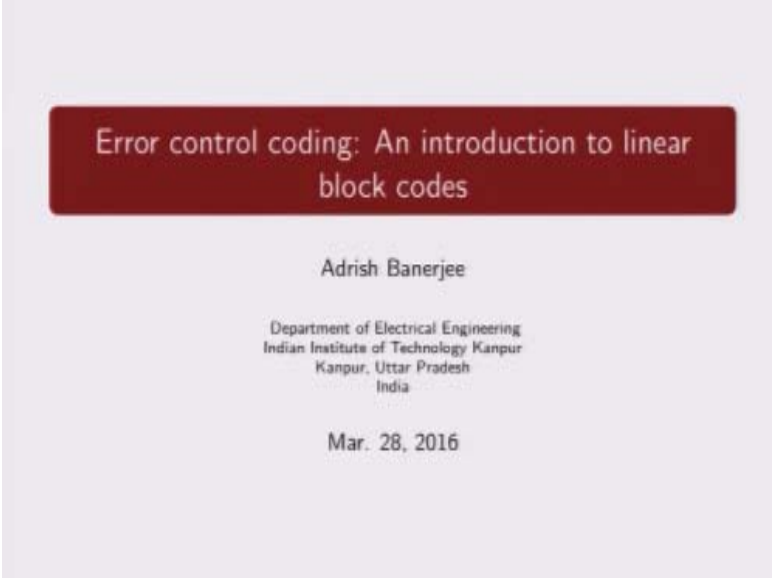
Indian Institute of Technology Kanpur
National Programme on Technology Enhanced Learning (NPTEL)
Course Title
Error Control Coding: An Introduction to Linear Block Codes

Lecture – 7B
Problems Solving Session – III

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

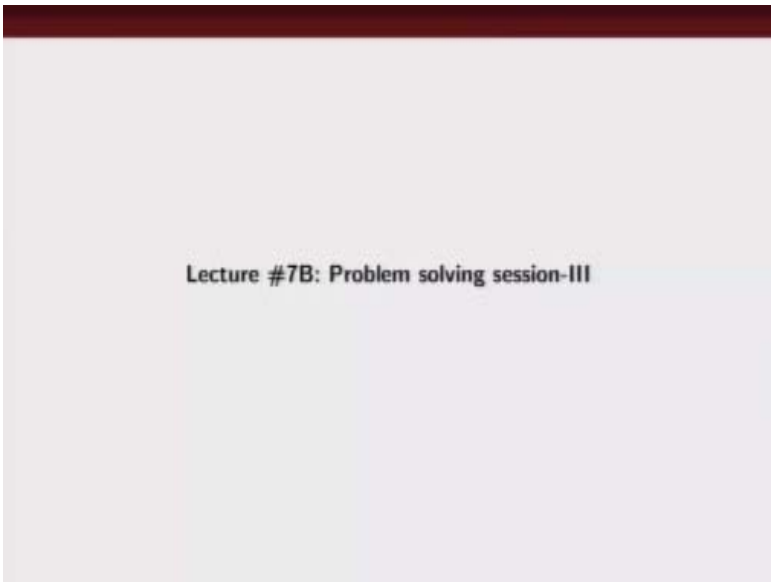
Welcome to the course on error control coding, an introduction to linear block codes.

(Refer Slide Time: 00:19)



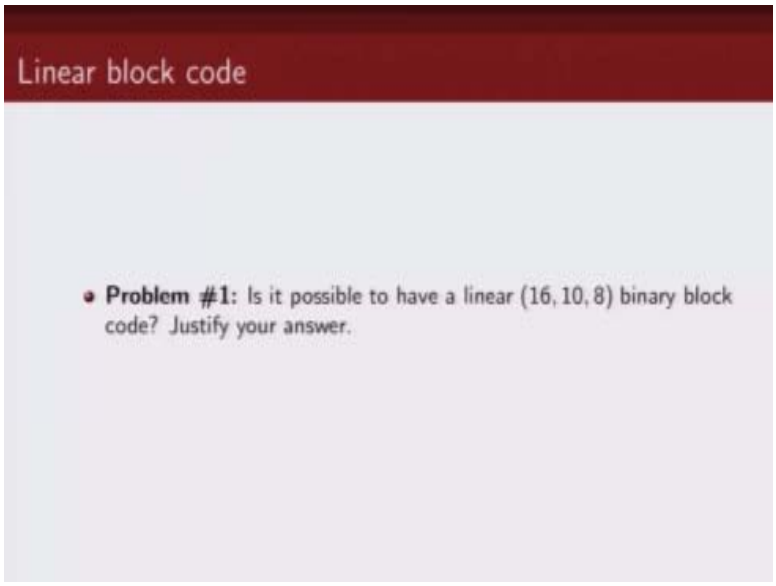
So in the last lecture we discussed about bounds on the size of the code.

