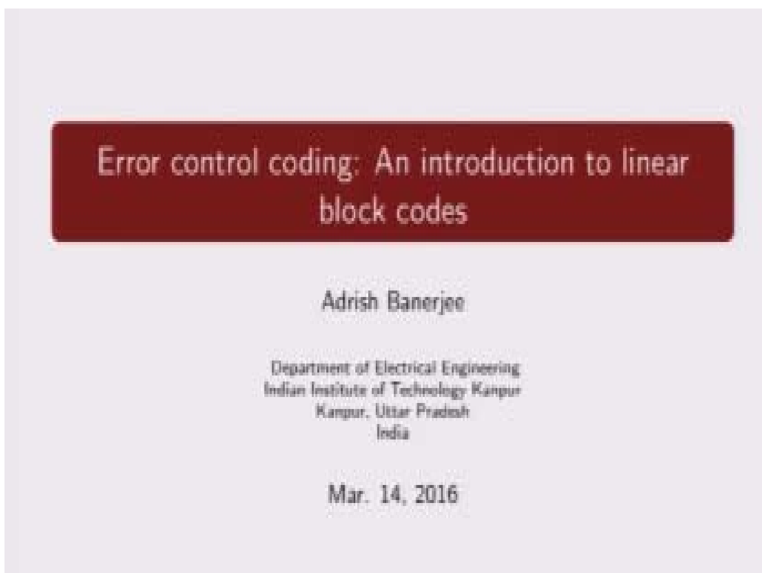
Indian Institute of Technology Kanpur
National Programme on Technology Enhanced Learning (NPTEL)
Course Title
Error Control Coding: An Introduction to Linear Block Codes

Lecture – 2
Generator Matrix and Parity Check Matrix

by
Prof. Adrish Banerjee
Department of Electrical Engineering, IIT Kanpur

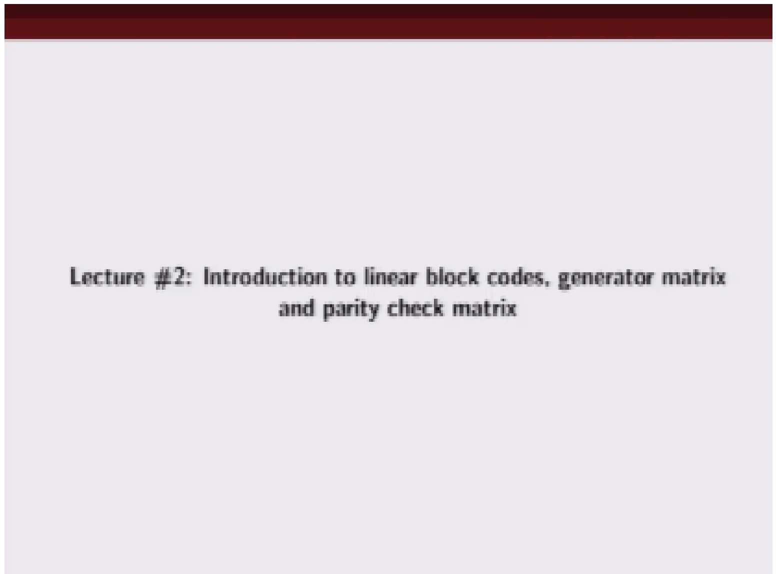
Welcome to the course on error control coding, an introduction to linear block codes.

(Refer Slide Time: 00:20)



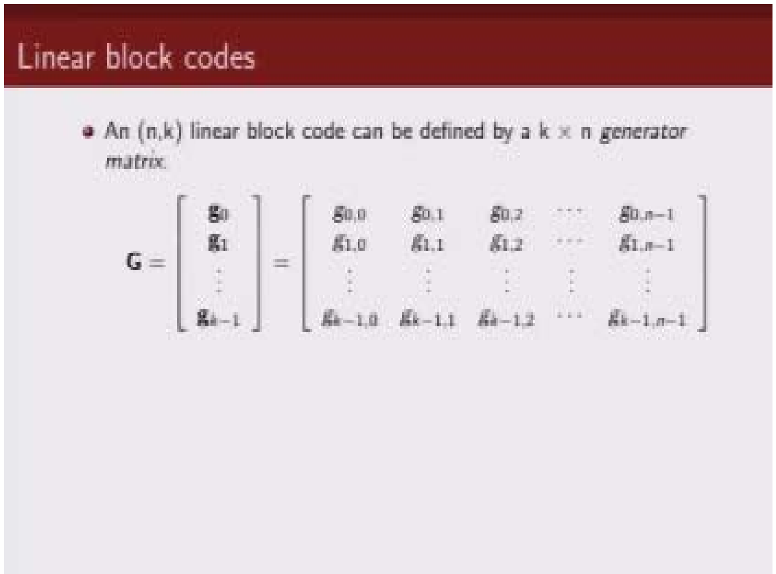
Today in this lecture we are going to describe what we mean by generator matrix and parity check matrix, so we will continue our discussion with introduction to linear block codes.

(Refer Slide Time: 00:39)



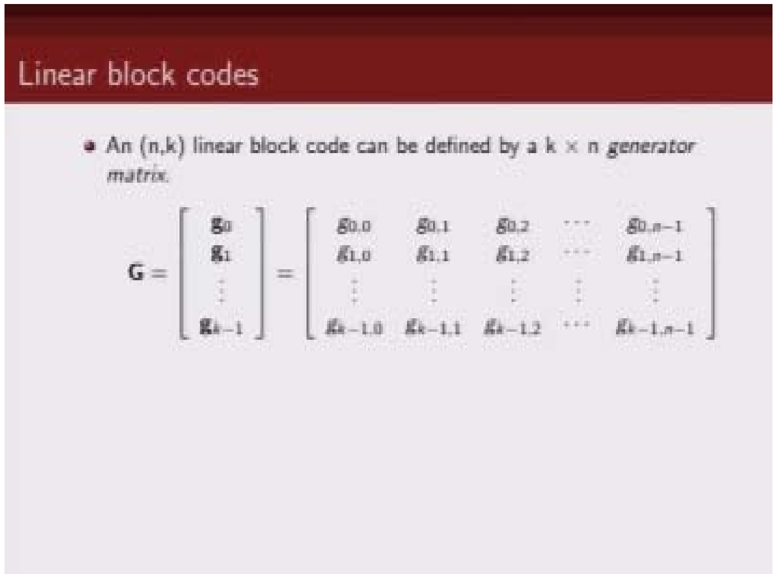
We will first describe, what is a generator matrix and what is a parity check matrix and how are they related, so as we described in the last class an encoder for a linear block codes what it does it takes a block of k bits and maps it to the two end bit.

(Refer Slide Time: 01:01)



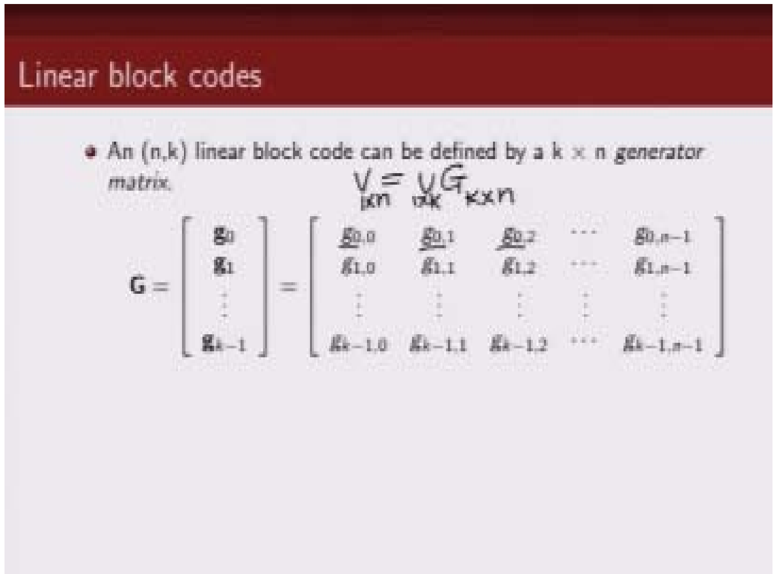
Now the matrix we can use a matrix k x n matrix to define this mapping from k information bits to n coded bits and this matrix is basically our generator matrix.

(Refer Slide Time: 01:17)



For a so for an (n, k) linear block code the mapping of k information bits to encoded bits is defined by this generator matrix G which is of rank k so if we denote the information bits by u.

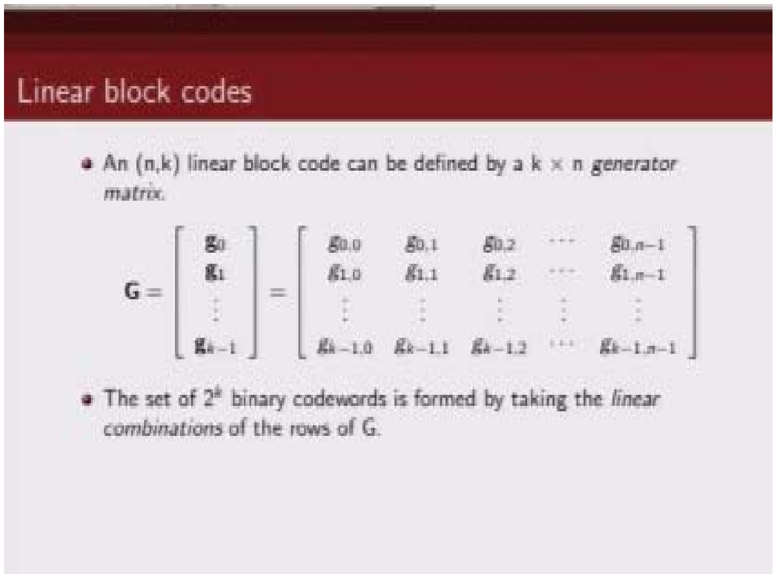
(Refer Slide Time: 01:36)



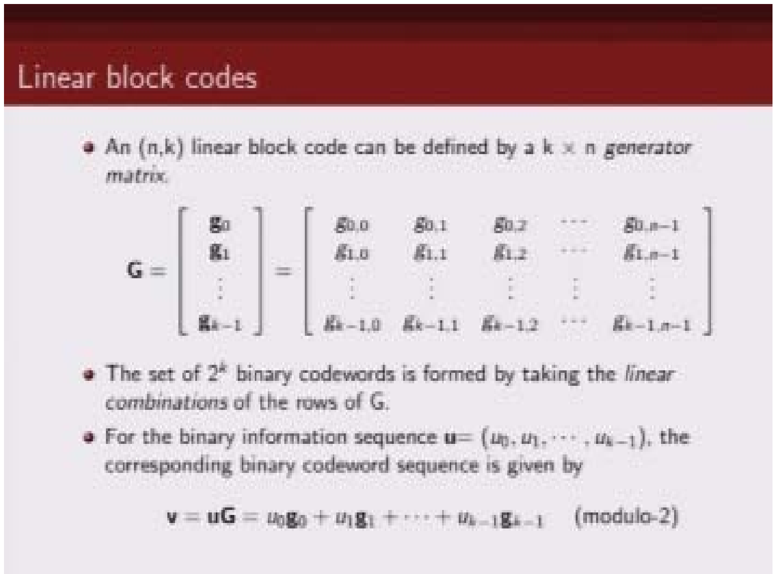
And we denote our coded bits by v then we can write v is u times G, where our u is 1 x k vector and this is, generator matrix is k x n matrix and our output coded bit is 1 x n vector. So as the name suggest basically generator matrix is used to generate our code word so we generate our code words using this generator map matrix and this generator matrix gives the mapping between the information bits u to the coded bits v, so how do we find code words?

We find code words by taking linear combinations of rows of these generator matrix, in case of binary codes so then these entries in the generator matrix are either zero or one depending upon which bits are used to generate a particular coded sequence. So we form a set of 2k code words by taking linear combinations of rows of these generator matrix.

(Refer Slide Time: 02:59)

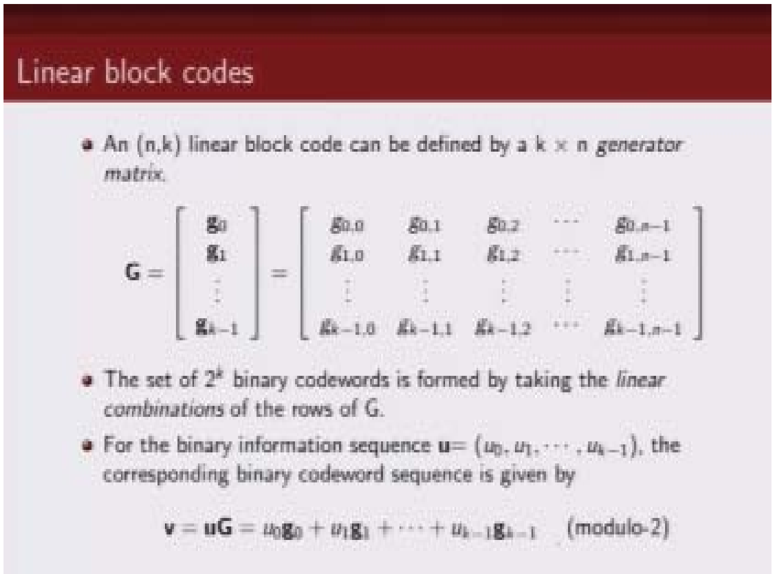


(Refer Slide Time: 03:05)



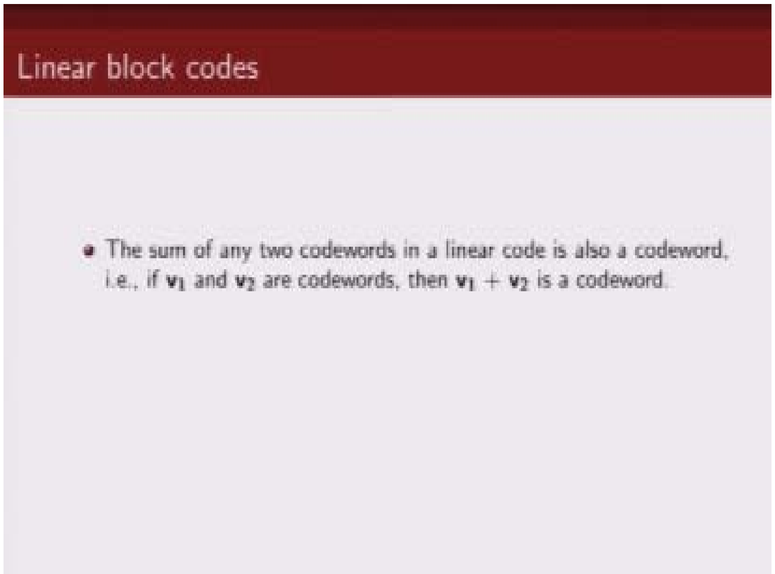
So we can, as I said we can write our coded sequence as u times G which is basically linear combination of rows of the generator matrix. So these are basically linearly independent k rows and the rank of this generator matrix is k, since we are without loss of generality since we are talking about binary linear block codes.

(Refer Slide Time: 03:39)



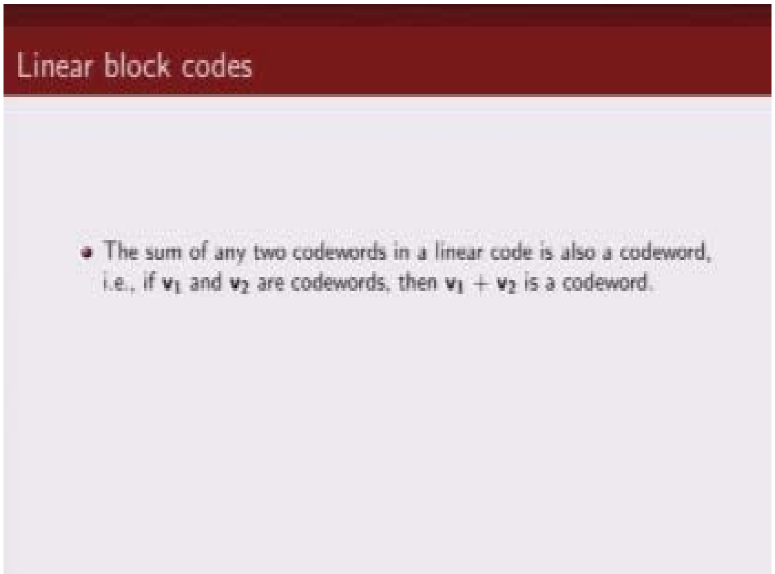
So we will be doing this addition modulus – 2.

