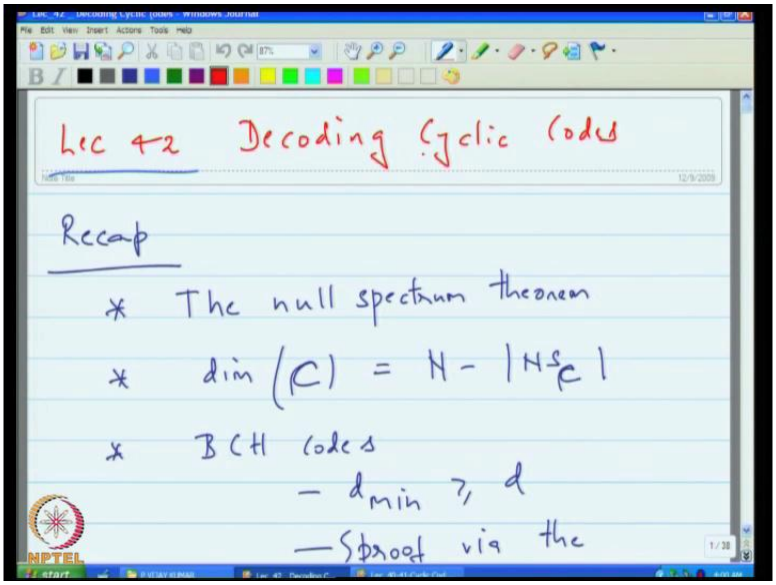
Error Correcting Codes

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

Lecture No. # 42
Decoding Cyclic codes

I guess this is the, this is the last lecture of the semester. I hope you believe me to learn at least something from this lectures. Its new experience for all of us. I am sure improvements are always possible. So, this till we do have full lecture ahead of us today, so I will just keep going.

(Refer Slide Time: 00:46)



Lec 42 Decoding Cyclic Codes

Note Title 12/9/2009

Recap

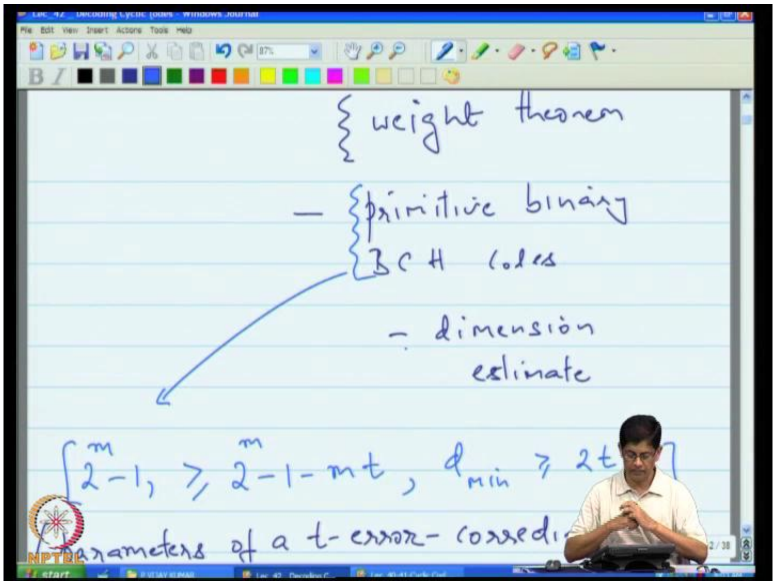
* The null spectrum theorem
* $\dim(C) = N - |NS_C|$
* BCH codes
  - $d_{min} \geq d$
  - proof via the

And again in the interest of making sure that of complete our lectures series today I am written out today’s lecture. So, let us is gets started. So, today so in the last class what we did was I started discussing, that is lecture 41 as started discussing cyclic codes. And I mention to you that we are going to discuss cyclic codes from a transformed domain point of you. And the connection was in terms of closed sets of frequencies and important theorem, that we are actually showed last time was that there is one to one corresponding between cyclic codes on one hand, and sets of frequencies there are closed and the conjugation on the other end.

And that is the null spectrum theorem which appears here. Then we moved on to discussing the parameters of cyclic codes, and the block length is obvious, the two other parameters of interest are the dimension, and minimum distance. So, the dimension we prove the theorem which stated that the dimension of the code is the comp, the size of the complement of the null spectrum in other words you cannot how many frequencies there in the null spectrum and N minus that amount is the dimension of the code. So, the dimension is straight forward once you are given the null spectrum. So, that you just to the minimum distance, and the minimum distance in general exaggerate problem to estimate the minimum distance.

What we did do is? We said well let us consider certain class of codes in which we structure the null spectrum to contain a conservative string of d minus 1 frequencies. Then the minimum distance is greater than or equal to d, and this d parameter d is called the design distance often the minimum distance is equal to the design distance. But it could be larger.

(Refer Slide Time: 02:46)



{ weight theorem

— { primitive binary
BCH codes

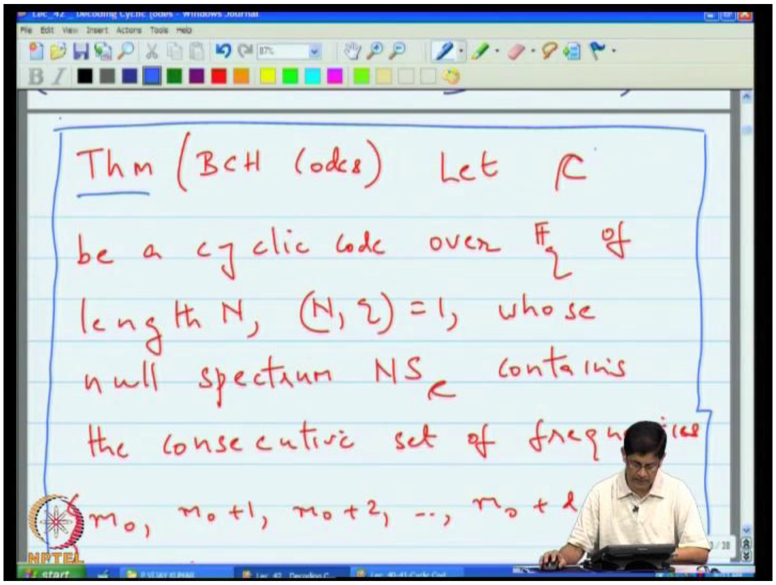
– dimension estimate

$[2^m - 1, \geq 2^m - 1 - mt, d_{min} \geq 2t \quad]$

parameters of a t-error-correcti

And the proof is we are theorem which we called the weight theorem, which said that if you have weight whose the timing weight the time domain. Then that translates in the frequency domain to linear recursion relationship amongst the transform co efficient where the degree of the linear recursion is equal to the hamming weight. So, w was the weight then the degree of the linear recursion would accelerate. Then after that, we discuss the class of we discussed an example of BCH codes known as primitive binary BCH codes, always wonderfully one common before I come back to this, that is in a last class

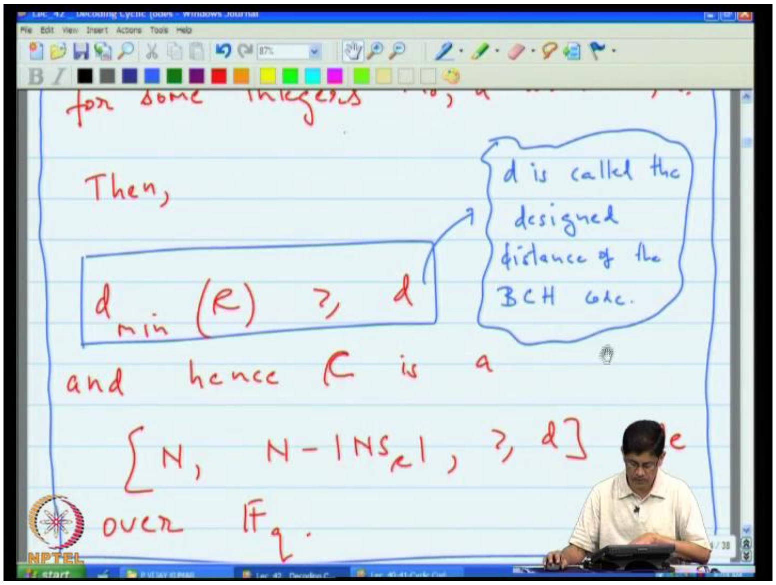
(Refer Slide Time: 03:35)



Thm (BCH Codes) Let C be a cyclic code over $\mathbb{F}_q$ of length N, $(N, q) = 1$, whose null spectrum NS_C contains the consecutive set of frequencies $\{m_0, m_0+1, m_0+2, \ldots, m_0+d$

We have a lecture in which actually discuss the class of cyclic codes where you have the usual conditions, and then I put in the additional conditions that you have a string of d minus 1 zeros I just want to highlight that this class of codes is generally known as class of BCH codes.

(Refer Slide Time: 04:03)



for some integers

Then,

$$\boxed{d_{min}(C) \geq d}$$

{ d is called the designed distance of the BCH code.

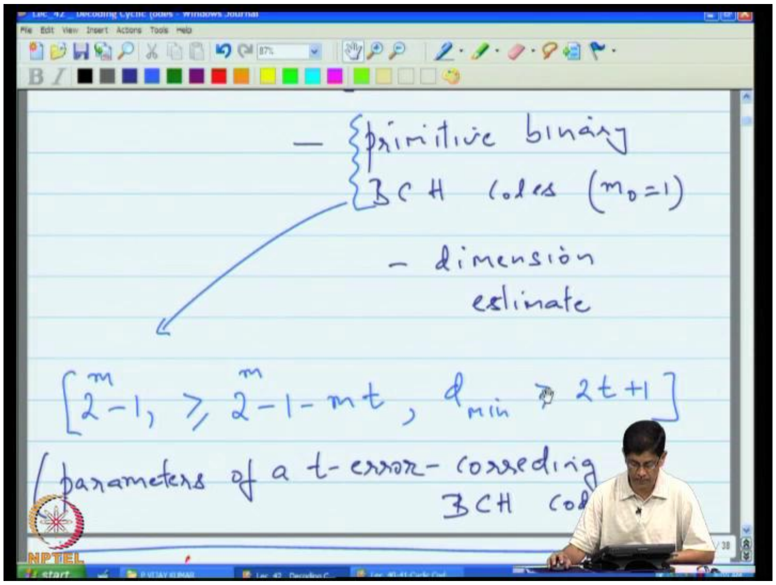
and hence C is a

$[N, N-|NS_c|, \geq d]$ e

over $\mathbb{F}_q$.

And this d is called the design distance of the BCH codes. I just want to make sure that you are identify this class of code with the class of BCH codes. So now so that is the reason for introducing a theorem which is saw in the last lecture.

(Refer Slide Time: 04:24)



— { primitive binary BCH codes $(m_0=1)$

– dimension estimate

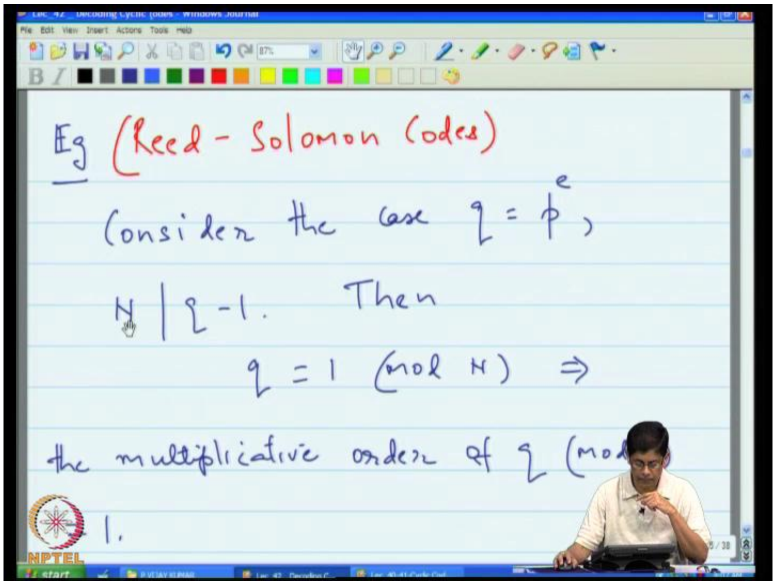
$[2^m-1, \geq 2^m-1-mt, d_{min} \geq 2t+1]$

(parameters of a t-error-correcting BCH cod

So, coming back here toward the end of the day it was look at the particular example of this BCH codes. In what way of this particular will it is particular in two aspects, first of all it was binary, because in general BCH codes could also be non binary. And in the in the second aspects was that the codes were primitive that means the length is of the form 2 to the m minus 1. So, primitive translates into this, and then now if you specify the null spectrum in terms of a conservative string of frequencies or mandating the null spectrum contain a conservative string of frequencies. Then you have really mole down the null spectrum exactly so that leaves some and certainty about the size of the null spectrum.

And because of that its have to give a precise count for the dimension of the codes, but in the in this particular case that is in the case of binary BCH codes, and in the particular the there is the other thing we did that predate which is particular that. We said the parameter in 0 to be 1 there is the first frequency z equal to 1, and these circumstances you can actually say that well my dimension is given by this. And this is my minimum distance, and this was an very good estimate of the dimension, and these codes are very efficient. There are amongst the best known binary codes so often if you if you required binary codes at last minimum distance. Then this generic construction which might will cover your case. I will regard as the parameters of the t error correcting BCH codes so that concludes the summary of it last time.

