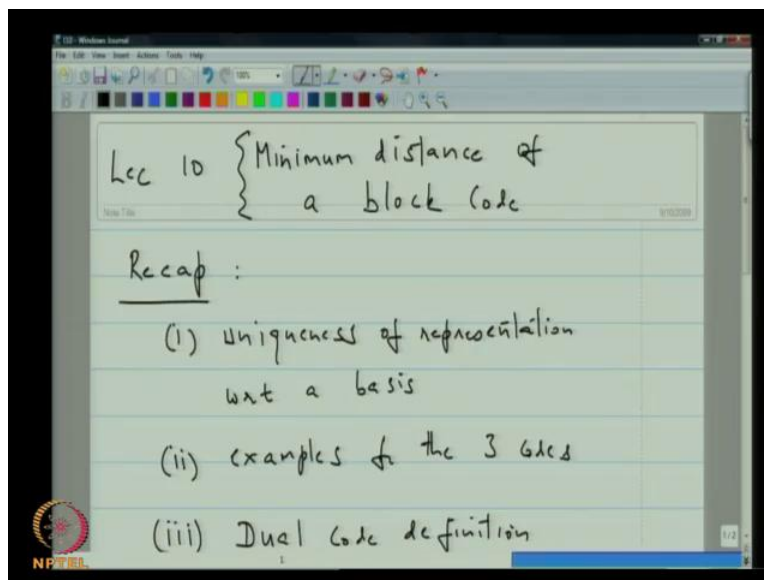


**Error Correcting Codes**  
**Prof. Dr. P. Vijay Kumar**  
**Department of Electrical Communication Engineering**  
**Indian Institute of Science, Bangalore**

**Lecture No. #10**  
**Systematic Generator Matrix**

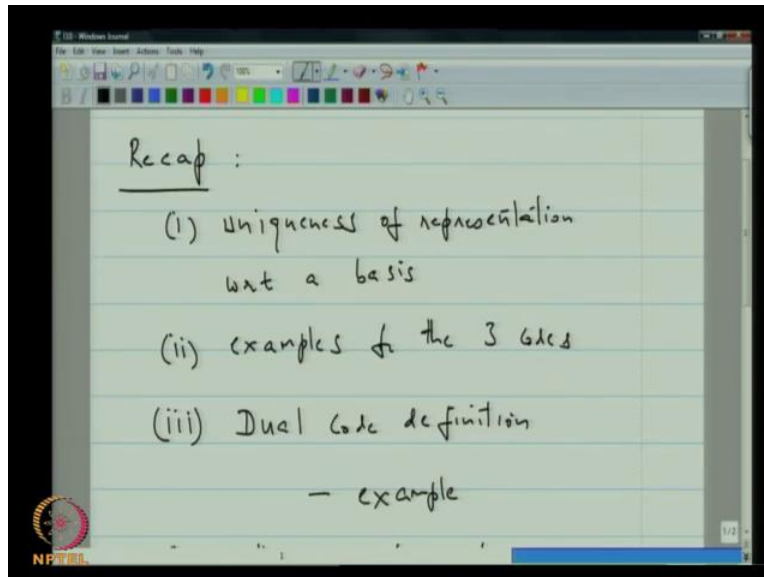
Good after noon. Today will begin our 10 th lecture. So, at the end of today's lectures will be roughly done with 25 percent of the course. And I think we are more or less on track. Now so, let me just begin by recapping what we did last time, perhaps you can go down to the pad.

(Refer Slide Time: 00:35)



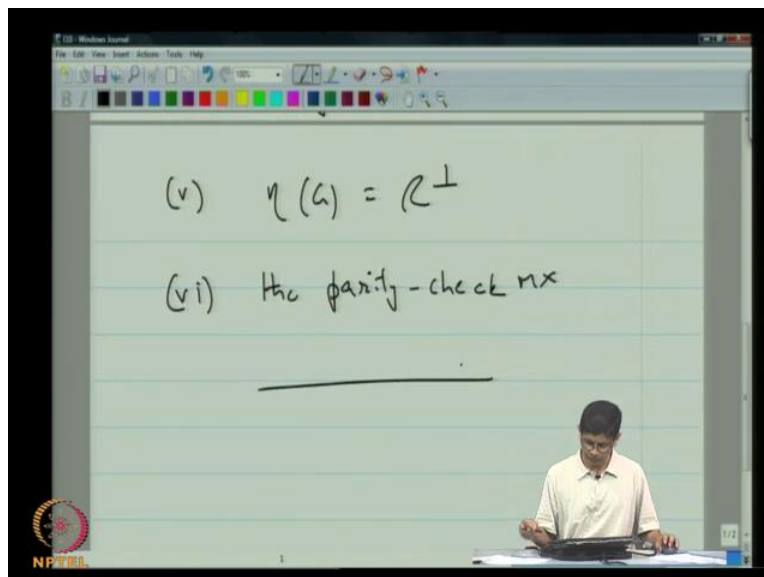
So, today we will talk about the minimum distance of a linear block code, of a linear block code. But before we do that, what we did last time was we first showed that even though for a given vector space, basis is not unique; if the representation of a given vector with respect to a fix basis is unique.

(Refer Slide Time: 01:10)



And then we looked at example basis for the three codes, for our 3 example codes, and then I introduce the notion of a dual code. We looked at the example, where we showed that the dual of the repetition code is the single parity check code.

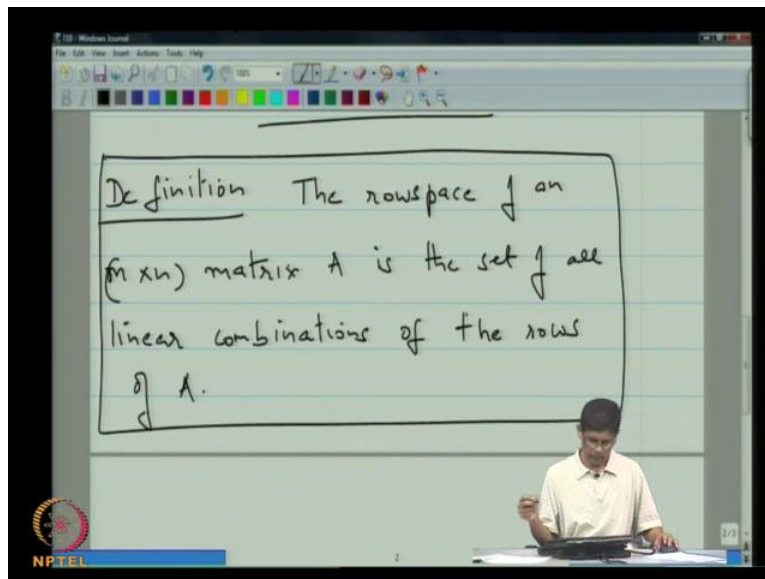
(Refer Slide Time: 01:35)



Then we introduced two matrices; first we introduce the generator matrix, then we introduce the second matrix called the parity check matrix. Now, we are going to use these two matrices to

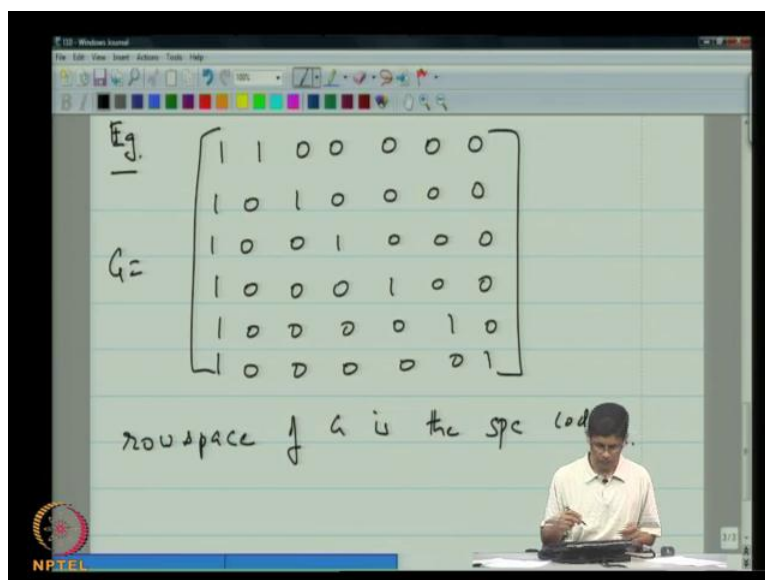
actually show; there if we take the dual of the dual of the code, then you get back to the original code. And then in between we actually proved theorem stating that the null space of the generator matrix is the original code. So, that is why will pick up the discussion. And before I start let me just state I give you a little bit of background taken from linear algebra.

(Refer Slide Time: 02:18)



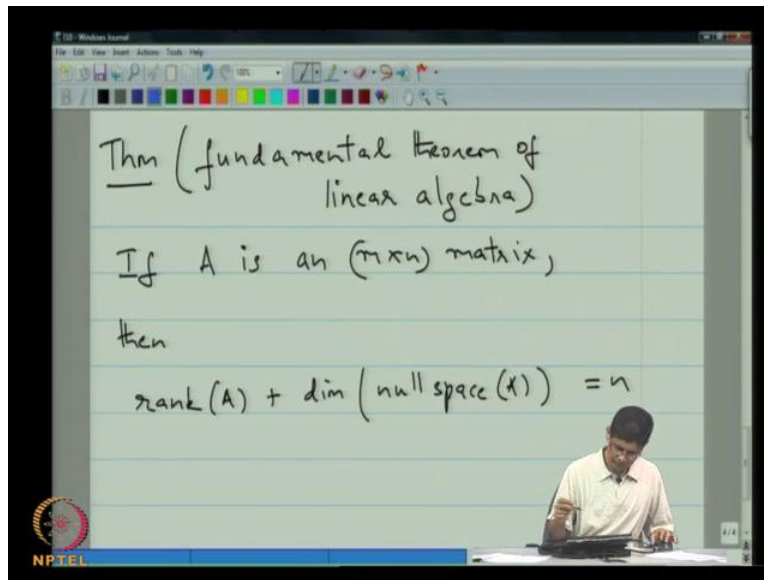
The row space of an  $m$  by  $n$  matrix  $A$  is the set of all linear combinations of the rows of  $A$ .

(Refer Slide Time: 03:22)



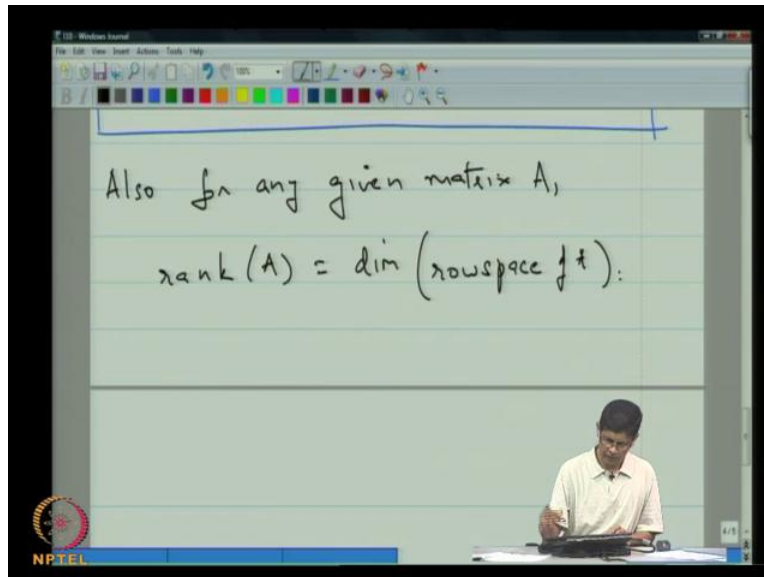
So for example, if we look at this matrix here, the row space of this matrix is the single parity check code. If we call this matrix  $G$ , and the row space of  $G$  is the single parity check code.