(Refer Slide Time: 00:27)



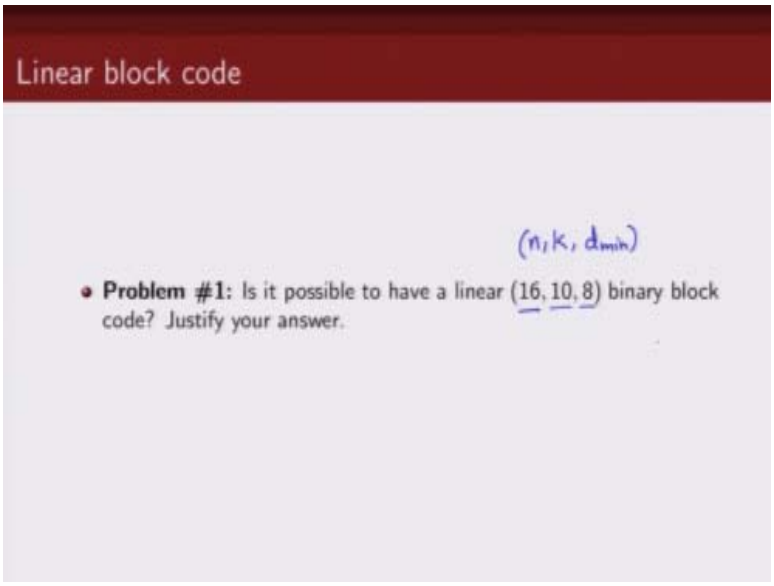
Now let us solve some problems related to that.

(Refer Slide Time: 00:29)



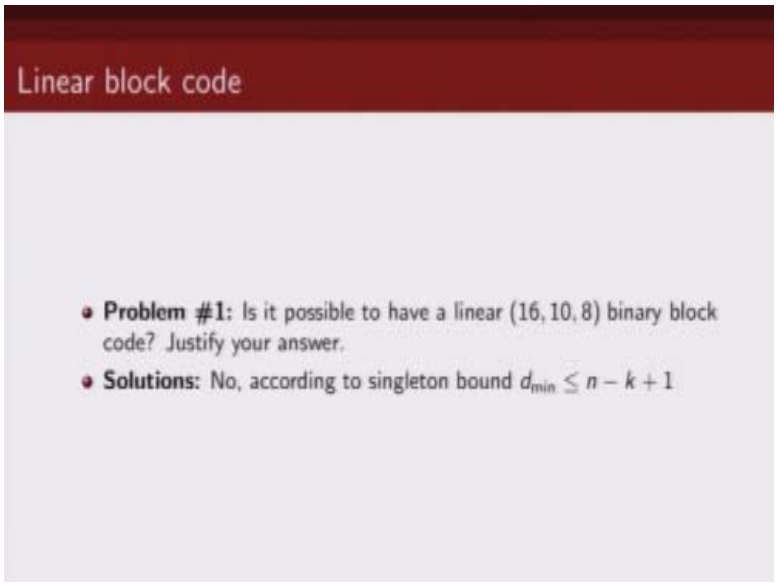
So first question is, is it possible to have a linear block code binary block code which has n given by 16.

(Refer Slide Time: 00:40)