(Refer Slide Time: 06:21)



Eg (Reed - Solomon Codes)

Consider the case $q = p^e$,

$N \mid q-1$. Then

$q = 1 \pmod{N}$ ⇒

the multiplicative order of q (mo

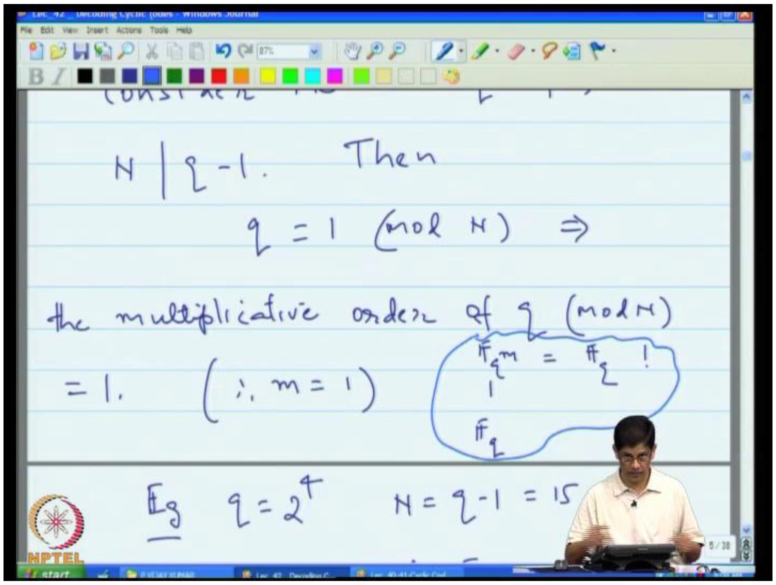
1.

Lec_42_Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL

So, now would I want to do, so I want to actually say the as the second example. I am going to say that class of codes this class of code is the most wide spread class of cod in use today is known as red Solomon codes And although from the way represented it here it appears. As an example of the BCH codes red Solomon codes can be given an independent definition, and in fact and discovered independently so this is just the unification that I am presenting here which actually so that the red Solomon codes can be regarded as the particular classes of BCH codes. So, what is special about this particular to this case? Is that here q is the part of N no surprises there.

But N divides q minus 1 that is new in other words you are saying that the block length is less than q less than or equal to q minus 1, now what that means is that, because N divides q minus 1 that means q minus 1 is a multiple of N. And therefore, q is 1 plus a multiple of N which means q is 1 mod N. So, the multiplicative order of q modular N is 1

(Refer Slide Time: 06:21)



$N \mid q-1.$ Then

$q \equiv 1 \pmod N \Rightarrow$

the multiplicative order of $q \pmod N$

$= 1.$ $(\therefore m = 1)$

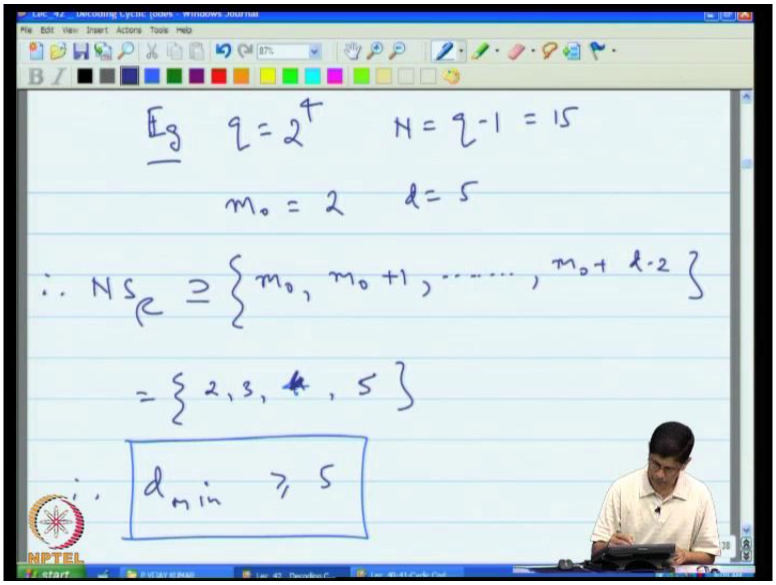
$\mathbb{F}_{q^m} = \mathbb{F}_q$!

$\mathbb{F}_q$

Eg $q = 2^4$ $N = q-1 = 15$

So, the parameter little N that will be using throughout in this case is just 1. Therefore, N the N that will be talking is just being one about is just one so in particular that means that in the case of red Solomon code. There is only one field is speak of because remember typically we are two fields we had f q and then we had the field f q to the N sitting on the top. But now in the current case this is equal to f q. So there no two fields is just a single fields in this particular case.

(Refer Slide Time: 08:18)



$\underline{\text{Eg}}$ $q = 2^4$ $N = q-1 = 15$

$m_0 = 2$ $d = 5$

$\therefore NS_{\mathcal{C}} \supseteq \{m_0, m_0+1, \ldots\ldots, m_0+d-2\}$

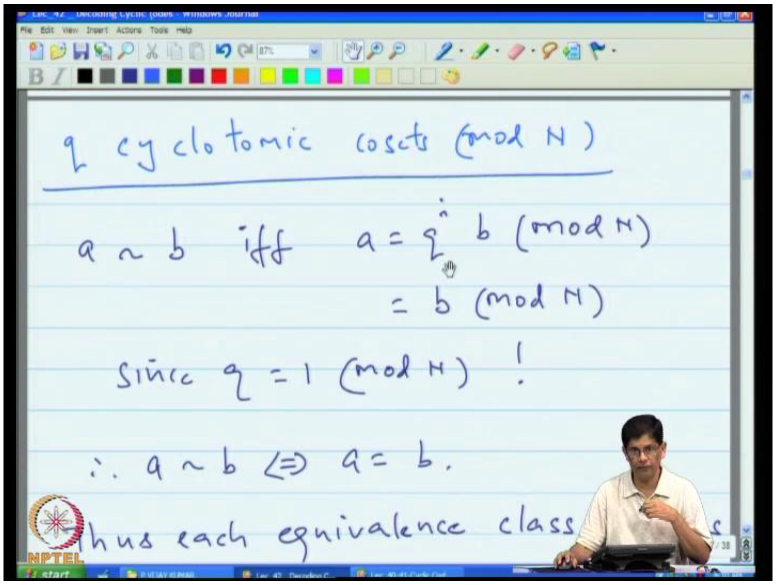
$= \{2, 3, 4, 5\}$

$\therefore \boxed{d_{min} \geqslant 5}$

So. an example suppose an q is 2 to the 4 N is 15, and then and so we know that N is 1. Now and go to fix the parameter m 0 to be 2 and d to be 5 so by this fermenting that BCH codes contain which is the red Solomon codes. Because its satisfy this conditions that this red Solomon code and the null spectrum is mandating to contain 0. And 0 plus 1 and m 0 plus d minus 2 which in this case means there is must contain the conservative string of frequencies 2 3 up to 1 0 plus d minus 2 which is 2 plus 3 which is 5 so its contains 2 3 4 5 which is the string of 4 conservative 0s so it has the 4 conservative 0s and therefore, the minimum distance is.

One more than the number of conservative 0s, so it is actually 5 there also examines. Because your design distances is 5, but now my doing my list because I want to actually say that in this particular case, you can actually determine that exactly is the null spectrum voice that.

(Refer Slide Time: 09:44)



q cyclotomic cosets (mod N)

$a \sim b$ iff $a = q^i b \pmod{N}$

$= b \pmod{N}$

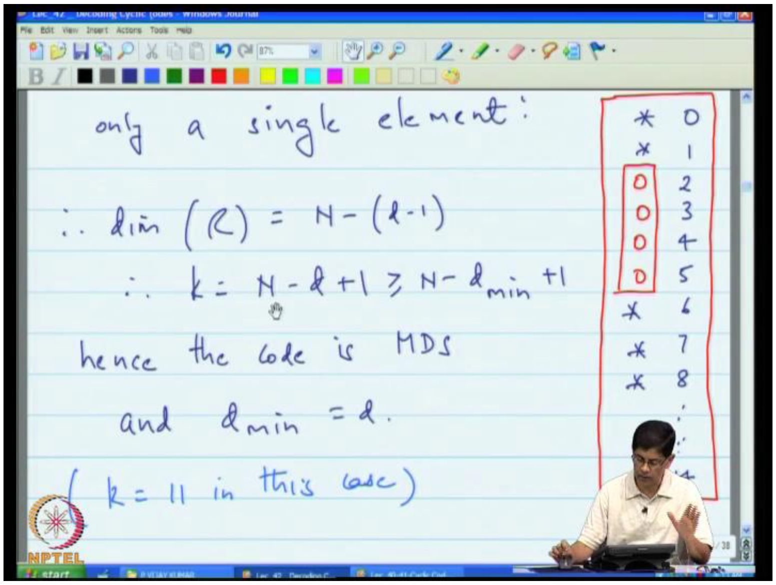
since $q = 1 \pmod{N}$!

$\therefore a \sim b \Longleftrightarrow a = b.$

Thus each equivalence class

Well look at the cilice q cyclotomic cosots mod N, look at the q cyclotomic cosots mod N. Now according to our definition is these cycltomic costs whether result of any question relationship in which we define a to b equal to b, if and only if a was b times some pair of q modular N. But remember since q is 1 mod N any pair of q is also 1 mod N. So, that means that a is equal to b if and only if a is equal to b, in other words each equalling class is singleton set it contains just single element, there are no conjugates of element other than itself.

(Refer Slide Time: 10:29)



only a single element:

$\therefore \dim(\mathcal{C}) = N - (d-1)$

$\therefore k = N - d + 1 \geq N - d_{min} + 1$

hence the code is MDS

and $d_{min} = d$.

($k = 11$ in this case)

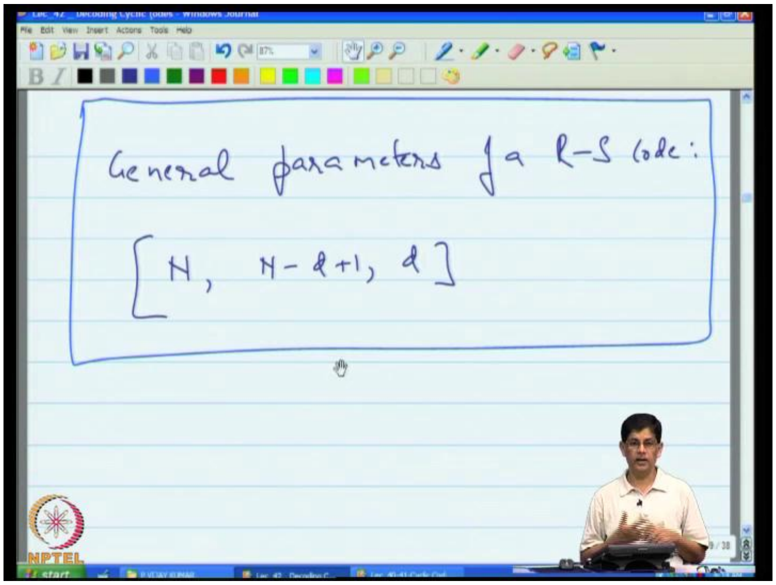
*	0
*	1
0	2
0	3
0	4
0	5
*	6
*	7
*	8
	⋮
	14

So, for you must particular cases you look at the frequency employ to petitionary equal classes of cyclotomic cosots. You find that basically there are 15 cycltomic cosots, each contain a single entry. Now you impose the condition that the null spectrum contains the 0 2 3 4 and 5, so put it that down here 0 2 3 4 5 and include in the null spectrum. And now then we try to estimate the meaning the dimension of the code. We know that the dimension is the code is the number of frequencies that lie outside the null spectrum, which in this case is 15 minus 4 is 11, so the minimum distance the dimension of the code in this case is 11.

So, in general it is always going to the case with red Solomon codes that the co sots are singleton co sots. And therefore, when you mandate the string of d minus 1 conservative frequency belong to the null spectrum, then the null spectrum can be tailor to contain exactly the frequency the nothing more, so the size of the null spectrum is d minus 1. So, the dimension of the code is size of the complement of the null spectrum so its N minus d minus 1 so 10 minus d plus 1. And it terms of that this d is actually the minimum distance of the code, because by the way since the minimum distance in general is larger greater than or equal to d. This quantity is greater than or equal to N minus d min plus 1 since subtracting potentially larger quantity.

But remember that code is maximum distance separable if k is equal to N minus d min plus 1. We stated that the binary case it extends to the non binary case in so in fact, because of the m d s condition in terms of that not only do you have this bond. But this bond in fact of any quality, because the minimum distance cannot any better than d because it works. Then we would have something exist the m d s bond so anyway that I think little quickly, but anyway terms out that this bond on the dimension of the red Solomon code is always going to be an tied so the minimum distance is the design distance.

(Refer Slide Time: 13:15)

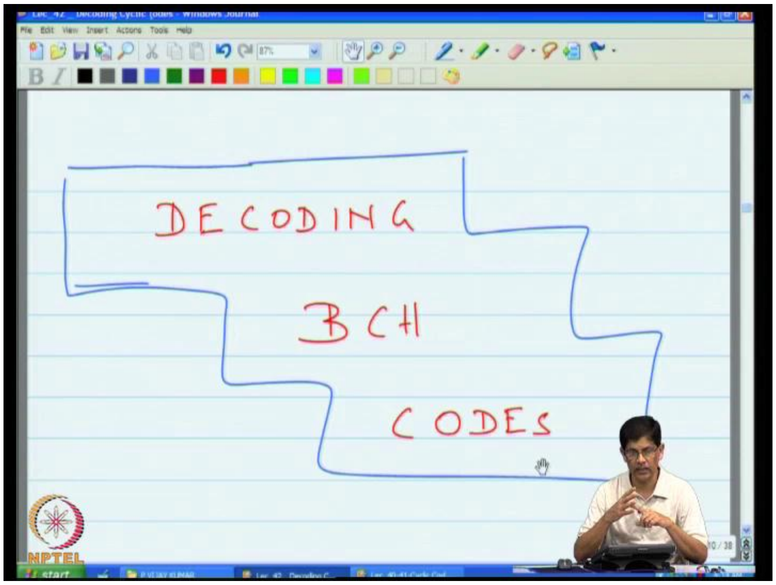


General parameters of a R-S code:

$[N, N-d+1, d]$

And thus the general parameters of any red Solomon code are block length N minimum distance d, and dimension m minus d plus 1, and hence there always m d s maximum distance separable that was the second class of codes. So, we gave you general definition of BCH codes, and show that value primitive BCH codes, and red Solomon codes are examples. And from a practical point of view these are very widely very much relevant, because both are used often in practice the red Solomon codes are design codes that used the must in applications worldwide.