(Refer Slide Time: 04:29)



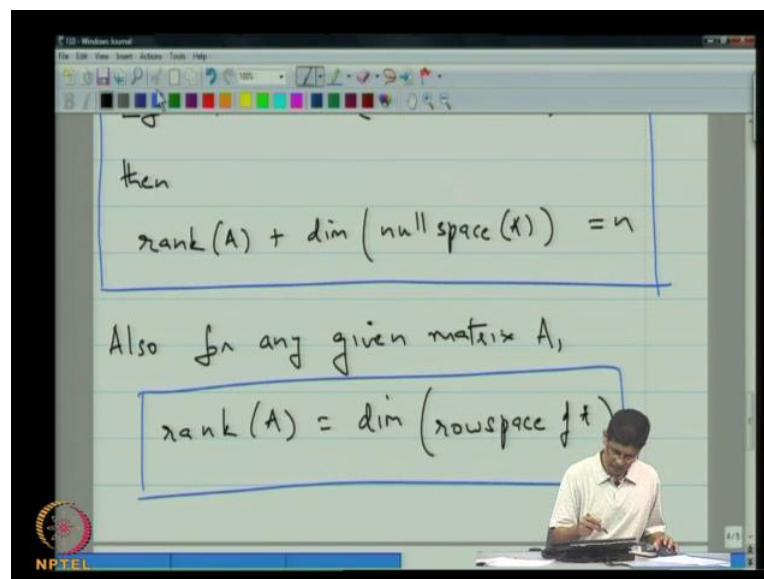
Then there is the theorem called the fundamental theorem of linear algebra, and we will take as a little too much time to prove it. So, I will skip the proof, and I merely stated. So, it is called the fundamental theorem of linear algebra; and what that actually says is that if  $A$  is  $m$  by  $n$  matrix then the rank of  $A$ , the rank of  $A$  plus the dimension of the null space of the null space of  $A$  is equal to the number of columns. So, we want prove this.

(Refer Slide Time: 06:20)



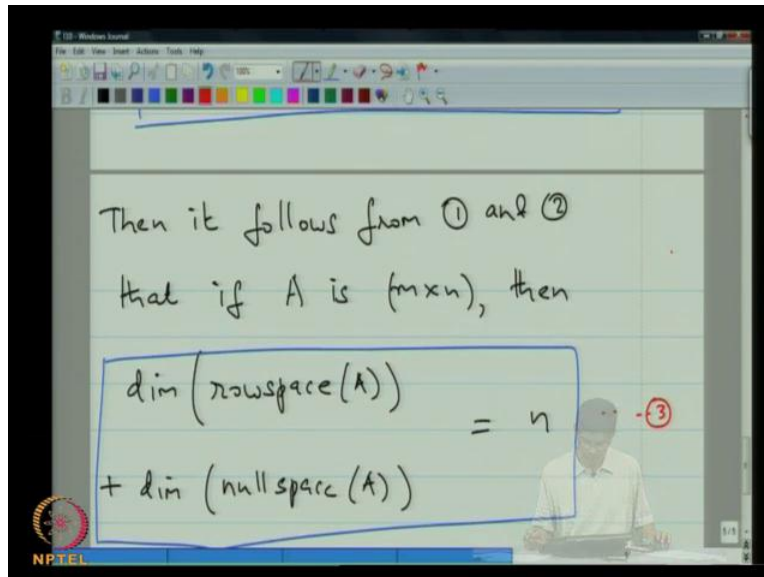
Then the other fact that we will need from linear algebra is the following also for any given matrix  $A$ , the rank of  $A$  is presides equal to the dimension of the row space of  $A$ .

(Refer Slide Time: 07:00)



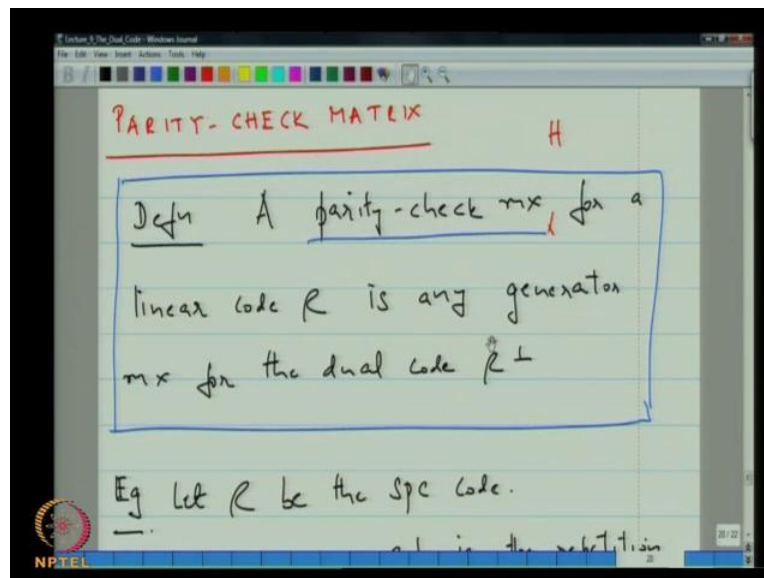
So if we put to this two together. So let say, I call this equation of a here, let say I call this equation 1, and I call this 2.

(Refer Slide Time: 07:17)



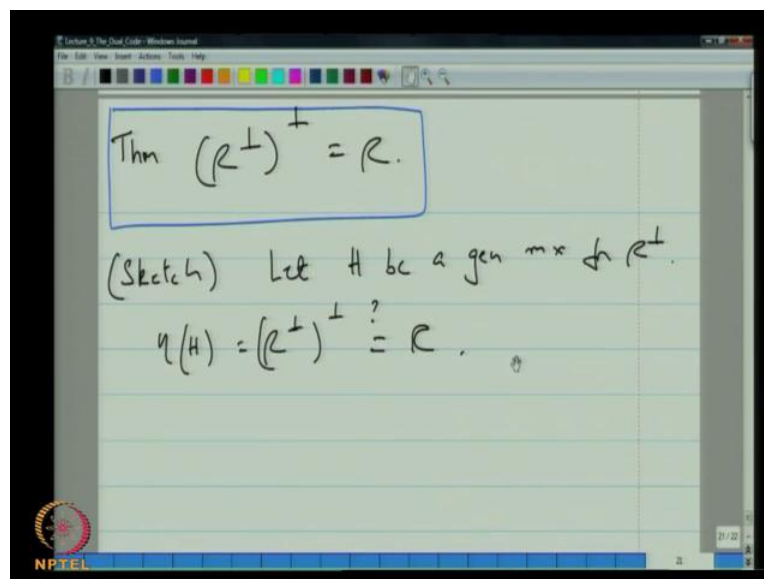
Then it follows from 1 and 2 that if  $A$  is  $m$  by  $n$ , then the rank of  $A$ , then the dimension of the row space of  $A$  plus the dimension of the null space of  $A$ . If we add the two, this will be equal to  $n$ . So, this is merely a restatement of the fundamental theorem of linear algebra. So, this is 3. So, once again to recap, the fundamental theorem tells us that if we add the rank to the dimension of the null space, you will get the number of columns. Also it is known that dimension of the row space of  $A$  is equal to the rank of  $A$ , and it follows from that, if we add that the dimension of the row space and the null space then will actually get the number of columns. Now we like to show, we like to actually show. So, let me just take a back quickly to some point in our earlier lecture last time towards the end.

(Refer Slide Time: 09:23)



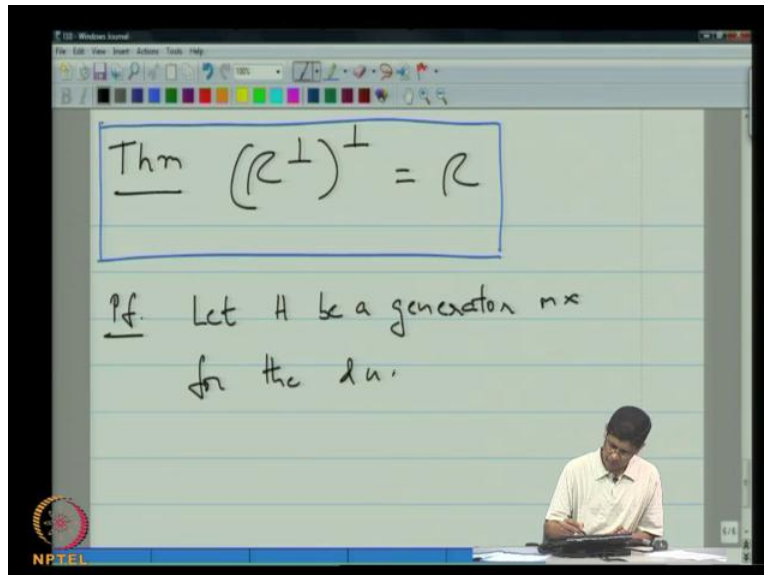
So, towards the end of the last lecture, we define what is meant by the parity check matrix of a code. It **is it** was defined as the generator matrix for the dual code.

(Refer Slide Time: 09:39)



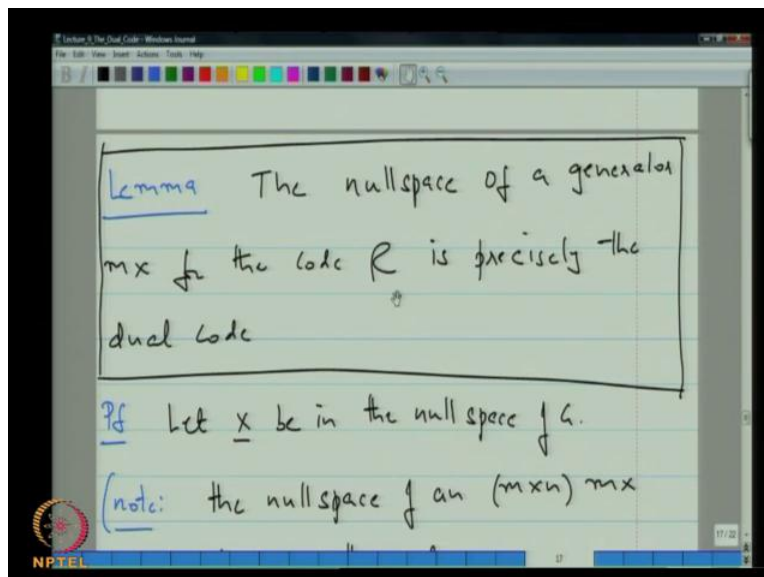
And then, we were in the mixed of actually proving a theorem, which said that the dual of the dual code is equal to the original code. So, we go ahead and actually prove that in a today's lecture. So, let us get back to our lecture.