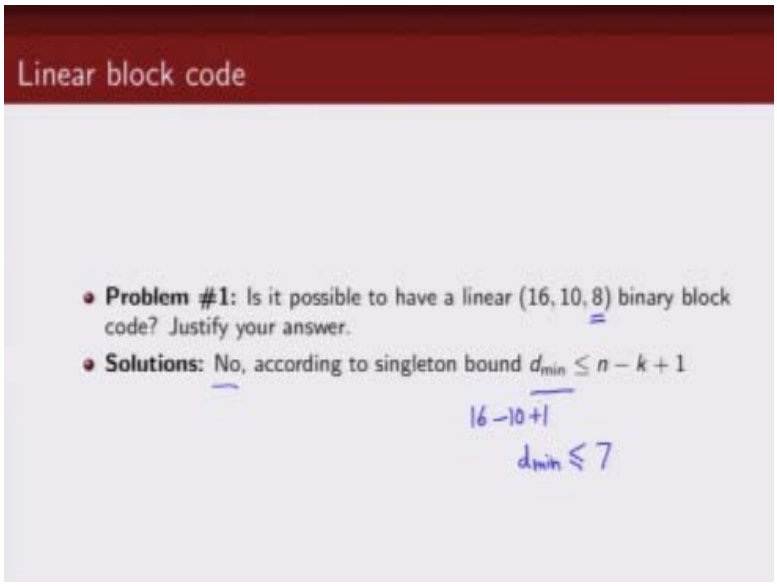
k given by 10 and minimum distance of 8, so when I write this like this it so this stands for n then this is k and this is minimum distance, so is it possible to have a code which has length 16 information, sequence length 10, and minimum distance of 8, now how do we solve it? We have talked about various bounds on minimum distance so let us see whether this satisfies the bounds on minimum distance.

(Refer Slide Time: 01:22)



So let us start with singleton bound, well the answer to this question is no.

(Refer Slide Time: 01:27)



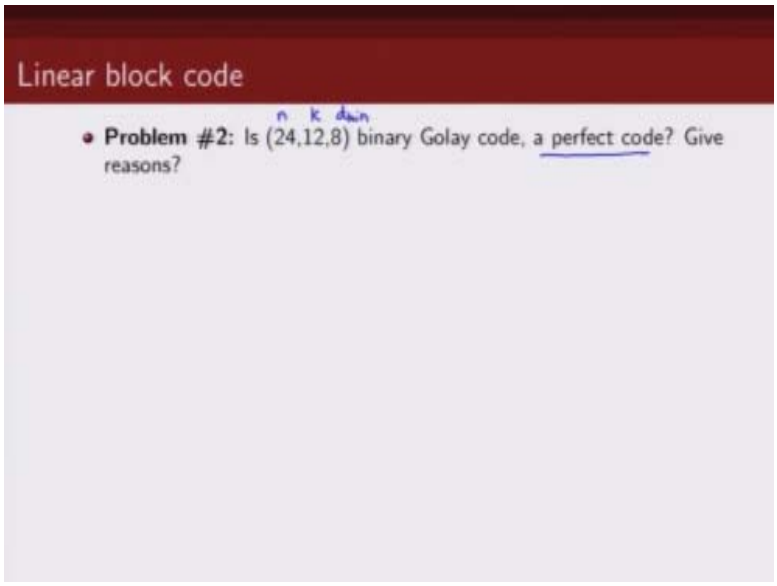
The reason being for example this does not satisfy the singleton bound, now what is singleton bound says? The minimum distance of a code has to be less than equal to n-k+1, now n here is 16, k is 10, and this is 1, so what singleton bound says that minimum distance of a 16 ten code cannot be more than 7.

And here we are saying minimum distance of 8 so that means it is not possible to have a linear code with these parameters. Now please note whenever such questions come you will have to check whether all the bounds that you, all the bounds on minimum distance are satisfied or not.

(Refer Slide Time: 02:24)

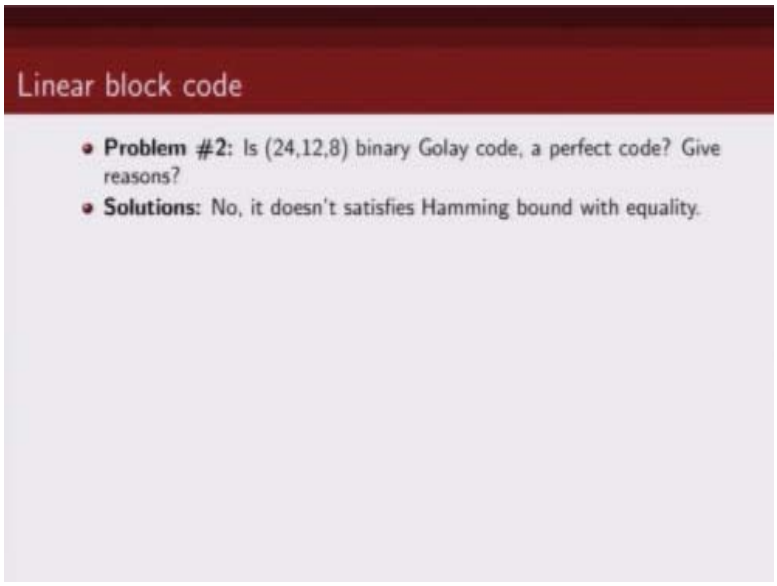
The next question is, is (24, 12, 8) binary Golay code, is this is a perfect code?

