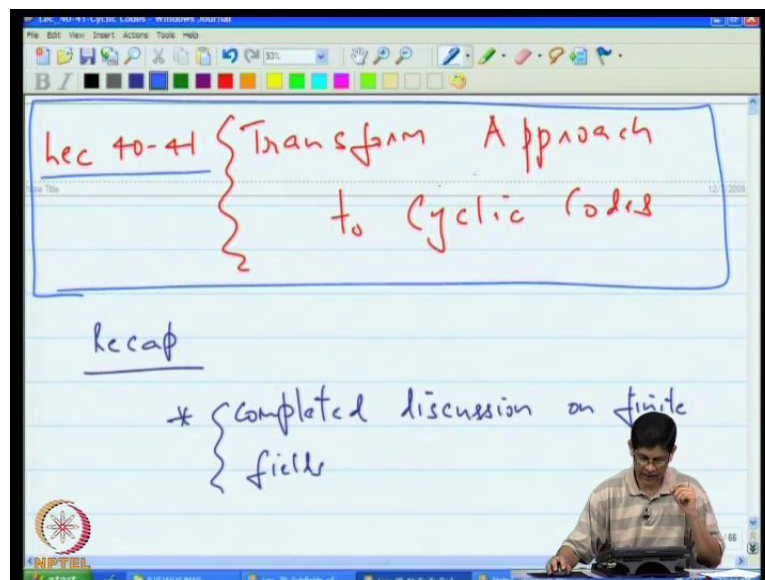


**Error Correcting Codes**  
**Prof. P Vijay Kumar**  
**Department of Electrical Communication Engineering**  
**Indian Institute of Science, Bangalore**

**Lecture No. # 41**  
**Estimating the Parameters of a Cyclic Code**

Now, I think that we will just be able to conclude the course in the next lecture. So, this is our penultimate lecture. So, let us just go over what we covered in the last class.

(Refer Slide Time: 00:34)



Now, what I have done is, I have taken the last lecture; and so this is an internal thing, I would like to make these notes for 40 and 41 blend into a single file. So, does not really matter, if you have access to the file; in either case, but now I rather than separate the lectures, I have combined them. And I have actually given it a slightly different title from what I had given it before. So, the title is a transform approach to cyclic codes. And so what we did last time, just to hit the highlights of our last lecture was basically we said, look we are going to discuss cyclic codes, and our view point of the cyclic codes is going to be from a, from the point of view of transforms. The particular type of transform is called the finite field transform.

So, first we said, well we need a little bit of machinery, in order to start talking about the transforms; and we needed that in particular that element  $\alpha$ ; so if you have a code over an alphabet of size  $q$ , and the block length is  $N$ , then you need to find a finite field that contains your original field, that contains an element of order  $N$ ; because your original field may not contain such an element. So, you have to expand the size of your field. Once you did that, you have the element  $\alpha$ , then we went ahead and defined the finite field transform.

And then we went about examining its properties, such as linearity, cyclic shifts, inversion, convolution, conjugacy. Once we had understood or reasonably, had a reasonable understanding of, excuse me of the transform, then we went **went** back, and said our interests is in cyclic codes; by which we meant we are interested in block codes, having the property that they are linear, and they are cyclic; they are closed in their cyclic shifts. And we were adapting a transformed view point of these codes. So, towards that and I think we just about got started over there. So, I think... So, let me take up the discussion on cyclic codes and lead you a little bit slower through that since will be continuing the discussion, discussion in the present lectures. So, here is our, here are some of our slides on cyclic codes. So, we defined what it means to be a cyclic code.

(Refer Slide Time: 03:24)

**EQUIVALENCE RELATION ON FREQUENCIES**

Define

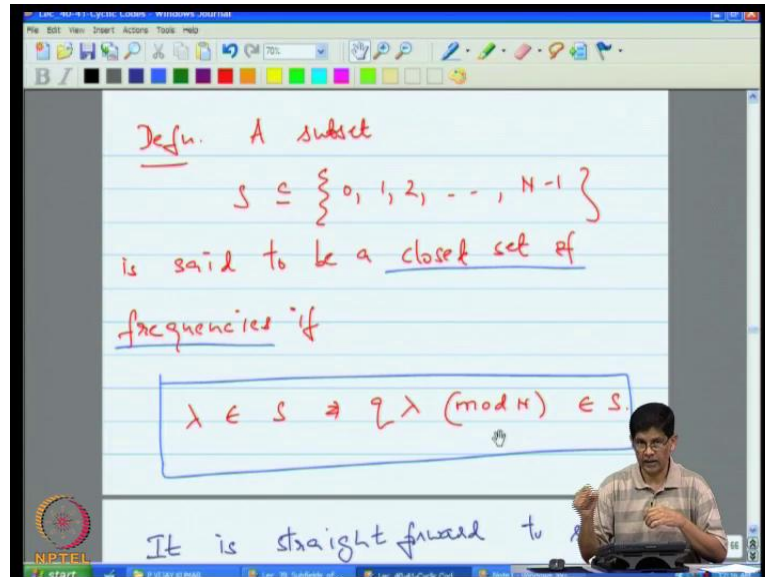
$$\lambda_2 \sim \lambda_1 \quad 0 \leq \lambda_1, \lambda_2 \leq N-1$$

if  $\lambda_2 = g^i \lambda_1 \pmod{N}$  some  $i \geq 0$ .

This can be verified to be an equivalence relation.

And then we put an equivalence relationship, so we said that when we take a codeword and we look at its transform. Then the subscripts lambda, which appear in the transform we will regard as frequencies.

(Refer Slide Time: 03:52)



So, then we define an equivalence relationship on the frequencies, which led to organising them according to cyclotomic cosets. So, here is an example. Then the smallest element in each coset is called its coset leader. Then we defined the notion of a closed set of frequencies; that is the set of frequencies is a closed set, if it is closed on the multiplication by  $q$  modulo  $N$ . And an easier way to actually picture this is that, the closed set is precisely the union of cyclotomic cosets, a set of  $q$  cyclotomic cosets mod  $N$ . So, then I... So then so that for example here, if we go back here, then any closed set is just the union of these cyclotomic cosets.

(Refer Slide Time: 04:24)

Slide content:

Eg  $q = 2$   $H = 15$

there are 5 equivalence classes  $\Rightarrow$

coset leader

frequencies

$\{ \lambda \}$

$\lambda \sim \lambda_1$

$\lambda_1 = 2 \lambda_2$

$(\text{mod } H)$

Diagram showing coset leader 0 and its equivalence class {0, 1, 2, 8, 3, 6, 12, 9, 5, 10, 7, 14, 13, 11}.

(Refer Slide Time: 04:34)

Slide content:

### NULL SPECTRUM

Defn Let  $\mathcal{C}$  be a linear, cyclic code of block length  $N$  over  $\mathbb{F}_2$ .

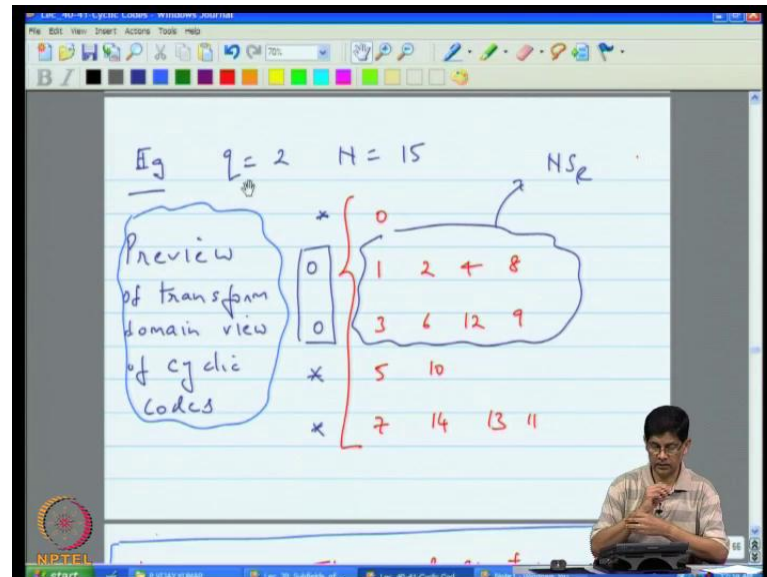
Then the collection of frequencies

$$NS_{\mathcal{C}} = \left\{ \lambda \mid \begin{array}{l} 0 \leq \lambda \leq N-1 \\ \hat{c}_{\lambda} = 0 \text{ all } (c_t) \in \mathcal{C} \end{array} \right\}$$

is called the null spectrum of  $\mathcal{C}$ .

Then, we introduced the notion of the null spectrum of a code. The null spectrum of a code is those collection of frequencies, at which every code has transform value equal to 0.