(Refer Slide Time: 10:05)



So theorem, the dual of the dual is equal to the code itself. So proof, let H be a generator matrix for the dual code. Now, it follows from an earlier Lemma. So, if we see, I can take back to that Lemma.

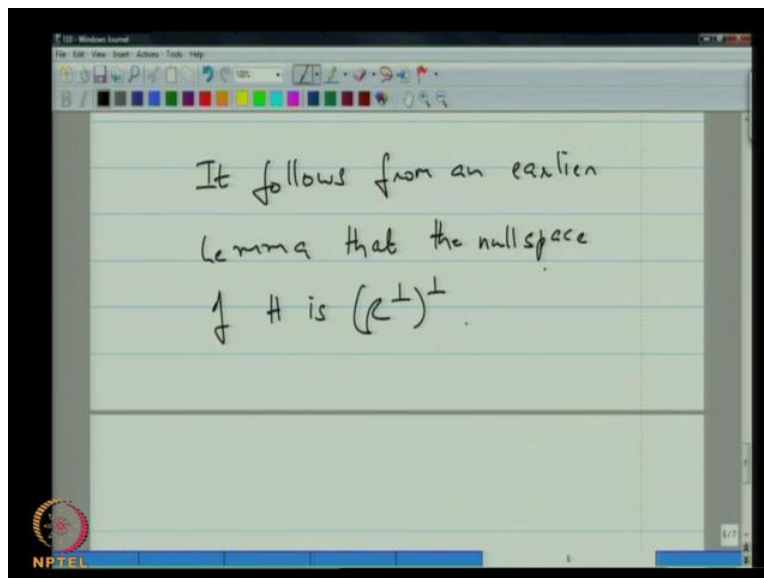
(Refer Slide Time: 11:40)



So, when we were talking about... So, here is the Lemma that we showed last time which said that the null space of the generator matrix for the code is precisely the dual code.



(Refer Slide Time: 11:52)



So now, we want to apply that except that, we want to apply that the dual code from an earlier Lemma that the null space that the null space of that the null space of  $H$  is the double dual.

(Refer Slide Time: 12:32)

Consider the equation:

$$\begin{bmatrix} h_1^t \\ h_2^t \\ \vdots \\ h_{n-k}^t \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \underline{0}$$

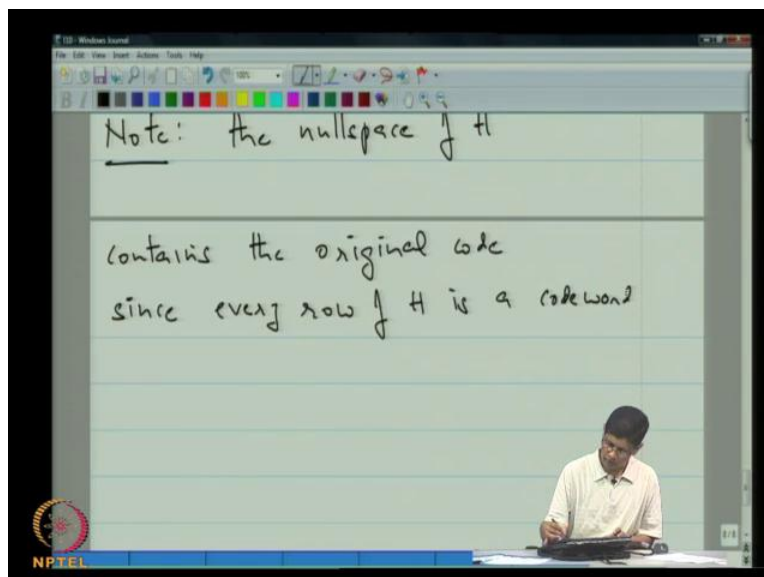
$H$   
 $((n-k) \times n)$

However, if you take a look at this equation, so consider the equation; I am going to put down the rows of  $H$  here, perhaps then we make it clear that these are row vectors, I put a transpose. Now, since the parity check matrix  $H$ , so this matrix here is your  $H$  matrix, and it is an  $n$  minus  $k$

by  $n$  matrix, and what you are going to do when you are looking at the null space of this is you going to look for vectors  $X$ , such that this times this is equal to the  $0$  vector. Now, if  $X$  is a codeword in  $C$ , then sends first for first observation is that, if the row of this matrix  $H$  is the code word belonging to the dual code we know that.

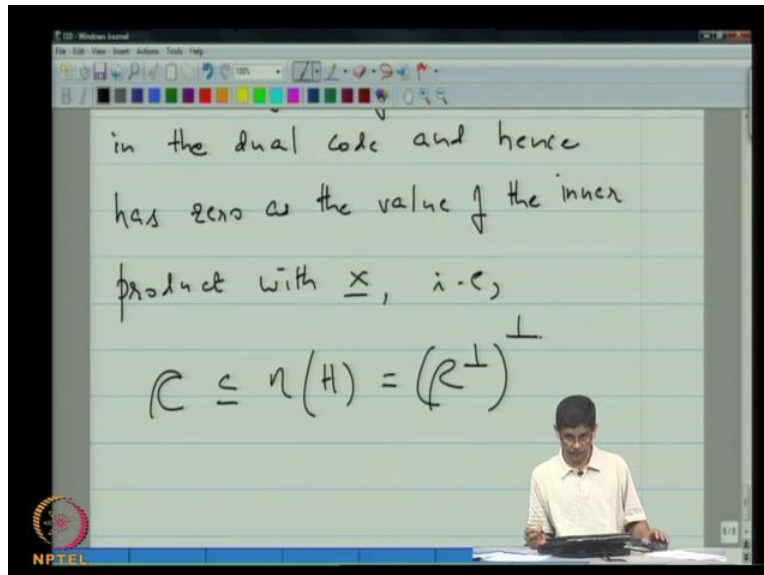
Now if this is the codeword in  $C$  then, since the rows are dual codes. Since the rows here are code words in the dual code it follows that their inner product must be  $0$ . Each of these inner products must be  $0$ , because for example  $h_1$  is in the dual code which means there it is orthogonal to be one of the codeword, similarly  $h_2$ . So, that means there every codeword is in the null space. So, what that establishes is that, the null space of this matrix  $H$  contains the original code.

(Refer Slide Time: 14:48)



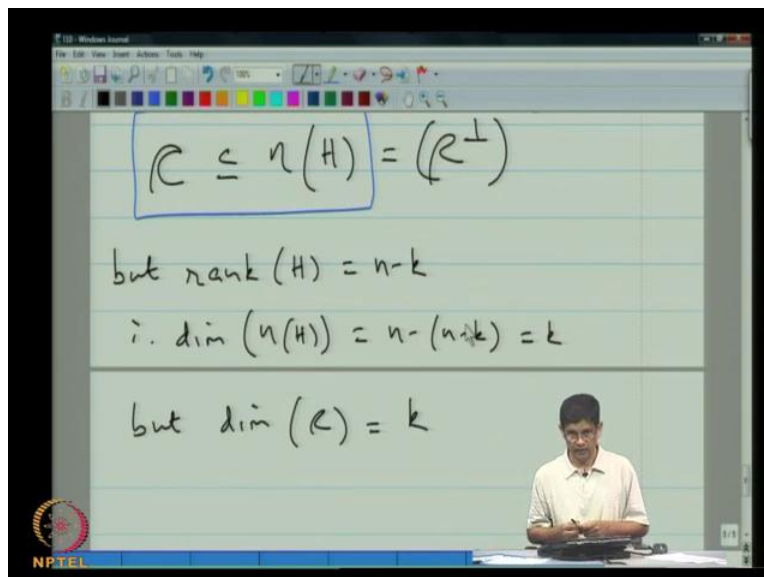
So, let us write that on, note null space of  $H$  contains the original code since every row of  $H$  is a codeword in the dual code and hence satisfies.

(Refer Slide Time: 15:48)



So, every row of  $H$ , and hence has zero as the value of the inner product with  $X$ . So therefore, so what we shown i.e, the original code is contained in the null space of  $H$ , which is equal to the dual.

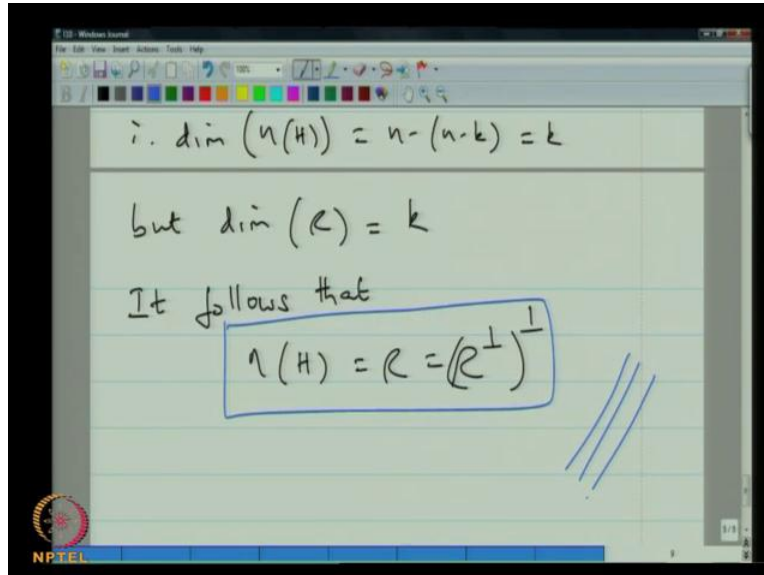
(Refer Slide Time: 16:51)



But if you just focus on this side of the equation, but the rank of  $H$  is  $n$  minus  $k$ . Therefore the dimension of the null space is  $n$  minus  $n$  minus  $k$ , which is  $k$ . But the dimension of the code is  $k$ .

So, what that is saying is that look you got the null space of the code, and the null space of the parity check matrix, and the null space of that has dimension  $k$ , and that your original code sets inside that null space, but the end your original code also has dimension  $k$ . So, it follows that the two must be one of the same.