(Refer Slide Time: 02:35)



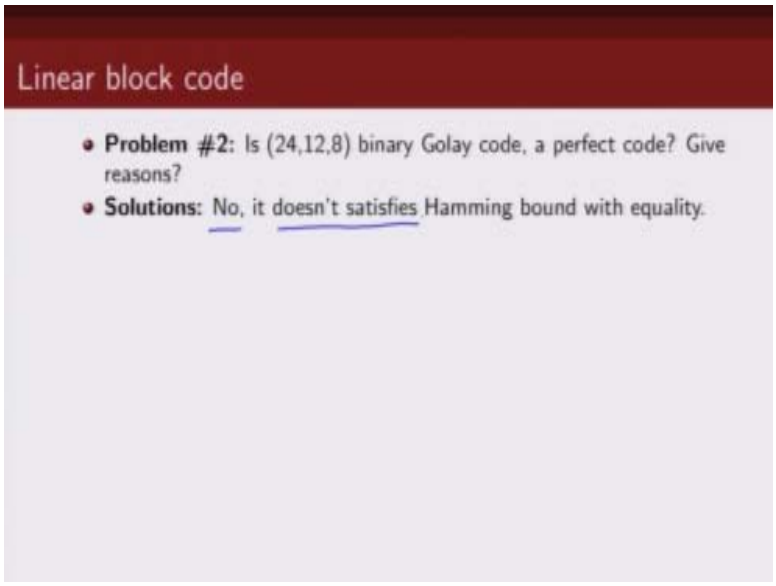
Now again here n is 24, k is 12, and minimum distance is 8, now what is a perfect code? A code that satisfies hamming bound with equality is a perfect code.

(Refer Slide Time: 02:53)



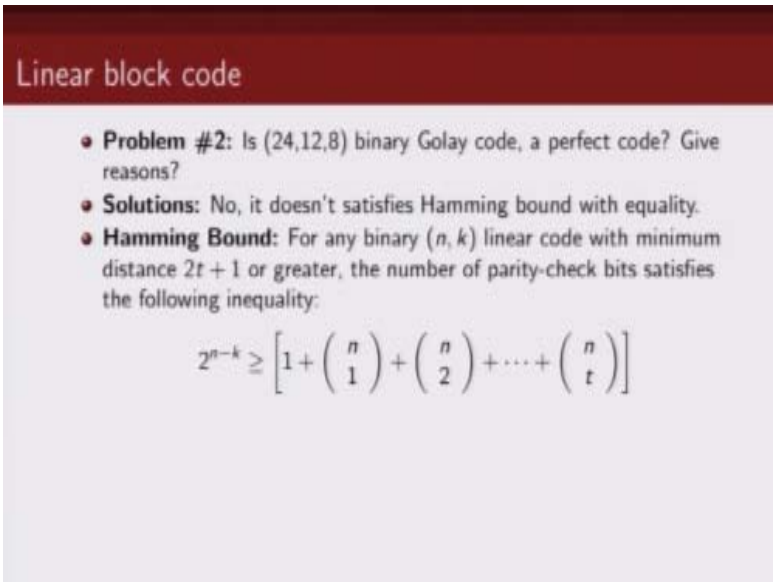
So we have to check whether this code satisfies hamming bound with equality.

(Refer Slide Time: 03:02)



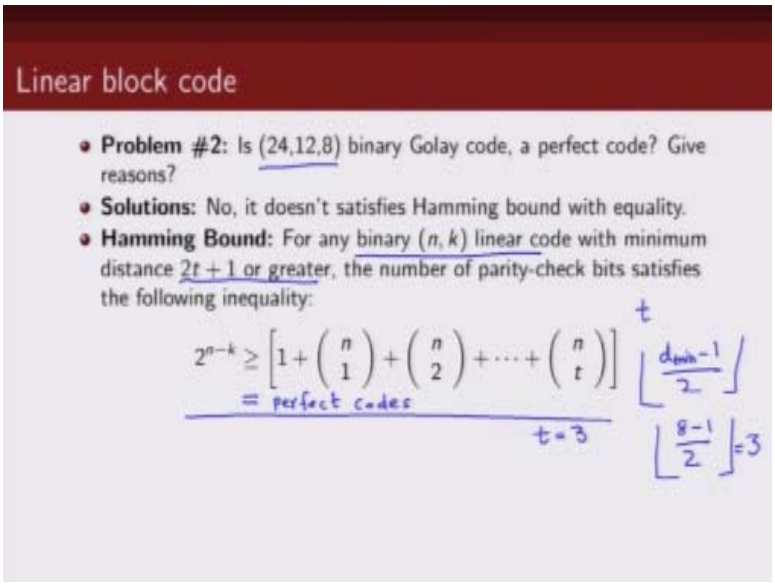
The answer to this question is no and we will come to that in a minute, it does not satisfy hamming bound with equality.