(Refer Slide Time: 14:03)



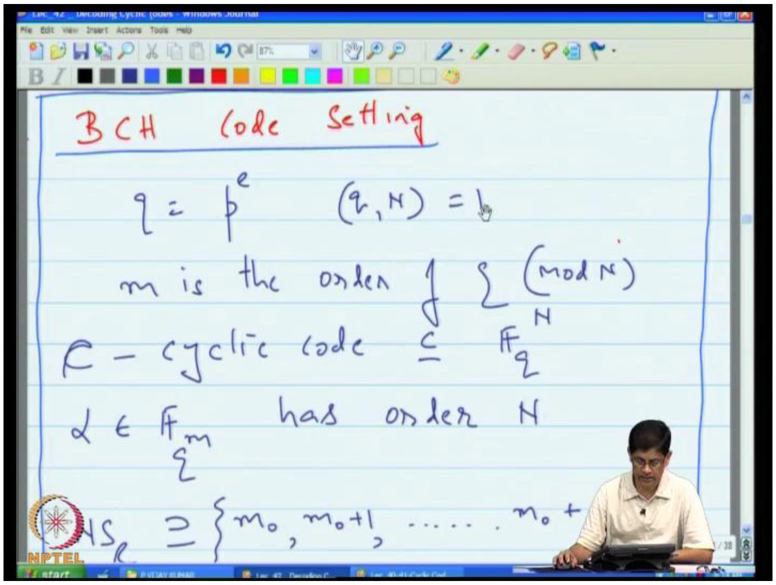
DECODING

BCH

CODES

Now how do you decode BCH codes? Now I am talking about BCH codes, in general so that includes both primitive binary BCH codes as well as red Solomon codes. So, it going to talk about both class of codes at the same time just reminder.

(Refer Slide Time: 14:20)



BCH Code Setting

$q = p^e$ $\quad (q, N) = 1$

m is the order of q (mod N)

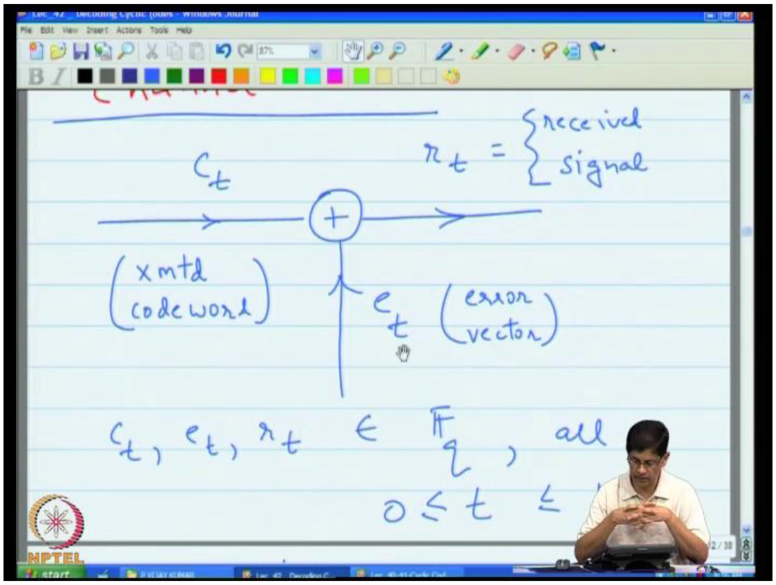
$\mathcal{C}$ - cyclic code $\subseteq \mathbb{F}_q^N$

$\alpha \in \mathbb{F}_{q^m}$ has order N

$HS_{\mathcal{C}} \supseteq \{m_0, m_0+1, \ldots\ldots m_0+$

So, what is the BCH code setting? So, you have q and you have block length which is relatively prime to q, N is the order of q mod N is always c is the cyclic codes of the block length n. So, its contains near, and there is an element alpha in some extension field f q meaning some field larger than f q, that contains N eth root of unity, or an element of order N. And then the noise spectrum is mandate to contain string of conservative d minus 1 conservative frequencies namely this starting with m 0.

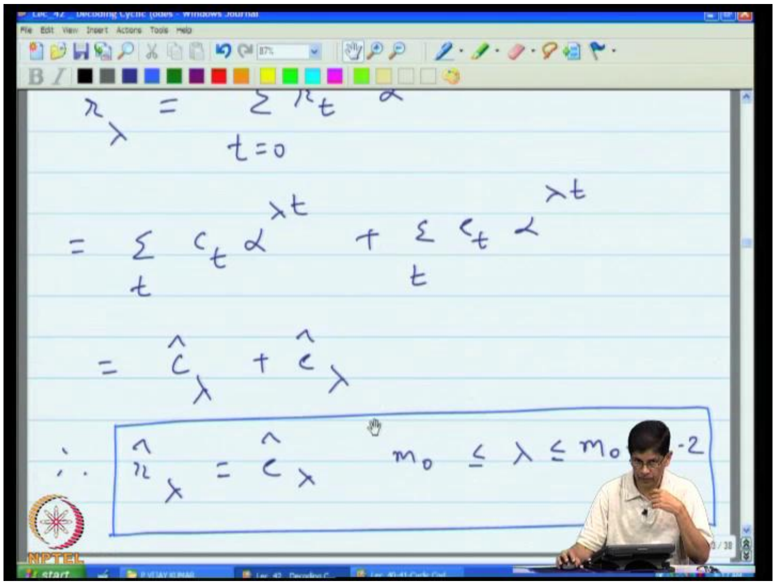
(Refer Slide Time: 15:01)


c_t
r_t = {received signal}
+
(xmtd codeword)
e_t (error vector)
$c_t, e_t, r_t \in \mathbb{F}_q$, all
$0 \le t \le$
NPTEL

Now we are going to decode over a channel which is modelled as follows, which could be modelled as an additive channel model, additive noise and in which his the transmitted code word. This is the noise of the error of the (( )) and that is your receive signal. So, this is transmitted code word, this is your error vector in this is the receive signal. Now in our channel model since I code is going to take on values from a finite field F q this others also resume to take on. So, you can think of this channel as kind of generalisation of the binary symmetric channel it is probably (( )) symmetric channel something like that.

But anyway we have this addictive channel model, and also assume the error vector has such that has smaller number of non zero values of the error is more likely than the larger values. So, you generally try to correct the certain number of errors up to the certain limit is always.

(Refer Slide Time: 16:34)


Lec_42 _ Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL

$$\hat{r}_\lambda = \sum_{t=0} r_t \alpha$$

$$= \sum_t c_t \alpha^{\lambda t} + \sum_t e_t \alpha^{\lambda t}$$

$$= \hat{c}_\lambda + \hat{e}_\lambda$$

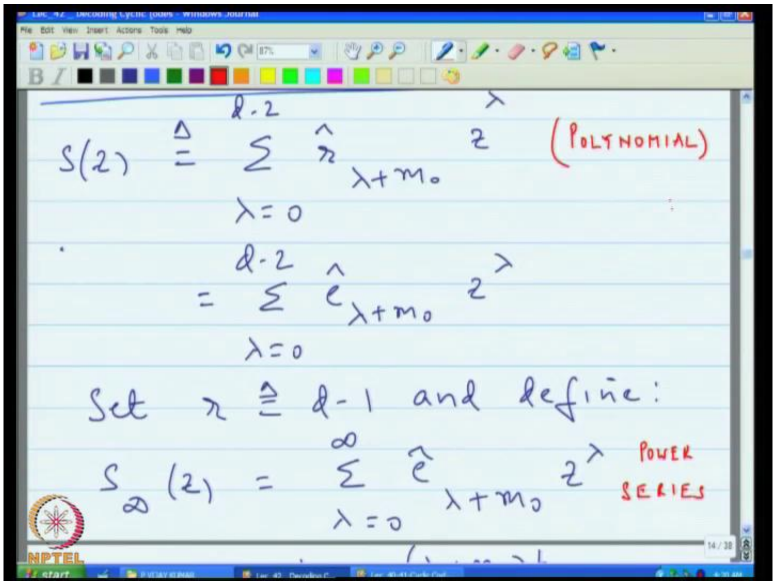
$$\boxed{\therefore \hat{r}_\lambda = \hat{e}_\lambda \quad m_0 \le \lambda \le m_0 \quad -2}$$

Now what are going to do? Now consider that that transform of the receive vector r of t is receive factor here, and consider its transform which is given by the registration r at lambda is the some r of t alpha to the lambda t. And now r of t can be broken up into c of t and e of t and this is c at lambda that is e at lambda. So, that means now you know that the code the transform of every code word, regardless of which code word it is that transform values are 0 for conservative set of frequencies. Namely these 1s so in these frequency window r at of lambda agrees with the e at of lambda, which means that the transform of the receive signal is precisely the transform of the error signal in this window.

So, that means that the null spectrum really give you small window through which you can clear at and look at the transform the error signal, because it is clear that you know you have in this channel model, you have access to the receive signal, you are interest to decoding the code word. But of course, if you know the error vector then we also know the code word. So, decoding the code word is equivalent to decoding the error vector so in fact our approach will be try to actually give determine what the error vector is? What angle do we have the error vector? Why we know that the error vector more likely to having small hamming weight than big hamming weight? Because we do not expect lot of else we expect handful errors much more than that.

So, we do not trying to use that aspect of error vector to actually determinate and what this is telling you that there is the small window, in which I actually get to look the transform of the error signal. Now I got two handles of the error vector, one I know it extends from certain range of frequencies, two I also know there it is most likely going to have small hamming weight. And these two together factor and actually determine the error pattern from just a fragment, so here is have you do it.

(Refer Slide Time: 18:49)



$$S(z) \triangleq \sum_{\lambda=0}^{d-2} \hat{r}_{\lambda+m_0} z^{\lambda}$$ (POLYNOMIAL)

$$= \sum_{\lambda=0}^{d-2} \hat{e}_{\lambda+m_0} z^{\lambda}$$

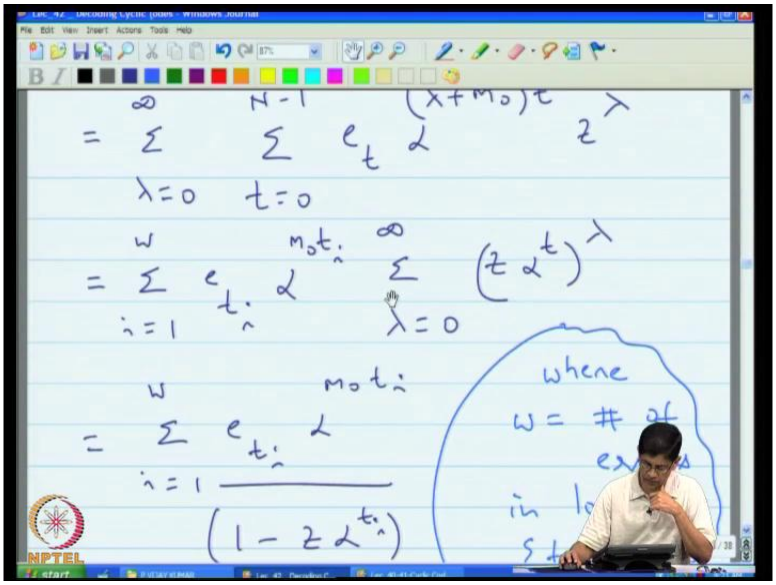
Set $r \triangleq d-1$ and define:

$$S_{\infty}(z) = \sum_{\lambda=0}^{\infty} \hat{e}_{\lambda+m_0} z^{\lambda}$$ POWER SERIES

Now, we define the term syndrome earlier, this is slightly difference definition of the syndrome. In fact the equivalent for the moment less, we say there is an equivalent syndrome and leave it at that so we define a polynomial is a s of z which is sigma r at lambda plus m not zero to the lambda, so this kind of like a normalising shift lambda going from 0 to d minus 2. So, this is precisely the collection of frequencies for which you can evaluate I have for which the transform of the receive signal equals, the transform of the error vector. So, these are the frequencies lambda through m 0 through m 0 plus d minus 2, you know the transform of the error vector now it is convenient to said d minus 1 to be r.

So the r is nothing to do that receive signal, and this is the symbol. So, let us define d minus 1 to be r and define s infinity subset. Now, we already defined is z, so this is the different term s infinity aspect where this is the polynomial s infinity. Aspect is actually a power series that is where noting down is this is actually form a power series, where as this symbol is here is a polynomial. So, there are 2 different entities, now also you not actually look at this wait a minute, how is it that you are able to complete as infinity of z after all. You only no you had to lambda plus m 0, so lambda going from 0 to d minus 2. How can actually said this to infinity well aware of that aware of that you are not able to complete the infinity as z now hesitates in this analysis, how is that help?