(Refer Slide Time: 17:49)



A digital whiteboard interface showing handwritten mathematical derivations. The text is as follows:

$$\therefore \dim(N(H)) = n - (n-k) = k$$

$$\text{but } \dim(C) = k$$

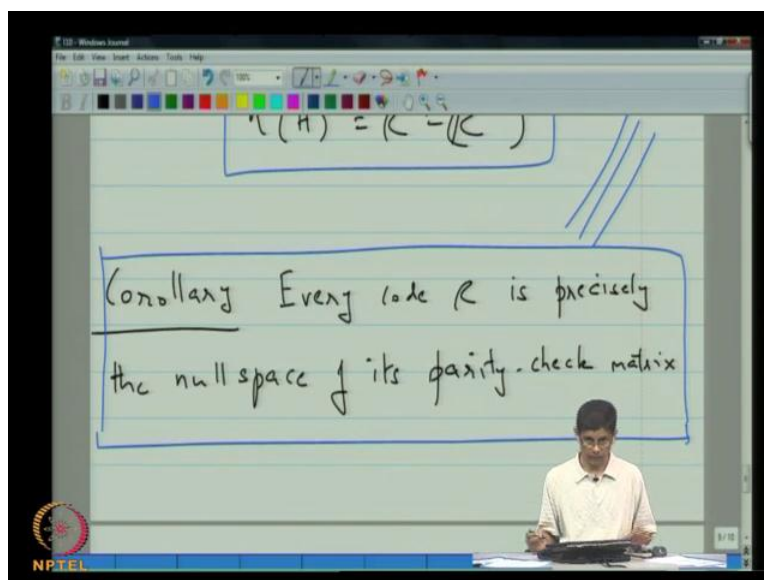
It follows that

$$N(H) = C = (C^\perp)^\perp$$

The equation is enclosed in a blue rectangular box. To the right of the box are three parallel diagonal lines. The NPTEL logo is visible in the bottom left corner.

It follows, it follows that the null space is equal to  $C$ , which is equal to the dual of the dual.

(Refer Slide Time: 18:33)



A digital whiteboard interface showing a handwritten conclusion. The text is as follows:

$$N(H) = C = (C^\perp)^\perp$$

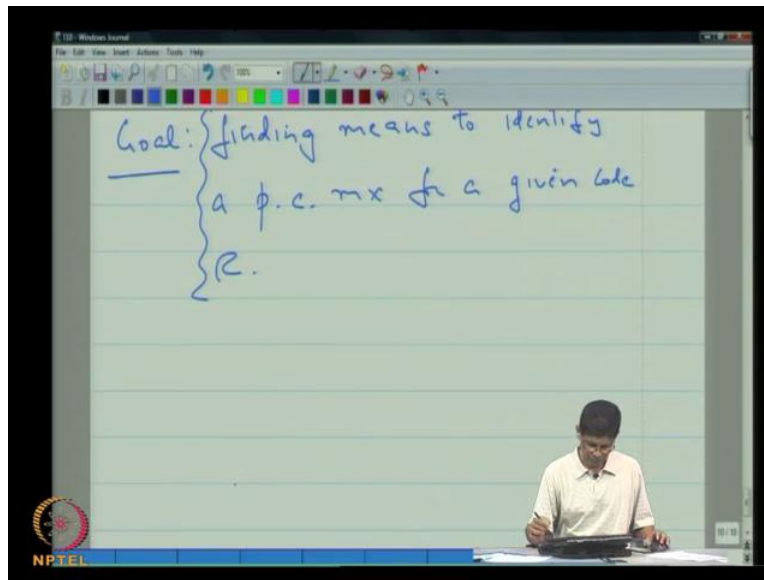
The equation is enclosed in a blue rectangular box. Below it, another blue rectangular box contains the following text:

Corollary Every code  $C$  is precisely the null space of its parity-check matrix

A lecturer is visible in the bottom right corner of the frame. The NPTEL logo is visible in the bottom left corner.

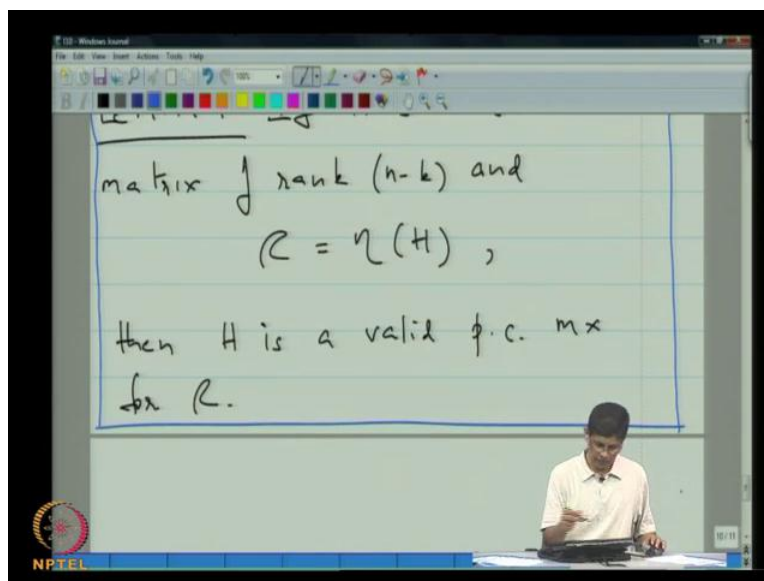
And will also so along with this theorem, let us also note down corollary. So, corollary to this is that every code  $C$  is precisely the null space of its of its parity check matrix.

(Refer Slide Time: 19:50)



Our next goal is we want to identify means of determining the parity check matrix. So, a next goal is therefore means to identify a parity check matrix for a given code  $C$ .

(Refer Slide Time: 20:55)



So, will state a two Lemmas, which will help us to precisely this lemma 1, if  $H$  is an  $n$  minus  $k$  by  $n$  matrix of rank  $n$  minus  $k$  and the code is precisely the null space of  $H$  then,  $H$  is a valid parity check matrix for the code  $C$ . Now, how do we prove that? So, proof. What is it exactly that we need to prove; what we need to show, because if you remember and the way we introduce the parity check matrix was by actually saying the parity check matrix is a generator matrix, so the dual code. So, what we have to show is that here by we actually finding  $H$  by looking at the code itself, that in fact it is a generator matrix so the dual code.

(Refer Slide Time: 23:00)

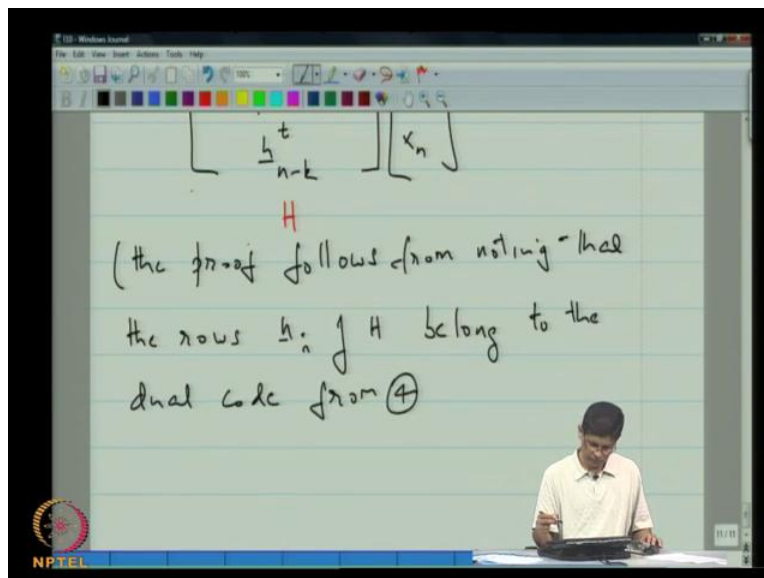
$$\text{pf. } \begin{bmatrix} h_1^t \\ h_2^t \\ \vdots \\ h_{n-k}^t \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \mathbf{0}$$

$H$

So, again you consider this equation here...

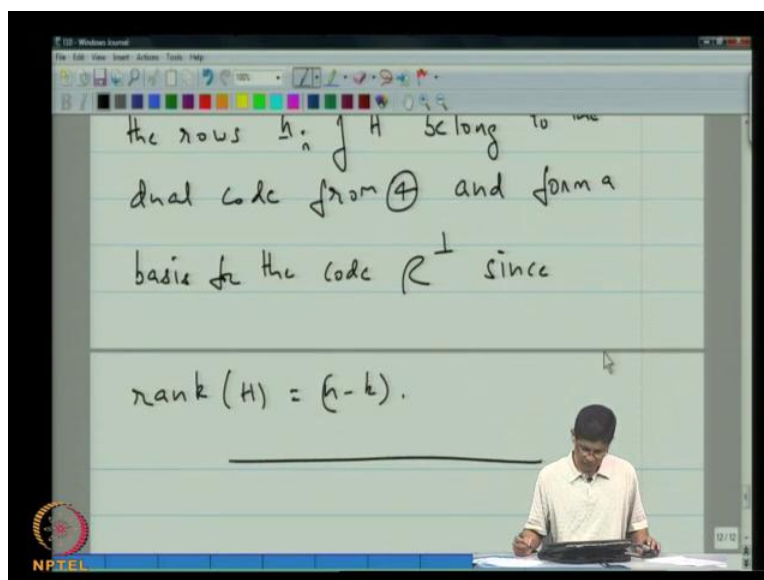
So, you look at this equation, and what you absorb is that since the code is the null space of this matrix  $H$ . It follows that each of the rows is has 0 inner product with the, which is of the code words. Therefore each of these vectors actually belongs to the dual code but in another hand since this matrix  $H$  has rank  $n$  minus  $k$  it follows the these vectors actually spend the dual code, and therefore the row space of this matrix is the dual code. So, it follows that this is a generator matrix. Since, these must therefore form basis for the code therefore it is a generator matrix so the dual code. I think in the interest of moving along I will just leave it at that, and I will leave it you to fill out the details, else I will say there it the proof follows from examination of this equation.

(Refer Slide Time: 24:45)



Above evolve the made the argument verbally. So, will just say the proof follows from noting that the rows  $h_i$  of  $H$  belong to the dual code from, so let us call this equation. I think let us track but let say it is equation 4 from equation 4.

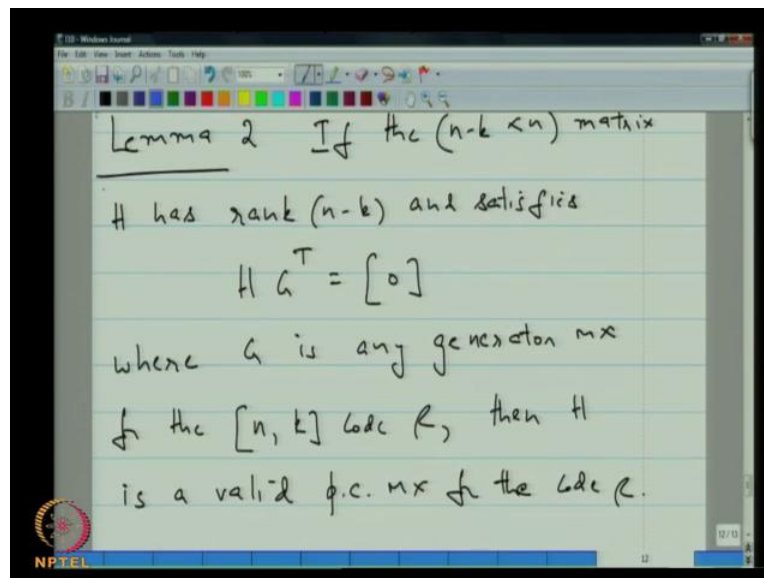
(Refer Slide Time: 25:40)



And form a basis maybe I should put transpose here basis for the code  $C$  prime. Since, the rank of  $H$  is equal to  $n$  minus  $k$ .