(Refer Slide Time: 03:42)

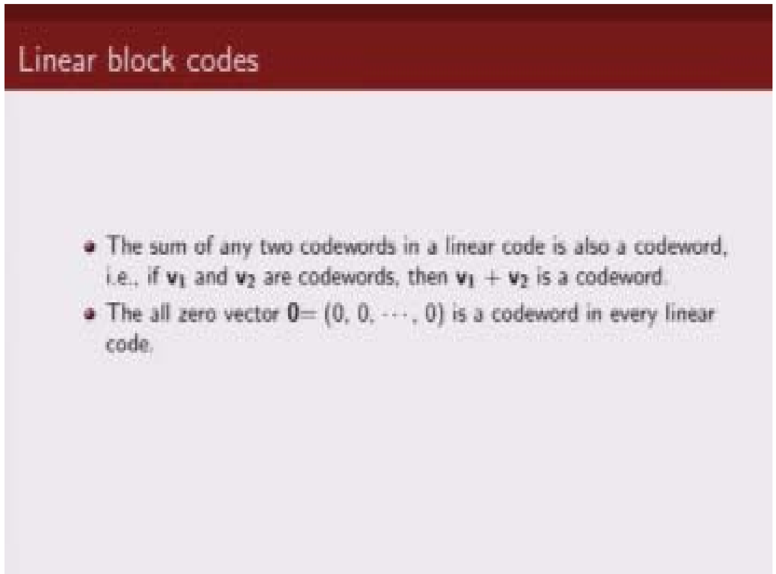


So what are the properties of a linear block code? Sum of any two code words in a linear code is also a valid code word, so if v_1 and v_2 are valid code words then v_1+v_2 will also be a valid code word.

(Refer Slide Time: 04:02)

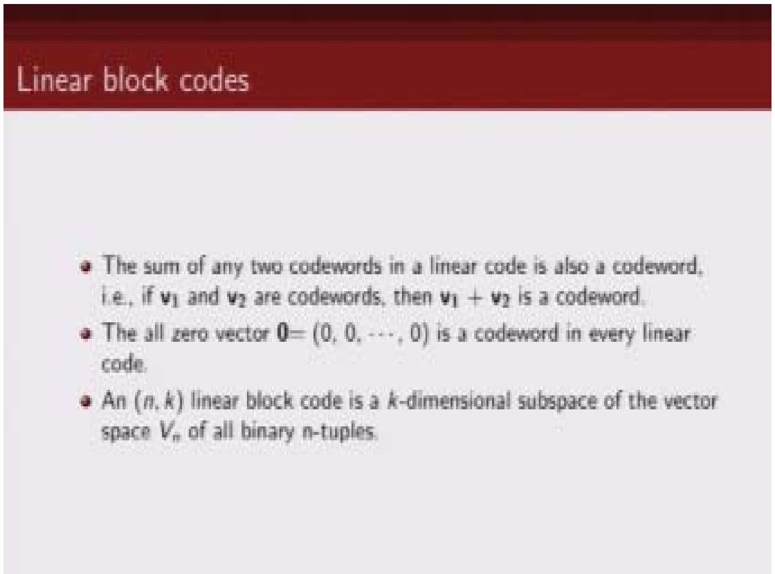


(Refer Slide Time: 04:04)



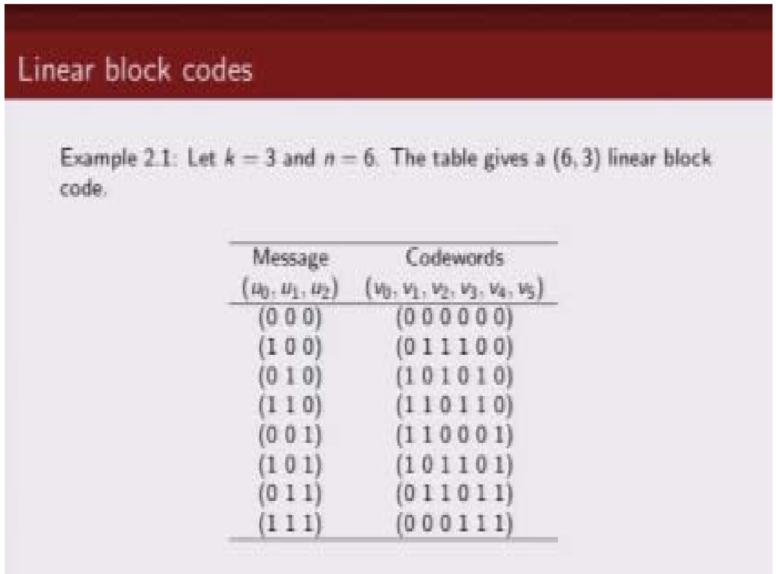
Also an all zero code word is a valid code word in any linear block codes.

(Refer Slide Time: 04:12)



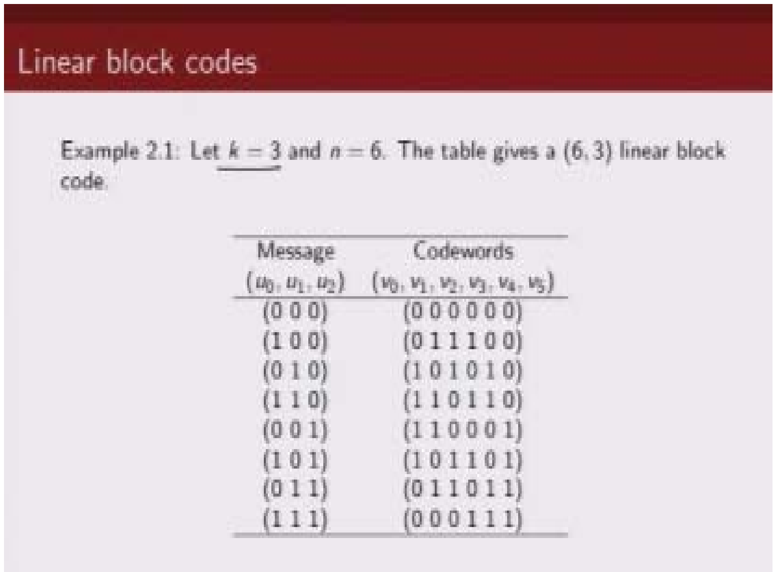
So we can define a linear block code (n, k) linear block code as a k dimensional subspace of vector space V_n of all binary n – tuples so we can define a linear binary block codes as a k dimensional subspace of vector space Vn of all binary n – tuples.

(Refer Slide Time: 04:39)



Now let us take an example to illustrate what is a generator matrix, so in this example we have considered.

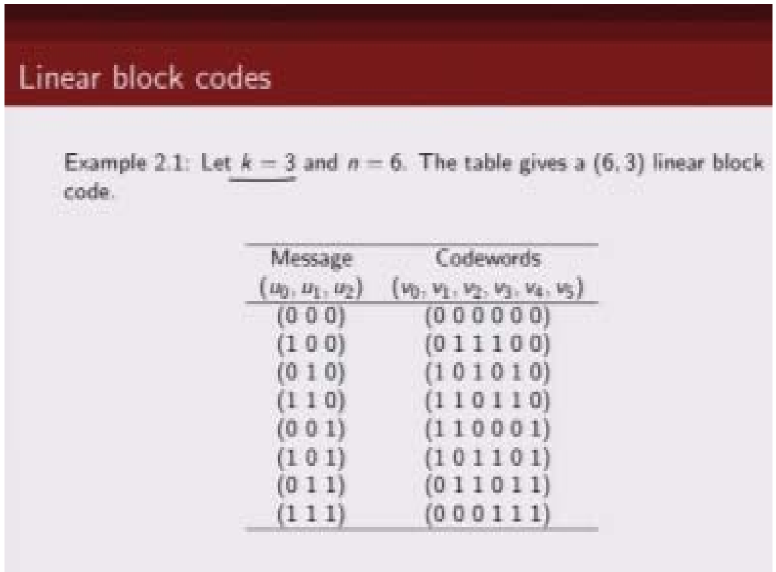
(Refer Slide Time: 04:49)



Message (u_0, u_1, u_2)	Codewords $(v_0, v_1, v_2, v_3, v_4, v_5)$
(0 0 0)	(0 0 0 0 0 0)
(1 0 0)	(0 1 1 1 0 0)
(0 1 0)	(1 0 1 0 1 0)
(1 1 0)	(1 1 0 1 1 0)
(0 0 1)	(1 1 0 0 0 1)
(1 0 1)	(1 0 1 1 0 1)
(0 1 1)	(0 1 1 0 1 1)
(1 1 1)	(0 0 0 1 1 1)

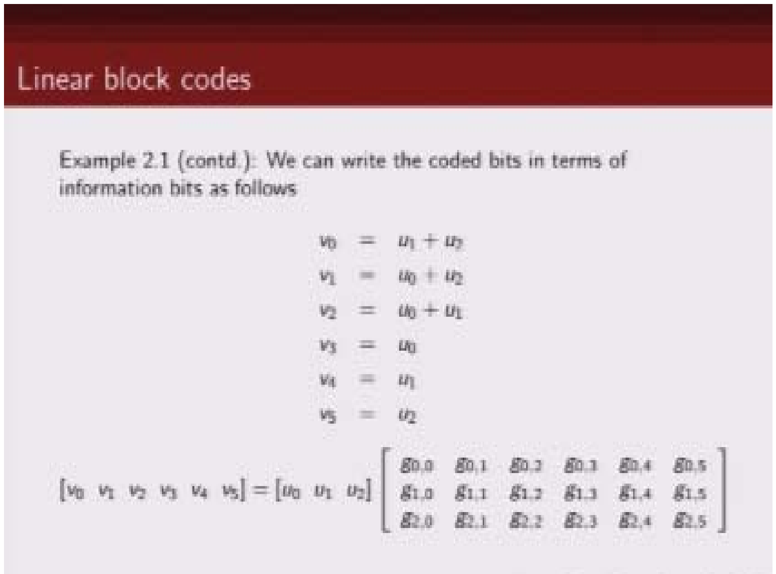
Three information bits and six coded bits and in this table I have given you the set of eight information sequences and their corresponding code words, so how do we find the generator matrix in this case? So we will have to look at each of these code bits and see how are we generating these code bits in terms of message bits u_0, u_1 and u_2.

(Refer Slide Time: 05:28)



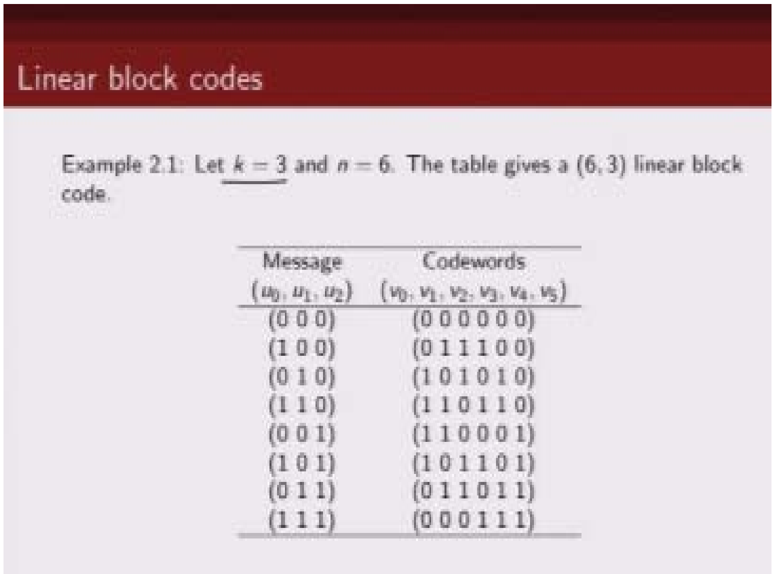
So first thing we are going to do is, look at each of these code bits v_0, v_1, v_2, v_3, v_4, v_5 and write them in terms of u_0, u_1, u_2, okay so let us look at each of these.

(Refer Slide Time: 05:47)



So v_0 is u_1+u_2.

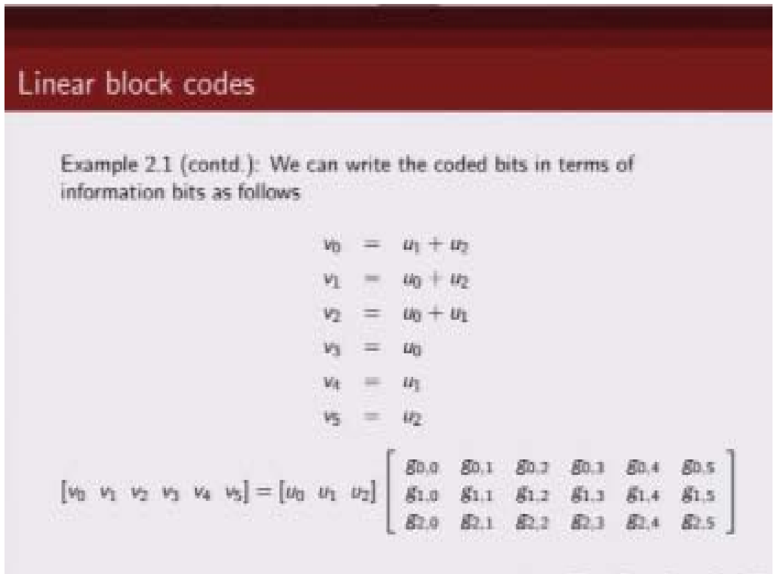
(Refer Slide Time: 05:50)



Message (u_0, u_1, u_2)	Codewords $(v_0, v_1, v_2, v_3, v_4, v_5)$
(0 0 0)	(0 0 0 0 0 0)
(1 0 0)	(0 1 1 1 0 0)
(0 1 0)	(1 0 1 0 1 0)
(1 1 0)	(1 1 0 1 1 0)
(0 0 1)	(1 1 0 0 0 1)
(1 0 1)	(1 0 1 1 0 1)
(0 1 1)	(0 1 1 0 1 1)
(1 1 1)	(0 0 0 1 1 1)

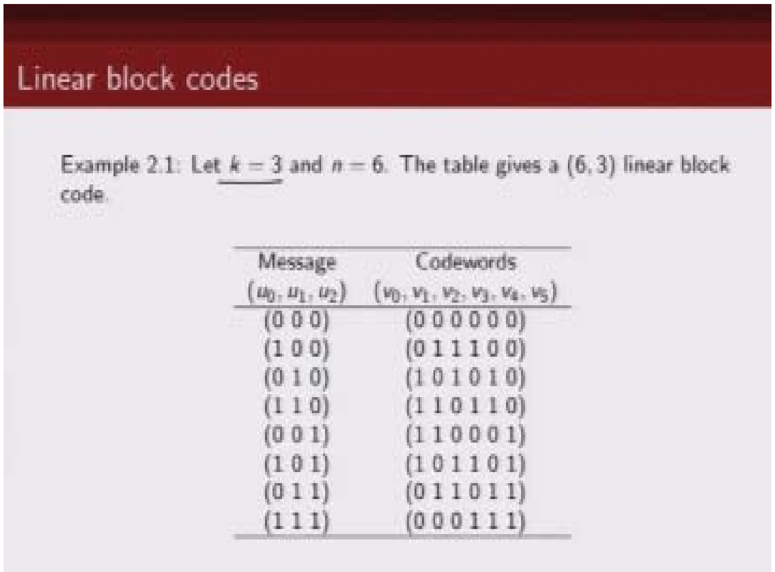
We can see easily v_0 is this column and we can see this is same as u_1+u_2, so u_1+u_2 in this case is zero, u_1+u_2 is zero, 1+0 is 1, 1+0+1 is 1, 1+1 is 0 modulo 2 and 1+1 is zero modulo 2, so this v_0 is basically given by u_1+u_2.