(Refer Slide Time: 20:38)



$$= \sum_{\lambda=0}^{\infty} \sum_{t=0}^{N-1} e_t \alpha^{(\lambda+m_0)t} z^{\lambda}$$

$$= \sum_{i=1}^{w} e_{t_i} \alpha^{m_0 t_i} \sum_{\lambda=0}^{\infty} (z\alpha^{t})^{\lambda}$$

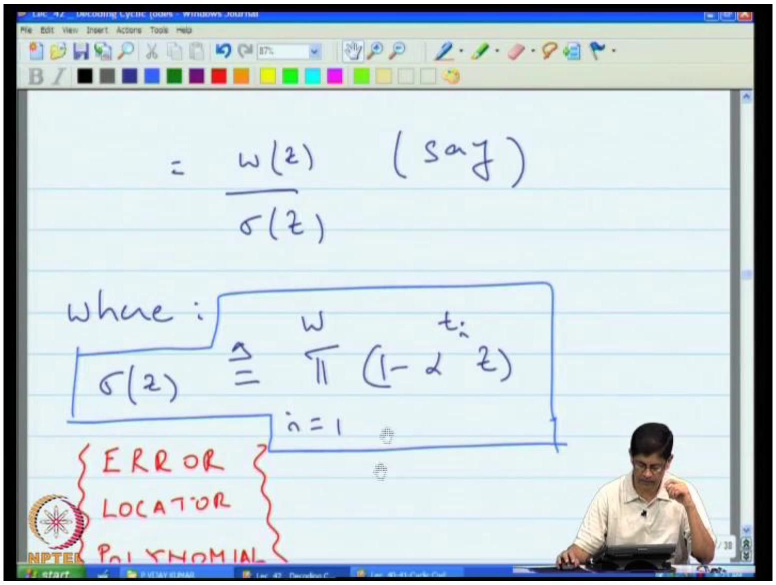
$$= \sum_{i=1}^{w} \frac{e_{t_i} \alpha^{m_0 t_i}}{(1 - z\alpha^{t_i})}$$

whene w = # of ex[illegible] in [illegible] s t[illegible]

Will you continue this is the sum, and then I am going to introduce the definition of e at of lambda here. So, I replace this expression here e of lambda e t after the lambda t. I rewrite this and I do two things first of all actually. I am going to resume that let w be the number of errors which means what which means that the number of symbols of that (( )) t which are non 0 is w. And for the marvellous seen that the for the subscribes t for which e t is non 0 of the t i so e of t i is non 0 for I ranging from 1 to w. And all the others are 0. So, in this really how do it look likes there are N terms in this information only w of t 's are non 0 so that I replacing this sum over this N values of t to the w values of I.

And then e of t i and then correspondingly obtain the alpha to the lambda t i m 0 t i term inside, and take the summation lambda inside so z to the lambda alpha to the t raise to the lambda. And this thing in field of semi pass it reduces to the 1 minus t alpha to the t i, so it is like 1 plus and plus square plus cube and so on. And you would getting 1 upon 1 minus z. So, exactly the same way if you keep some of the terms but you like you get 1 minus 1 upon 1 minus z alpha to the t i.

(Refer Slide Time: 22:38)



$$= \frac{w(z)}{\sigma(z)} \quad (\text{say})$$

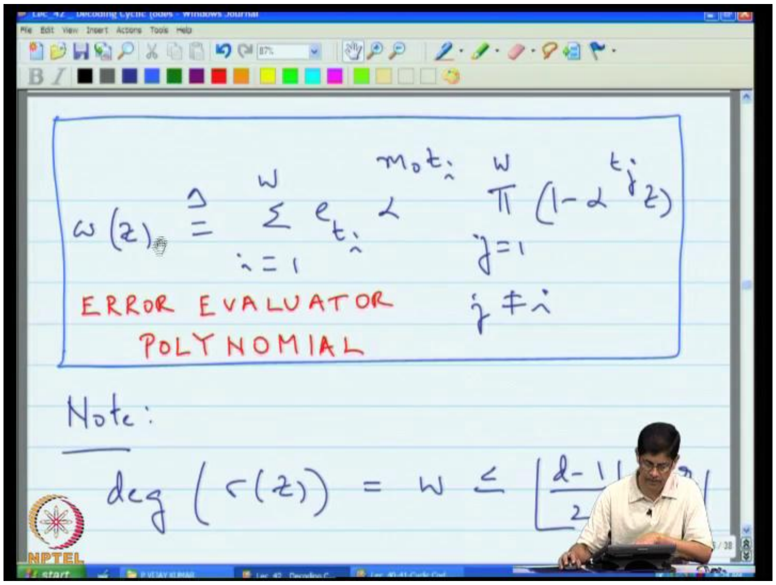
where :

$$\boxed{\sigma(z) \triangleq \prod_{i=1}^{w} (1 - \alpha^{t_i} z)}$$

$\left\{ \begin{array}{l} \text{ERROR} \\ \text{LOCATOR} \\ \text{POLYNOMIAL} \end{array} \right\}$

Now let us strike that omega of z by sigma of z and lets we say that, what it is that? What is sigma of z sigma of z is nothing but the denominator once you put on this on a common denominator which is this. And because the t i appear in terms on the 0 of this polynomial this polynomial is called the error locator polynomial not as that it as degree w.

(Refer Slide Time: 23:08)



$$\omega(z) \triangleq \sum_{i=1}^{w} e_{t_i} \alpha^{m_0 t_i} \prod_{\substack{j=1 \\ j \neq i}}^{w} (1 - \alpha^{t_j} z)$$

ERROR EVALUATOR POLYNOMIAL

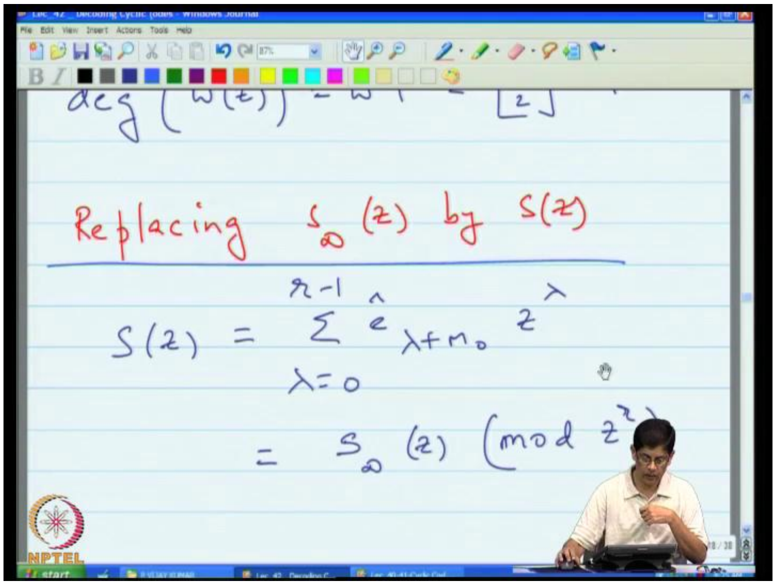
Note:

$$\deg(\sigma(z)) = w \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

Similarly, if you actually what decide you find that omega z is given expression is like this is sum. I is equal to 1 to w e of t i alpha to the m 0 t i for j is equal to 1 to w j molecule to I 1 minus alpha to the t j sigma. And you can see the if you divide this by sigma observe you will get the term for omega by sigma that we had earlier now, because the e of t i here this is called the error evaluator polynomial, and the point being that if you can determine sigma of z and omega of z, then you can actually find both the error locations as well as the error values. Now our goal so initial goal was to determine the transmitted code word and then we said we never determining the code word is as same as determining the error pattern that like to the receive factor.

And then we said the what are really I am interested to receive the error locator, and the error evaluator polynomial, because I know those values and I can recover the error values and error locations and correct the errors that is our goal. And as pointed out the degree of sigma z is w then which is the number of errors, and degree of the error evaluator polynomial is 1 less than that in terms of since. The number of errors is expected to be less than or equal to the d minus 1 upon 2 w is less than or equal to r upon 2, because we defined d minus 1 to be r remember d is equal to 2 t plus 1 where t is the maximum number of errors you can correct.

(Refer Slide Time: 25:03)



$\deg(\omega(z)) =$

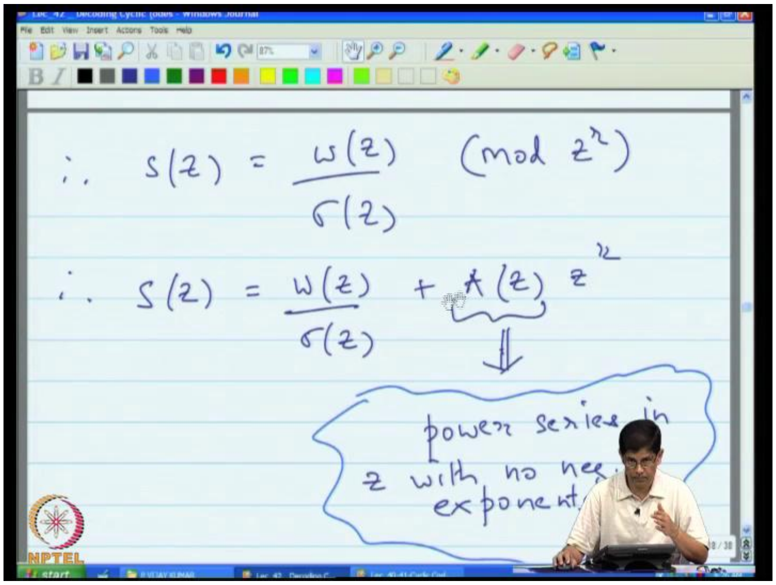
Replacing $s_\infty(z)$ by $s(z)$

$$S(z) = \sum_{\lambda=0}^{r-1} \hat{e}_{\lambda+n_0} z^{\lambda}$$

$$= S_\infty(z) \pmod{z^r}$$

So, that is where I derive this equality from, and the degree of omega z is 1 minus this, so it is given by this expression now all of this is in terms of an infinity of z. But I am not I just pointed out that I do not have access to infinity of z. So, not ask well what is the use of this if we do not know the infinity of z is, that is true, but here is what can do? What we can say so replacing as infinity of z by s of z, so here of s of z and notice that its equal to s infinity of z provided you go not z to the r, which means that if you neglect the terms in z to the r or higher than those no distinction between as z in as infinity as z.

(Refer Slide Time: 26:00)



$$\therefore \quad s(z) = \frac{\omega(z)}{\sigma(z)} \pmod{z^r}$$

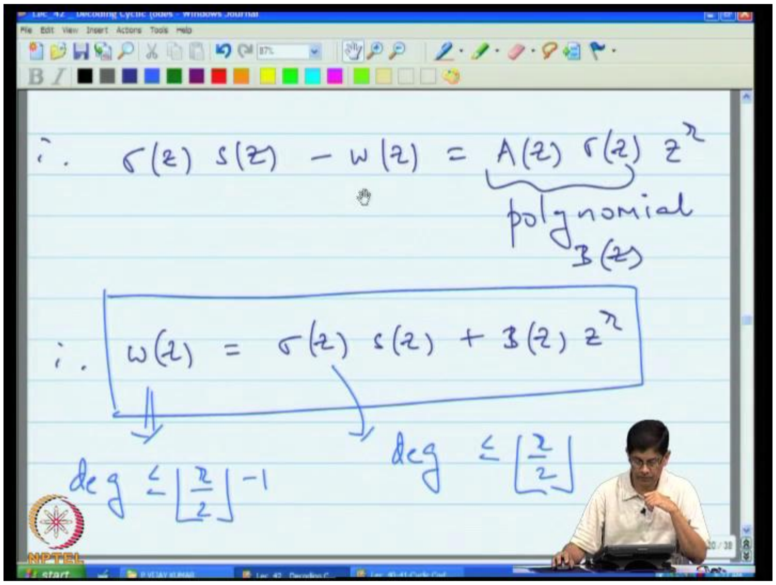
$$\therefore \quad s(z) = \frac{\omega(z)}{\sigma(z)} + \underbrace{A(z)}_{} z^r$$

$\Downarrow$

power series in z with no neg. exponent.

Therefore, s of z is omega of z, by sigma of z provided you restrict to modular z to the r or equality s of z is omega by sigma plus some polynomial terms z to the r. Now if you think about it here neglecting terms z to the r in higher. So, this is a funny power series however there are no negative expenses in it. That is important to keep in mind these are technicalities by the way. So, if you some of 1 or 2 of these points goes past you do not worry, and this kind to be careful, little bit care full here. So, this is a formal power series, however there are no negative expenses there are appear in this. Now multiply through by sigma of z. So, sigma of z is a z which is a polynomial because this is a polynomial, this is a polynomial, omega is a polynomial, and therefore, what I have on this side must be a polynomial.

(Refer Slide Time: 27:16)


Lec_42 _ Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL

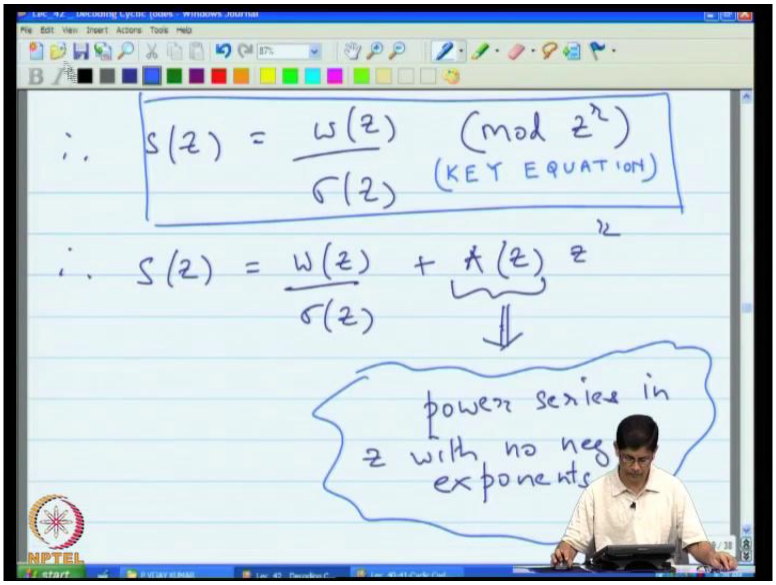
$$\therefore \quad \sigma(z)\, s(z) - \omega(z) = \underbrace{A(z)\, \sigma(z)}_{\text{polynomial } B(z)} z^{r}$$

$$\therefore \quad \boxed{\omega(z) = \sigma(z)\, s(z) + B(z)\, z^{r}}$$

$$\deg \leq \left\lfloor \frac{r}{2} \right\rfloor - 1 \qquad \deg \leq \left\lfloor \frac{r}{2} \right\rfloor$$

So, from that I get that sigma of z and s of z minus omega of z is this and this must be a polynomial, because these are polynomials. So, this must be a polynomial. Therefore, the entire thing must be a polynomial. It has only a finite number of terms simply because a finite number of terms here, and even to begin like 1 more negative expenses of z. So, these had only positive expenses of z so what next these the polynomials, now I can write omega of z sigma of z s of z plus b of z times z to the r.