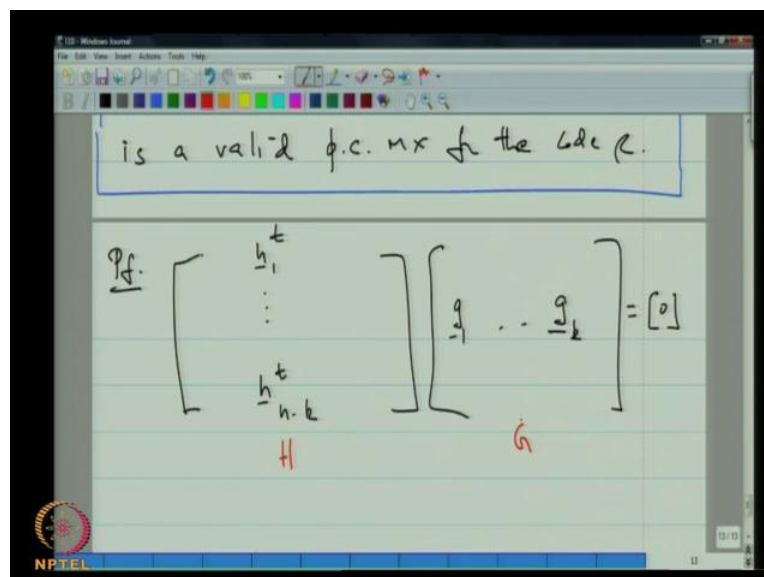


(Refer Slide Time: 26:26)



Now the next Lemma so this is a that was Lemma 1. So this will be Lemma 2 Lemma 2. And, if the  $n$  by  $k$  by  $n$  matrix  $H$  matrix  $H$  has rank  $n$  minus  $k$  and satisfies  $H$  times  $G$  transpose is equal to  $0$ , where  $G$  is any generator matrix for the  $n, k$  code  $C$ , then  $H$  is a valid parity check matrix for the code.

(Refer Slide Time: 29:00)

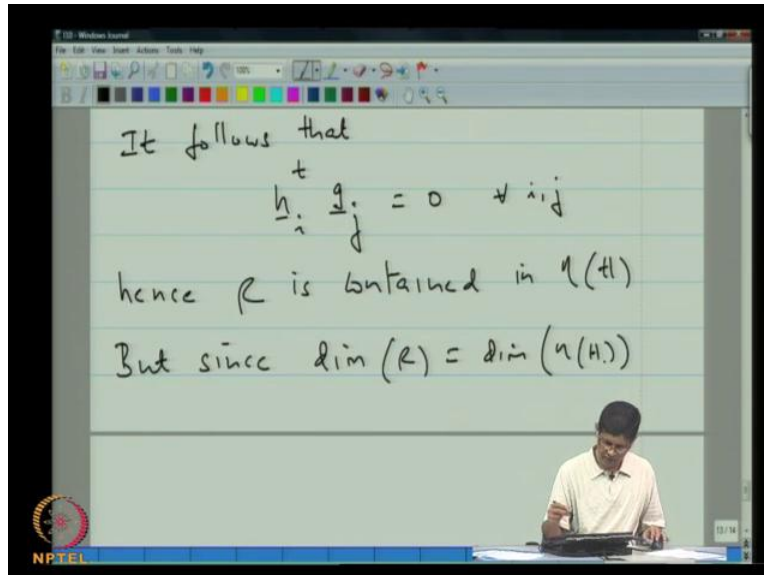


So, the proof follows from looking at this equation here.



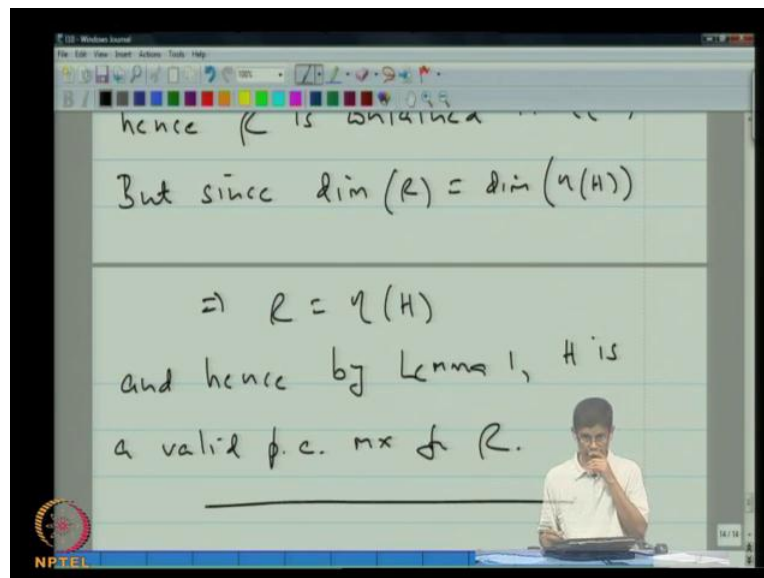
This matrix is H, this matrix is G. So, these vectors are the rows, keep in mind that since this is actually G transpose. So, in G these are row vectors of G after transposition. So they actually form a basis for the code.

(Refer Slide Time: 30:12)



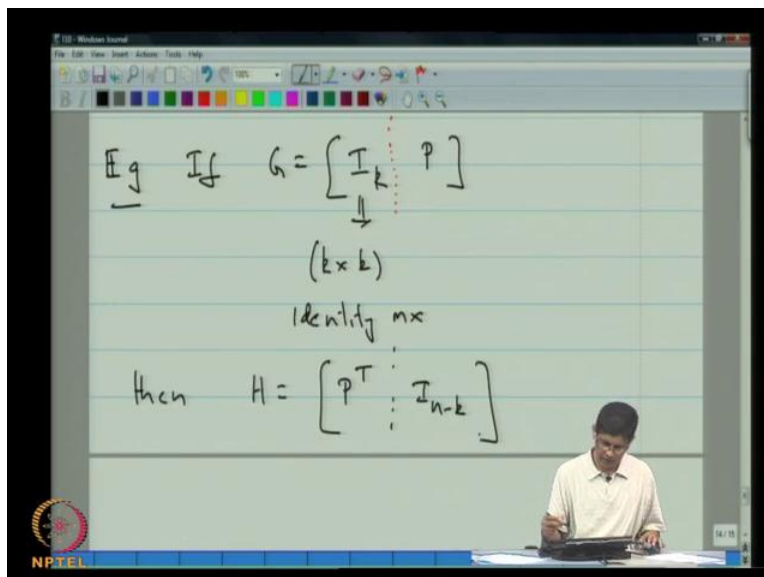
So, it follows it follows it follows that  $H_i^T g_j$  is equal to 0, for all  $i, j$ . Hence  $\mathcal{C}$  is contained in the null space of  $H$ , but since the dimension of  $\mathcal{C}$  is equal to the dimension of the null space of  $H$ .

(Refer Slide Time: 31:00)



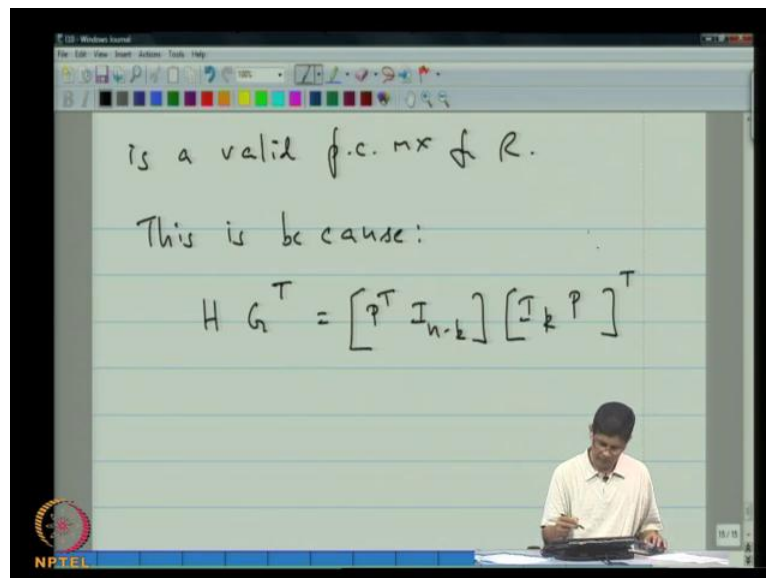
It follows that  $C$  is precisely the null space of  $H$ , and now and hence by Lemma 1,  $H$  is a valid parity check matrix for the code  $C$ . So, in fact it is the second theorem that will actually put to use, the 2-nd Lemma that will actually put to use in order to help us find  $H$ .

(Refer Slide Time: 32:04)



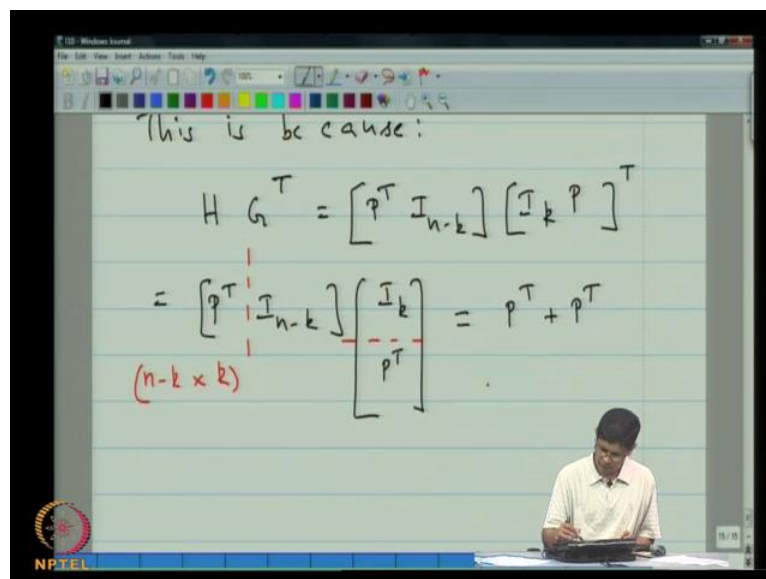
So, let us look at some examples if  $G$  is of the form  $I_k \mid P$ , where this is the  $k$  by  $k$  identity matrix then,  $H$  equal to  $P$  transpose  $I_{n-k}$ .

(Refer Slide Time: 33:00)



Is a valid parity check matrix for C, and where is that? This is because this is because if you consider H times G transpose this is P transpose I n minus k times the transpose of I k and P.