(Refer Slide Time: 06:17)



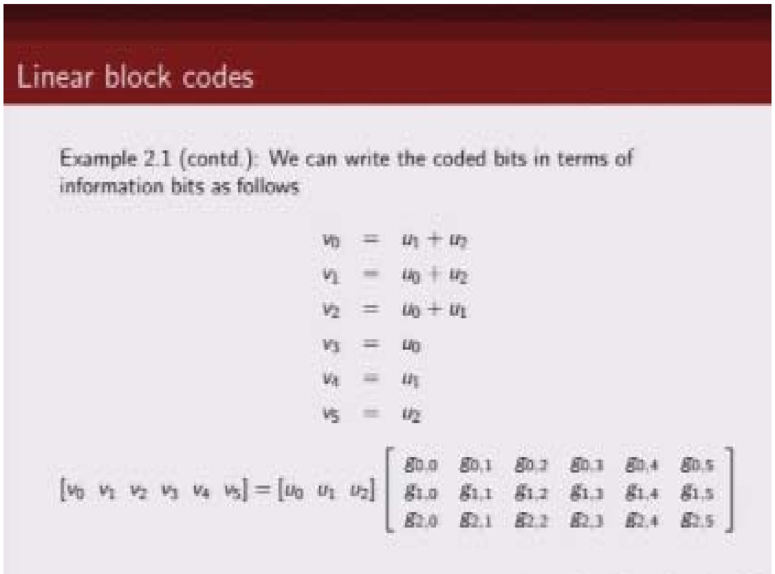
Similarly we can see v_1 is given by u_0+u_2 and v_2 is given by u_0+u_1.

(Refer Slide Time: 06:30)

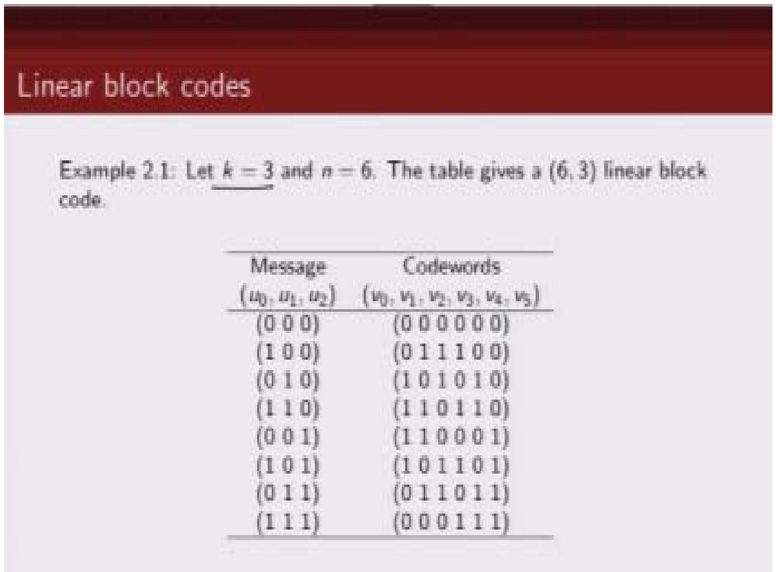


So let us just check and say v_2, v_2 we can see is given by, v_2 is given by u_0+u_1.

(Refer Slide Time: 06:38)

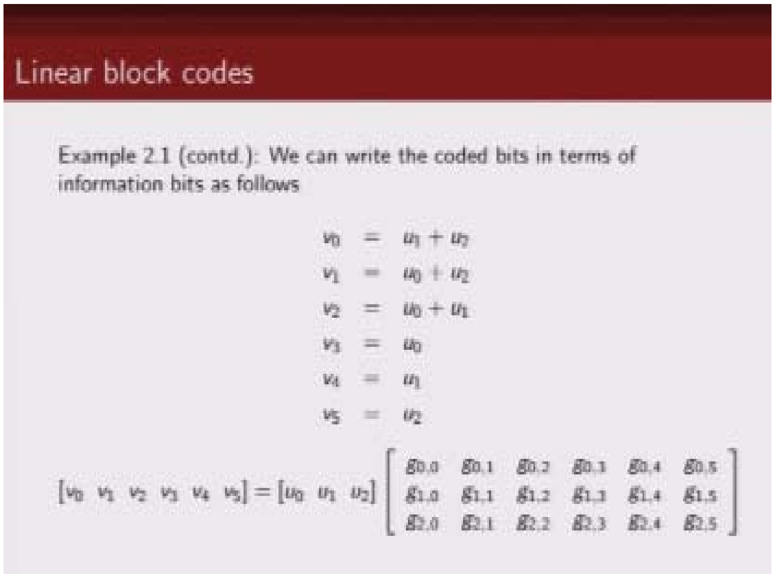


(Refer Slide Time: 06:40)



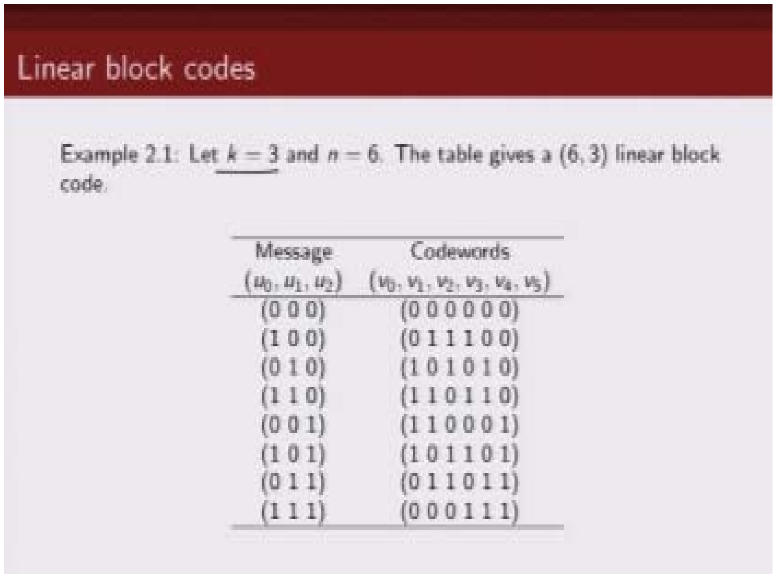
You can check v_2 is given by so u_0+u_1, 0+0 is 0 , 1+0 is 1, 0 +1 is 1, 1+1 is 0, 0+ 0 is 0, 1+0 is 1, 0+1 is 1 and 1+1 is 0.

(Refer Slide Time: 07:03)



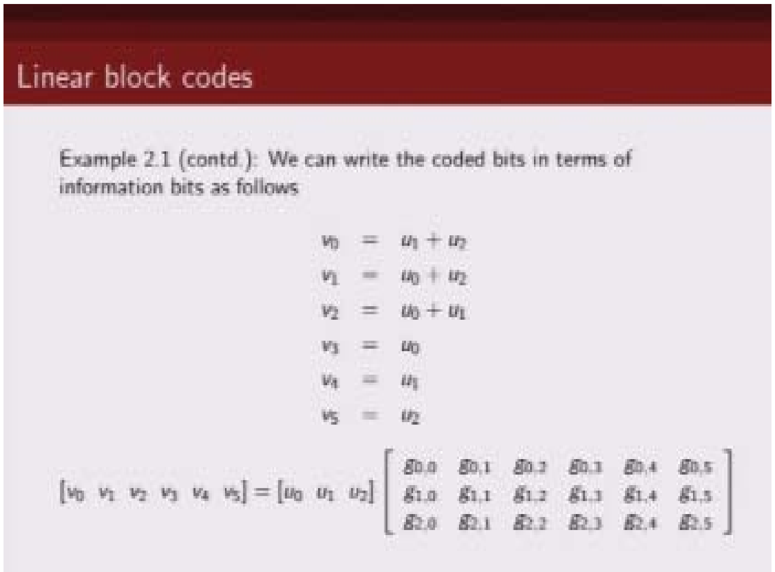
Similarly we noticed that v_3, v_4, v_5 are nothing but information bits u_0, u_1, and u_2 respectively.

(Refer Slide Time: 07:15)



So let us go back, v_3 is this column and we can see this is same as u_0, 01, 01, 01, 01, similarly v_4 is equal to u_1 and v_5 is same as u_2.

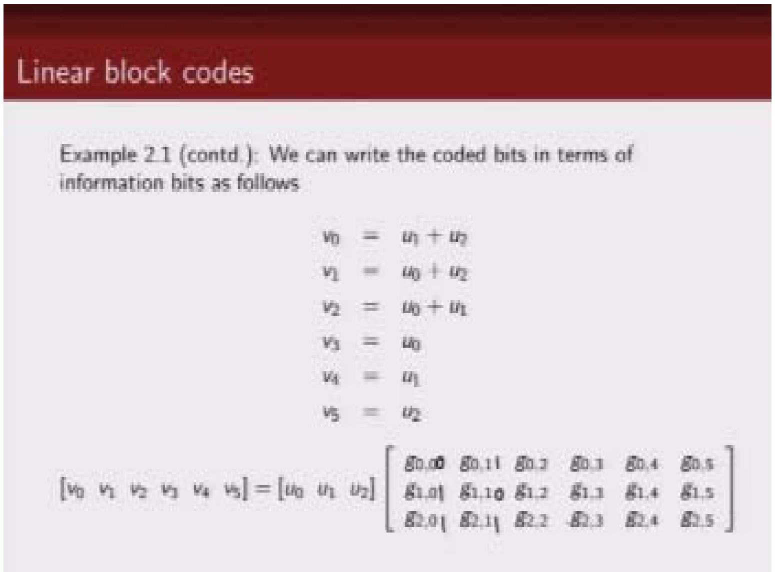
(Refer Slide Time: 07:35)



So now we have written our coded bits in terms of our information bits, this set of six equations I can write it in a matrix form so I can write my coded bits in terms of information bits and this matrix G which is our generator matrix will tell us how are we generating each of these coded bits as a linear combination of these information bits, so if we compare each equation let us look at v_0.

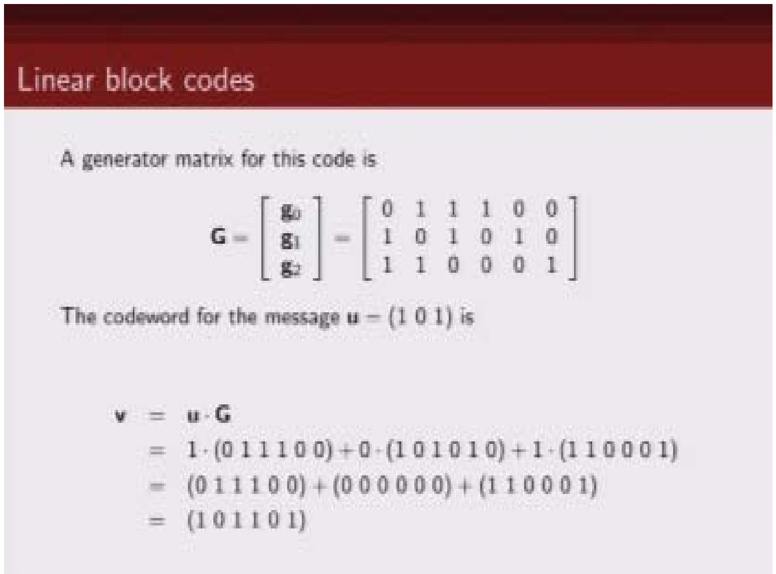
So what is v_0? V_0 is u_0 g_{00}+ u_1 g_{10}+ u_2 g_{20} and what do we see here? v_0 is u_1+u_2 so that means g_{00} is 0 because there is no u_0 term here, g_{10} is 1 because there is a u1 term here and g_{20} is 1 because there is a u_2 term here, so this will be 0, 1, 1.

(Refer Slide Time: 08:51)



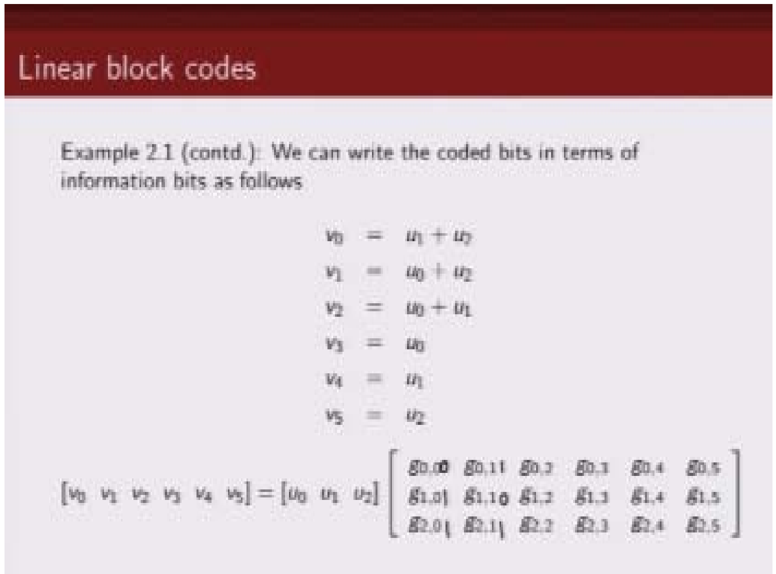
Similarly look at v_1, v_1 is $u_0\, g_{01} + u_1\, g_{11} + u_2\, g_{21}$ and if we compare it with v_1 here we see v_1 is $u_0 + u_2$ that means this g_{01} should be 1, g_{11} should be 0 and this should be 1, likewise we build up the other columns of this matrix.

(Refer Slide Time: 09:31)



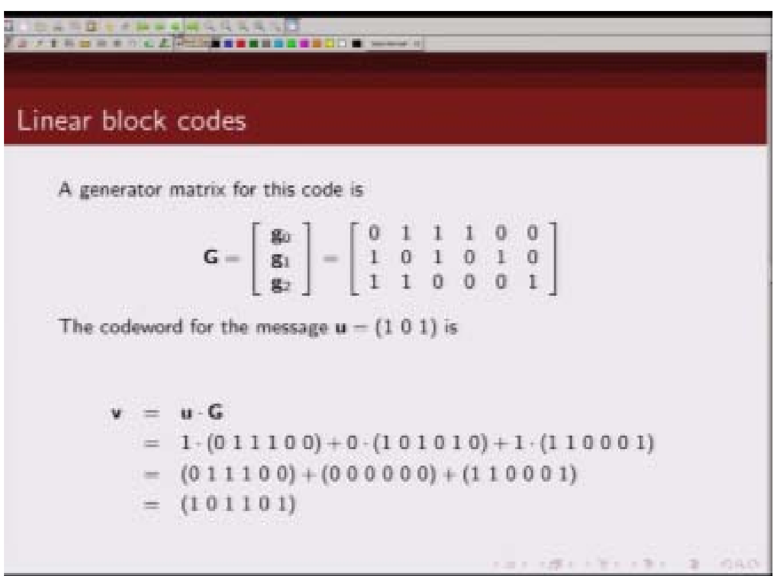
So if we do that what we get is something like this, we can verify basically let us take second last column.

(Refer Slide Time: 09:42)



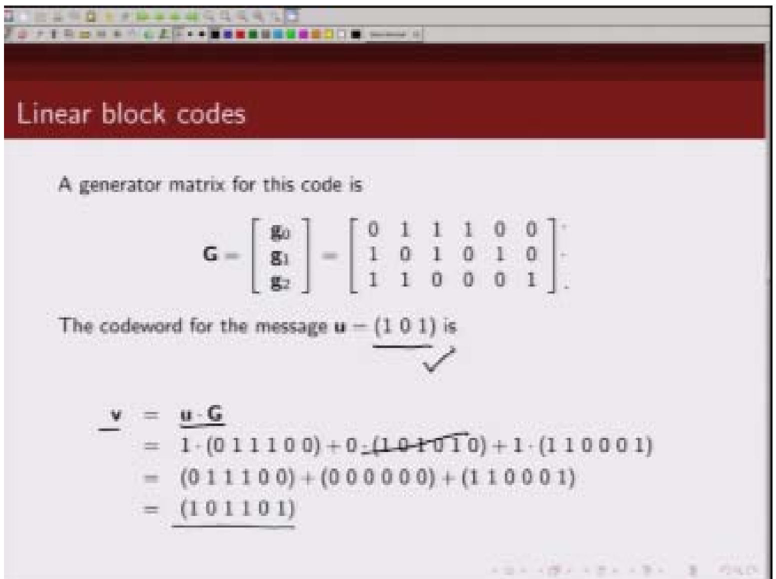
So what is v4? V_4 is u_0 times g_{04} + u_1 times g_{14}+ u_2 times g_{24} and what is v_4? V_4 is u1 so then this should be 1 and this should be 0 and this should be 0 and this is what we have.