(Refer Slide Time: 04:48)



And, I gave you an example here, and said that actually, this is the general picture of cyclic codes; that is, that you organise a given a cyclic codes, given an alphabet size  $q$ , given an element  $N$ , you find a field that contains the primitive element  $\alpha$ ; then you organise the frequencies according to these cyclotomic cosets, the  $q$  cyclotomic cosets mod  $N$ . And then, you pick the closed set as the union of certain of the cyclotomic cosets, for example, you might pick the union of these two, and then you say I am going to insist that my code words have transform value equal to 0 on these elements; and outside these, I do not care, because of conjugacy, if you insist that the transform is 0 at frequency one, then it is automatically going to be 0, at all these other frequencies.

And so the design of cyclic codes in some sense, it just a matter of, either including, or exclusive, excluding, cyclotomic cosets from inclusion in the null spectrum. So, that is why, there are only 32 codes for example, having block length 15, over the finite field of two elements. That is about where we had left off. So, I think, what I will do is, I will begin our lecture, let me just insert page and put in a quick summary.

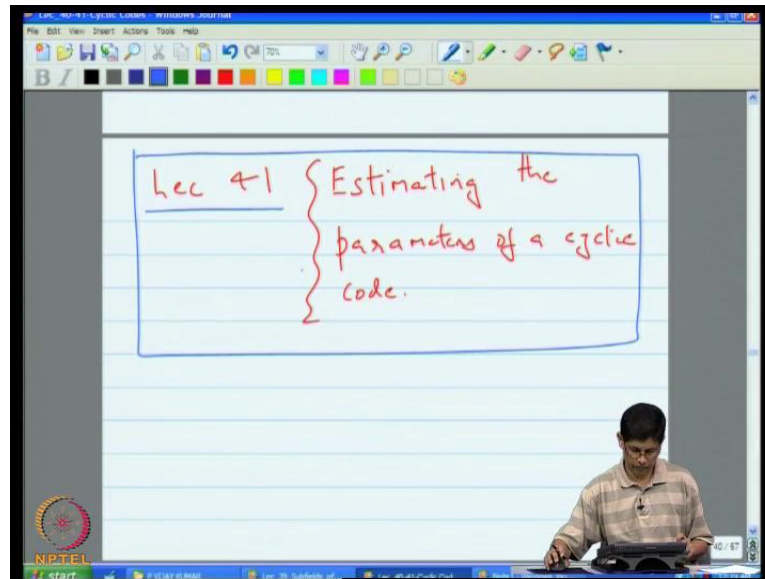
(Refer Slide Time: 07:14)

Recap

- \* finite field transform
  - expanding  $\mathbb{F}_2 \rightarrow \mathbb{F}_{2^m}$
  - defn
  - properties
- \* cyclic codes
  - closed set
  - cyclotomic cosets
  - null spectrum

So, this is rather quick; is a rather quick summary of what we did last time. We looked at finite field transforms. The first, **first** was the expansion of the finite field to find an element of order  $N$ . Then we gave the formal definition of the transform. We looked at its properties. We started discussing cyclic codes, we discussed cyclotomic cosets, closed sets. So, I think these two got interchanged in their order here. So, perhaps, let us make a note of that, in terms of the order in which we discuss them. And then, finally, we introduced the notion of a null spectrum.

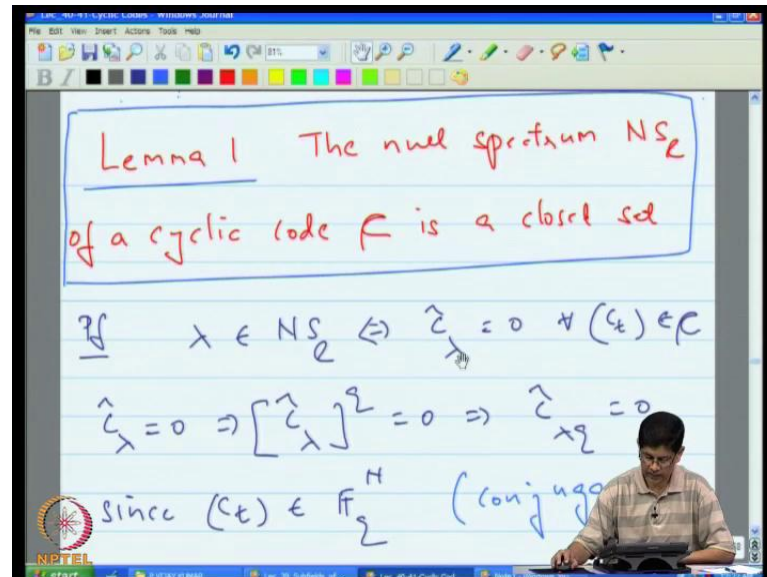
(Refer Slide Time: 09:19)



Now, we want to proceed with the theory of the cyclic codes, and our goal, as the title says, is to actually estimate the parameters of a cyclic code. So, what do we mean by the parameters? Well, the block length is clear; the alphabet size and the block length are clear, clear. So, what is of interest, are the other parameters, namely the dimension of the cyclic code, and its minimum distance. So, those are the two things that we are going to target in this lecture.



(Refer Slide Time: 09:46)



So, the first result, we will show today is that, the null spectrum of the cyclic code is a closed set. I remember, what we mean by the null spectrum of the cyclic code is that, it is those collection of frequencies, where every code word has transformed that evaluates to 0. So, we will, the proof actually starts from there. So, here, if  $\lambda$  belongs to the null spectrum of the code, then that implies that,  $\hat{c}_\lambda$  of  $\lambda$  is 0, for all code words. That is, if  $\hat{c}_\lambda$  of  $\lambda$  is 0, then,  $\hat{c}_\lambda$  of  $\lambda$  raised to the  $q$ th power is 0. Again, by the conjugacy relationship,  $\hat{c}_\lambda$  of  $\lambda$  raised to the  $q$ th power is  $\hat{c}_{\lambda^q}$  of  $\lambda^q$ ; the reason being that your code word belongs to the ground field. Whenever you have a code word that belongs to the ground field, its transform will satisfy the conjugacy relationship. So, that forces this equal to 0. But then, so this means that, if  $\lambda$  belongs to the null spectrum, so does  $\lambda^q$ ; and hence, this is a closed set.



(Refer Slide Time: 11:06)

$\Rightarrow \lambda q \in (NS)_R$  Hence  $(NS)_R$  is a closed set.

---

**Lemma 2** Let  $S \subseteq \{0, 1, \dots, N-1\}$  be a closed set of frequencies.

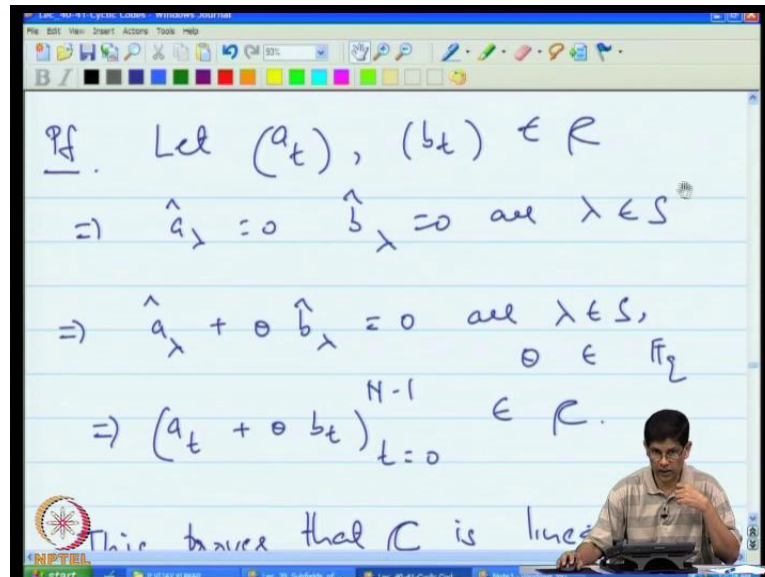
Then

$$C \triangleq \left\{ (c) \in \mathbb{F}_2^N \mid \sum_{\lambda \in S} c_{\lambda} = 0, \text{ all } \lambda \in S \right\}$$

is a linear cyclic code.

So hence, the null spectrum of a code is a closed set. Second lemma, then... So, what we actually said is, given a code, we said, we are going to let this set of all frequencies, where the code word transforms evaluate to 0, then that is a closed set. There is a converse, sort of converse of this that says look, supposing on the other hand, if I started out with a set of frequencies, which was closed under the conjugation. So, this is the closed set of frequencies, and if I then define my code to be all  $n$  tuples  $n$  tuples, whose transform evaluates to 0, at all frequencies contained in  $S$ , then that in fact, is a linear cyclic code. So, it is, it is kind of a converse. So, it says that I can start from a code, and I can go to a closed set, or I can start from a closed set, and I am led to a linear cyclic code.