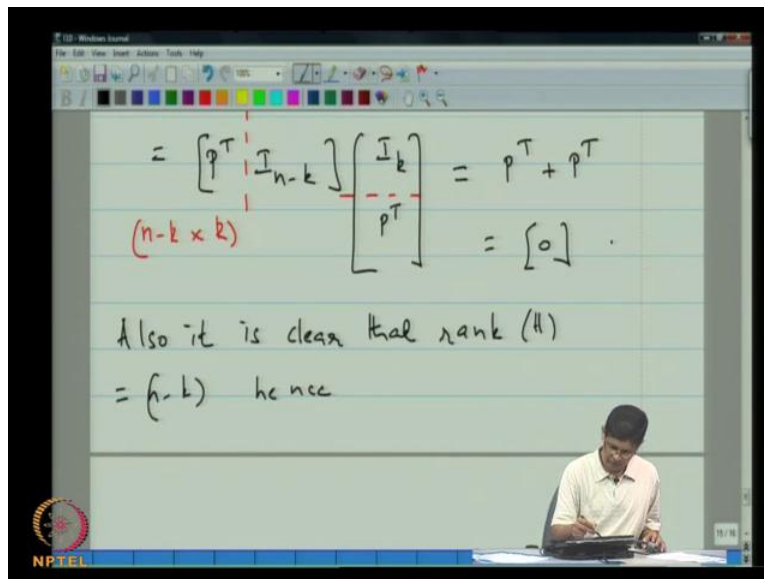
(Refer Slide Time: 33:45)



Which is times I k P transpose and with may to see you can carry a block multiplication, and you can check that the size is a correct. For example this matrix here this P matrix here is this P transpose matrix is n minus k by k. So, the partitioning is correct your partitioning you taking the

first  $k$  columns here the first  $k$  rows. So, the partitioning is correct, and allows you to carry out this multiplication. So, this is nothing but  $P$  transpose plus  $P$  transpose which is 0. That is the first point. So, now we found the parity check matrix  $H$  that there is  $G$  transpose 0 then, the other condition that we have to verify that the rank of  $H$  is  $n$  minus  $k$ . But that is obvious because if you look at the format here it's clear that the rows of  $H$  are linearly independent, because it contains the identity matrix.

(Refer Slide Time: 35:18)



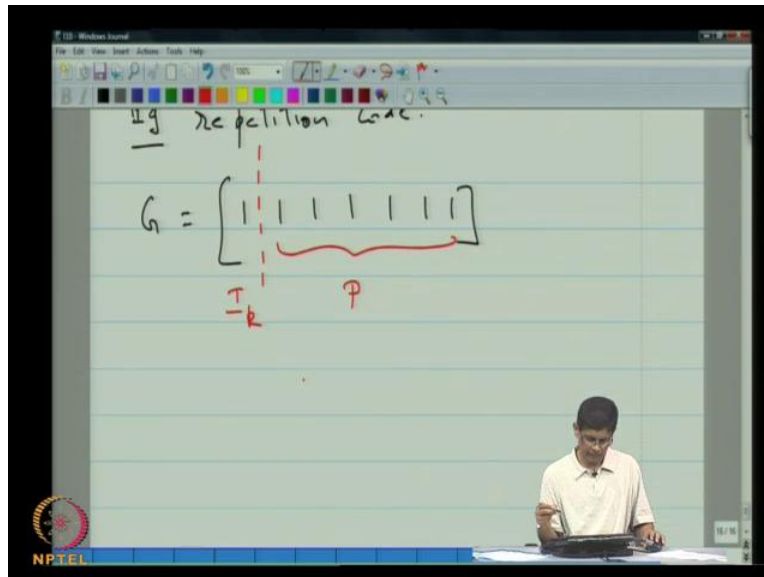
$$= \begin{bmatrix} P^T & I_{n-k} \end{bmatrix} \begin{bmatrix} I_k \\ P^T \end{bmatrix} = P^T + P^T = [0]$$

$(n-k \times k)$

Also it is clear that  $\text{rank}(H) = (n-k)$  hence

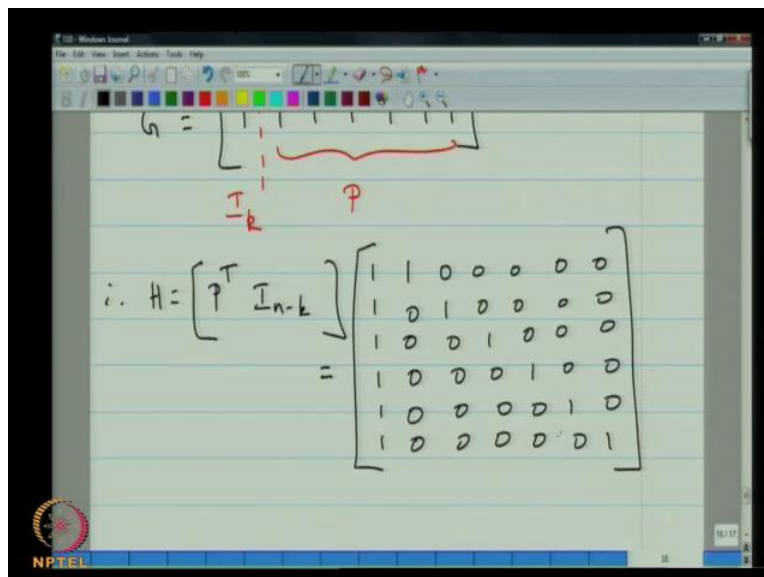
Also it is clear that the rank of  $H$  is equal to  $n$  minus  $k$  hence so, hence. So, both conditions are satisfied and that is enough to actually tell us that we found parity check matrix.

(Refer Slide Time: 36:05)



So, let us look at an example within an example supposing we look at the repetition code we already know that a generator matrix so, this is just this matrix. So, in this case we can actually drop a partition like this, this then forms  $R I_k$ , this thing here is  $R p$ .

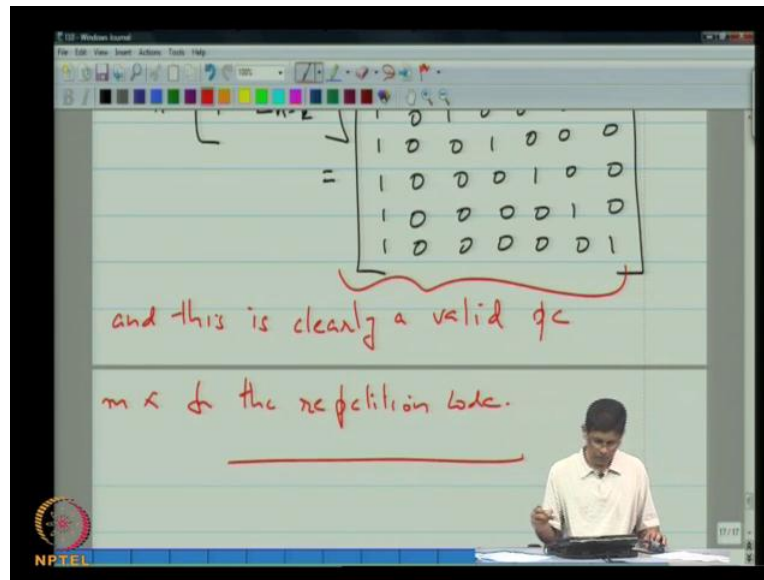
(Refer Slide Time: 36:55)



Therefore a candidate H is  $P^T I_{n-k}$ . If you think about it that will end up being...

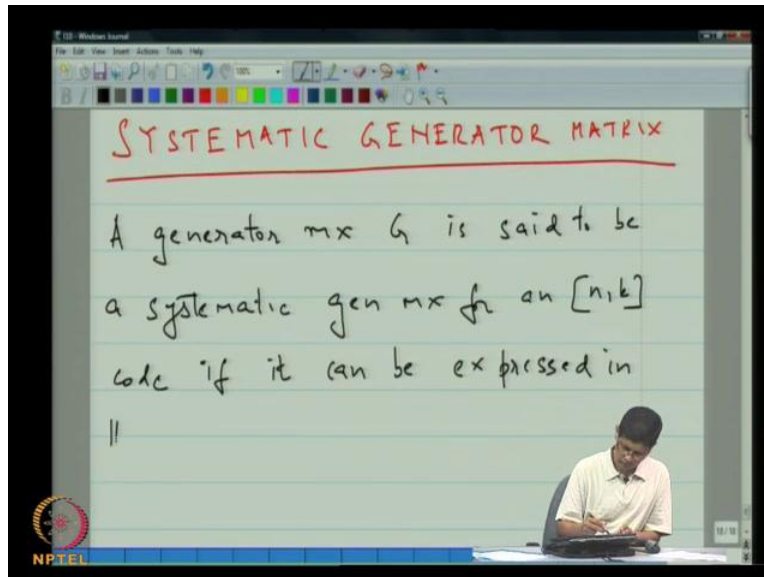
And this is a parity check matrix for the single parity code for this is a parity check matrix for the repetition code.

(Refer Slide Time: 38:08)



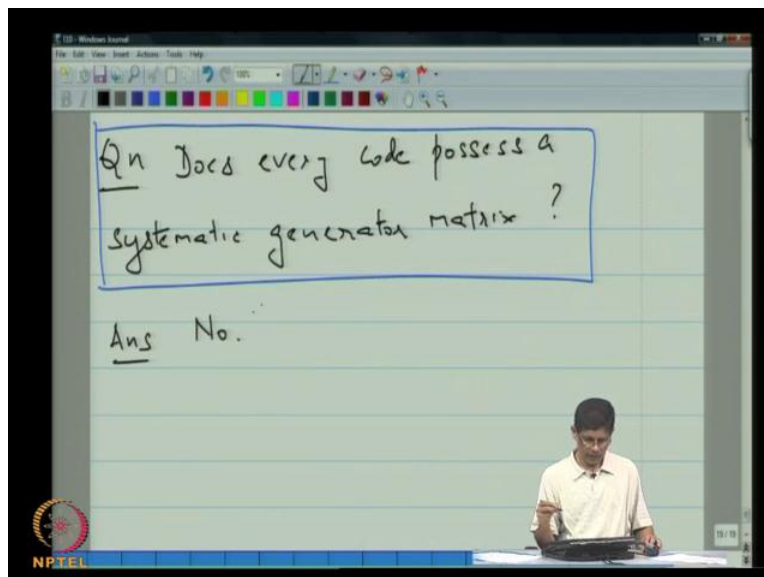
And this is clearly a valid parity check matrix for the repetition code. Because if you look at this each row of this matrix imposes the condition, the first row imposes the condition that the second symbol must agree with first. The next row imposes the condition that the third symbol must agree with the first, and so on. So, always these symbols must be equal, and that is why it is the valid parity check matrix.

(Refer Slide Time: 39:16)



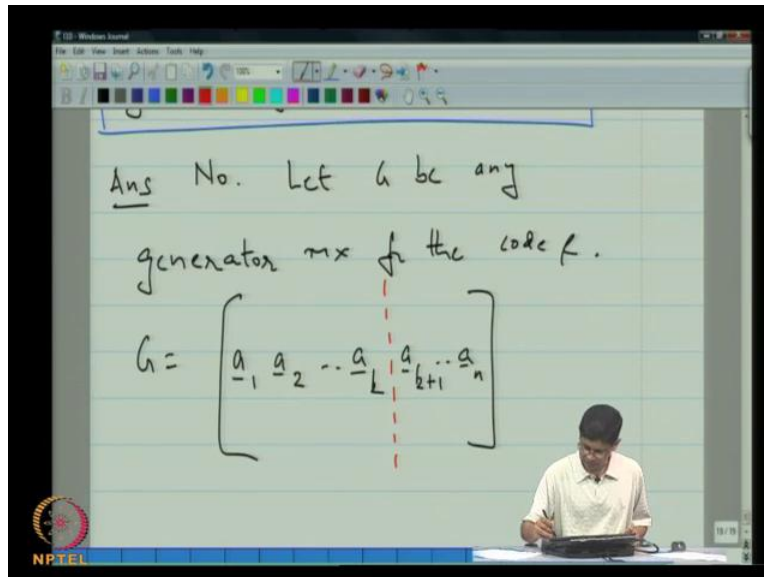
So, this motivates us to define the notion of a systematic generator matrix. A generator matrix  $G$  is said to be systematic generator matrix for an  $[n, k]$  code if it can be put it can be expressed **it** can be expressed in the form  $G$  is equal to  $I_k$  followed by  $P$ .