(Refer Slide Time: 10:05)



Zero one zero, so now we can basically find out the generator matrix. So a linear block code is completely describe by a, it is generator matrix and as we said we can use the generator matrix to generate our code words for example if my

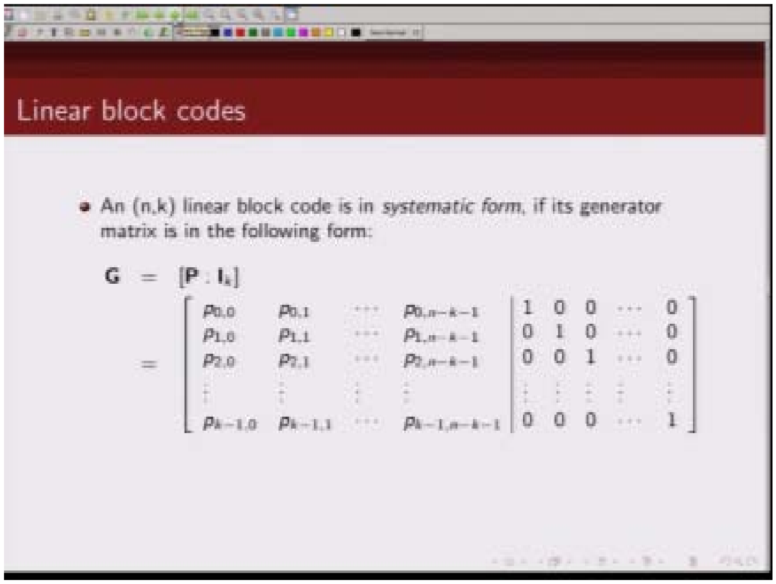
(Refer Slide Time: 10:05)



Information sequence is one zero one, what should be my corresponding coded bits for the information sequence one zero one, how do I find that so as I know my output code word is basically u times G so I will take linear combinations of rows of my generator matrix. What are the rows of my generator matrix, these are the three rows of my generator matrix, so my coded bit corresponding to this information sequence would be one times G zero plus zero times G one plus one times G2.

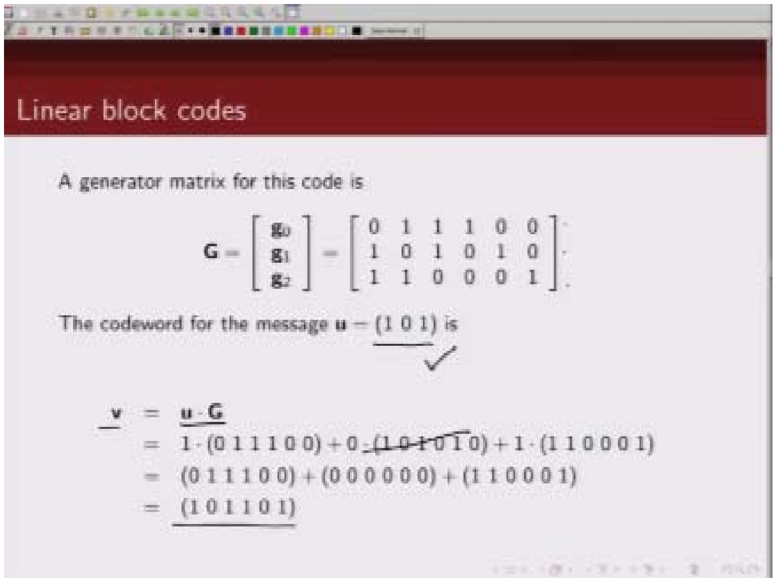
So that is what I have written here this is one times G zero, zero times G one plus one time G2 so this is basically zero, so what I have is then this plus this right, so let us look at 0 plus 1 would be 1, 1+1 would be 0, 1+0 is 1, 1+ 0 is 1, 0 + 0 is 0 and 0 plus 1 is 1, so my code word corresponding to this information message bits information bit is given by 1 0 1, 1 0 1 okay.

(Refer Slide Time: 11:56)



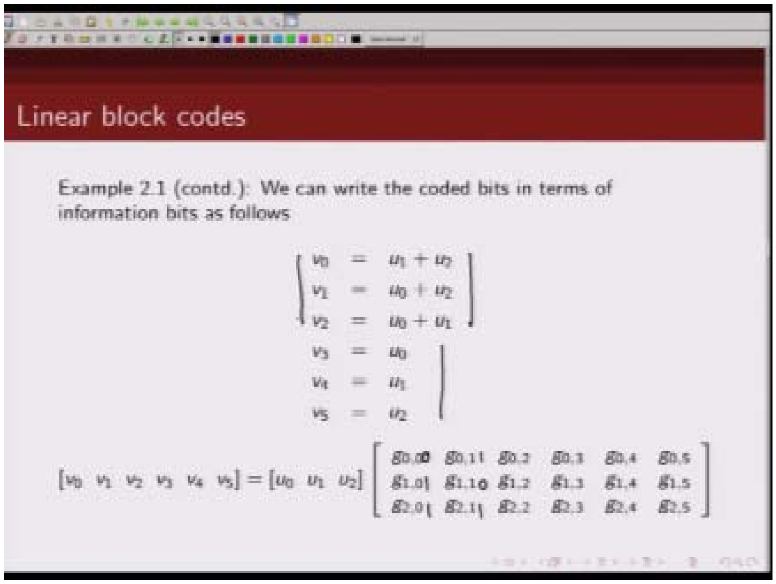
Now what do we mean by a linear code in systematic form? Now if we are able to, among the coded bits if we are able to separate them out into, if the message bits appear directly in the coded bits sequence then we can separate out the message bits from the parity bits, for example.

(Refer Slide Time: 12:24)



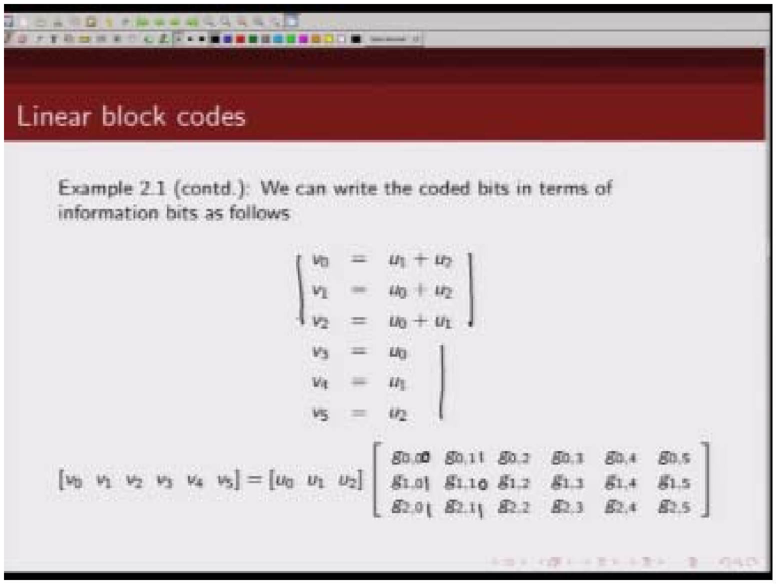
Go back to this example.

(Refer Slide Time: 12:25)



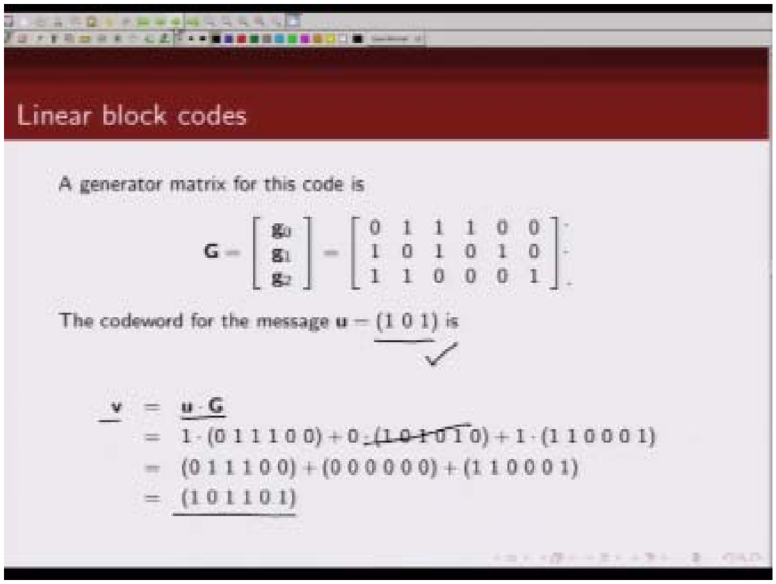
What do we have here, we have 3 of these coded bits exactly same as information bits and the other 3 bits parity bits are linear combination of this message bits, so from the output code word we, we can clearly separate out the information sequence which is in this case we given by V3, V4 and V5 so in this case V1, V2, V3 are these N – K parity bits.

(Refer Slide Time: 13:05)

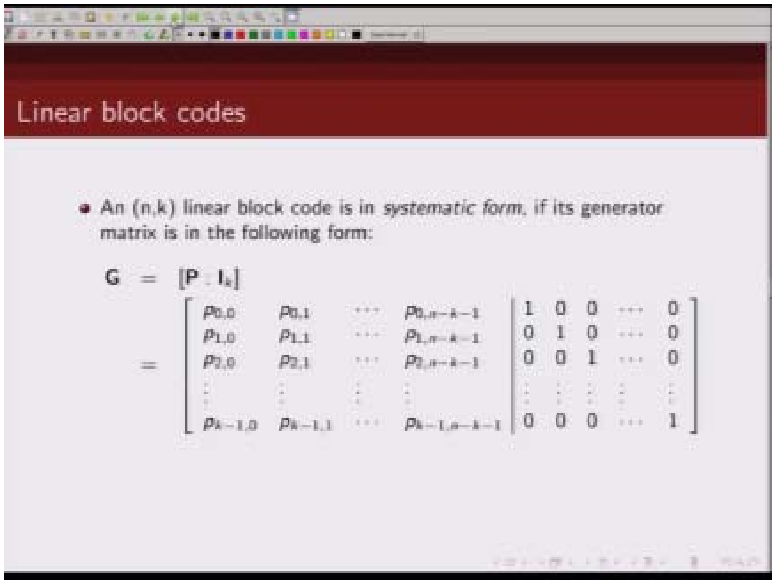


And V3, V4 , V5 are my information bit, so in this particular example we can see that we are able to separate out information bits directly from the coded bits, so in a systematic, a block

(Refer Slide Time: 13:20)

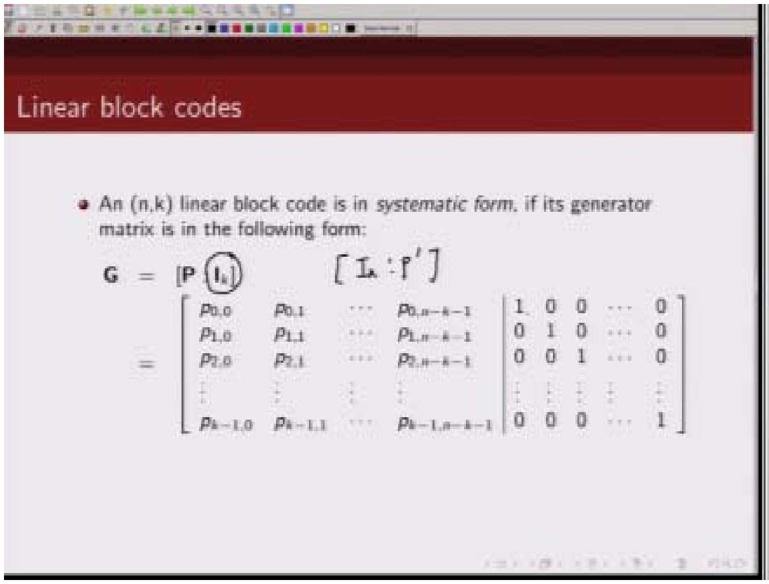


(Refer Slide Time: 13:21)



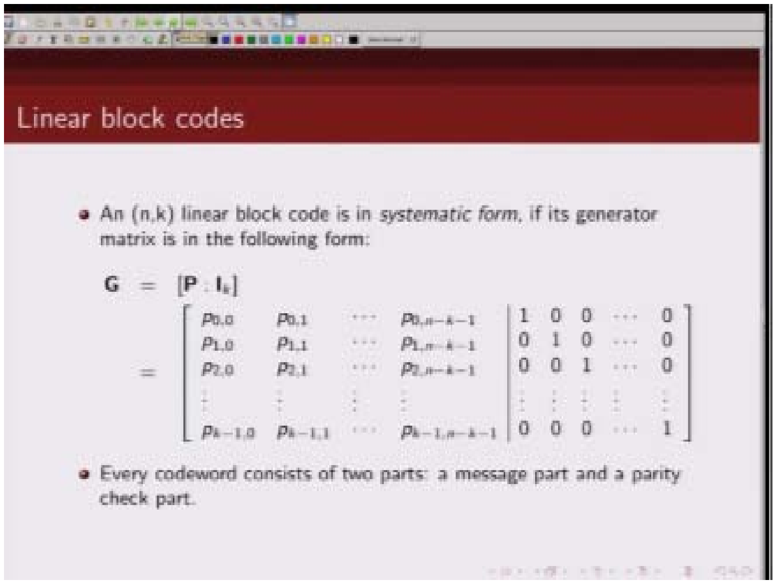
Code in a systematic form we are able to separate out the information bit part from the coded bits, so a generator

(Refer Slide Time: 13:33)



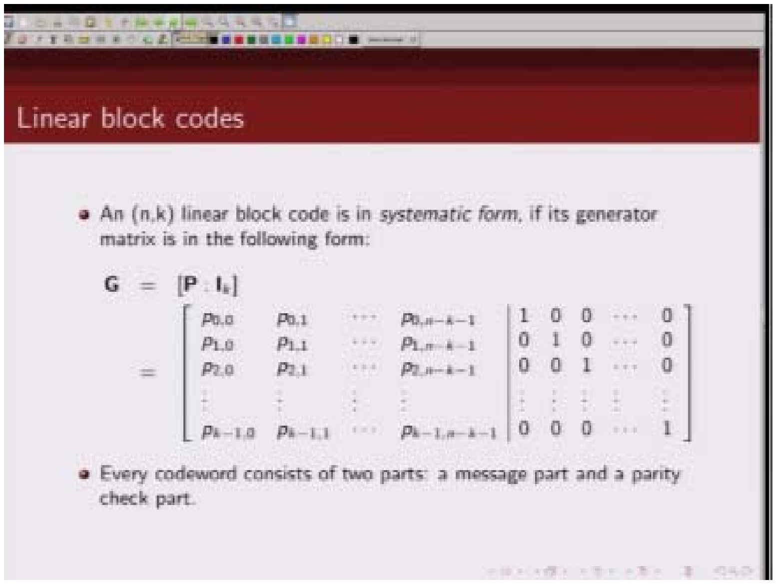
Matrix for a linear block code in systematic form will be of the form like this or it would be basically I times I K times something of this, either of this one, now why do we say that? So only when we have our a part of our generator matrix of the form of identity then what is going to happen, when we multiply our information sequence with this sort of generator matrix you will see

(Refer Slide Time: 14:13)



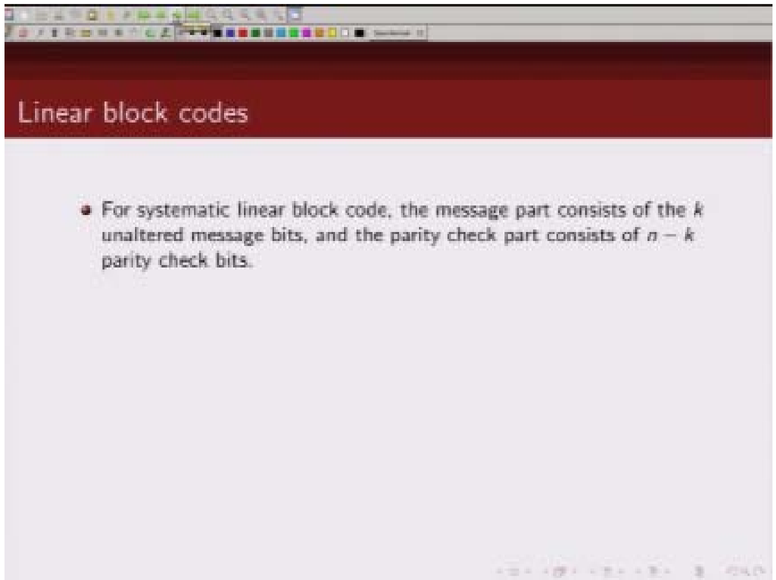
Part of my coded bits will just depend on one particular information bit sequence, so if I write down the corresponding equations for coded sequence what you will see that some coded bits directly depend on the message bits and then rest R which are parity bits are linear combination of these message bits.