(Refer Slide Time: 12:21)



$$\text{Pf. Let } (a_t), (b_t) \in \mathcal{C}$$

$$\Rightarrow \hat{a}_\lambda = 0 \quad \hat{b}_\lambda = 0 \text{ for all } \lambda \in S$$

$$\Rightarrow \hat{a}_\lambda + \theta \hat{b}_\lambda = 0 \text{ for all } \lambda \in S, \quad \theta \in \mathbb{F}_q$$

$$\Rightarrow (a_t + \theta b_t)_{t=0}^{N-1} \in \mathcal{C}.$$

This proves that  $\mathcal{C}$  is linear.

So, let  $a_t$  and  $b_t$  be code words; then so that means, that  $\hat{a}_\lambda$  and  $\hat{b}_\lambda$  are both 0s, for all  $\lambda$  in the closed set. But then, that is also true, if I take a linear combination of them, where  $\theta$  belongs to  $\mathbb{F}_q$ . And, so that means that, but then by the linearity property of the transform, this quantity here, is the transform of the  $a_t$  plus  $\theta b_t$ . So, that means that, if  $a_t$  and  $b_t$  are code words, so is  $a_t + \theta b_t$ . So, that proves that your code is linear, which is not surprising. So basically, we have used the linearity of the transform, to prove that the code is linear.

(Refer Slide Time: 13:15)

Next, if  $(c_t) \in C$

and  $a_t = c_t - \tau a_{t-1}$

$\Rightarrow \hat{a}_\lambda = d^{\lambda \tau} \hat{c}_\lambda$

$\Rightarrow \hat{a}_\lambda = 0 \quad \text{all } \lambda \in S$

$\Rightarrow (a_t)_{t=0}^{N-1} \in C.$

Next, if the code, if  $c_t$  is a code word, so, it only remains to actually prove that this code is not only linear, but it is also cyclic. So, we have to now worry about cyclic shifts. So here, supposing  $c_t$  is a code word, and you define  $a_t$  to be a cyclic shift of  $c_t$ , and you take the transform of  $a_t$  that is  $\alpha$  to the  $\lambda \tau$   $\hat{c}_\lambda$  of  $\lambda$ . But then since  $\hat{c}_\lambda$  of  $\lambda$  is 0 for all  $\lambda$  in  $S$ , so is  $\hat{a}_\lambda$  of  $\lambda$ . But then, you defined your code word as a set of all vectors, whose transform is 0 on  $S$ , right; and so that the automatically means that,  $a_t$  of  $t$ , that, it means that,  $a_t$  of  $t$  is also a code word and therefore, the code word, therefore the code is cyclic.

So we basically, the way we have proved this, is just by using the property of the finite field transform and the cyclic shift; you just get a multiply it, the transform values are just multiplied by some constant. So, it does not change the fact that, the transform is 0 at a certain frequencies. For this reason, the code is closed under the cyclic shifts.

(Refer Slide Time: 14:35)

REMINDER: COMMON SETTING

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

$m$  is the order of  $q \pmod{N}$

$C$  is a cyclic code of block length  $N$  over  $F_q$ .

Now, just a reminder here, reminder slide here to say that in all the subsequent discussion, we will be working with the set of parameters, the standard parameters. So, this is the common setting;  $q$  will always denote a power of a prime; and then,  $N$  will be a reference to the block length, and we will always have that,  $q$  and  $N$  are relatively prime.  $m$ , the smaller  $m$  is going to be order of  $q$  modulo  $N$ , and  $c$  will be a cyclic code of block length  $N$  over  $F_q$ .

(Refer Slide Time: 15:10)

Defn A basic sequence  $(B_t)$  of frequency  $\lambda_0$ ,  $0 \leq \lambda_0 \leq N-1$  is a sequence satisfying:

$$\hat{z}_\lambda = \begin{cases} 1 & \lambda = \lambda_0 \\ 0 & \text{else} \end{cases}$$

So, in this setting, we are going to define something, that is called a basic sequence. A basic sequence of frequency lambda naught, where lambda naught lies between 0 and N minus 1, is a sequence satisfying that B hat of lambda is 1, whenever lambda is either lambda naught, or else a conjugate of lambda naught, meaning that, it is some part of q times lambda naught and it is 0 everywhere else.

(Refer Slide Time: 15:42)

Handwritten notes on the whiteboard:

Ex:  $q = 2$   $N = 15$   $m = 4$

$\lambda_0 = 3 \Rightarrow$

Note:  $\hat{B}_3 = 1 \Rightarrow$

$\hat{B}_6 = \hat{B}_{12} = \hat{B}_9 = 1$

as well!

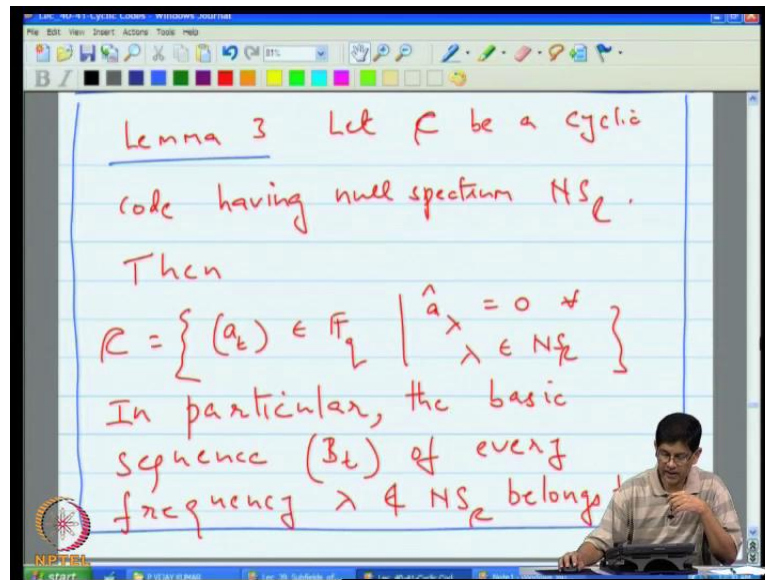
Diagram showing a sequence of 15 elements (0 to 14) arranged in a grid. The sequence is 0, 0, 1, 0, 0, 0, 0, 1, 2, 8, 3, 6, 12, 9, 5, 10, 7, 14, 13. The sequence is 0 everywhere except at frequencies 3 and its conjugates.

For example, here is the case when... So, this is the case, when q is 2 and N is 15, and m is equal to 3, in this case; that should be, m is equal to 4, pardon me. So, supposing I pick lambda naught to be 3, then what I want to illustrate is, a basic sequence of frequency lambda naught; meaning its transform value is 0 everywhere, except at frequencies corresponding to lambda naught and its conjugates.

So, that means that, this B of t is sequence has transform, which is 0 on all these cosets and it is 0, every, under all cosets, other than the cosets corresponding to 3. And here, it is 1; and the conjugacy also tells us that, its value at 6 is 1 to the q is, 1 times, 1 to the q, which is still 1, and so on. So, it actually takes on the same value for every element within a coset. It takes on 1, the value 1, for all the elements in this particular coset, and it takes on the value for everywhere else. Once again, that is because if B hat of 3 is 1, then, B hat of 6 is B hat of 12 equal to B hat of 9 is 1; because B hat of 6, recall I will put this on this side here, B hat of 6

is,  $B$  hat of 3 square. So, for this reason, if  $B$  hat of 3 is 1, then  $B$  hat of 6, which is its square, is also 1. So, this is going to clutter this. So, let me raise this.

(Refer Slide Time: 17:45)

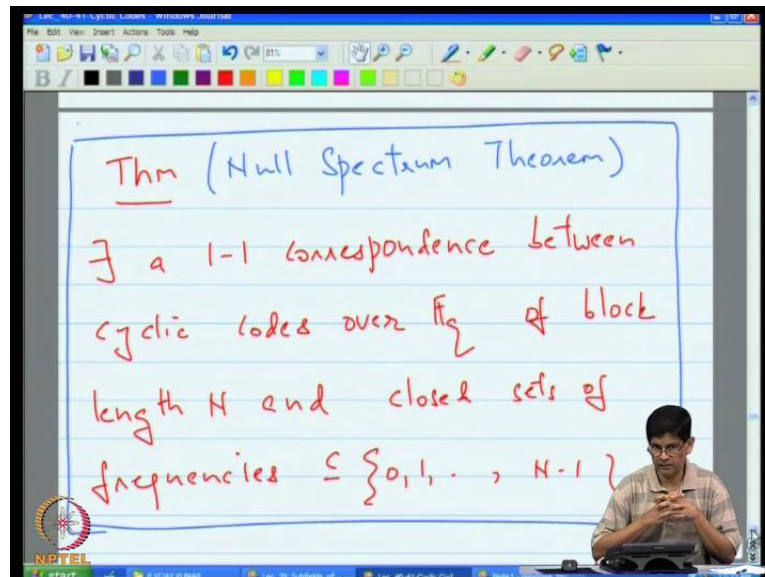


Now, the next lemma says that if  $C$  is so it is now, **now** we are exploring the connection between closed sets and **and** cyclic codes, further. So, let  $C$  be a cyclic code, whose null spectrum is given by this. Then, it is telling you that really, there is only one code, that can have this null spectrum; namely, it is that code, which corresponds to all vectors, all  $n$  tuples over  $F_q$ , whose transform values are 0 at every frequency in the null spectrum. So, we started out by saying,  $C$  is some subset of  $F_q^n$ , whose transform values are 0, at all frequencies in the null spectrum. But it turns out that, the linearity and cyclic properties that  $C$  possesses cause  $C$  to, in fact, be precisely, the largest possible collection of vectors that you could have, when you just impose the constraint on the transform values.