(Refer Slide Time: 41:24)



So, this graces the interesting question of... question, Does every code possess a systematic generator matrix?

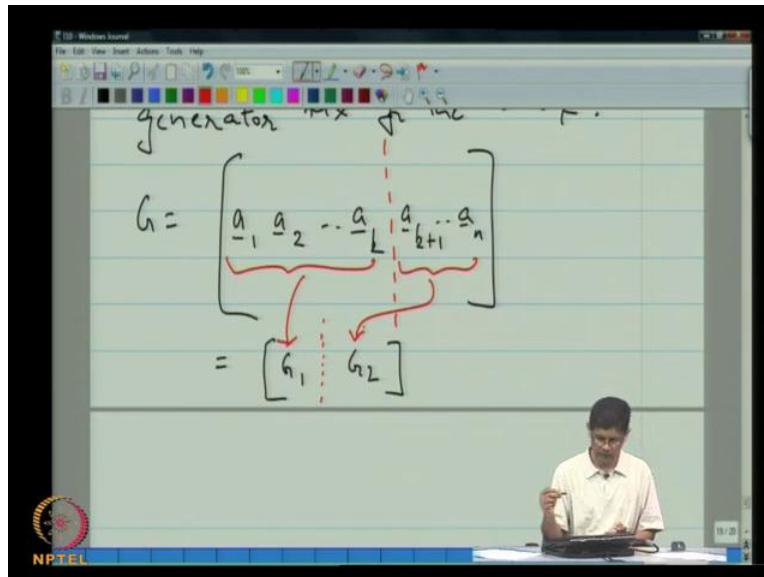
(Refer Slide Time: 42:05)



The answer to this is, No in fact you can tell whether or not a code possesses a systematic generator matrix between the following you can take any generator matrix for the code, any generator matrix for square, and then you can examine the first  $k$  columns of the generator matrix. If that result in  $k$  by  $k$  matrix as full rank then, it has a systematic generator matrix otherwise it does not. Let  $G$  be any generator matrix for the code  $C$ , and let us tell out  $G$  like this. So, now I am going to talk in terms of the columns of  $G$ . So, let say that they are  $a_1, a_2, a_k, a_{k+1}$  to  $a_n$ ; so let say that these are the columns of the matrix  $G$ .

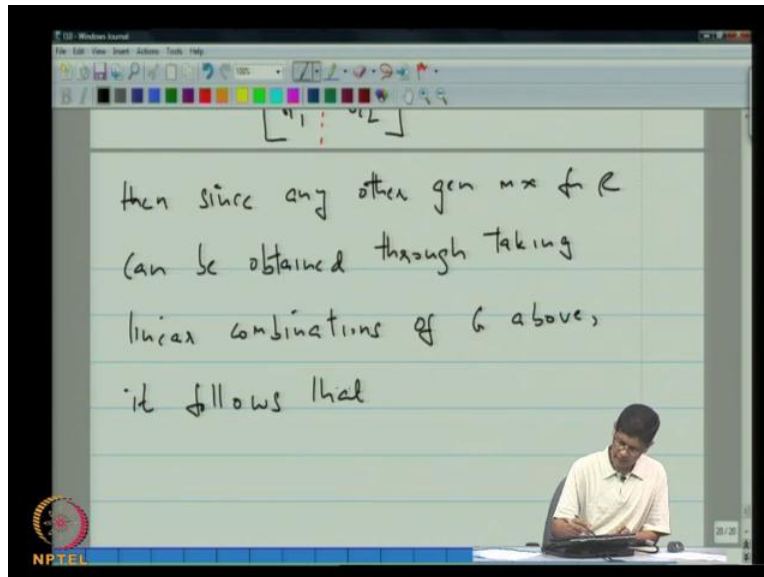


(Refer Slide Time: 43:56)



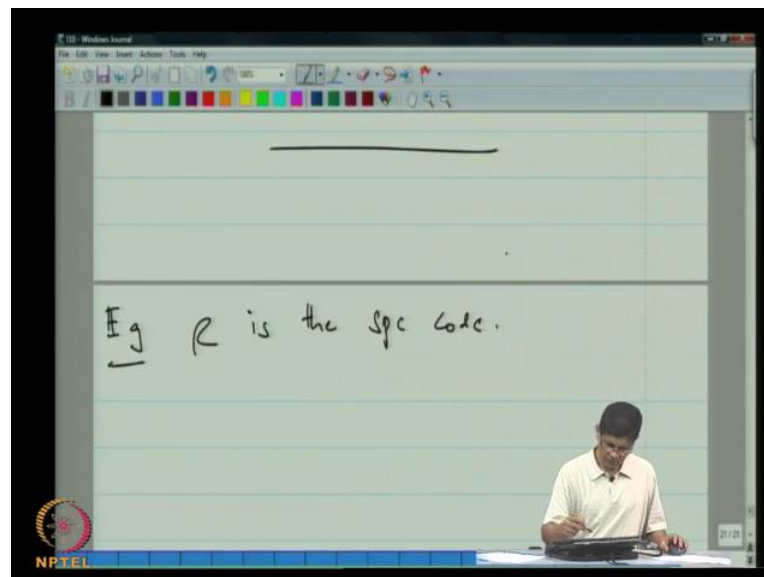
And, let say that this can be express in the form  $G_1, G_2$ ; so that means that I am going to call this part here  $G_1$ , and this part here  $G_2$ , and so the simple answer to this question is that if  $G$  is any generator matrix, if  $G_1$  has full rank then it has a systematic generator matrix, otherwise not. Now, why is that the case? That is just because you know the difference between you can go from it should be clear that, since the row space is of any two generator matrix is are the same you can go from one generator matrix to the other simply by carrying out a linear combinations of the rows. So, linear combinations however, and also you it can never increase the rank if we start up with this as a generated matrix and if in terms of that the  $G_1$  is rank efficient meaning that there is not equal to  $k$ . Then you mat a what linear transformations you do on the row you can never transform into another matrix  $G_1$  prime with rank is equal to  $k$ , and for this reason its necessity insufficient condition is that  $G_1$  have full rank.

(Refer Slide Time: 45:36)



Then since any other general matrix for  $C$  can be obtained through taking linear combinations of  $G$  above, it follows that  $C$  has a systematic generator matrix if and only if rank of  $G_1$  is equal to  $k$ .

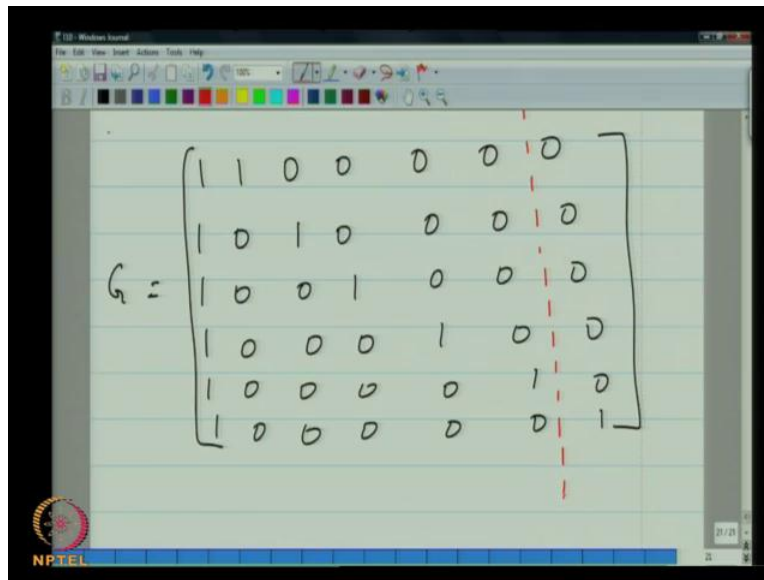
(Refer Slide Time: 47:13)



Let us look at some examples or other let us look at one example, now supposing  $C$  is the single parity check code. Now we were already written down a generator matrix for this. So, let me see

fact a hunt it down from one of our previous lectures. Here it is I am going to copy this matrix, and now let us go back to our lecture today, and will put this down here.

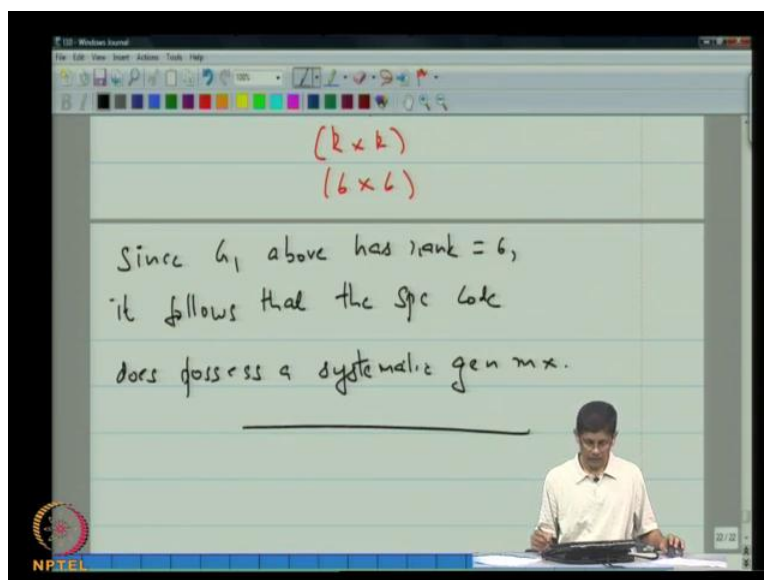
(Refer Slide Time: 48:04)



$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Here we go. So, we have this generator matrix for this; and now in this example the issue is concerning the matrix  $G_1$  where this is  $G_1$ , and this is  $G_2$ , and the question is, does  $G_1$  have rank 6 or does it not?