(Refer Slide Time: 14:46)



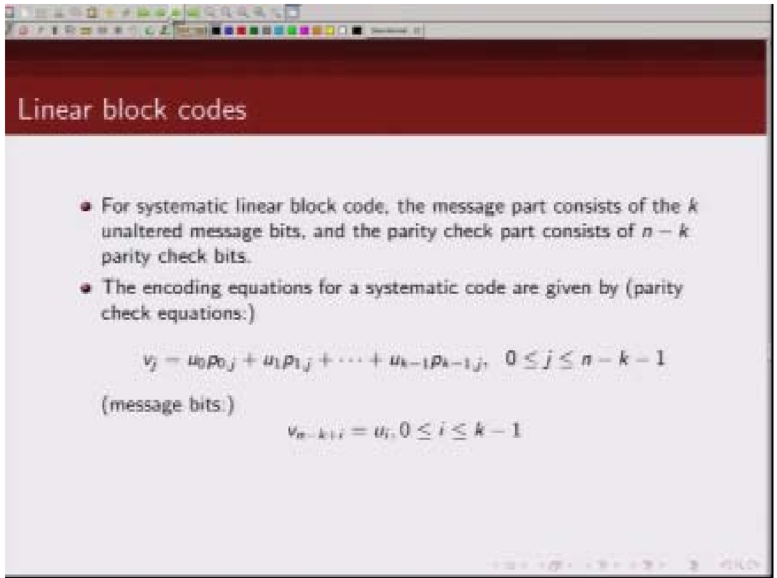
So in a systematic form basically we can separate out the message part from the parity bit part, so as I said

(Refer Slide Time: 14:49)



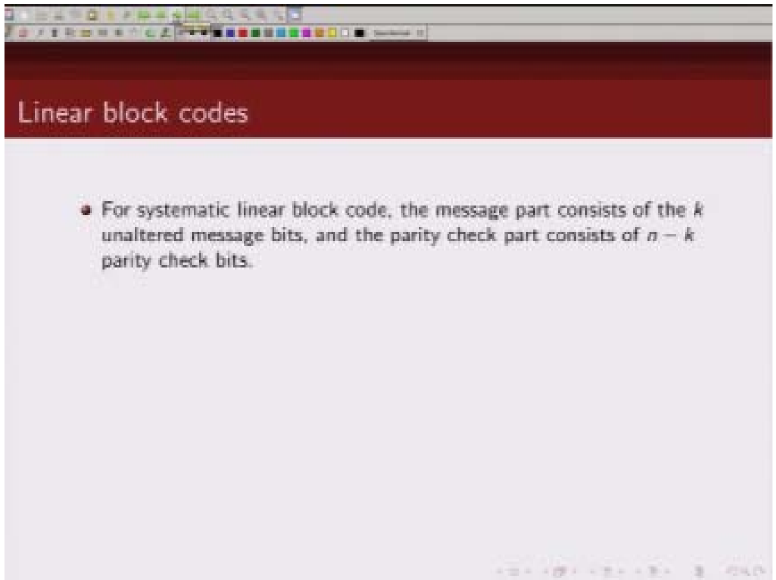
For a systematic linear block codes the message part will consist of the K information bits and the remaining N – K bits which are

(Refer Slide Time: 15:09)

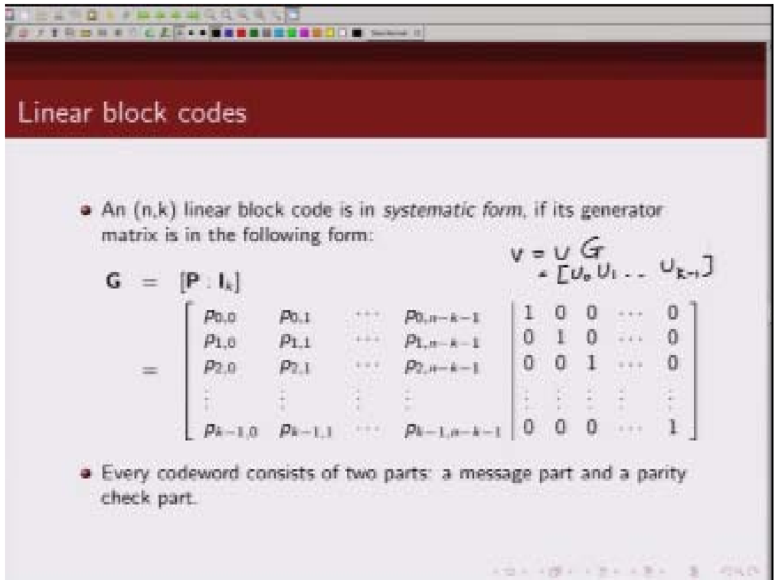


The parity bits basically they will be linear combination of these message bits, so we can write down the encoding equations for these matrix's for these, for systematic code. So if you look at what is our encoding equation, our V is U times G where G is a form like this, okay.

(Refer Slide Time: 15:23)

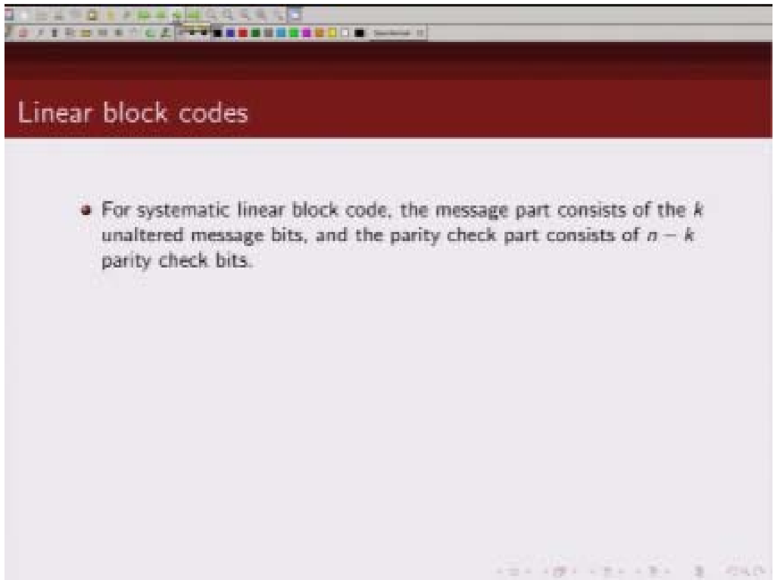


(Refer Slide Time: 15:25)



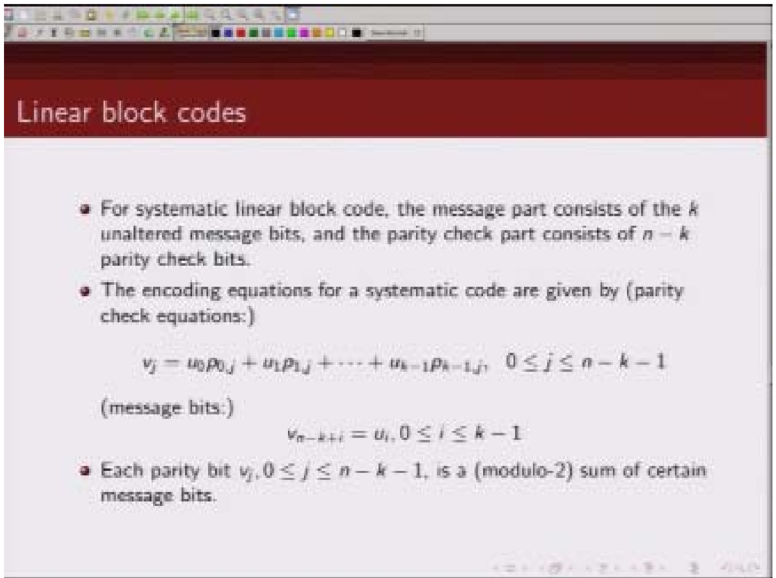
So if we write U which is basically U (0) U (1), UK – 1 times this G matrix what we will get.

(Refer Slide Time: 15: 50)



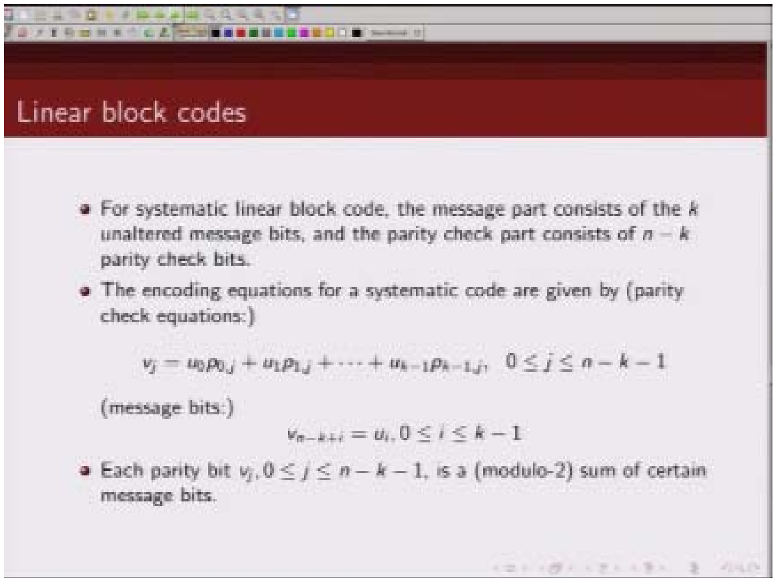
Is a form.

(Refer Slide Time: 15: 51)



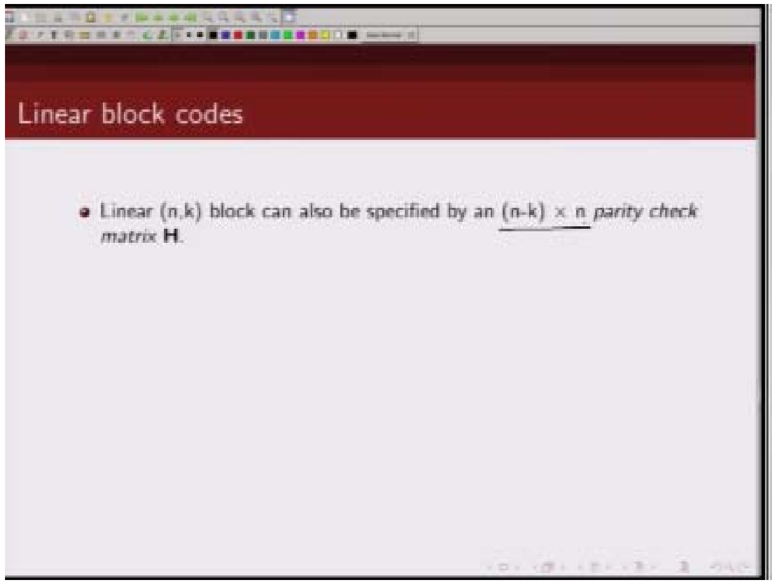
Like this so you will have N- K parity equations, parity check equations which are given by this expression and then you will have remaining K unaltered message bit, so for a linear block code in a systematic form the encoding equations will be of this form, and as I said since we are restricting ourselves without any loss of generality to binary code words this addition is basically.

(Refer Slide Time: 16: 26)



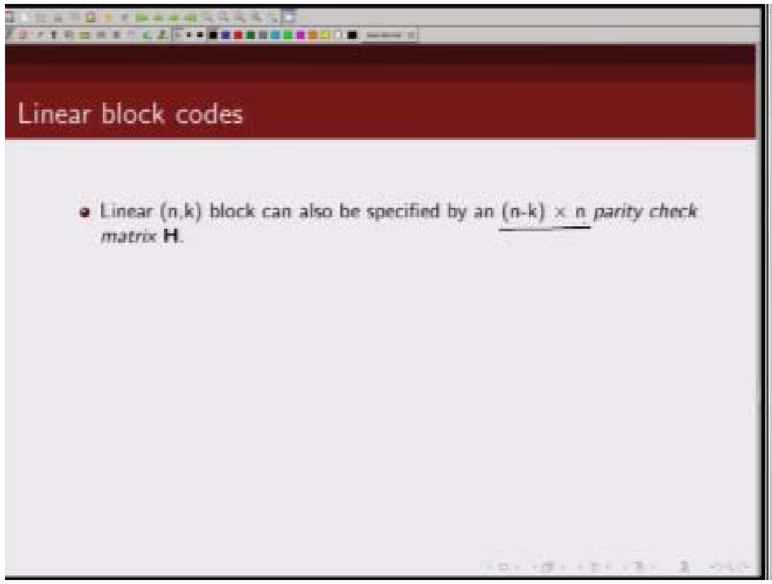
Done modulo-2, so what we have seen so far is we can describe a linear block code by its generator matrix which is a K cross end matrix, and we can use this generator matrix to generate our set of code words. Now there is another matrix which we call parity check matrix which is related to our generator matrix we will show which can also be used to completely describe a linear block code, so for a NK linear block.

(Refer Slide Time: 17: 07)

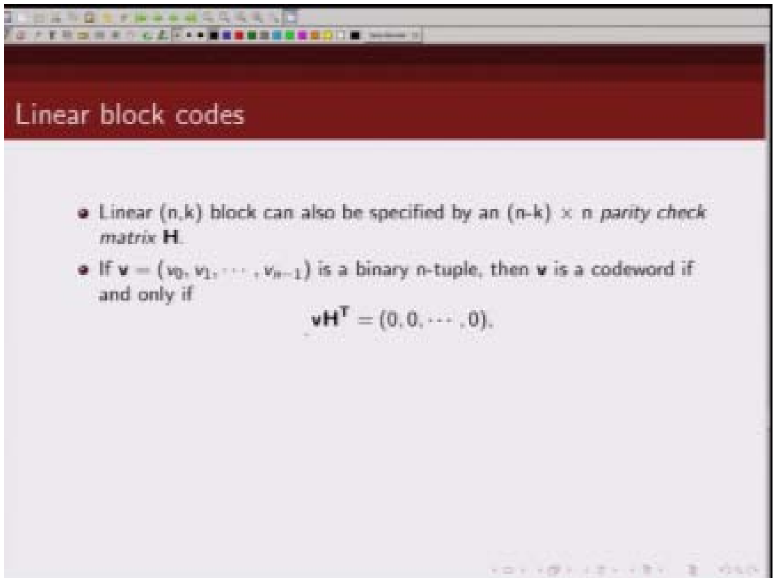


Code can be specified by a N- K x n parity check matrix which we denote by G, H the generator matrix we denote by G and the parity check matrix we denote by H.