So, in this sense, given a null spectrum, there is a unique code that is associated to it. And in particular, the basic sequence of frequency, every frequency  $\lambda$ , that are not in the null spectrum, belongs to the code. So, that is, that is a side comment; I think I will ignore that for now. I do not believe the way I am presenting it, that we will call upon it. If I need to, I can always come back to this. The proof is in the appendix. So, I want actually go through that.

So, once again, let us recap the 3 lemmas that we have. The first lemma, the first lemma says that, the null spectrum of a code is a closed set. The second lemma says that the set of all vectors, whose null set is a closed set, whose null spectrum is a closed set, is actually a linear cyclic code. The third one says, where I can actually say something stronger; in fact, I can actually say that if you tell me that a code has a certain null spectrum, I can actually tell you, which code it is because there is essentially, just a single code for a given null spectrum. And that is precisely, the set of all  $n$  tuples which possess the null spectrum; because, that forms the cyclic code. And, it turns out that, any cyclic code within this null spectrum is essentially, this one.

(Refer Slide Time: 20:53)



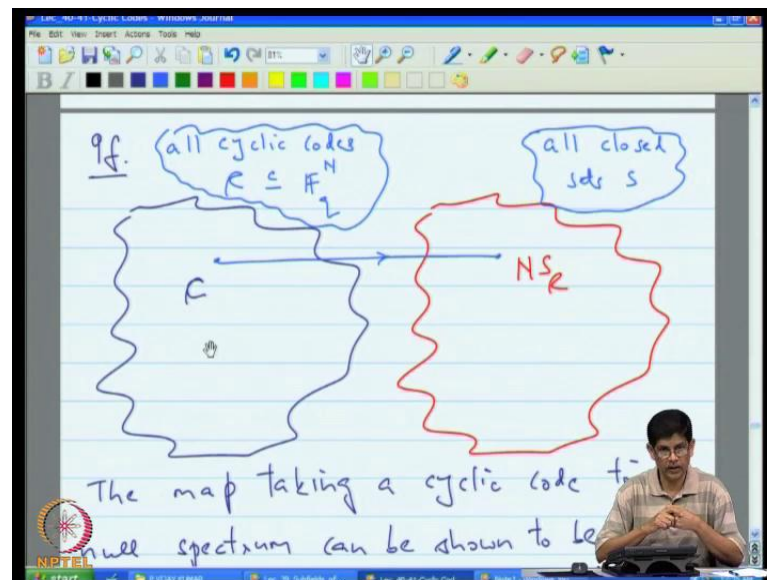
Thm (Null Spectrum Theorem)

$\exists$  a 1-1 correspondence between cyclic codes over  $F_q$  of block length  $N$  and closed sets of frequencies  $\subseteq \{0, 1, \dots, N-1\}$

So, not surprisingly, when you put these together, you have this important null spectrum theorem, which says that there is a one-to-one correspondence between cyclic codes over  $F_q$  of block length  $N$  and closed sets of frequencies.



(Refer Slide Time: 21:08)

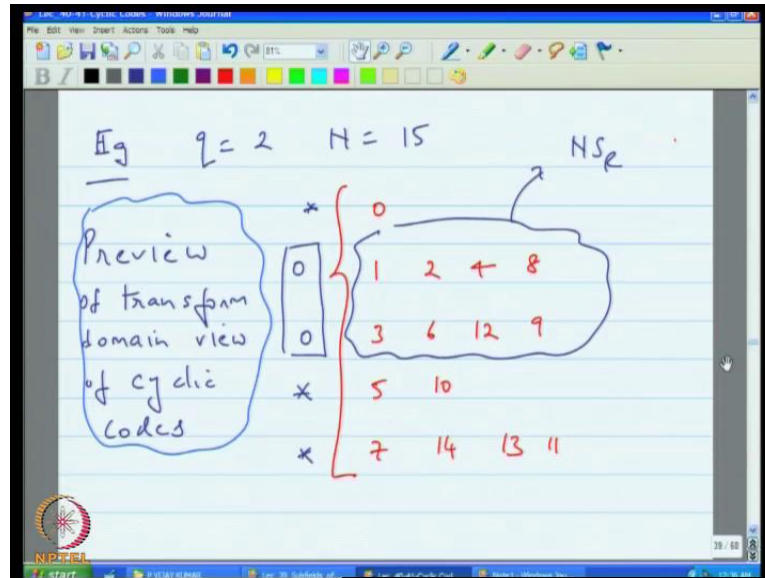


So, what is the correspondence? The correspondence is just this, that on the left side, what you have is the collection of all cyclic codes of block length  $N$  over  $F_q$ . So, let us note that; by the way, I just remind, whenever I say cyclic code, I do mean, linear and cyclic; that is the common usage. So, the linearity is sort of taken for granted. So, when you talk about a cyclic code, you really mean a linear cyclic code. And on the right side here, what I have is the collection of all closed sets.

So, these are the two sets on both sides; and then to show the one-to-one correspondence, you just pass from a code to a closed set, by just looking at its null spectrum. Given a code, you identify the null spectrum; we know that from one of our earlier lemmas that it is a closed set. And, so that makes this mapping actually make sense, and it is one-to-one and onto, because of the properties that we have proved in lemmas 1 to 3, because I mean, how do you, what you have to show is that, it is onto and one-to-one. To show that it is onto, you have got to show that, a given closed set, that there is cyclic code associated to it. But that is clear, because you just look at the set of all vectors, whose, which, whose transform value is 0 on that closed set and you will get a linear cyclic code. And furthermore, that cyclic code will have null spectrum, exactly the closed set that you started out with. So, it is onto, and it is one-to-one, because two different codes cannot have the same null spectrum; we have just seen that, the null spectrum, for a given null spectrum, this is essentially one code. So, it is

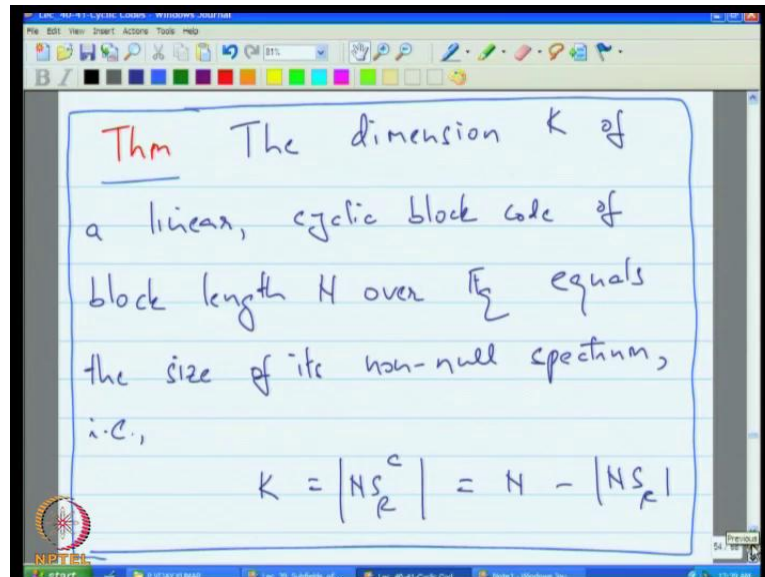
really a consequence of lemmas 1 to 3, above. But the important thing is that, we are clear that, clear about what this one-to-one correspondence is.

(Refer Slide Time: 23:59)



Let me just, again go back to this earlier example we had. And so once again, now I think, you will perhaps have a slightly better understanding of what I was saying earlier; earlier, I was saying that, look picking a cyclic code is exactly the same, as picking a bunch of cyclotomic cosets and saying I am interested in all those vectors, whose transform values are 0, for every frequency, which is in the union of those cyclotomic cosets, that we just picked. So, in terms of that particular, the selection of null spectrum here corresponds to a double error correcting BCH code, right. Good. Now, that we have this correspondence between cyclic codes and closed sets in the frequency domain.

(Refer Slide Time: 25:02)



We can now start talking about the parameters of these codes. So, the parameters that are of interest are two; one is the dimension, and the second is the, and the second property that is of interest is its minimum distance. And this theorem actually is telling us that that the dimension is precisely the set of frequencies outside the null spectrum. So, since the null spectrum is of size  $N S$ , the dimension is  $N$  minus the size of  $N S$ . So, I think, let me just make a correction here; that should read  $N S$ ;  $N S^c$ . The proof is in the appendix; perhaps what we will do is, we will just look at an example.