(Refer Slide Time: 28:08)



$$\therefore \quad \boxed{s(z) = \frac{\omega(z)}{\sigma(z)} \pmod{z^{r}} \quad \text{(KEY EQUATION)}}$$

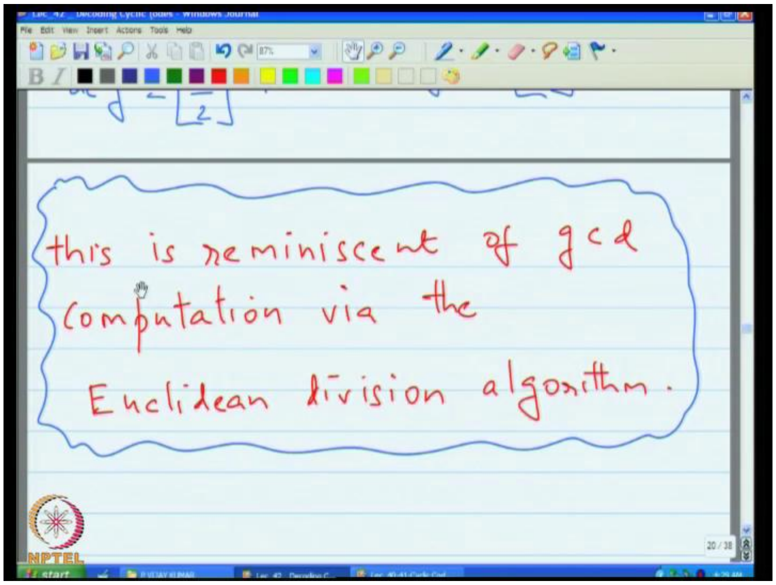
$$\therefore \quad S(z) = \frac{\omega(z)}{\sigma(z)} + \underbrace{A(z)}\, z^{r}$$

$$\Downarrow$$

power series in z with no neg exponents

And you can think of this, by the way this equation here is often called the key equation of for decoding BCH codes. Now you look at this expressions inside you know, what this looks like? I am trying to actually compute the g c d of z to the r and s of z, because I know verify and try to compute that using the extensity algorithm there are the other end that such as an expression that this is the g c d. So, this suggest that the may be may be Euclid algorithm will carried out it starting with z to the r and s of z we will do give a sigma and omega that terms are to be true.

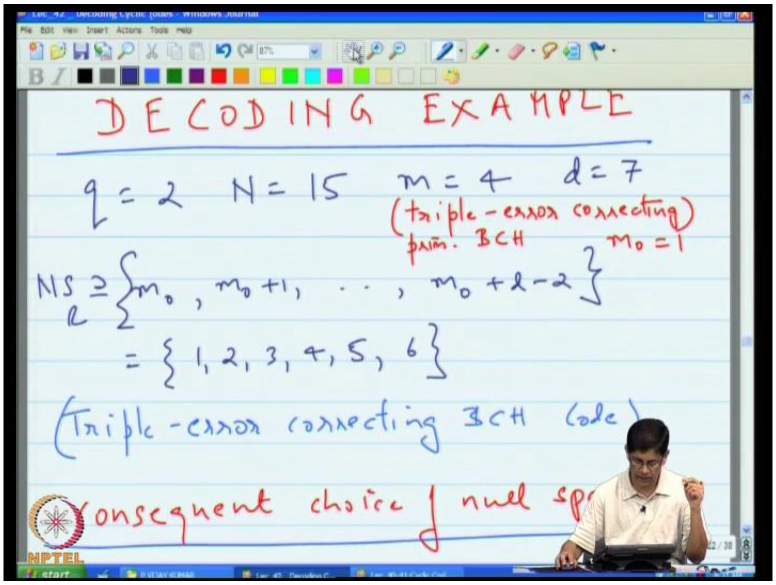
(Refer Slide Time: 29:06)



this is reminiscent of gcd computation via the Euclidean division algorithm.

Although the proof somewhat lengthy the proof is somewhat lengthy so actually skip that. So, what will actually done is that? We start it I introduce the problem of trying to decode BCH codes, and I took it to a serious of steps through the key equation to this point. And I said Euclid algorithm looks like a good handle it this is gap to fill. Because I am not proving the nuclear algorithm can do it, but we know react the time. Because I will take a several lectures which we do not have now would I going to do next I am actually going to go through complete decoding example with you and show you how it actually works.

(Refer Slide Time: 30:02)



DECODING EXAMPLE

$q = 2 \quad N = 15 \quad m = 4 \quad d = 7$

(triple-error correcting)

prim. BCH $\quad m_0 = 1$

$NS_c \supseteq \{m_0, m_0+1, \ldots, m_0+d-2\}$

$= \{1, 2, 3, 4, 5, 6\}$

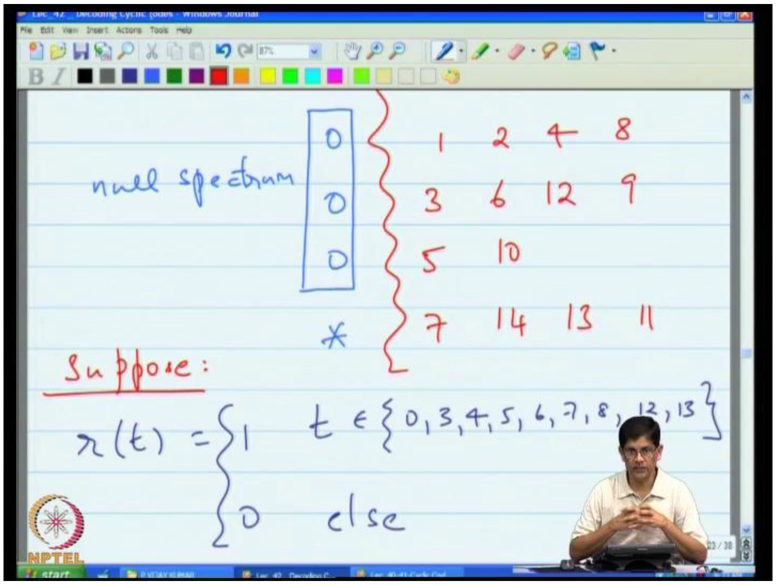
(Triple-error correcting BCH code)

Consequent choice of null sp

The decoding example is here. So, here in this example that code is binary so q is 2 the block length is 15 so m is 4 the multiplicative order of q not 15 is 4, and let us say that the minimum the design distance of the code is they should have been 7. Let us see that the design distance of the code is 7, which means that this code is capable of correcting 7 errors, 3 errors d minus 2 upon 2 which is 3 errors. So, this is in fact triple error correcting BCH codes. Let us make a note this is triple error correcting code. Now according to the BCH definition and also the resume that so this BCH it is primitive BCH so in 0 is equal to 1.

So, that means that in this case of these codes the mandated string of 0s or conjunctive frequencies in the null spectrum is 1 to 6. So, we are saying now that the null spectrum of the code must contain this conservative string of 6 frequencies. So, this is called check error correcting BCH codes.

(Refer Slide Time: 31:54)


Lec_42 _ Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL
23 / 38

null spectrum

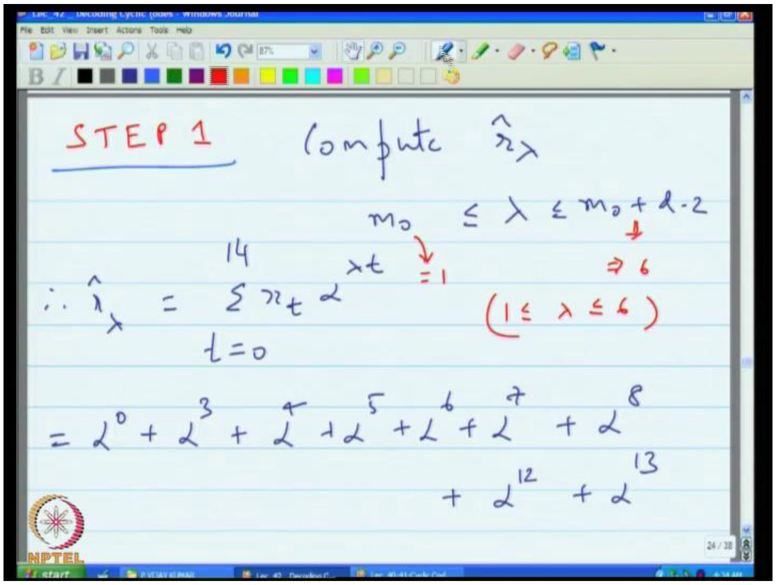
$$\begin{array}{c|cccc} 0 & 1 & 2 & 4 & 8 \\ 0 & 3 & 6 & 12 & 9 \\ 0 & 5 & 10 & & \\ * & 7 & 14 & 13 & 11 \end{array}$$

Suppose:

$$r(t) = \begin{cases} 1 & t \in \{0,3,4,5,6,7,8,12,13\} \\ 0 & \text{else} \end{cases}$$

And I am just that here is well. Now here are the cyclotomic cosots, the mandating field to pick this in the null spectrum so you want to pick 1 2 3 4 5 and 6. And you know that something belong to the null spectrum, then its conjugates and must also appear in the null spectrum. So, because of that you must pick the null spectrum to be the union of these 3 cylotomic co sots as 1 2 4 8 3 6 12 9 5 10. So, you first pick this 3 and this term is a null spectrum. And the dimension of the code now you know is the size of the complement which is 5. Now we want to consider an example of decoding. So, in this example so let us say suppose so suppose in the certain incidence the receive vector so there is a transmitted code word, and let us see there is an error sequence which corrupted the transmitted code word. Suppose they receive vector was 1 for t lying in the set 0 3 4 5 6 7 8 12 and 13 and it was 0, otherwise now we want to actually carried decoding.

(Refer Slide Time: 33:13)



STEP 1 Compute $\hat{r}_\lambda$

$$m_0 \leq \lambda \leq m_0 + d - 2$$

$$m_0 \xrightarrow{} = 1 \qquad m_0 + d - 2 \Rightarrow 6$$

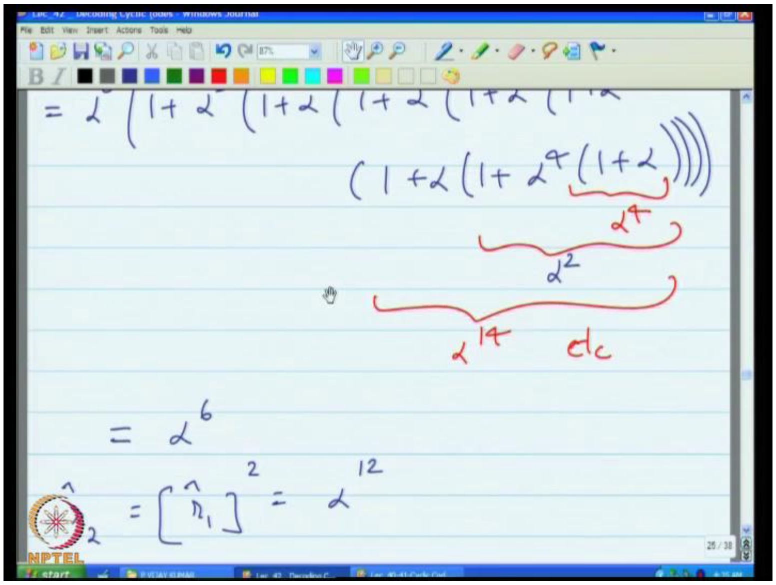
$$(1 \leq \lambda \leq 6)$$

$$\therefore \hat{r}_\lambda = \sum_{t=0}^{14} r_t \alpha^{\lambda t}$$

$$= \alpha^0 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^8 + \alpha^{12} + \alpha^{13}$$

The first step is compute r at of lambda, for lambda for frequencies is lying between the m 0 and m 0 plus d minus 2. So, recall that here m 0s this is equal to 1 and this thing is equal to 6, because this is 1 plus 7 minus 2 which is 6. So, is what you compute the transform for lambda ranging from 1 to 6? Is that is your range of interest. Now, since r of t is non zero precisely for this dimension that means that you have to actually complete this. So, suppose you want to complete this for. So, before I got 1 so if we said lambda to be 1, that is your computing to the first frequency in the string and that gives alpha to the 0 alpha to 3 7 5 6 7 8 12 13.