(Refer Slide Time: 17: 24)

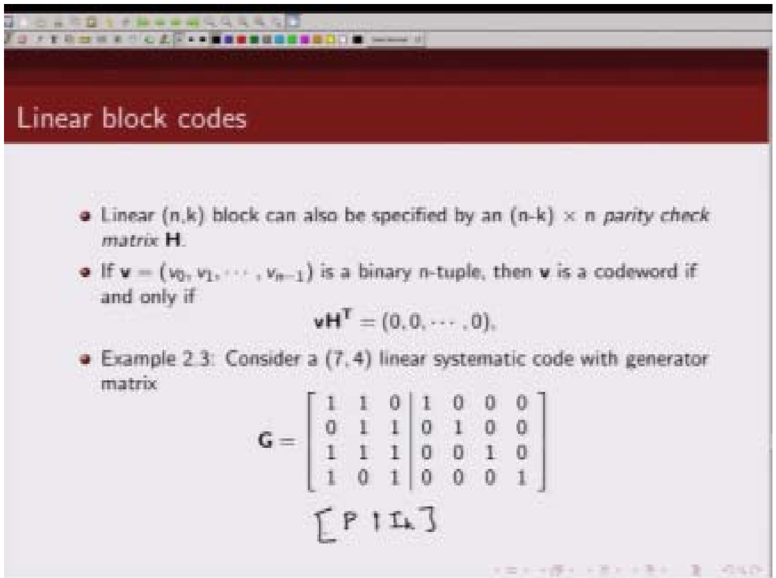


(Refer Slide Time: 17: 25)



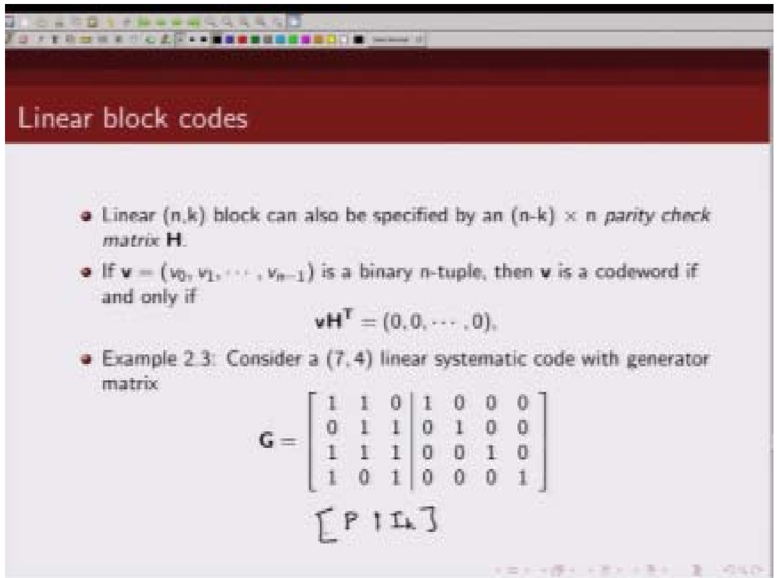
Now this parity check matrix has this property that if V is your valid code word, if and only if VH transpose is going to be zero, so if V is a valid code word V^H transpose will be zero so let us see how we can derive our parity check matrix.

(Refer Slide Time: 17: 50)

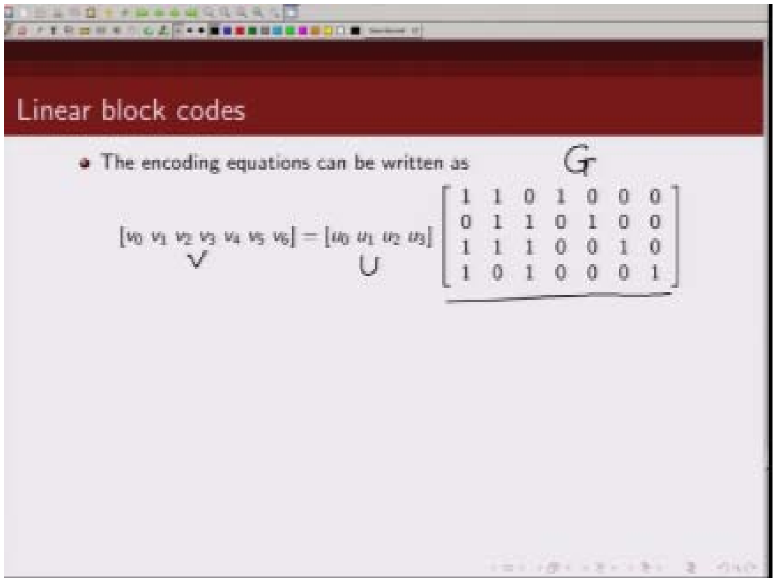


From a generator matrix and what is the relation of the generator matrix with parity check matrix. So we will take an example of a 7, 4 systematic linear block code whose generator matrix is given by this so since this is a systematic code we can write it of the form E times this I_K this generator matrix can be written of this form okay. Now from this generator equation we can write our coded bits in terms of our message bits so let us do that.

(Refer Slide Time: 18: 34)

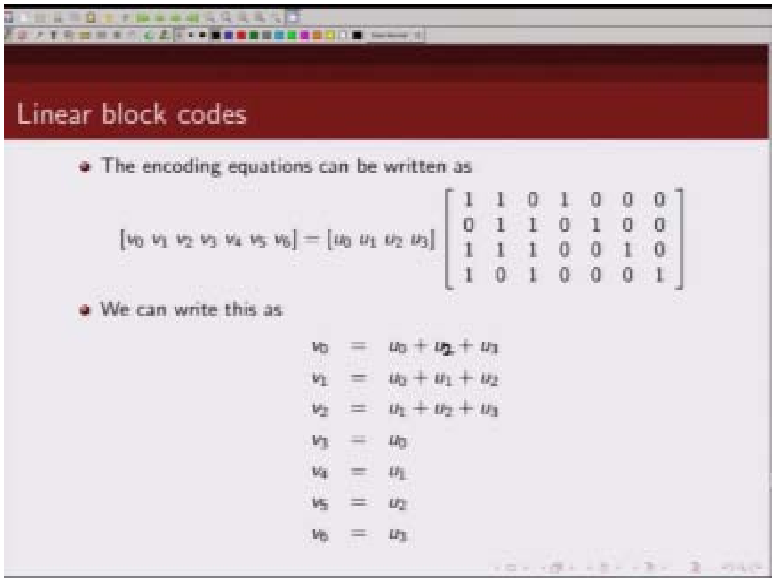


(Refer Slide Time: 18: 36)



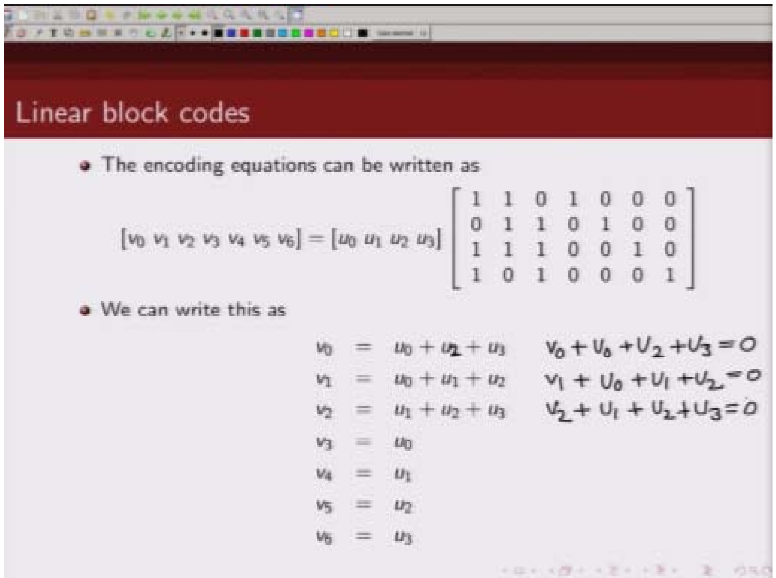
So the encoding equation says this one was our generator matrix G, this is our information bits message bits U and this is our coded bits V, so we can write V as U times G, so it is a 7, 4 code so there are 4 information bits, I denote them by U_0, U_1, U_2, U_3 and there are 7 coded bits I denote them by V_0, V_1, V_2 to V_6 and this generator matrix I have already given you this so I can write down the encoding equations.

(Refer Slide Time: 19: 14)



We do that, you can see from this what is v_0 it is $u_0+u_2+u_3$, there is a typing mistake here this would have been u_2, so v_0 is u_0 times 1 plus 0 times u_1+ 1 times u_2 + 1 times u_3 so this V_0 is given by u_0+ u_2 +u_3. Similarly what is v_1, v_1 is given by $u_0+u_1+u_2$, v_2 is given by u_1 u_0x0, u_1x1, u_2+u_2x1+u_3x1. So v2 is given by $u_1+u_2+u_3$, so that is what I have here. What is v3, v3 is given by u0x1 and rest are all 0, so v_3 is nothing but u_0. Similarly v_4 is u_1, v_5 is u_2 and v_6 is u_3. So I now have set of seven coded bits and this shows the relation between the coded bits and information bits. Now we are since we are restricting ourselves to binary code.

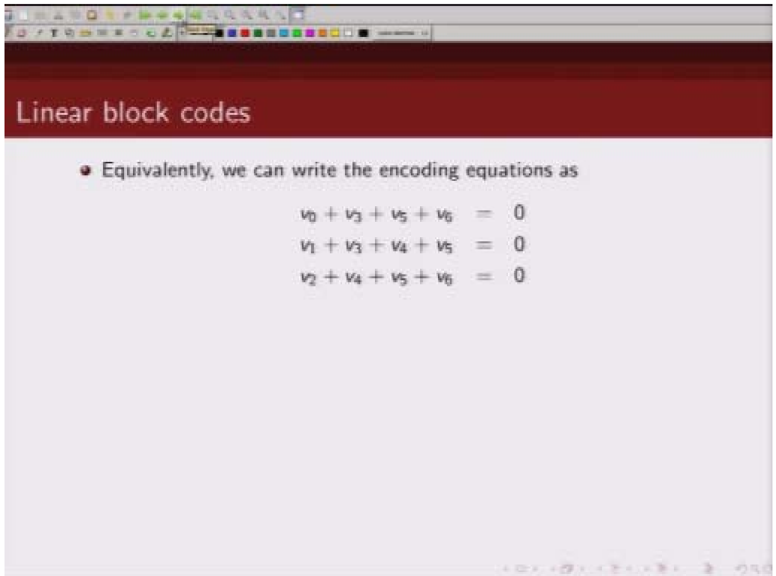
(Refer Slide Time: 20:57)



We can even write this equation like this, $v_0+u_0+u_2+u_3 = 0$, correct? Because this v_0 v_1 is nothing but parity bit which is basically like 1 or 0 so if we add this to this modulo 2 sum will be 0. So this similarly we can write as $v_1+u_0+u_1+u_2=0$ and this can be written as $v_2+u_1+u_2+u_3=0$. The next what we would try to do is we would try to write these parity check equations in terms of other coded bits. So we can see here, u_0 is nothing but v_3 so wherever u_0 appears we can replace it by v_3.

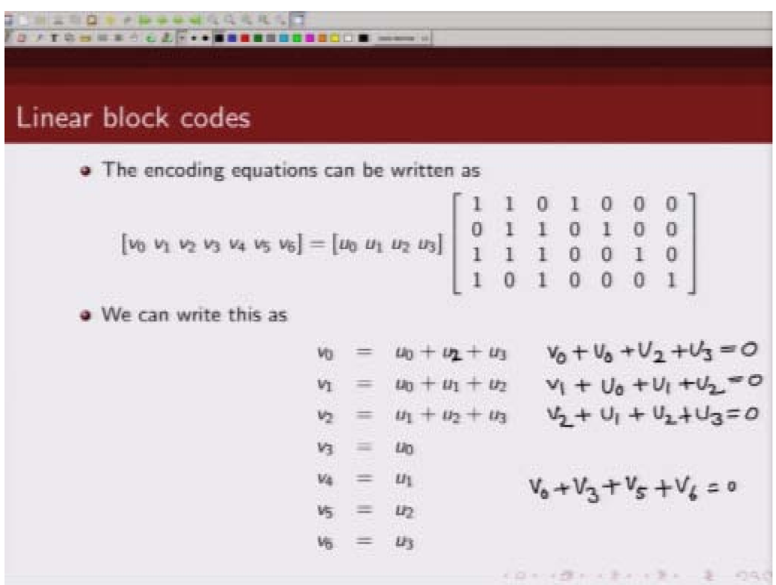
Similarly, u_1 is equal to v_4 so wherever u_1 appears we can replace it by v_4, u_2 is equal to v_5 so we can replace u_2 by v_5 and u_3 is equal to v_6 we can replace u_3 in terms of v_6. By doing this what we will get is set of equations which basically are dependent on these coded bits. So if we do that.

(Refer Slide Time: 22:44)



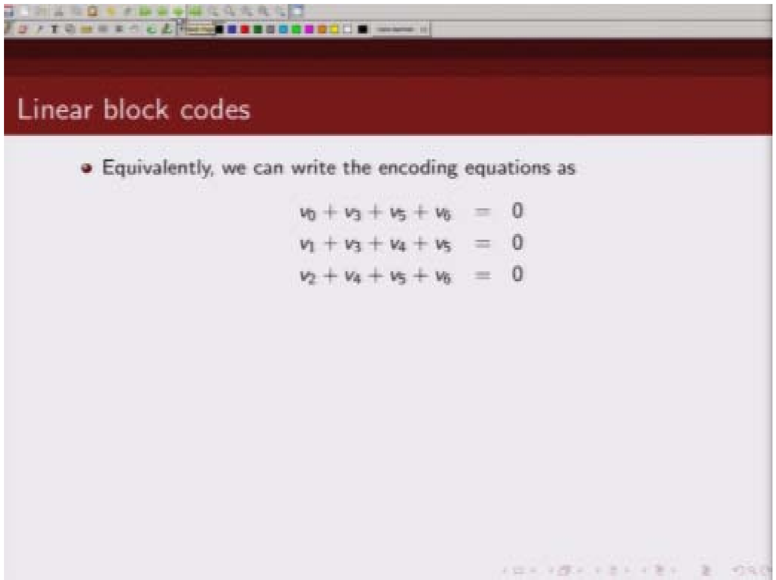
What we get is something like this. The first equation basically which was.

(Refer Slide Time: 22:51)



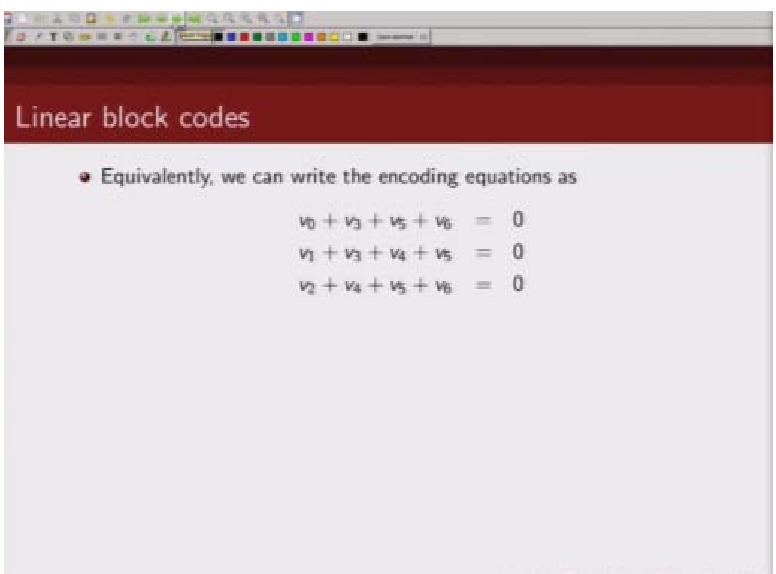
$v_0+u_0+u_2+u_3$, now this can be re-written as v_0+ what is u_0, u_0 is v_3, v_3+ what is u_2, u_2 is v_5, v_5+ what is u_3 it is v_6 so $v_0+v_3+v_5+v_6=0$ and that is what we have here.

(Refer Slide Time: 23:22)

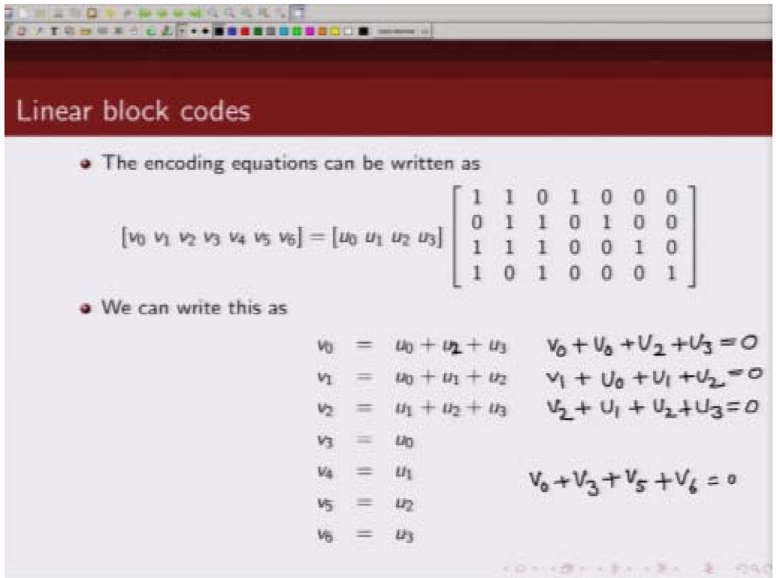


$v_0+v_3+v_5+v_6=0$.