(Refer Slide Time: 26:09)

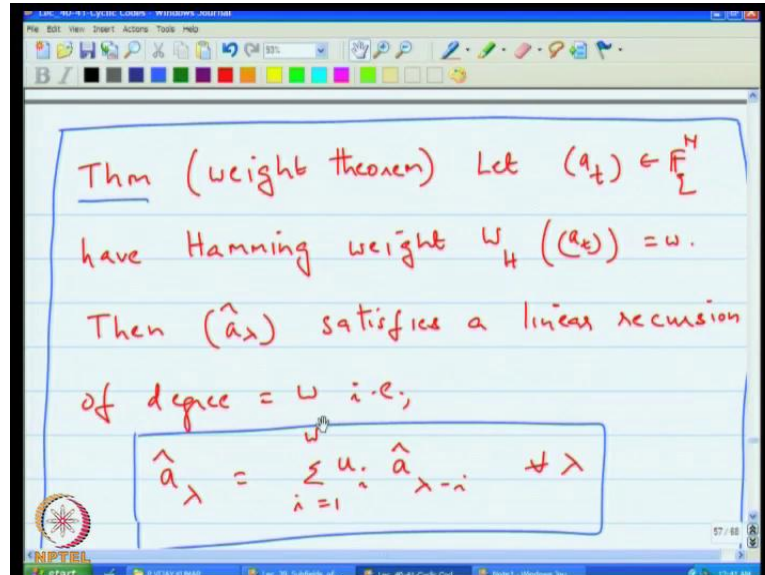
$q = 2 \quad N = 15$   
 $NS = \{1, 2, 4, 8, 3, 6, 12, 9\}$   
 $\Rightarrow \dim(\mathcal{C}) = 15 - 8 = 7.$

Diagram illustrating the null spectrum (NS) and the resulting dimension calculation:

*	0 (null spectrum)
0	1 2 4 8
0	3 6 12 9
*	5 10
*	7 14 13 11

So, here is an example. This is our familiar example by now.  $q$  is 2;  $N$  is 15 and our null spectrum has been chosen to be the union of these two cyclotomic cosets. The null spectrum has to be a closed set. So, it has to be the union of cyclotomic cosets; we have chosen these two. So, that is indicated by the presence of these zeroes. This star means that, the transform value here can be either 0, or non-zero; and you give it full freedom. And the theorem that I had just, we just read out, read out just now. This theorem says that the dimension is simply the number of frequencies that do not belong to the null spectrum. So here, there are 15 frequencies in all; 8 of them belong to the null spectrum. So, the number of frequencies outside is 4 plus 2 plus 1 is 7. So, the dimension of the code is actually 7, in this case.

(Refer Slide Time: 27:17)



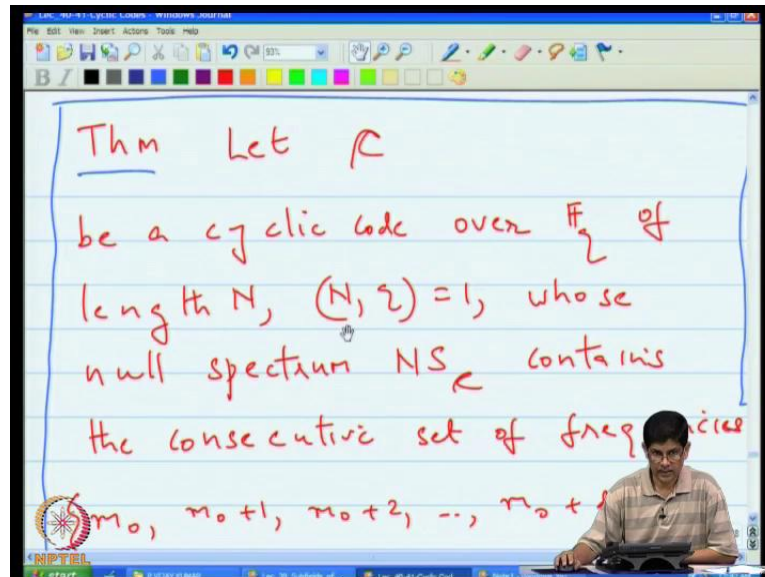
Thm (weight theorem) Let  $(a_t) \in \mathbb{F}_q^M$  have Hamming weight  $w_H(a_t) = w$ . Then  $(\hat{a}_\lambda)$  satisfies a linear recursion of degree  $= w$  i.e.,

$$\hat{a}_\lambda = \sum_{i=1}^w u_i \hat{a}_{\lambda-i} \quad \forall \lambda$$

Then, we have a weight theorem. So, the two parameters that we were interested in, one is the minimum, the dimension of the code; the second is the minimum distance. So, now, we are trying to establish the minimum distance of the cyclic code. So, the weight theorem says, let  $c$  of  $t$  be an  $n$  tuple whose Hamming weight is  $w$ . Now, it is not necessarily, a code word is just any  $n$  tuple. So, this is a rather general property. Then **then**, I am just thinking that, perhaps I should change the notation, from  $c$  of  $t$  to  $a$  of  $t$ , so that, there is no confusion and it is clear that, this applies in general. So, let me make that small change; let  $a$  belong... So, this is  $a$ ,  $a$ ,  $a$ ,  $a$ .

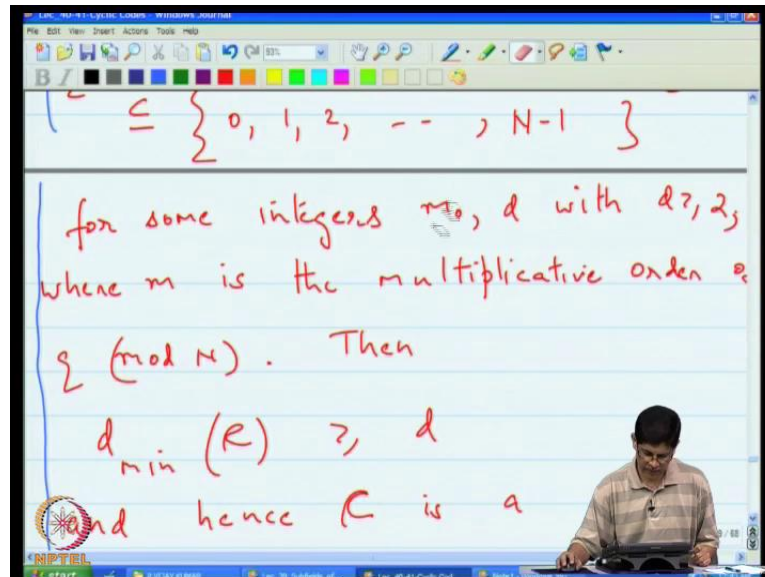
So, let  $a$  be any vector whose Hamming weight is  $w$ . Then, its transform value satisfies the linear recursion of degree  $w$ , in the frequency domain. So, what is that mean? It means that, it means precisely what this equation says here; that is, you can recover the transform values at any frequency  $\lambda$ , by looking back in the past, at the past  $w$  values of the transform. So,  $\hat{a}_\lambda$  is some linear combination of  $\hat{a}_{\lambda-i}$ , for  $i$  ranging between  $1$  to  $w$ ; and, these coefficients  $u_i$  are in  $\mathbb{F}_q$  to the  $m$ . once again, in the interest of moving along, I have left the proof in the appendix. What we will do is, however see an application of this here.

(Refer Slide Time: 29:45)



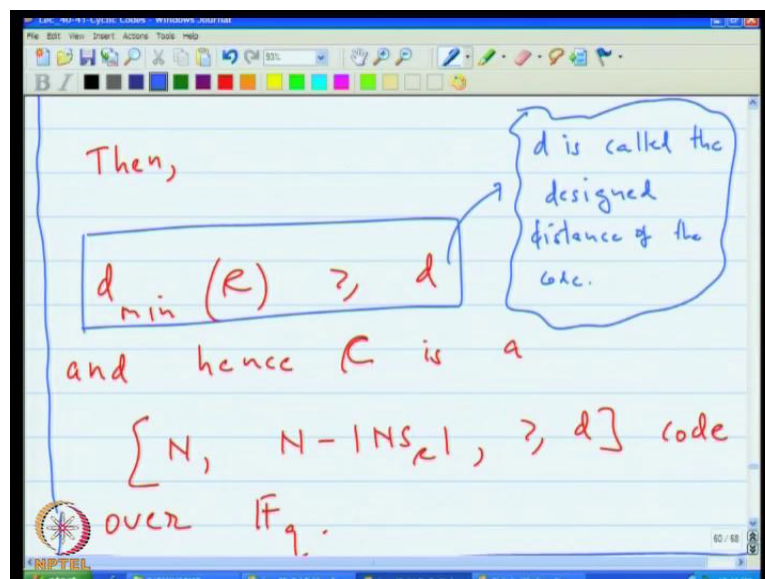
So, this is a key theorem in cyclic codes and it says that, supposing  $C$  is the cyclic code over  $\mathbb{F}_q$  of length  $N$ , where  $N$  and  $q$  are relatively prime, and let us assume that the null spectrum contains a stretch of consecutive frequencies; that is, you have a starting point  $m_0$ ,  $m_0 + 1$ , up to  $m_0 + d - 1$ . So, the number of consecutive 0s, in this particular case, is  $d - 1$ . So this is, obviously, a subset of the set of all frequencies; actually, this should have been  $N - 1$ ; let me correct that. And here, this freedom in choosing  $m_0$ , so  $m_0$  is some integer and  $d$  is some integer, also an integer, which is greater than or equal to 2.