(Refer Slide Time: 48:50)



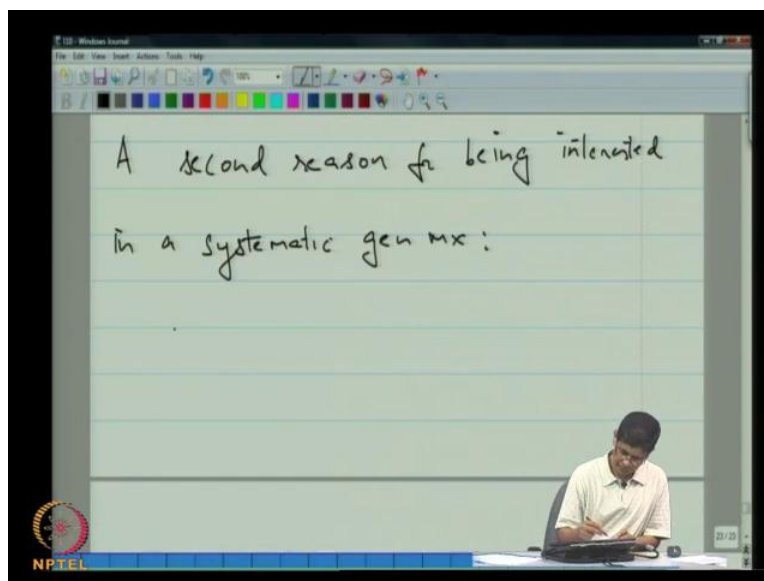
(k x k)  
(6 x 6)

Since  $G_1$  above has rank = 6,  
it follows that the Spc  $C_{0k}$   
does possess a systematic gen mx.

So, this a matrix here is in general a  $k$  by  $k$  matrix which in this particular instance is for 6 by 6 matrix. So the question is does those have rank 6 or not? And it is pretty easy to see there it has rank 6 just by inspection. So, we conclude from this that, since  $G$  1 above has rank equal to 6, it follows that the single parity check code does possess a systematic generator matrix. Now however having set that coming this say something else you know this now by the way yes I should really point out something else. Which is so why are we interested in a systematic generator matrix? By the way, I am not code sure how much time we have left I am imagine we getting very close to the end of assertion should trap assertion to just first quickly summarize and before I continue.

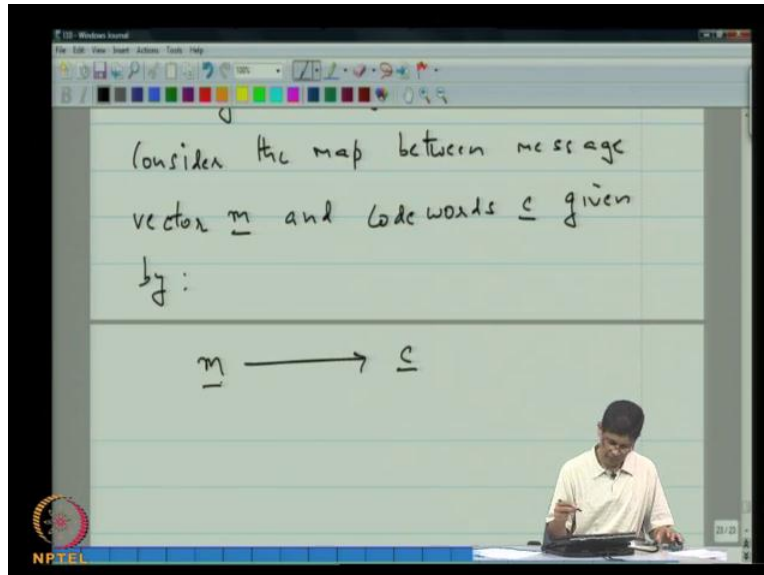
So, what we did today? I was basically filled in little bit of linear algebra background by at define what is meant by the row space of matrix, and I stated the fundamental theorem of linear algebra, and then we prove the dual of a dual of a code is the code itself, and as a corollary to that we found out that the code is the null space of its parity check matrix, and then we note down to the question of well how do we actually find  $H$ , and we said one we are finding it  $H$  is to actually find it  $H$  from  $G$ , and so that is why we concentrating upon, and now in the systematic case is very easy to write down age, but apart from the ease of generating age this another reason for being interested in a systematic generator matrix, and I am coming to that.

(Refer Slide Time: 51:56)



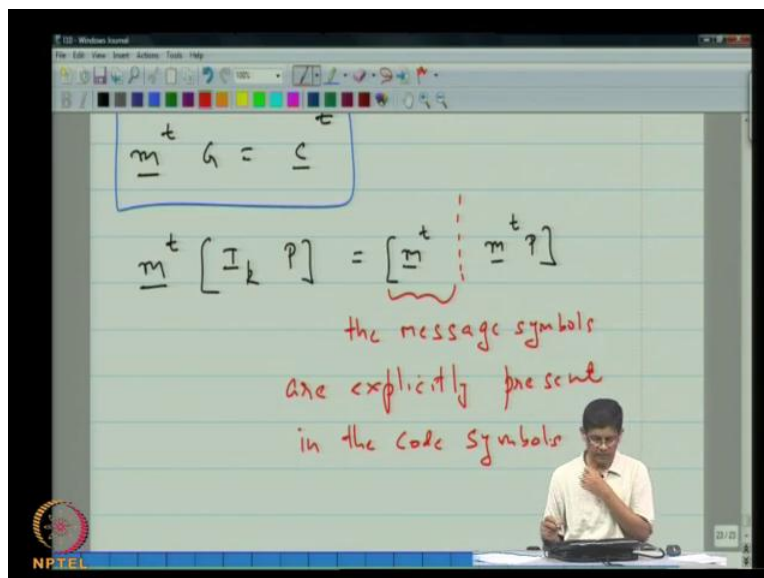
So, let me put this down instead of saying a question let me say a second reason for being interested in systematic generator matrix, a second reason for being interested in a systematic generator matrix is this.

(Refer Slide Time: 52:32)



Consider the map between message vectors  $m$  and codewords  $c$  given by so you are going from  $m$  to  $c$  like this.

(Refer Slide Time: 53:16)



m transpose G is equal to c transpose, and in the systematic case this becomes m transpose I k P is equal to m transpose, and then m transpose P. So, what that means is that the first few symbols of your codeword or the message symbol themselves. So, the message symbols are explicitly are explicitly present within the code symbols. So, that is convenience, because when you consider the task of decoding, lets you receive the codeword and, you decoded it to certain codeword then you do not have to do any processing at all to recover them message symbols apart from dropping the last few symbols. So, that is in other good reason for being interested in a systematic code.

But other hand if you think about it this business of insisting I mean, after all from this point of view so that the two issues one is that, wrap if the generator matrix is systematic then it has to be find the parity check matrix. But on the other hand it features thinking in terms of being able to see in a transparent way the message symbols is being part of the code vector then, you do not have to be so strict or you do not have to worry so much if your metrics is not systematic.

(Refer Slide Time: 56:00)

Ans No. Let  $G$  be any generator  $m \times n$  for the code  $C$ .

$$G = \begin{bmatrix} a_1 & a_2 & \dots & a_k & a_{k+1} & \dots & a_n \end{bmatrix}$$

The matrix is partitioned into two parts,  $G_1$  and  $G_2$ , separated by a vertical dashed line:

$$= \begin{bmatrix} G_1 & G_2 \end{bmatrix}$$

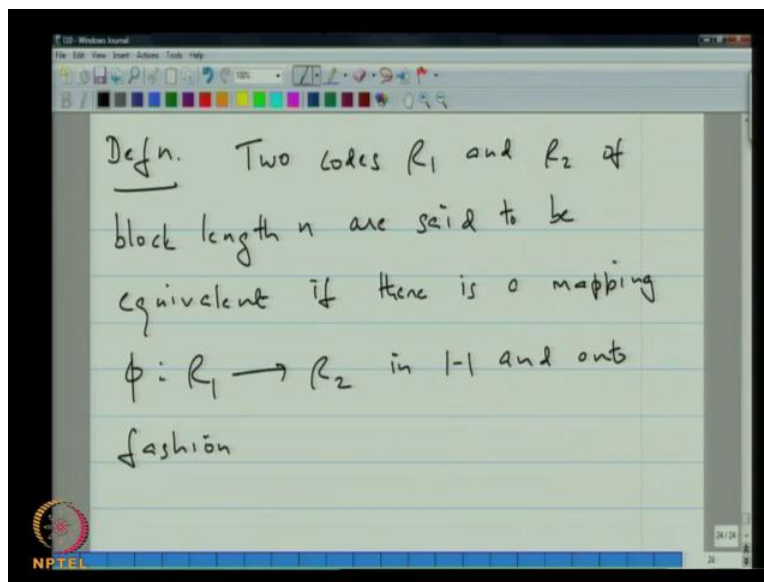
NPTEL logo is visible in the bottom left corner of the whiteboard.

Because you know so, looking at a generic generator matrix as given by the matrix in front of us here. We know that this matrix has rank  $k$ , that means that some  $k$  columns of it will be linearly independent, and some sub matrix of size  $k$  by  $k$  will have full rank. So, you can certainly row reduce that to make that the identity matrix, what is that mean? That means your message

symbols after own it as will now be explicitly present in the code vector, except that they would not they necessarily appear as the first case symbols will appear as a collection of  $k$  symbols stone along the codeword that is in some positions. But that is not too bad, because if you know that once you can always shuffle the symbols, and recover the message symbols.

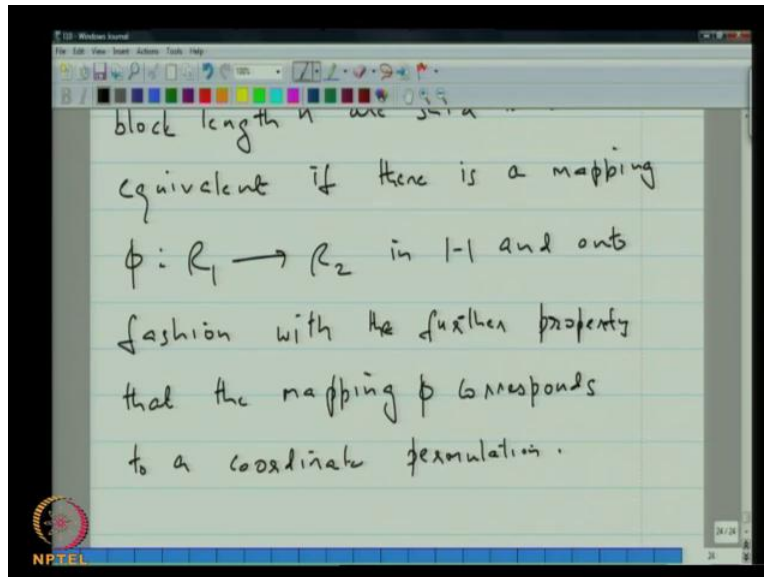
So, again to repeat that the point making that since a generated matrix whose rank  $k$  some sub set of  $k$  columns of the generated matrix must be linearly independent. So, that particular sub matrix must have rank  $k$ . You can row reduce that to get the second generator matrix where in those columns we have the identity matrix, and then that means that when you use that matrix for generating codewords, the message symbols will be explicitly present in those positions. And so you do get this benefit of ease, and decoding you mean without the requiring that have this specific form.

(Refer Slide Time: 57:40)



So, this motivates the definition of equal length codes, two codes  $C_1$  and  $C_2$  of block length  $n$  are said to be equivalent if there is a mapping  $\phi$  which maps  $C_1$  to  $C_2$  in 1 to 1, and onto fashion.

(Refer Slide Time: 58:55)



So, it establishes a one to one correspondence, which with the further property that the mapping  $\phi$  corresponds to a coordinate permutation that the definitions are now time is up. So will stop here and continue next time, thank you.