(Refer Slide Time: 34:37)



$= \alpha \left(1+\alpha \left(1+\alpha \left(1+\alpha \left(1+\alpha \left(1+\alpha\right.\right.\right.\right.\right.$

$$\Big(1+\alpha\Big(1+\alpha^4\underbrace{(1+\alpha}_{\alpha^4}\Big)\Big)\Big)\Big)\Big)$$

α^2

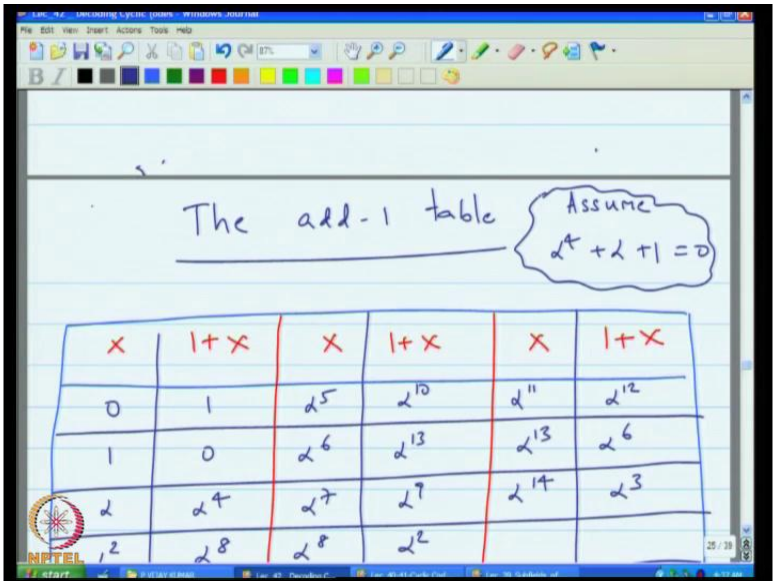
α^{14} etc

$= \alpha^6$

$\hat{\ }_2 = [\hat{r}_1]^2 = \alpha^{12}$

You can use another method to compute it so that is alpha 0 1 plus alpha 3 1 plus alpha 4 alpha 5 alpha 6 alpha 7 alpha 8 alpha 12 alpha 13 this is honours method to actually compute this so 1 plus alpha is alpha 4 alpha 4 plus alpha 4 is alpha 8 plus 1 is alpha 2 alpha alpha 2 alpha alpha 3 plus 1 is alpha 14. Now alpha 14 times alpha is alpha 15 plus 1 is 0. So, you left with starting the computation from here again so that is 1 plus alpha alpha to the 4 alpha to the 5 alpha to the 10 alpha to the 13plus one is alpha to the 6. Now in case you wondering well how do you actually do this leaving just. So, there is no (( )) even through this before so that is, but I will do here is I will pull up we add 1 table from a previous from a previous lecture.

(Refer Slide Time: 35:42)



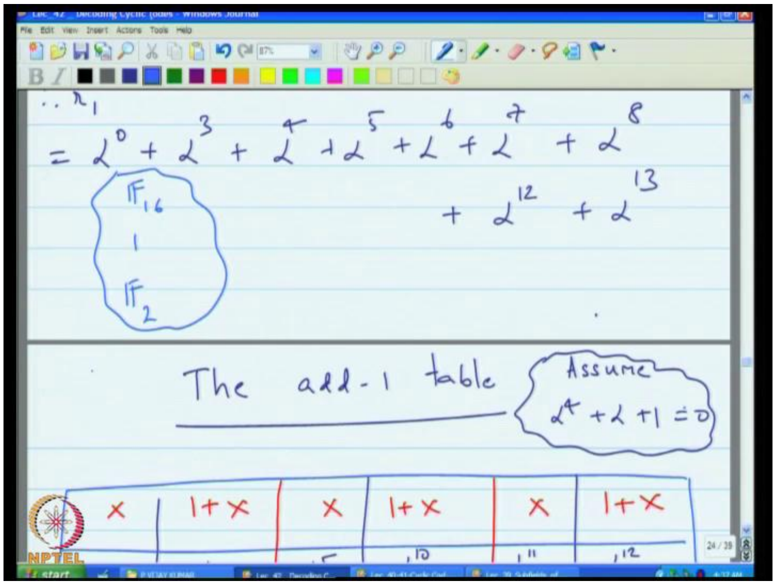
The add-1 table

Assume $\alpha^4 + \alpha + 1 = 0$

x	1+x	x	1+x	x	1+x
0	1	α^5	α^{10}	α^{11}	α^{12}
1	0	α^6	α^{13}	α^{13}	α^6
α	α^4	α^7	α^9	α^{14}	α^3
α^2	α^8	α^8	α^2		

Here is the add 1 table. What I am in music honours method I am also use the add 1 table this 1 at field? So, I am going to resume here in the computations. I am going to resume that alpha 4 alpha plus 1 is equal to 0 that alpha is the primitive element in particular finite field recall that.

(Refer Slide Time: 36:24)



$$\therefore r_1 = \alpha^0 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^8 + \alpha^{12} + \alpha^{13}$$

$\mathbb{F}_{16}$

|

$\mathbb{F}_2$

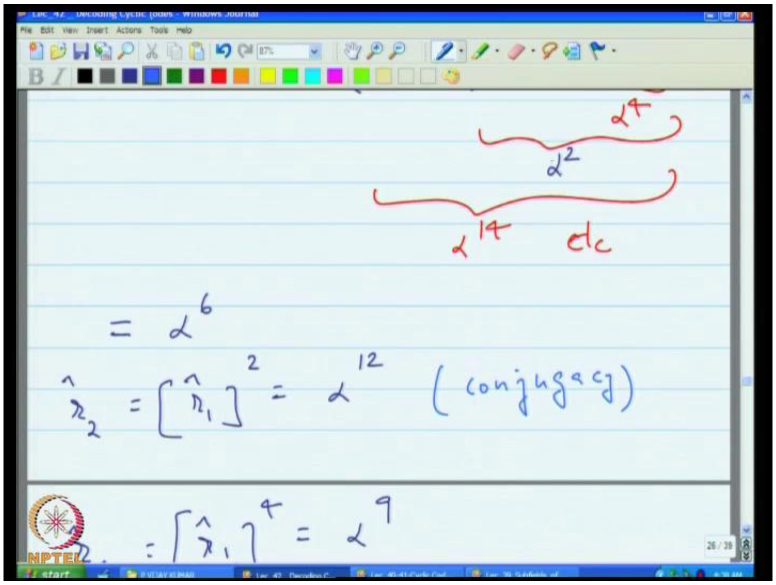
The add-1 table

Assume $\alpha^4 + \alpha + 1 = 0$

x	1+x	x	1+x	x	1+x
		^{5}	^{10}	^{11}	^{12}

Here we start it we start it with f 2 we will lead to f 16 and in this larger field which we called the big field alpha is an element of order 15 so alpha is primitive, and because alpha is primitive. I can actually choose this to be the primitive element which may use. So, often in the past so that is why I using this and this is the add one table and this add one table. I am using here so 1 plus alpha alpha to the 4, and we can see that. So, we complete this informed alpha to the 6. What that means is that? r at 1 has been computed and found to the alpha to the 6 r at 2 by the conjugacy.

(Refer Slide Time: 37:16)



$$\underbrace{}_{\alpha^2} \quad \alpha^4$$

$$\underbrace{}_{\alpha^{14}} \quad \text{etc}$$

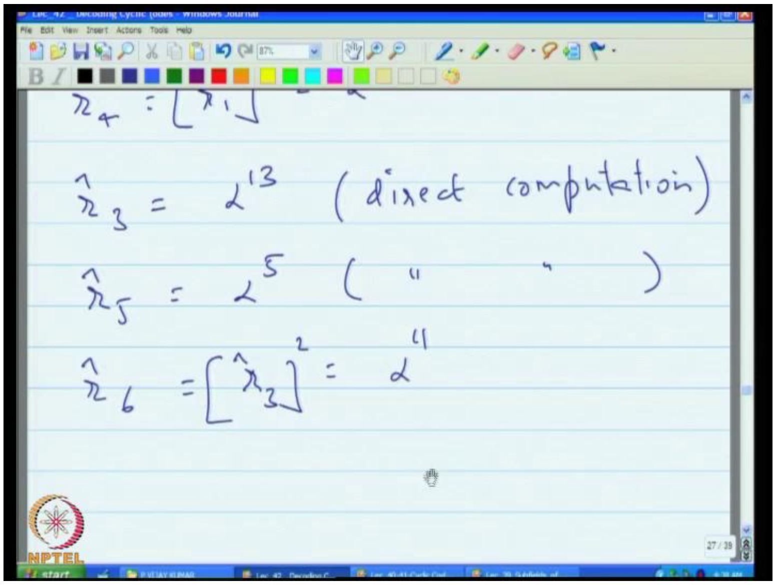
$= \alpha^6$

$\hat{r}_2 = [\hat{r}_1]^2 = \alpha^{12}$ (conjugacy)

$\hat{r}_4 = [\hat{r}_1]^4 = \alpha^9$

So, this is by the conjugacy.

(Refer Slide Time: 37:28)



$r_4 = [r_1] = \alpha$

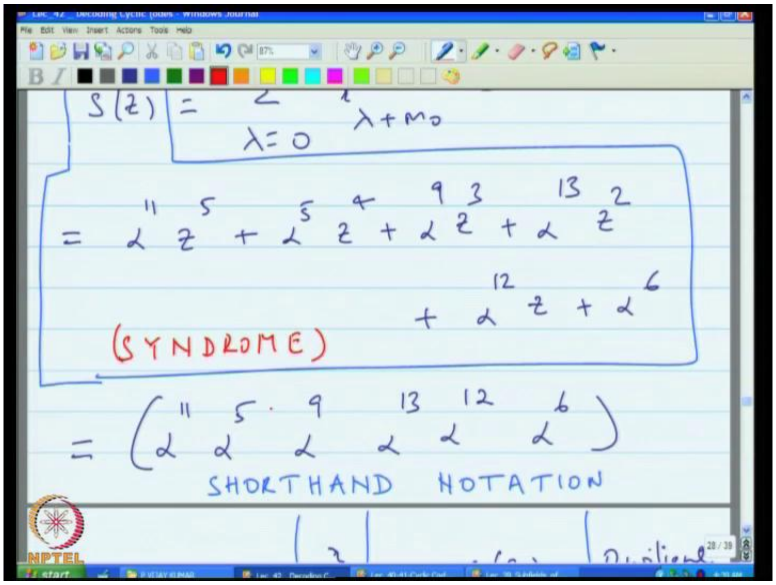
$\hat{r}_3 = \alpha^{13}$ (direct computation)

$\hat{r}_5 = \alpha^{5}$ (" ")

$\hat{r}_6 = [\hat{r}_3]^2 = \alpha^{11}$

The conjugacy r at of 2 is r at of 1 square. Which is alpha to the 12 r at of 4 is r at of 1 to the 4 is which is alpha to the 9 r at 3 alpha to the 13 having shown this here which follows from direct computation r at 5. Similarly, alpha to the 5 r at 6 r at 3 square alpha 13 square alpha to the 26 which is alpha to the 11. So, in this we actually computed the transformed the transform co efficient can be evaluated 6 alpha to the 6 alpha to the 12 alpha to the 9 alpha to the 13 alpha to the 5 and alpha to the 11.

(Refer Slide Time: 38:02)



$$S(z) = \sum_{\lambda=0} \quad {}_{\lambda+m_0}$$

$$= \alpha^{11} z^{5} + \alpha^{5} z^{4} + \alpha^{9} z^{3} + \alpha^{13} z^{2} + \alpha^{12} z + \alpha^{6}$$

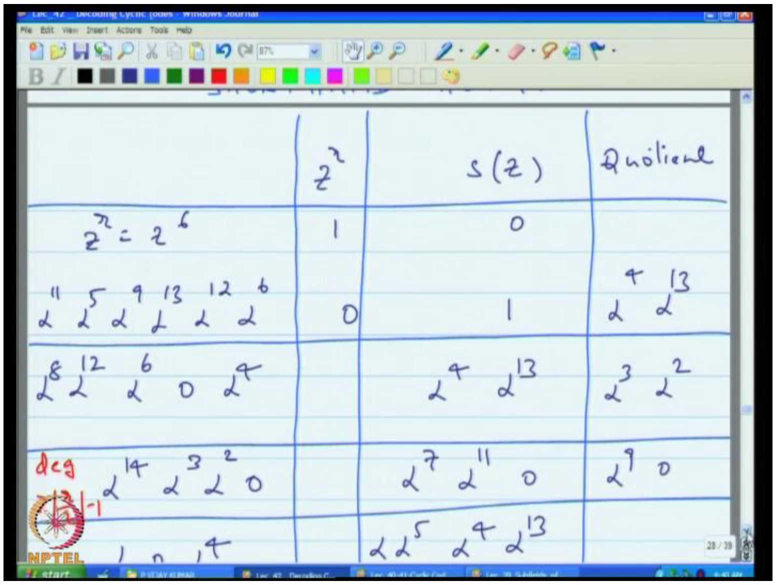
(SYNDROME)

$$= \left(\alpha^{11}\ \alpha^{5} \cdot \alpha^{9}\ \alpha^{13}\ \alpha^{12}\ \alpha^{6}\right)$$

SHORTHAND HOTATION

So here these co efficient write not in the particular order, I had 1 I had 2 3 4 5 6 so these is your syndrome. So, this first is step to the second step is to compute the syndrome, and since it is come to sum work with polynomial like this full. You short hand and just write it like this. So, here and getting read of these z just putting down co efficient alpha 6 alpha 12 alpha 13 alpha 9 alpha 5 alpha 11.

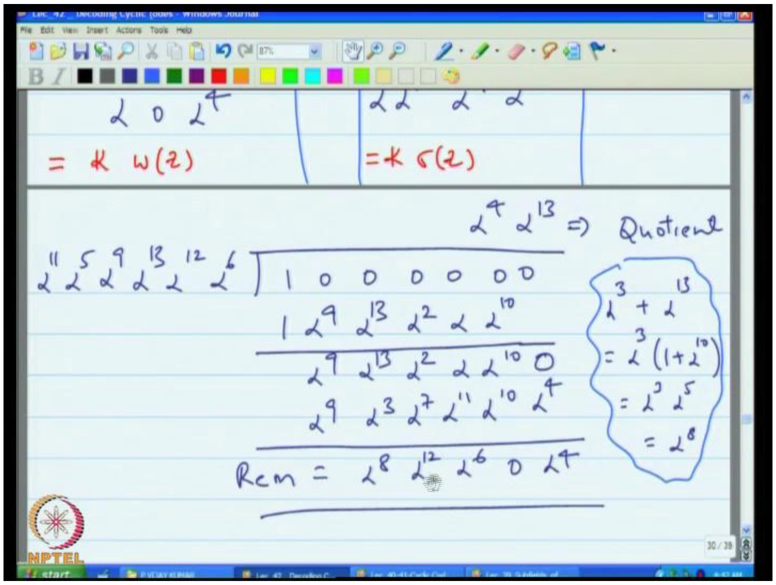
(Refer Slide Time: 38:58)



	z^{r}	$s(z)$	Quotient
$z^{r} = z^{6}$	1	0	
$\alpha^{11}\ \alpha^{5}\ \alpha^{9}\ \alpha^{13}\ \alpha^{12}\ \alpha^{6}$	0	1	$\alpha^{4}\ \alpha^{13}$
$\alpha^{8}\ \alpha^{12}\ \alpha^{6}\ 0\ \alpha^{4}$		$\alpha^{4}\ \alpha^{13}$	$\alpha^{3}\ \alpha^{2}$
deg $\alpha^{14}\ \alpha^{3}\ \alpha^{2}\ 0$		$\alpha^{7}\ \alpha^{11}\ 0$	$\alpha^{9}\ 0$
[illegible]		$\alpha\ \alpha^{5}\ \alpha^{4}\ \alpha^{13}$	

Now what we do is we want to use the freehand algorithm right and we are going to pretend right we are going to pretend that we want to compute the g c d of z to the r and s of z (( )) here is the s of z here is the z to the r r is 6. Now so Euclid algorithm says that you take you divide this by this and put down that remainder here, and thus your quotient so carried this computation from the sides.