(Refer Slide Time: 31:06)



And so, excuse me. It says here that,  $m$  is the multiplicative order of  $q \pmod{N}$ ; but since that does not appear in the theorem now; I am just going to delete that.

(Refer Slide Time: 31:38)

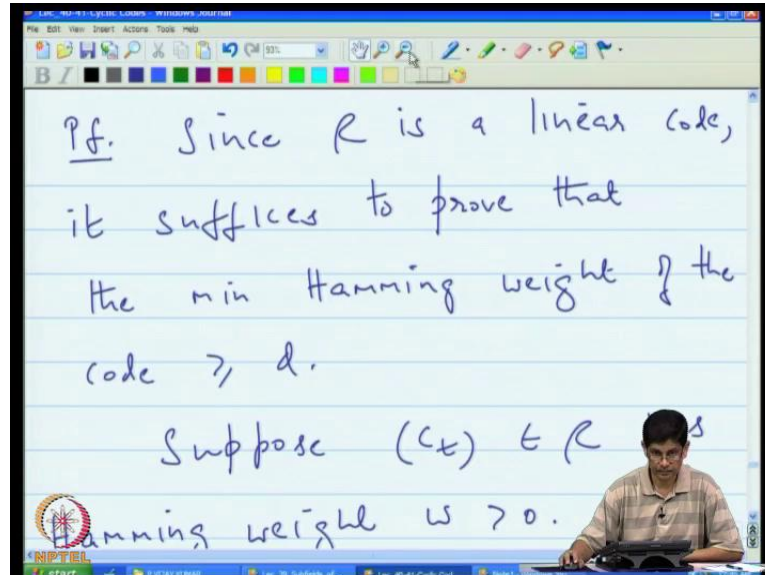


So, the assertion of the theorem is that, the minimum distance of the code is, in this case, greater than or equal to  $d$ . So, just a quick remark here, and not a part of the theorem, but, just quick comment. And  $d$  is called the designed distance of the code, and so, the minimum



distance of the code is at least  $d$ ; and therefore, the parameters of the code, the block length is  $N$ ; that is obvious; the dimension is  $N$  minus the size of null spectrum; we covered that in the previous theorem; and, the minimum distance is greater than or equal to  $d$ , which is the content of this theorem.

(Refer Slide Time: 32:40)



The proof is actually, quite straight forward, as we will go through with it. So, since  $C$  is a linear code, it is enough to show that the minimum Hamming weight of the code is greater than or equal to  $d$ . This we proved in connection with binary codes. We showed that a binary, in the case of the binary codes, the minimum distance is equal to the minimum Hamming weight. But that is, also, that proof also extends to the non-binary case; that is, the minimum Hamming distance of a linear code over any finite field, that is whose symbol alphabet is any finite field, has the property that the minimum Hamming weight is equal to the minimum Hamming distance; the minimum non-zero Hamming weight is the minimum Hamming distance.

Now, supposing you have a code word, and let us say that its Hamming weight is  $w$ ; and let us assume that  $w$  is greater than 0; because, we are trying to estimate the minimum distance and we know that, the code contains the all zero code word. When, we talk about minimum Hamming weight, we are interested in the minimum non-zero Hamming weight. So, we will

assume that, the  $w$  is greater than 0. Then, our earlier lemma, that we just read out, says that, says that the theorem says that, if the, if a vector has Hamming weight  $w$ , then, its transform satisfies the linear recursion of degree  $w$ .

(Refer Slide Time: 34:39)

Then  $(\hat{C}_\lambda)$  satisfies a linear recursion of the form:

$$\hat{C}_\lambda = \sum_{i=1}^w \hat{C}_{\lambda-i} u_i + \lambda$$

so in particular

$$\hat{C}_{m_0+d-1} = \sum_{i=1}^w \hat{C}_{m_0+d-1-i} u_i$$

So, because of this, therefore,  $\hat{C}$  of  $\lambda$  satisfies the linear equation of this form;  $\hat{C}$  of  $\lambda$  is the sum  $i$  equal to 1 to  $w$ ,  $\hat{C}$  of  $\lambda$  minus  $i$   $u_i$ , for all  $\lambda$ . So, in particular, what that means is that, if you put  $\lambda$  equal to  $m_0$  plus  $d$  minus 1, what, where did I get that from? Well, all that I am doing here... So, maybe, I can actually, at this stage, draw a picture, before continuing with the proof. So, let me insert a page here. So, the picture is like this.

(Refer Slide Time: 35:21)

$$\hat{C}_{m_0+d-1} = \sum_{i=1}^W \hat{C}_{m_0+d-1-i} y_i$$

$$x = [0, 0, 0, *, *, *]$$

$$0 \ 1 \ - \ m_0 \ m_0+1 \ \dots \ m_0+d-2 \ m_0+d-1 \ \dots \ (N-1)$$

$$\subseteq (Ns)_R$$

So, let us look at your transform,  $\hat{C}$  of  $\lambda$ , and let us say that these are your indices, you start with 0, 1, and then somewhere you encounter  $m_0$ ,  $m_0 + 1$ ,  $m_0 + d - 2$ ,  $m_0 + d - 1$ ,  $m_0 + d$  on upto  $N - 1$ . Let me see, if I can group this pattern. So, let us say, these are the frequencies and when you look at  $\hat{C}$  of  $\lambda$ ,  $\hat{C}$  of  $\lambda$ , we know that since this is the null spectrum, this is included in the null spectrum. So, it is contained in the null spectrum of the code. Because of that when you look at  $\hat{C}$  of  $\lambda$ , you see, you are going to see a 0, a 0 and a 0. You are going to see,  $d - 1$ , after here, yes, sorry about that; I, the string of consecutive 0s only runs from  $m_0$  to  $m_0 + d - 1$  minus 2; let us go back and check that. So, you see that, it goes from  $m_0$ , all the way up to  $m_0 + d - 2$ .

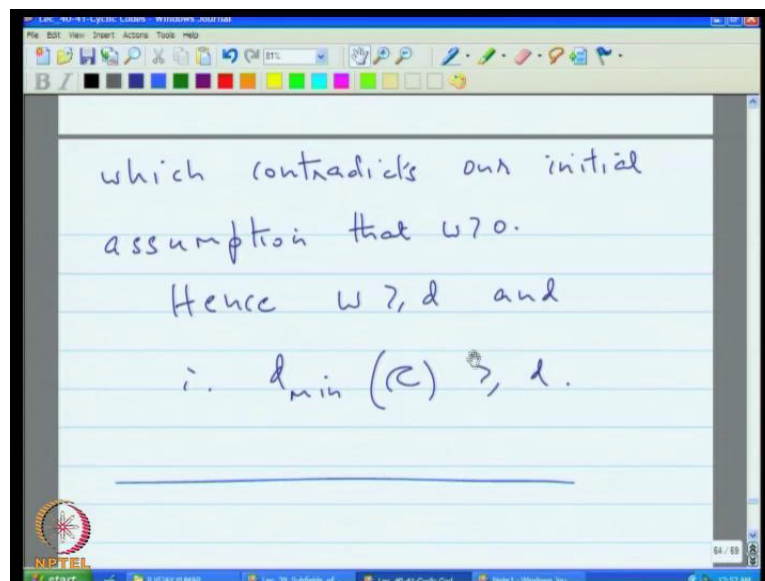
So, we know that the transform is 0 out here, and in general, we do not know, what the transform values are outside. So, I can actually put some star values in here. But we do know that  $\hat{C}$  of  $m_0 + d - 1$ . So, if you pick, in particular,  $\hat{C}$  of  $m_0 + d - 1$ ; let me do one thing; let me pick this relationship and bring it down, so that we can talk about it, while looking at the figure; here.

So, let us look at this expression here; and so picture this, that you are saying that, the transform value at frequency  $m_0 + d - 1$  is some linear combination of the ones that

came before it; the  $w$  terms that came before it; but if  $w$  is less than  $d$  then since you are going back up to  $m_0$  plus  $d$  minus 1 minus  $w$ , this is at most  $m_0$  plus  $d$  minus 1; you are going back into the past, the earliest, or the smallest index is, this minus  $d$  minus 1. So, the  $w$  can be at most  $d$  minus 1, since we are assuming it is less than  $d$ . So, this comes out to  $m_0$ ; so that means that what we have actually shown is that, if it has weight  $w$ , then, this value must be the linear combination of these 0s, which means that this entry must be 0. Now, you move over here. This one must be a linear combination of the preceding, preceding I guess,  $d$  minus 1 terms, and it is again 0 and so on.