(Refer Slide Time: 23:31)

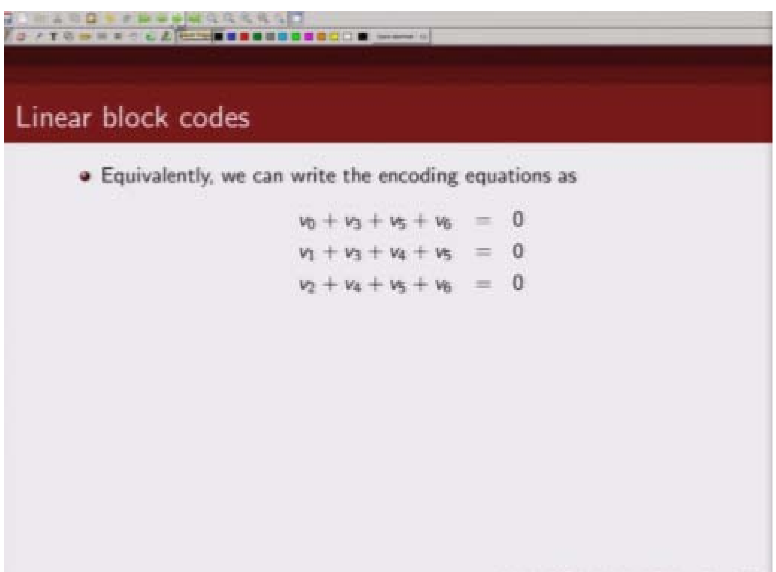


(Refer Slide Time: 23:32)



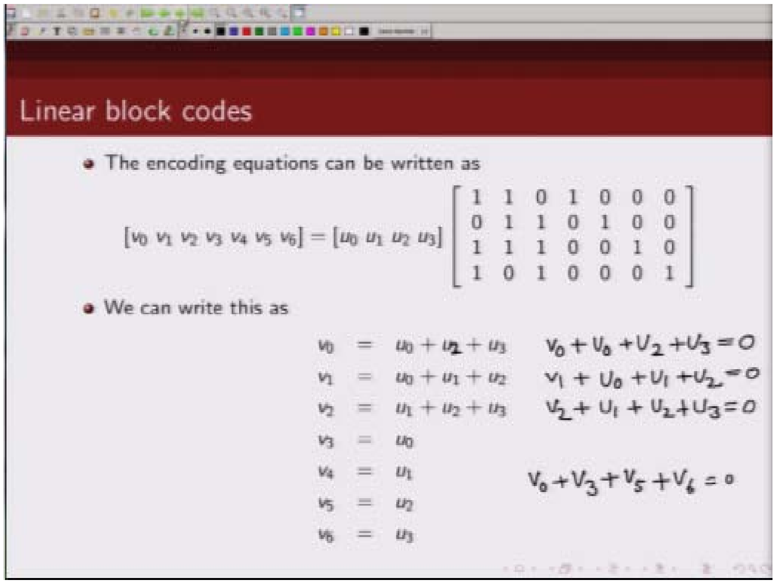
Similarly we can write the other equations as well, here also we will replace u_0, u_1, u_2 by v_3, v_4, v_5 and what we will get is.

(Refer Slide Time: 23:43)



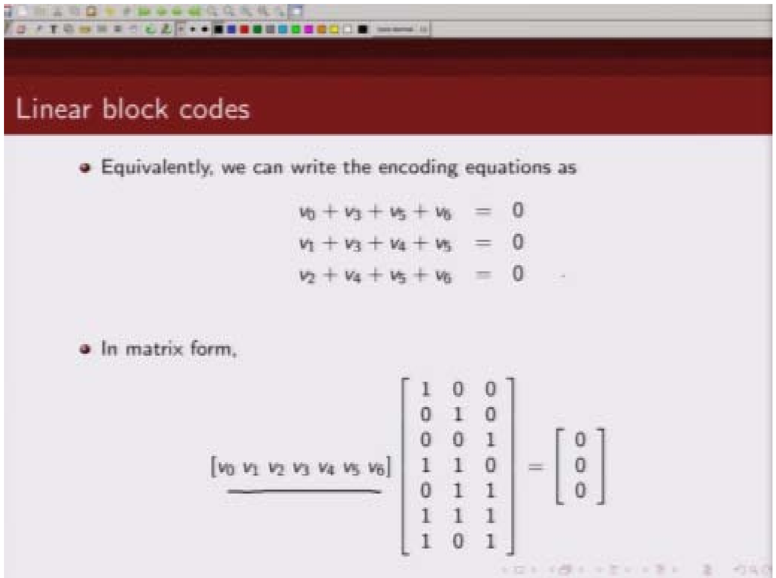
$v_1+v_3+v_4+v_5=0$ and similarly the last parity check equation can be written as.

(Refer Slide Time: 23:55)



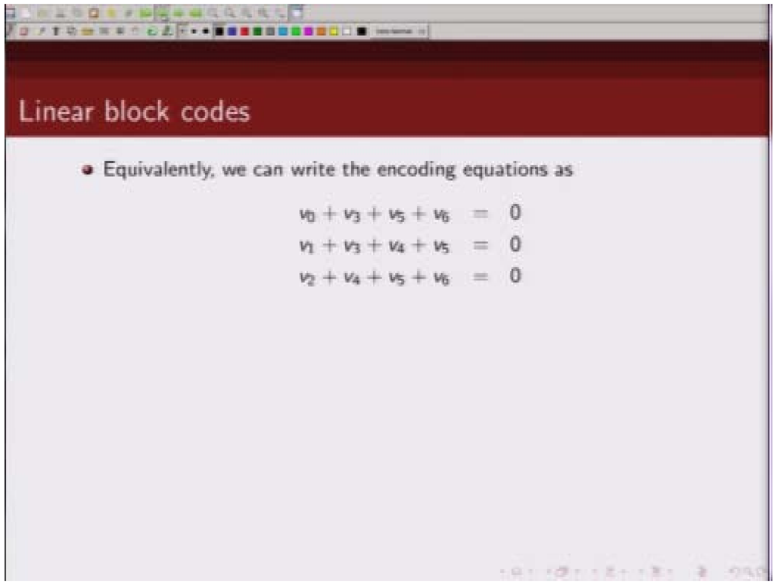
v_2+u_1 is v_4+u_2 is v_5+u_3 is v_6, so that is what we have here.

(Refer Slide Time: 24:04)

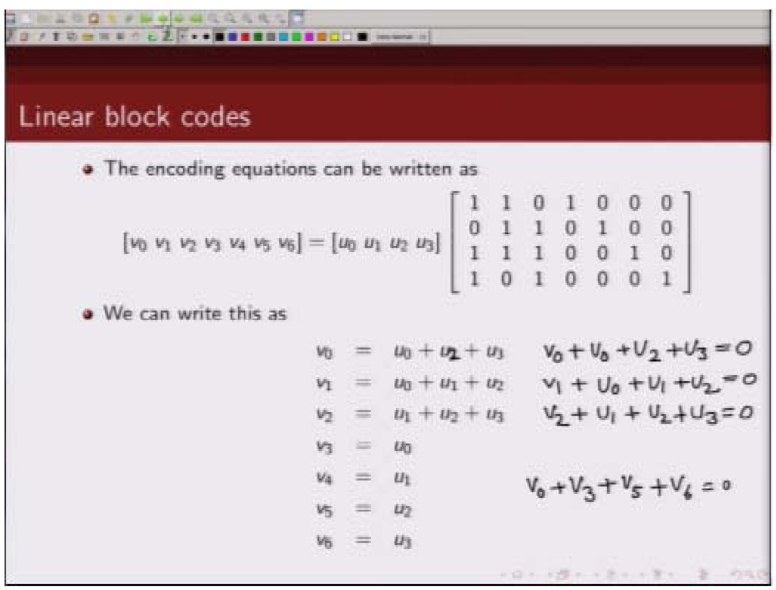


u_2 $v_2+v_4+v_5+v_6=0$. So now we have set of encoding equations in terms of coded bits. Next the same thing we can write it in a matrix form, so I have my coded bits v_0 to v_6, I have three sets of parity check equations this, this and this. And the same thing I can write it in a matrix form like this. Now you can see these are equivalent so look. Let us look at first equation, this is $v_0+v_3+v_5+v_6 = 0$. So you can see which are the elements which are, so v_0 times 1, this is v_3 times $1+v_5$ times 1 $+v_6$ times 1. So that is what define this equation. Similarly you can see this equation, this $v_1+v_3+v_4+v_5=0$ and this last equation this is $v_2+v_4+v_5+v_6=0$. And what did we say

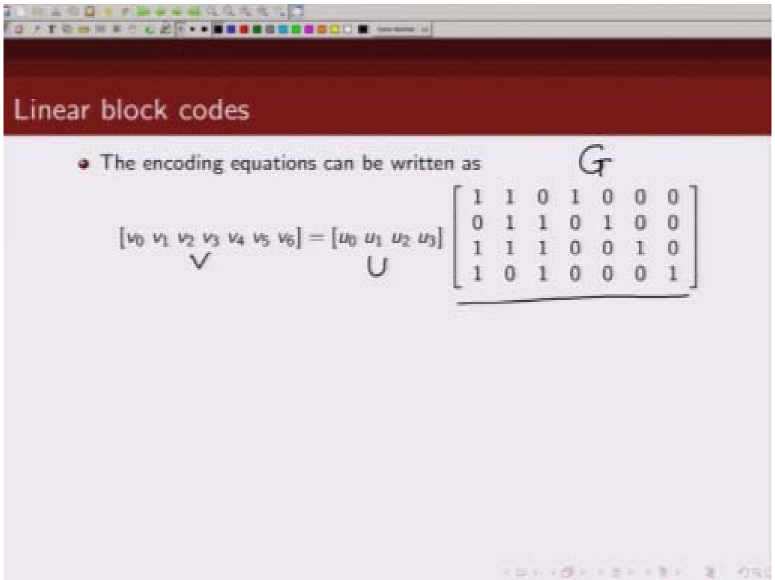
(Refer Slide Time: 25:22)



(Refer Slide Time: 25:23)

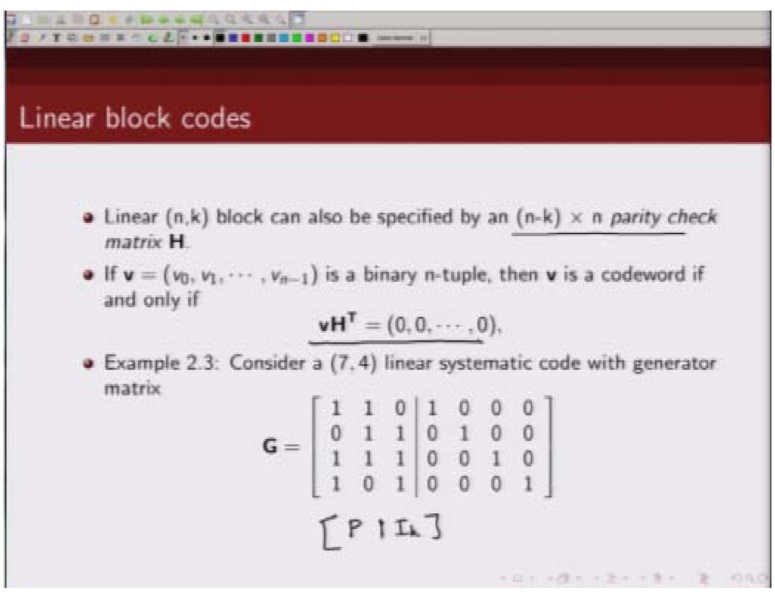


(Refer Slide Time: 25:24)



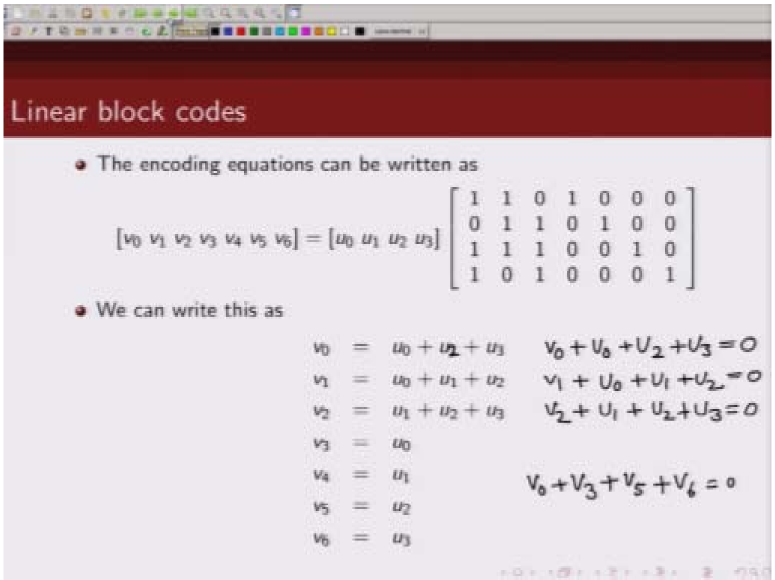
About parity check matrix.

(Refer Slide Time: 25:25)



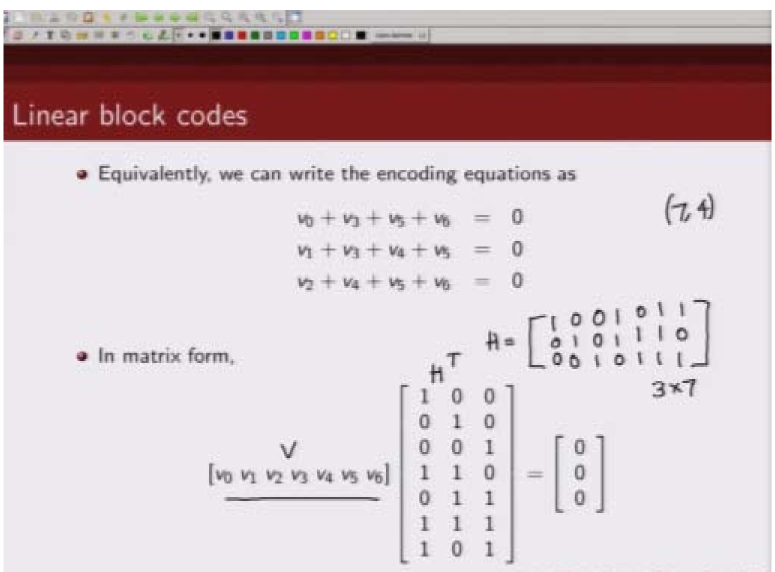
We said that if H is a parity check matrix it is an (n-k) x n matrix and it has this property that vH^T is 0.

(Refer Slide Time: 25:41)



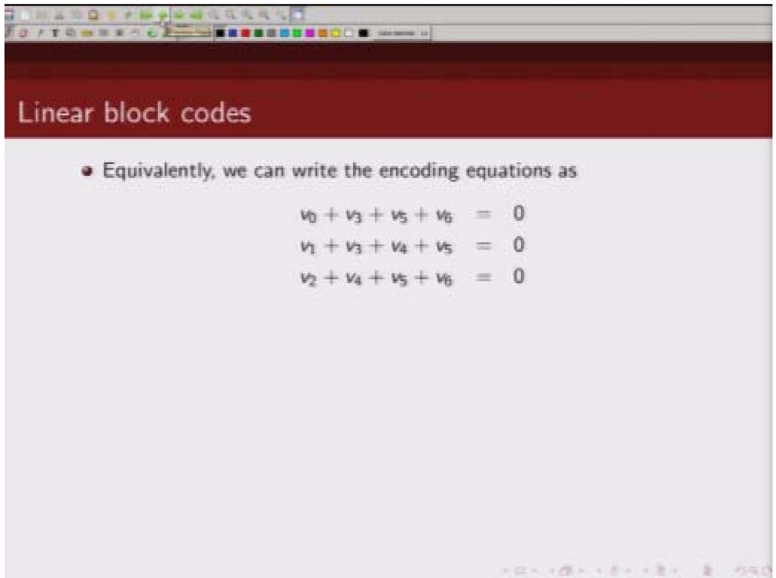
So we have.