(Refer Slide Time: 39:38)


Lec_42 _ Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
87%
NPTEL
30 / 39
start

$\alpha \; 0 \; \alpha^4$ | $\alpha \alpha \; \alpha \; \alpha$

$= \kappa \; w(z)$ | $= \kappa \; \sigma(z)$

$\alpha^4 \; \alpha^{13} \Rightarrow$ Quotient

$$\alpha^{11} \alpha^5 \alpha^9 \alpha^{13} \alpha^{12} \; \alpha^6 \; \big) \; 1 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0$$

$$1 \; \alpha^9 \; \alpha^{13} \; \alpha^2 \; \alpha \; \alpha^{10}$$

$$\alpha^9 \; \alpha^{13} \; \alpha^2 \; \alpha \; \alpha^{10} \; 0$$

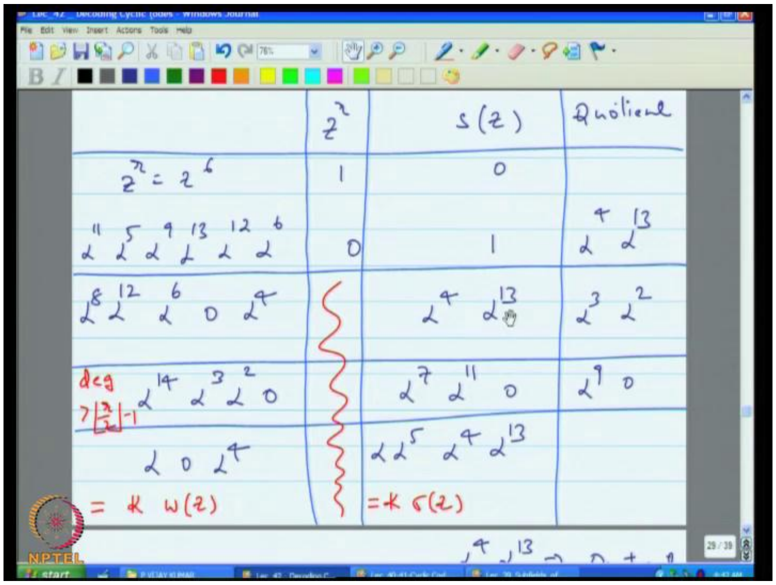
$$\alpha^9 \; \alpha^3 \; \alpha^7 \; \alpha^{11} \; \alpha^{10} \; \alpha^4$$

$$\text{Rem} = \alpha^8 \; \alpha^{12} \; \alpha^6 \; 0 \; \alpha^4$$

$$\alpha^3 + \alpha^{13}$$
$$= \alpha^3 (1 + \alpha^{10})$$
$$= \alpha^3 \alpha^5$$
$$= \alpha^8$$

Let us take the look at that. So, here z to the 6 and short form notation and here is the s of z. And we want to divide this by this. So, this is alpha to the 15 alpha to the 4 which will give you 1 alpha to the 9 13 alpha square alpha, alpha to the 10 we subtract we get this row you look at alpha to the 9 and alpha to the 11. So, that must be alpha to the 13, because that gives you alpha to the 20 4 which is alpha 9. And are again and again here I need to use the 1 add 1 table. For example, alpha cube plus alpha 13 so alpha cube plus alpha 13 is alpha cube into 1 plus alpha to the 10 which is alpha cube into alpha to the 5 which is alpha to the 8. After you use this for after we work with add 1 table for while we soon we soon none of (( )). So, we able to do it automatically I just decided it here. So, lets the alpha 8 give me here; similarly, this is 12 this is 6 0 alpha to the 4 and this your remainder now 8 12 6 0 4 0 is a remainder.

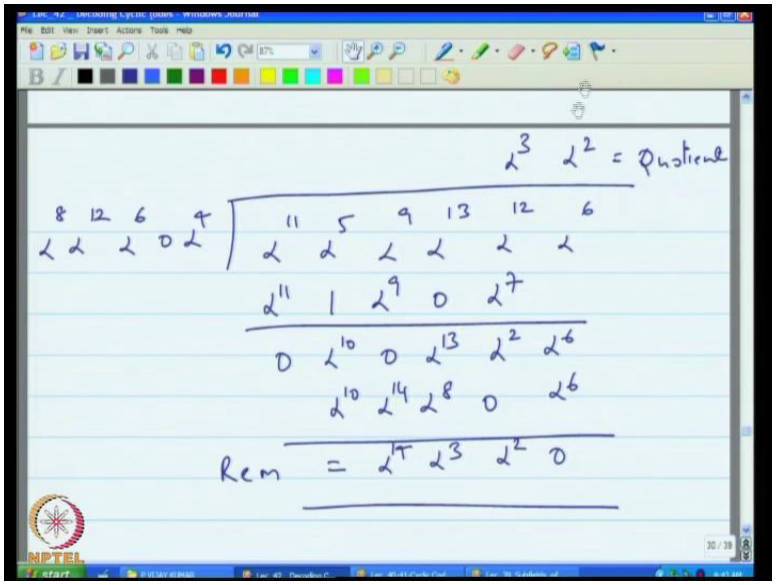
(Refer Slide Time: 41:09)



	z^2	$s(z)$	Quotient
$z^{r} = z^{6}$	1	0	
$\alpha^{11}\ \alpha^{5}\ \alpha^{9}\ \alpha^{13}\ \alpha^{12}\ \alpha^{6}$	0	1	$\alpha^{4}\ \alpha^{13}$
$\alpha^{8}\ \alpha^{12}\ \alpha^{6}\ 0\ \alpha^{4}$		$\alpha^{4}\ \alpha^{13}$	$\alpha^{3}\ \alpha^{2}$
deg $> \lfloor \frac{r}{2} \rfloor - 1$ $\alpha^{14}\ \alpha^{3}\ \alpha^{2}\ 0$		$\alpha^{7}\ \alpha^{11}\ 0$	$\alpha^{9}\ 0$
$\alpha\ 0\ \alpha^{4}$		$\alpha\ \alpha^{5}\ \alpha^{4}\ \alpha^{13}$	
$= k\ w(z)$		$= k\ \sigma(z)$	

And the quotient is alpha 4 alpha 13 now in the Euclid algorithm we have to take this like an excel spread sheet. And whatever you do here? You must replicate here now it terms of that this these columns is really we do not really care. But happens in it because in terms of there is not material for calculation by just raise that, we focus only on replicating the calculation that give us this here. So, give this entry we took this multiplied it this and subtracted from this. So, we get this by subtracting from this, times is that gives thus this, times for the polynomial alpha to the 13 plus alpha to the 4 z next we divide this by this, and take the remainder. And that computations are carried out here.

(Refer Slide Time: 42:12)


Lec_42 _ Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
30 / 39
NPTEL
start

$\alpha^3 \quad \alpha^2$ = Quotient

$\alpha^8 \, \alpha^{12} \, \alpha^6 \; 0 \; \alpha^4 \,\big)\; \alpha^{11} \; \alpha^5 \; \alpha^9 \; \alpha^{13} \; \alpha^{12} \; \alpha^6$

$\alpha^{11} \; 1 \; \alpha^9 \; 0 \; \alpha^7$

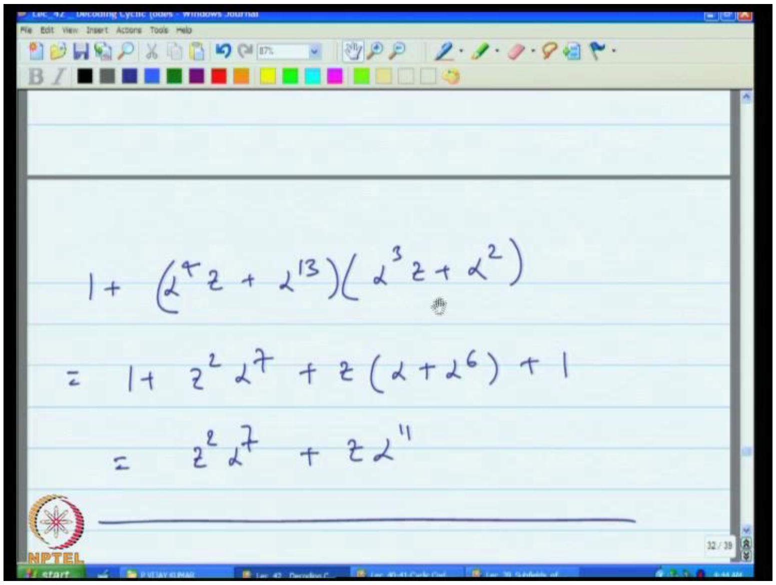
$0 \; \alpha^{10} \; 0 \; \alpha^{13} \; \alpha^2 \; \alpha^6$

$\alpha^{10} \; \alpha^{14} \; \alpha^8 \; 0 \; \alpha^6$

Rem $= \alpha^4 \; \alpha^3 \; \alpha^2 \; 0$

I just look at it as you look at it I will also check the computations are correct. So, this is our new remainder. And that is are new quotient. So, in this table we put on the quotient and your new remainder there. Even that is look so we get back here. And now we need again to pretend the excel table. So, we got this by multiplying by taking this and subtracting the product of these two from this, so that will give us alpha 7 alpha 11 0 and even that computation we multiply these 2 and add 1 and done this little later.

(Refer Slide Time: 43:41)


Lec_42 _ Decoding Cyclic Codes - Windows Journal
File Edit View Insert Actions Tools Help
NPTEL
32 / 39
start

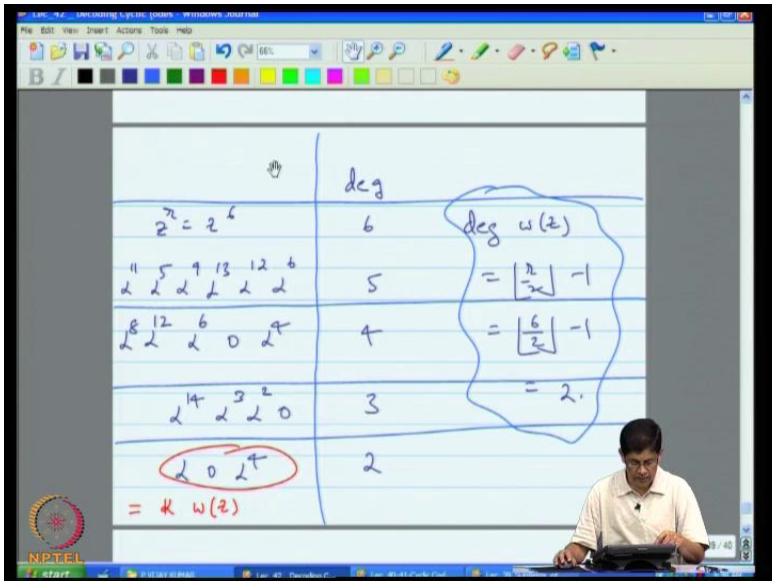
$$1 + (\alpha^4 z + \alpha^{13})(\alpha^3 z + \alpha^2)$$

$$= 1 + z^2 \alpha^7 + z(\alpha + \alpha^6) + 1$$

$$= z^2 \alpha^7 + z \alpha^{11}$$

So, here we go. So, alpha 14 we multiply and add 1, and again the computation look so this seems correct. So, we should have alpha 7 alpha 11 in the table alpha alpha 11 alpha 7 0 alpha 11 alpha 7 0, and now you divide by this, by this we get this remainder see this last division, this again lets correct so we left with the remainder of this quantity here now. Of course, 1 question remainder right keep going on forever. So, there is an stopping point and its terms out there is a stopping point, where is the stopping point. You stop so let me could just make this clear let me copy this page, and where I can know see this page. And now have room two make some put some marks on it so here if you keep track of the degree. So, let us happening here is that your getting possible candidates for omega of z.