So, what it says is that if you have a string of  $d$  minus 1 consecutive 0s and you have a linear recursion whose degree is  $d$  minus 1 or less, then you are going to, this string of 0s is going to extend all the way round, until you get the all 0 code word. So, what that proves is that every code word must have Hamming weight  $w$ , which is greater than or equal to  $d$ ; because the only way it can have a Hamming weight less than or equal to  $d$  minus 1 is, if it is in fact, the all 0 code word.

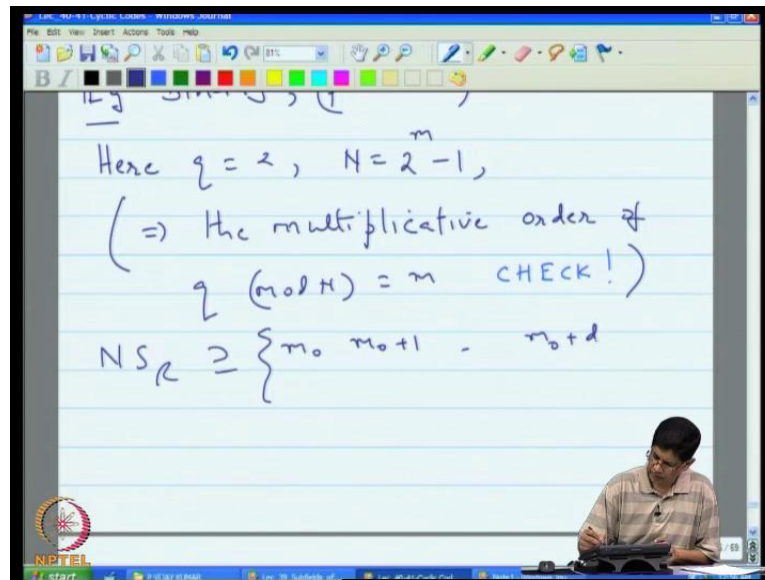
(Refer Slide Time: 40:27)



And that proves that, which contradicts our assumption that,  $w$  is greater than 0. Therefore,  $w$  is greater than or equal to  $d$ , and hence,  $d_{\min}$  of the code is greater than or equal to  $d$ . So,

that completes our derivation of the parameters of the code. Now, we have the parameters of the code under control. Next what we will do is, let us examine two classes of codes.

(Refer Slide Time: 41:00)



We will look at an example of BCH codes. So, BCH class of codes falls into the class associated with this theorem. So, BCH codes turn out to be codes, having a null spectrum, which contains a consecutive set of frequencies. Here,  $q$  is equal to 2 and  $N$ ,

so, for the primitive case,  $N$  is of the form  $2^m - 1$ . So actually, if you start out, that is I should start out... Supposing, I said that, it is  $2^e - 1$ , then this means that the multiplicative order of or actually, let me put back the  $m$  here; if  $N$  is  $2^m - 1$ , and then you ask, what is the multiplicative order of  $q \text{ mod } N$ , and then, you will see that, it is actually equal to  $m$ . So, this implies that the multiplicative order of  $q \text{ mod } N$  is equal to  $m$ . So, I will leave that as a small exercise for you to check is quite straight forward. And so, and then, the null spectrum is, the null spectrum of the code is required to, is required to contain these consecutive string of frequencies.

(Refer Slide Time: 44:34)

$[N = 2^m - 1, N - |NS_c|, d_{\min} \geq d]$   
 A popular choice is  $m_0 = 1$ .  
 $\therefore NS_c \geq \{1, 2, \dots, m_0 + d - 2 = d - 1\}$   
 $= \{1, 2, \dots, 2t\}$  if  $d = 2t + 1$   
 Note that in the  $q$ -cyclotomic cosets mod  $N$  (i.e., the

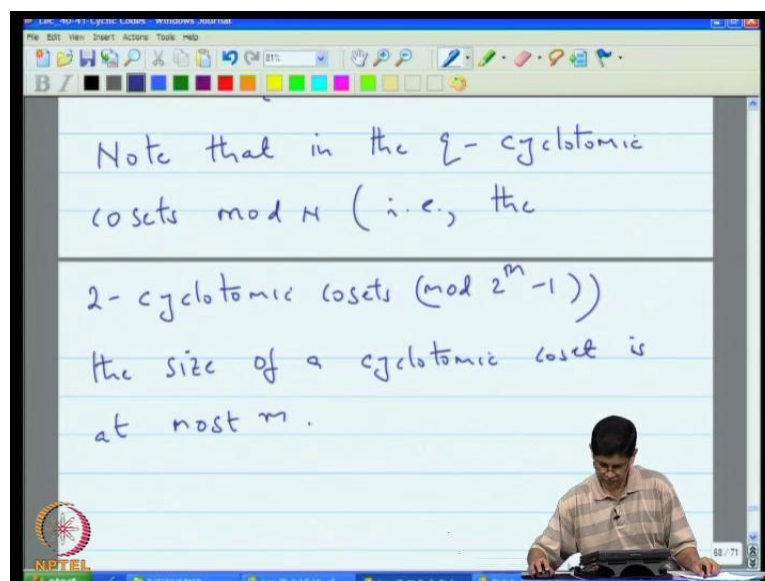
Therefore, a BCH code, therefore such therefore, binary BCH codes have parameters, have parameters;  $N$  is equal to  $2^m - 1$  and the dimension is  $N$  minus the size of the null spectrum, and  $d_{\min}$  is greater than or equal to  $d$ . Now, it turns out that, it turns out a popular choice choice is  $m_0$  equal to 1. So that means, your consecutive...Therefore, in which case, your null spectrum contains 1, 2, all the way up to  $m_0 + d - 2$ , which is  $d - 1$ . So, you have a consecutive stretch of 0s from 1 to  $d - 1$ . Then, let so what I am trying to get at is the following. Here, in describing BCH codes, I have given you the length and the minimum distance, and I have left the dimension expressed in terms of the complement of the null spectrum.

The catch here is, we do not really know what the null spectrum is; because all that we know is that, it contains these frequencies; we do not exactly know what it is. So, that leaves a question mark over the dimension of this code. Now, you cannot completely erase that, but what you can do is, in this particular case, you can estimate, or atleast (( )) on the dimension of this code as follows. So, let us say that  $m_0$  is 1, and in which case, the string of consecutive 0s, actually ranges from 1 to  $d - 1$ ,

which can be rewritten, which can be rewritten as 1, 2, all the way upto  $2t$ , if  $d$  is equal to  $2t + 1$ ; because typically, when you are looking for error correction, then, your minimum

distance is  $2t + 1$ . For example, if you, if you want to correct 2 errors, you will make your minimum distance 5 and so on. So, this is a popular situation that you are likely to come across. So, what can you say in this case? Then note that, note that in the 2 cyclotomic cosets, cosets, I will make it clearer; let me call this, in the  $q$  cyclotomic cosets mod  $N$ , i.e., in our case, this simply amounts to, the 2 cyclotomic cosets mod 2 to the  $m$  minus 1.

(Refer Slide Time: 47:38)



The size of a cyclotomic coset is at most  $m$ . Let me explain why that is but let us just look at the example that we had earlier. Here we go. So, you see that, here  $q$  is 2,  $N$  is 15. So,  $N$  is 2 to the 4 minus 1. So, that parameter  $m$ , in this case...



(Refer Slide Time: 48:39)

Eg  $q = 2$   $N = 15$   $m = 4$

$NS_{\leftarrow} = \{1, 2, 4, 8, 3, 6, 12, 9\}$

$\Rightarrow \dim(\mathcal{C})$   
 $= 15 - 8$   
 $= 7.$

Diagram illustrating the construction of cyclotomic cosets for  $N=15$  and  $m=4$ . The cosets are shown as a vertical list of elements, with some elements marked with an 'x' to indicate they are not in the null spectrum. The null spectrum is highlighted in a box and labeled "0 (null spectrum)". The elements in the null spectrum are 0, 1, 2, 4, 8, 3, 6, 12, and 9. The elements not in the null spectrum are 5, 10, 7, 14, and 13.

I may as well write it down here. The parameter  $m$  was equal to 4, and you can see here that, the cyclotomic cosets, none of them is larger than 4; because no matter where you start, if you keep multiplying the powers of 2, eventually when you reach 2 to the 4, you will get back to where you started, because 2 to the  $m$  minus 1, 2 to the  $m$ , mod 2 to the  $m$  minus 1 is 1. For that reason, your cyclotomic cosets are never going to be bigger than  $m$ .