(Refer Slide Time: 25:43)



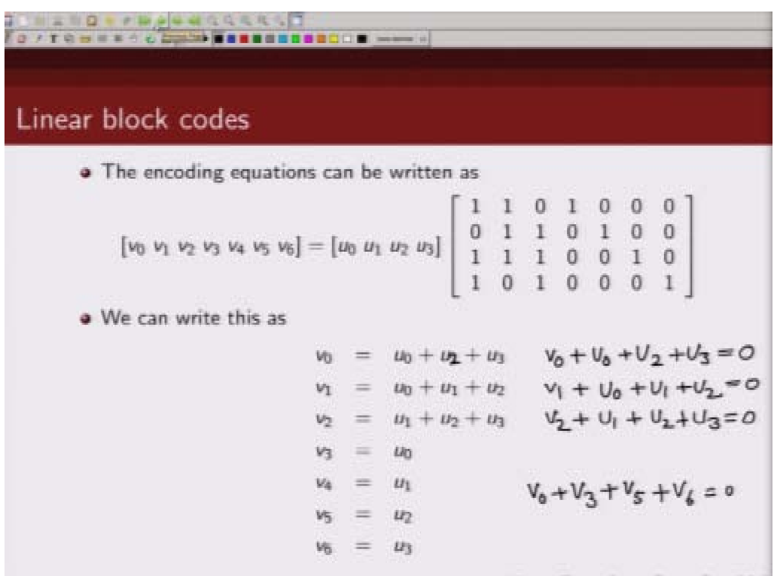
Can write this as, this is my v, this is my H^T vH^T is 0. So then what is my H matrix, H matrix is a transpose of this matrix so this will be 100 010 001 110 011 111 and 101 and this is my, so for the (7, 4) code (7, 4) code this is basically 3x7, as I said (n-k) x n matrix this is my parity check matrix corresponding to this same code.

(Refer Slide Time: 26:32)

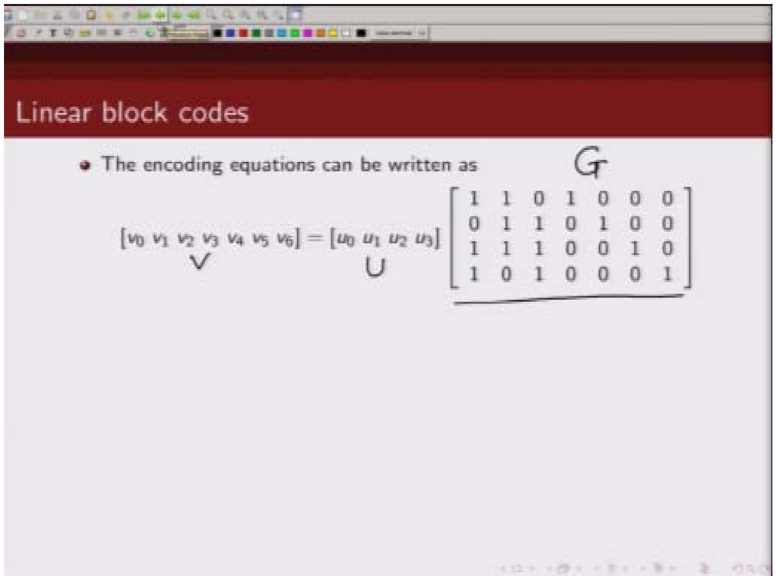


Which is generated by this

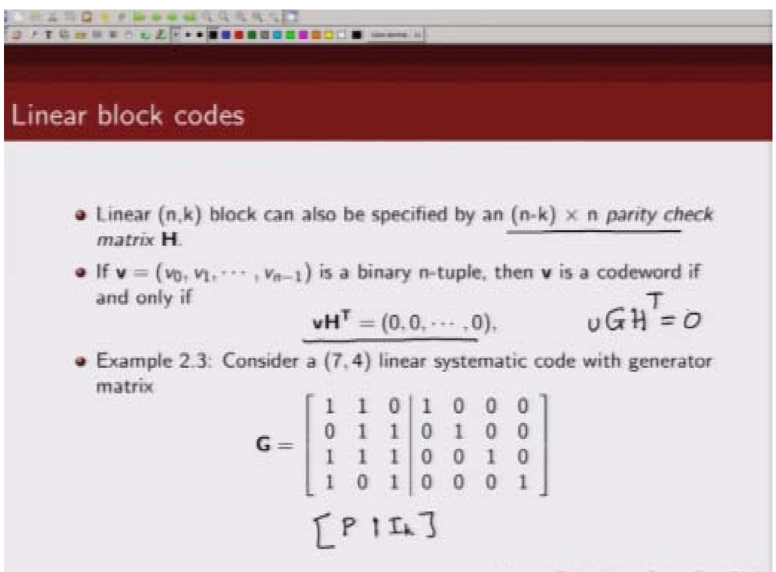
(Refer Slide Time: 26:34)



(Refer Slide Time: 26:36)

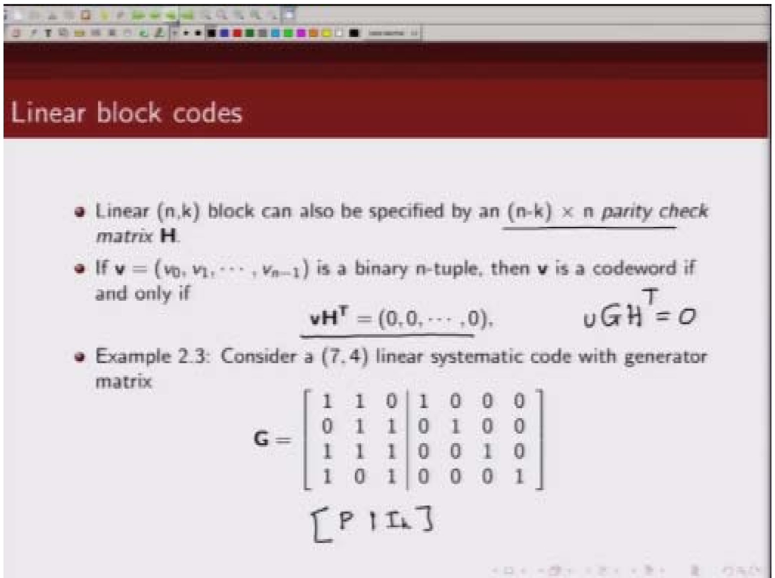


(Refer Slide Time: 26:38)

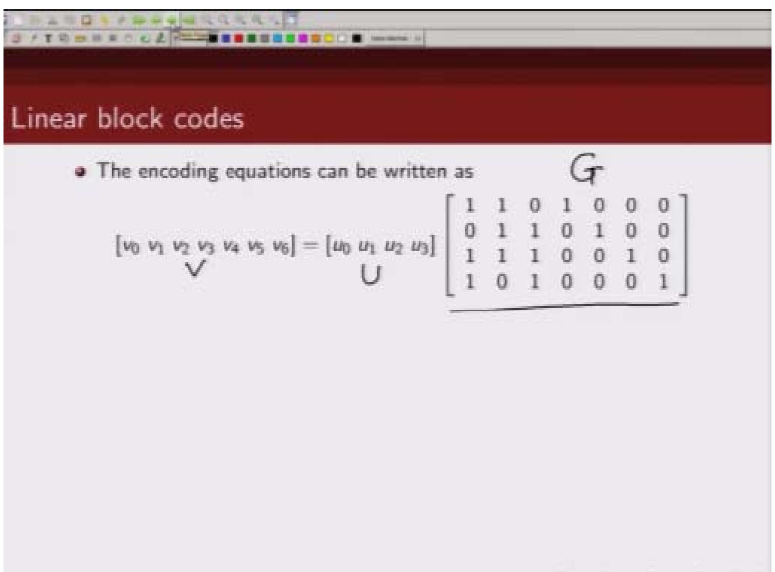


Another interesting property that you can basically see is so vH^T is 0, I can write this is u $GH^T = 0$. In other words vH^T is 0 so what does that mean, the rows of G matrix and rows of H matrix are orthogonal to each other.

(Refer Slide Time: 27:03)

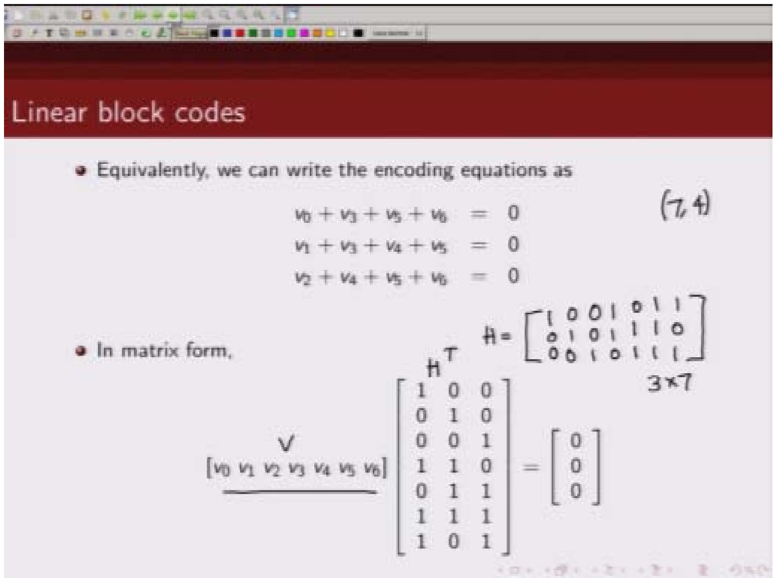


(Refer Slide Time: 27:03)



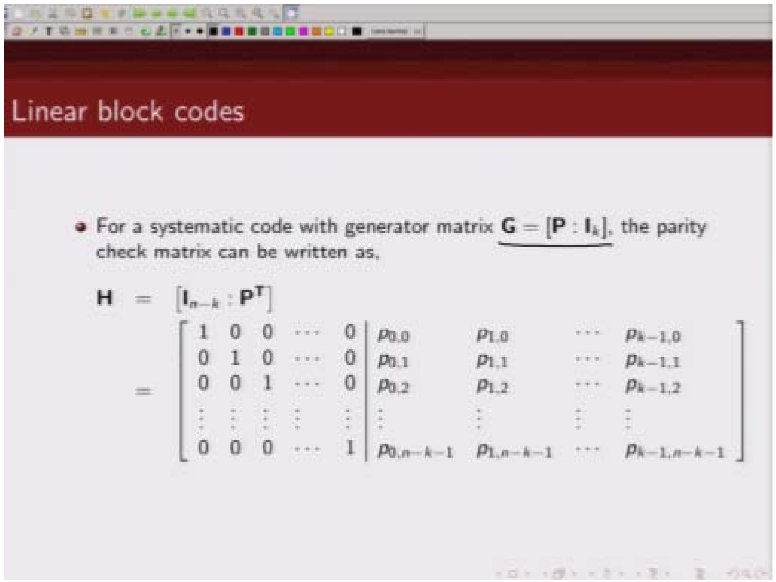
So the H lies in the null space of G.

(Refer Slide Time: 27:08)



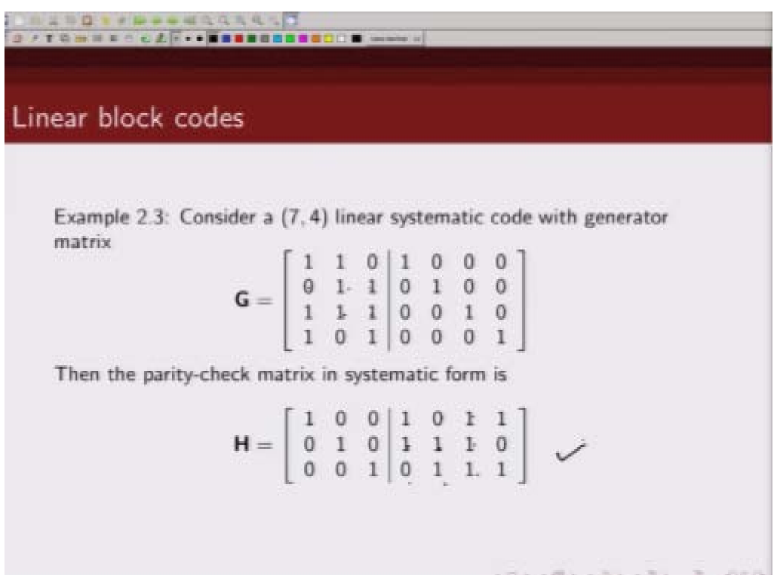
So as we can see from this that generator matrix and parity check matrix are related to each other and they have this property that rows of G matrix and H matrix are basically orthogonal to each other.

(Refer Slide Time: 27:27)



So if you have a systematic code whose generator matrix can be written in this form because the H lies in the null space of G we can write down its corresponding H matrix very easily and this is basically given by, so if a generator matrix can be written of the form Pn identity matrix we can write its parity check matrix as identity matrix and P^T.

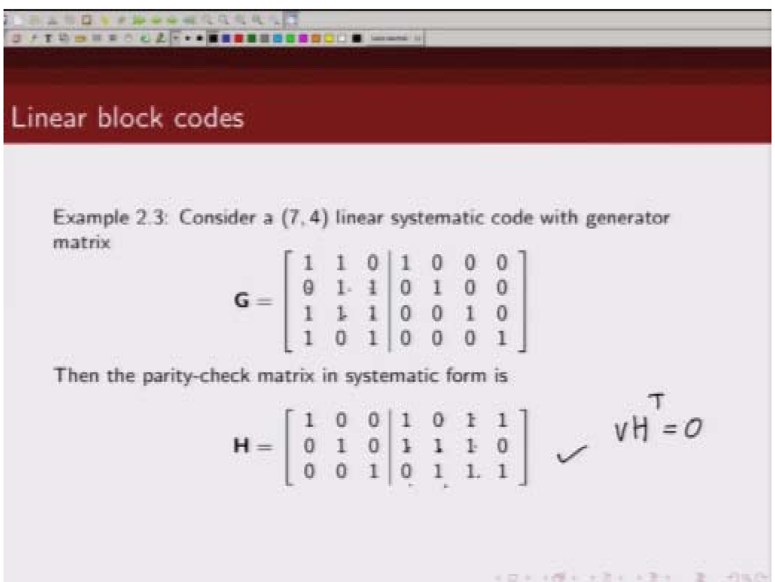
(Refer Slide Time: 27:58)



So let us take an example of a generator matrix for a systematic code, this is systematic code we can see, we can separate out this generator matrix as some matrix P and some identity matrix. So this we can write as the H matrix we can write as identity matrix and P^T. So then this can be written as 110 is 110, 011, 011, 111, 111, 010, so this is my H matrix corresponding to this. So whether you are given a generator matrix or a parity check matrix your linear block code is completely specified by either of them.

And as I said we use the generator matrix we generate our code set of code words whereas parity check matrix as the name suggest is used to check whether the parity check constraints are satisfied.

(Refer Slide Time: 28:58)



As we said basically parity check matrix has this property that is if v is a valid code word if and only if vH^T is 0. And we use this property in decoding and that is why you see the name parity check matrix because this matrix H is essentially used to in some sense check whether the parity check constraints of the code are satisfied or not. Thank you.

Acknowledgement
Ministry of Human Resource & Development

Prof. Satyaki Roy
Co-ordinator, NPTEL IIT Kanpur

NPTEL Team
Sanjay Pal
Ashish Singh
Badal Pradhan
Tapobrata Das
Ram Chandra
Dilip Tripathi
Manoj Shrivastava
Padam Shukla
Sanjay Mishra
Shubham Rawat
Shikha Gupta
K. K. Mishra
Aradhana Singh
Sweta
Ashutosh Gairola
Dilip Katiyar
Sharwan
Hari Ram
Bhadra Rao
Puneet Kumar Bajpai
Lalty Dutta
Ajay Kanaujia
Shivendra Kumar Tiwari

an IIT Kanpur Production

©copyright reserved