(Refer Slide Time: 46:02)



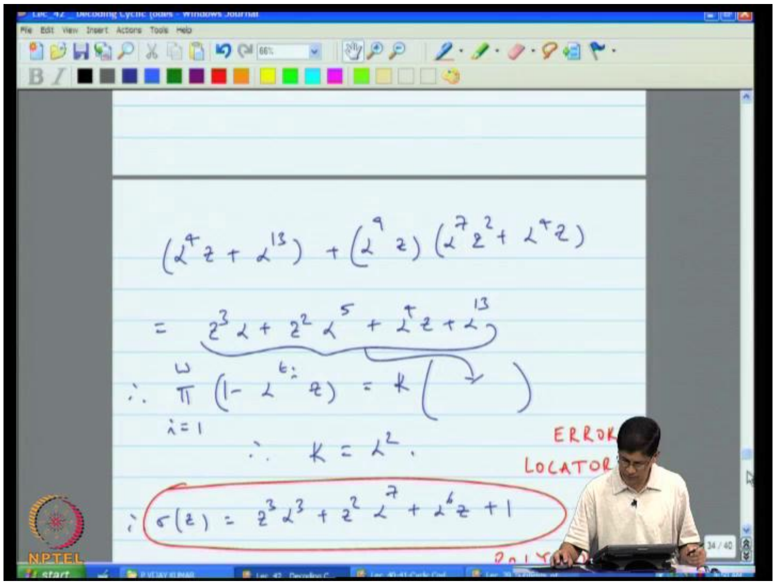
	deg
$z^{r} = z^{6}$	6
$\alpha^{11}\ \alpha^{5}\ \alpha^{9}\ \alpha^{13}\ \alpha^{12}\ \alpha^{6}$	5
$\alpha^{8}\ \alpha^{12}\ \alpha^{6}\ 0\ \alpha^{4}$	4
$\alpha^{14}\ \alpha^{3}\ \alpha^{2}\ 0$	3
$\alpha\ 0\ \alpha^{4}$	2
$= k\ \omega(z)$	

$$\deg\ \omega(z) = \left\lfloor \frac{r}{2} \right\rfloor - 1 = \left\lfloor \frac{6}{2} \right\rfloor - 1 = 2.$$

Now the degrees let us keep track of the degrees of the entries this is 6, this is 5, this is 4 this is 3, this is 2, on the other hand we said that the degree of omega z is equal to r over 2 minus 1 which other cases 6 by 2 minus 1 which is 2. So, what for actually looking for is the first instance when the degree? We know that 2 less than 2. So, notice that this is the first instance of the degree of this polynomial of left most column is 2 or less than 2

So, the moment you see that, you draw circle what it terms out of that polynomial what you get here is not perhaps omega of z there is a constant times of omega of z. Now again I am not proving the theory you can actually read the book (( )) which goes through this it is a somewhat lengthy proof we will take a lecturer two, along to prove that. So, this is our starting point the starting point is look for one the degree in the left most column dips to 2 or less that is r by 2 minus 1 or less. So, that is what happen here, the degree did here and then we actually said here this is some constant terms omega of z and this is some constant terms sigma of z. Remember we said the g of r terms something plus s of z terms something, which giving you omega of z. Now we know sigma and omega up to a constant.

(Refer Slide Time: 47:46)



$$(\alpha^4 z + \alpha^{13}) + (\alpha^9 z)(\alpha^7 z^2 + \alpha^4 z)$$

$$= \underbrace{z^3\alpha + z^2\alpha^5 + \alpha^4 z + \alpha^{13}}$$

$$\therefore \prod_{i=1}^{w}(1-\alpha^{t_i}z) = k(\ \rightarrow\ )$$

$$\therefore k = \alpha^2.$$

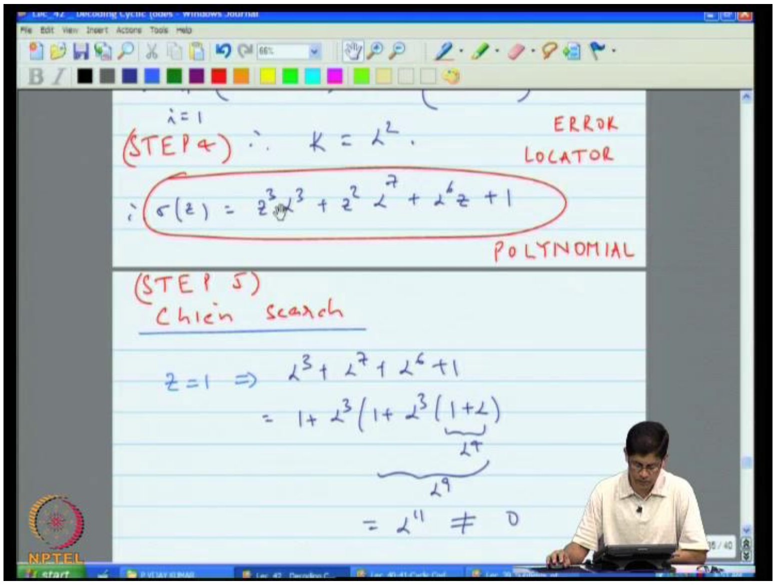
$$\therefore \boxed{\sigma(z) = z^3\alpha^3 + z^2\alpha^7 + \alpha^6 z + 1}$$

ERROR
LOCATOR

How do figure out that constant? That is easy, because what you know is that so here we are this is some, this now and other point here to be made here is that in this table, what we actually got is omega of z and sigma of z. Now in the non binary case you need to find the error locations, as well as error values. In the binary case once you know the error locations then you know the error values, because the error values can only take on the value of one. So, in the binary case as in this example its fizzes to determine sigma of z now focuses on the particular polynomial of degree 3 which is sigma of z now.

What we know is that this polynomial may not be sigma of z, but the sigma z up to some constant multiplication. Now we look at this inside the constant term here is one. So, after make this constant term one I have to multiply this entire polynomial by alpha square. So, that is what you do? You multiply this entire candidate for sigma z by alpha square and you get z cube alpha cube plus z square alpha to the 7 plus alpha 6 and plus 1. This is the now this is the error locator polynomial. This is the error locator polynomial, and now after those factorate, and next lead to factorate so in terms of these steps I guess we have the step 2 is to complete this Euclid algorithm is step 3. Its Euclid individual algorithm and then once you found is you could call this sealing step 4.

(Refer Slide Time: 50:04)



$i=1$

(STEP 4) $\therefore \quad K = \alpha^2.$

ERROR LOCATOR

$\therefore \sigma(z) = z^3\alpha^3 + z^2\alpha^7 + \alpha^6 z + 1$

POLYNOMIAL

(STEP 5)

Chien search

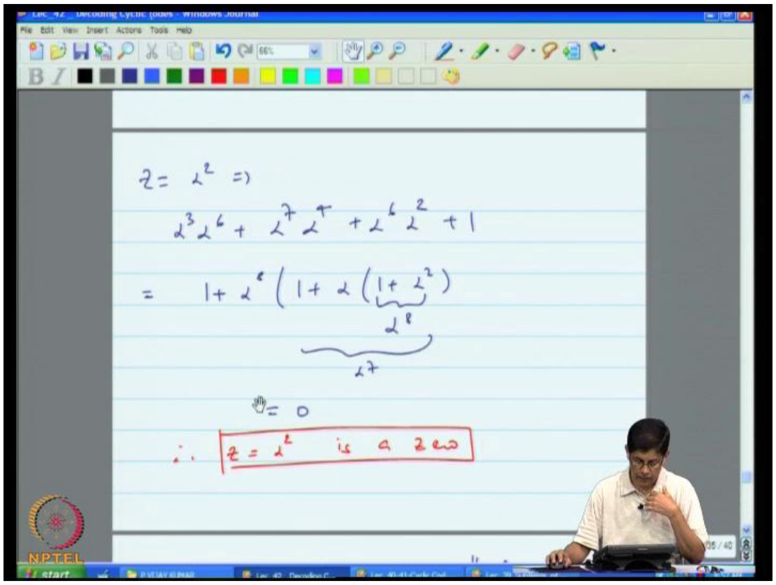
$z=1 \Rightarrow \alpha^3 + \alpha^7 + \alpha^6 + 1$

$= 1 + \underbrace{\alpha^3(1 + \alpha^3\underbrace{(1+\alpha)}_{\alpha^4}}_{\alpha^9})$

$= \alpha^{11} \neq 0$

And finally, what you do is? You find you try to find the 0s of this polynomial, and you do something that called chine search there are alternatives. But finalist we search by jus this checking all the elements in the finite field to see this is 0. So, example z to the 1 here you notice that alpha cube plus alpha 7 plus alpha 6 plus 1 which terms to evaluate to alpha to the 11 and therefore, is non zero. So, we can z equal to and then z is equal to alpha square, in terms of that alpha square so plug in alpha z is equal to alpha square. You will get z cube alpha to cube alpha to the 6 alpha cube plus alpha to the 4 alpha 7 and so on.

(Refer Slide Time: 50:47)



$z = \alpha^2 \Rightarrow$

$\alpha^3\alpha^6 + \alpha^7\alpha^4 + \alpha^6\alpha^2 + 1$

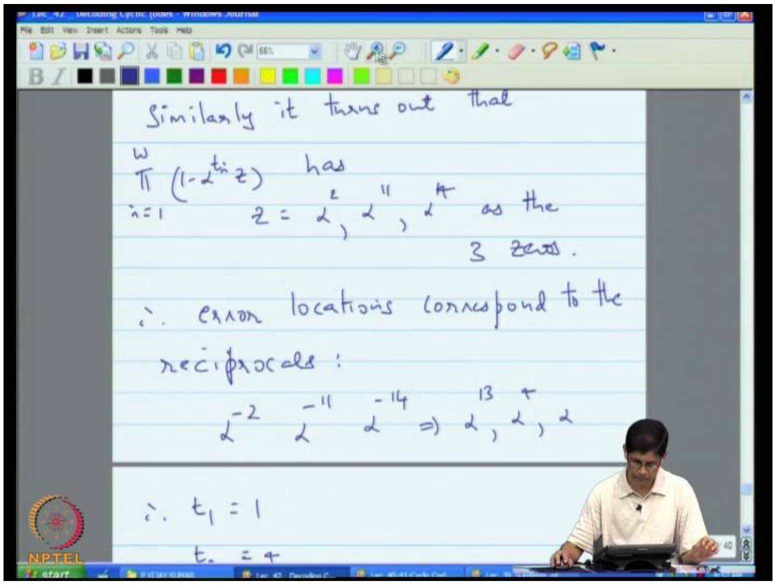
$= 1 + \alpha^6\underbrace{\left(1 + \alpha\left(\underbrace{1 + \alpha^2}_{\alpha^8}\right)\right)}_{\alpha^7}$

$= 0$

$\therefore \boxed{z = \alpha^2 \text{ is a zero}}$

So get this polynomial, and evaluate this using honours method you find that is equal to 0, and z to the alpha square is equal to 0.

(Refer Slide Time: 51:03)



Similarly it turns out that

$\prod_{i=1}^{w}(1-\alpha^{t_i}z)$ has

$z = \alpha^2, \alpha^{11}, \alpha^{14}$ as the 3 zeros.

$\therefore$ error locations correspond to the reciprocals :

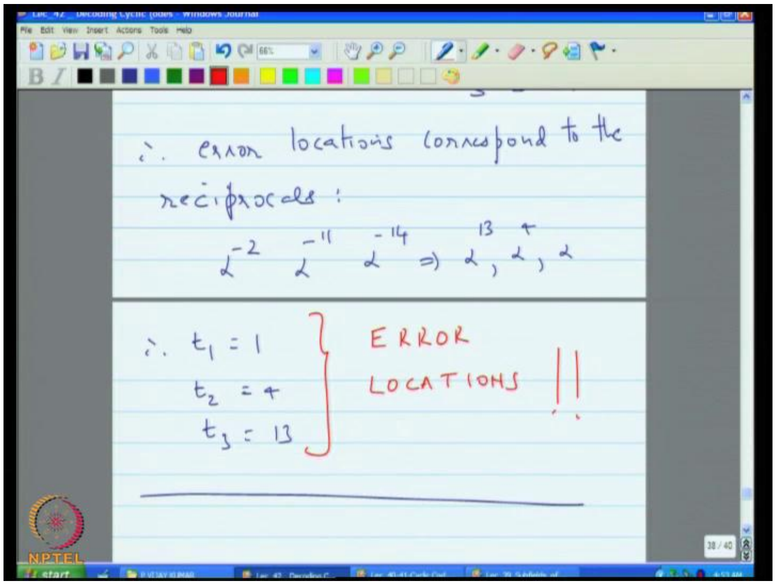
$\alpha^{-2} \quad \alpha^{-11} \quad \alpha^{-14} \Rightarrow \alpha^{13}, \alpha^{4}, \alpha$

$\therefore t_1 = 1$

$t_2 = 4$

Similar it terms of that this polynomial here as 3 0s alpha square alpha 11 alpha to the 14. And you can see from the way this is actually structured that the error locations are the correspond to the so the error locations are not are not the reciprocals. But rather correspond to the reciprocals. So, the reciprocals been alpha to the minus 2 alpha to the minus 11 alpha to the minus 14 this is alpha 13 alpha 4 and alpha.

(Refer Slide Time: 51:42)



∴ error locations correspond to the reciprocals :

$\alpha^{-2} \quad \alpha^{-11} \quad \alpha^{-14} \Rightarrow \alpha^{13}, \alpha^{4}, \alpha$

$$\therefore \left.\begin{array}{l} t_1 = 1 \\ t_2 = 4 \\ t_3 = 13 \end{array}\right\} \text{ERROR LOCATIONS !!}$$

So that means the error location were actually there are 3 error locations, and these are the 3 error locations. We actually successfully decoded the code, now in the non binary case you would actually have to use partial fractions. And the error evaluated polynomial to then determine the error values, but we want actually go through that. So, there actually is more or less (( )) I want to cover today, and there also finishes our course for us. I think what was basically done, in this course is you know it took us some time because I first one through the basics of the error correcting codes. And then I took you to the g d i which I feel is important (( )) right, I am very block and convolutional codes then the g d i, and then we applied it to understand l d p c codes which is the modern class of codes.

And then we can mark in the classically codes, red Solomon codes. And so typical some time that help fully benefit from that benefited from that, where are do is? What we will do is? What kind of lecture is made available? And possibly some homework success where that wish you the best it is been interesting and enjoyable experience. I hope you find this useful. So, thank you. I think I like to actually thank him the staff here. I see the staff here has been excellent ranging from professor Gotha Kumar who was really very encouraging right from the start and motivated. I think the bike of the faculty sign on here as well as the local staff here Mr Singh Mr Singh here a k Singh as well as persistence here that he very helpful. I like to also thank him that I like to close.