(Refer Slide Time: 49:17)

2-cyclotomic cosets (mod  $2^m - 1$ )

the size of a cyclotomic coset is at most  $m$  since

$\lambda 2^m \pmod{N}$

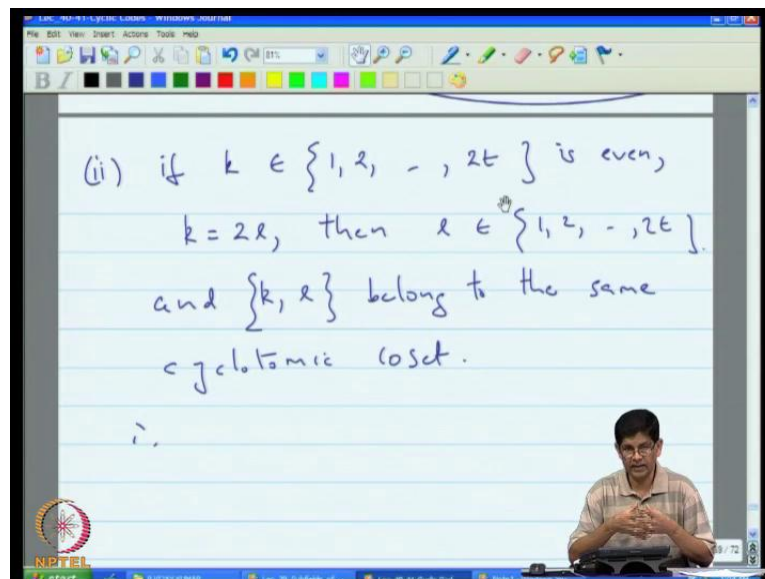
$= \lambda 2^m \pmod{2^m - 1}$

$= \lambda !$

Diagram illustrating the size of a cyclotomic coset. The size is shown to be at most  $m$  because the order of 2 modulo  $N$  is at most  $m$ . The calculation shows that the size of the coset is the least common multiple of the order of 2 modulo  $N$  and the order of 2 modulo  $2^m - 1$ , which is 1.

So, let us... Since  $\lambda^{2^m} \bmod N$  is equal to  $\lambda^{2^{m-1}}$ , which is equal to  $\lambda$ . So, that means that if you start from  $\lambda$ , and keep multiplying by powers of 2, after  $m$  steps, you are going to be back where you started. So, your cyclotomic cosets cannot contain more than  $m$   $\lambda$ . So, what you will do is, you will go a  $\lambda$ , you will go a  $2\lambda$ , you will go  $4\lambda$  and then, at most, you might end up with  $2^{N-1}\lambda$ ; but at the next step, you will, you will come back to the  $\lambda$ . So, the size of your cyclotomic coset can never be more than  $m$ . So, that is one thing to keep in mind. And so that is, that is observation one. The second observation, remember that we are looking for, we are trying to estimate the size of the null spectrum, which contains these  $2t$  consecutive 0s. The second observation is that, the second observation is the following:

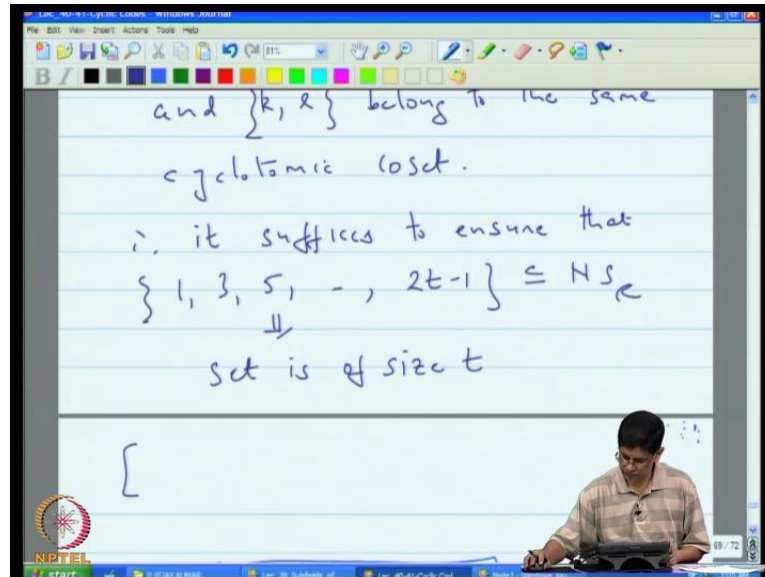
(Refer Slide Time: 50:45)



If  $k$  in  $1, 2$ , upto  $2t$  is, is even, excuse me, if  $k$  is even, let us say that,  $k$  is equal to  $2l$ , then, then  $l$  is already in this set; and,  $k$  and  $l$  belong to the same cyclotomic coset. So, I should, let me write this differently; and  $k, l$ , belong to the same cyclotomic coset. So, what that tells is that, therefore, therefore... So, what you are saying here is that look I have  $2t$  distinct elements here, and I am worried about, I want to keep my, see that, the fact that I have  $2t$  consecutive 0s, guarantees my minimum distance is  $2t + 1$ ; but, now, how large do I have to make my null spectrum to guarantee the presence of these  $2t$  consecutive 0s;

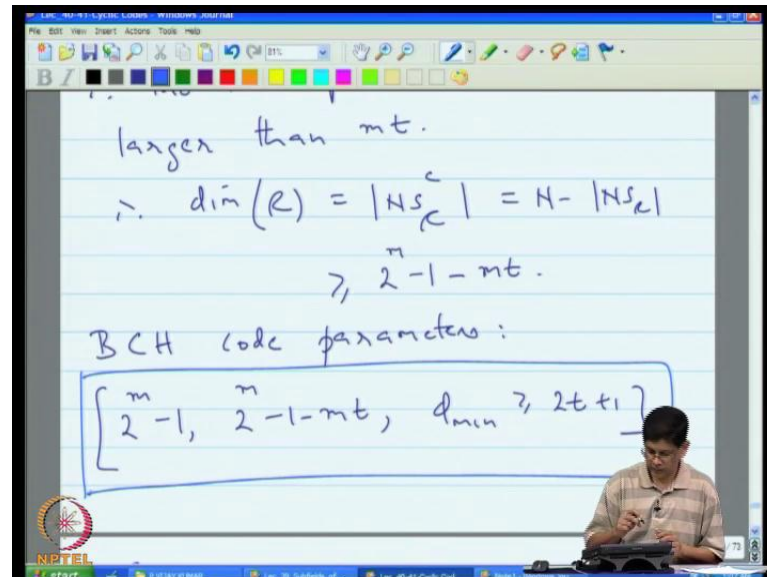
and the point is that, you only have to ensure that, the odd integers in this, belong to the null spectrum; because the even ones come for free, because of the fact that, if you are picking cyclotomic coset, so, if you pick 1, you will also be picking 2 1, to that cosets.

(Refer Slide Time: 50:45)



Therefore, it suffices, it suffices to ensure that 1, 3, 5, all the way to 2 t minus 1, are a subset of the null spectrum of the code; but the number of these is only t, right; because you start with t equal to, there are only two, this set is of size, this set is of size t; this set here, is of size t.

(Refer Slide Time: 53:44)



Therefore, therefore, the null spectrum need be no larger than  $m$  times  $t$ . Therefore, the dimension of the code, which is the size of the complement of the null spectrum, is greater than or equal to  $2^m - 1 - mt$ . For this reason, you will actually see that, the parameters of a BCH code, described in this way...This is how you typically find the parameters of the BCH code described.

(Refer Slide Time: 48:39)

And, our earlier example here, was of the same flavour because this (( )), this code here, was actually a BCH code of minimum of distance 5; because, in that case, you would insist that, they would be, the consecutive 0s would be 1, would be, 1, 2, 3 and 4; and by, just by ensuring that, 1 and 3 belong, you ensure that 1, 2, 3, 4 belong; so, the minimum distance is 5. So, in this particular case, our  $t$  was equal to 2. So, the size of the null spectrum was at most  $mt$ , which is 8 in this case. Therefore, the dimension of the code is at least 7. This is an example of the very same statement, and I am just going to quickly copy this slide over to that page, where we were at.

But perhaps I should just summarise. So, what we have done is that we have actually looked at... So, we had started out by looking at cyclic codes from a transform domain perspective,

and so, we defined this quantity called the null spectrum of a code; we made the link between cyclic codes and the closed sets of frequencies strong by showing there is a one-to-one correspondence. And then, we said ok, now that we know how to design cyclic codes in the frequency domain, what can we say about the parameters; and the minimum, the dimension is easy; it is just the number of frequencies outside the null spectrum.

The minimum distance is complicated, but what we can do is, if we ensure, there are certain string of frequencies, which are consecutive, belong to the null spectrum, that the minimum distance is one more, is at least one more than the length of that string. So, that is, that is kind of the BCH construction of cyclic codes. So, we use that to estimate the minimum distance. And what was behind that estimate is, what I called the weight theorem, because it turns out that, if a vector in the time domain has Hamming weight  $w$ , in the frequency domain, its transform satisfies a linear recursion of degree  $w$ , and that is what enabled us to prove that. So, in the next class, what we will do, next and final lecture, we will define Reed Solomon codes and then, quickly locate, how one actually decode this codes. So, we will stop at this point. Thank you.