(Refer Slide Time: 03:11)



So what does hamming bound says? If you have a binary (n, k) code.

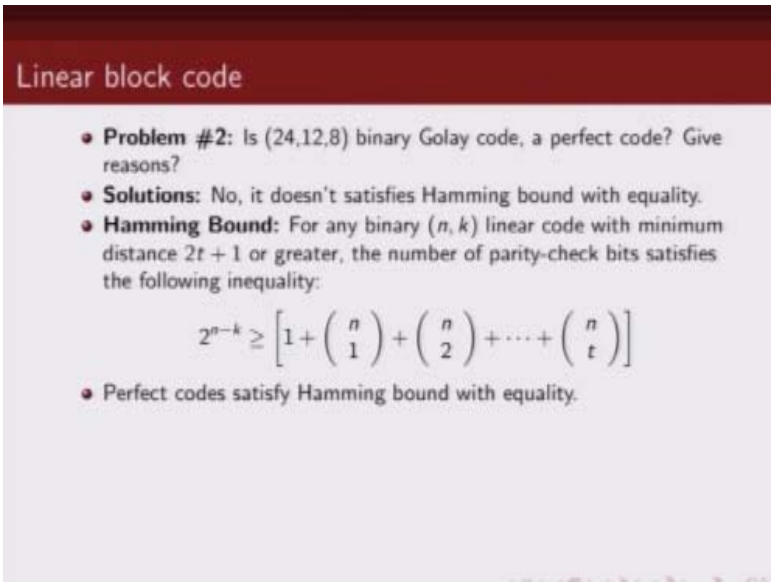
(Refer Slide Time: 03:15)



Whose minimum distance is 2t or greater then number of parity check bits must satisfy this constrain, and codes that satisfy this inequality with equality are known as perfect codes. So we will have to check whether this (24, 12, 8) Golay code satisfies this hamming bound with equality.

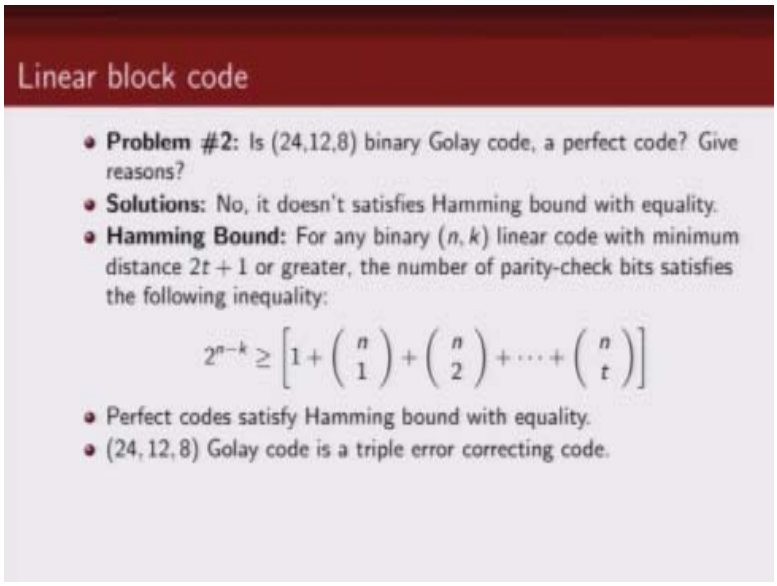
So the minimum distance is 8, now what would be the error correcting capability of this code? So this will be d_{min} -1/2 and floor of that, so in this case it is 8-1/2, so this is a triple error correcting code (24, 12, 8) Golay code can correct three errors, so t in this, t for this code is three okay.

(Refer Slide Time: 04:27)

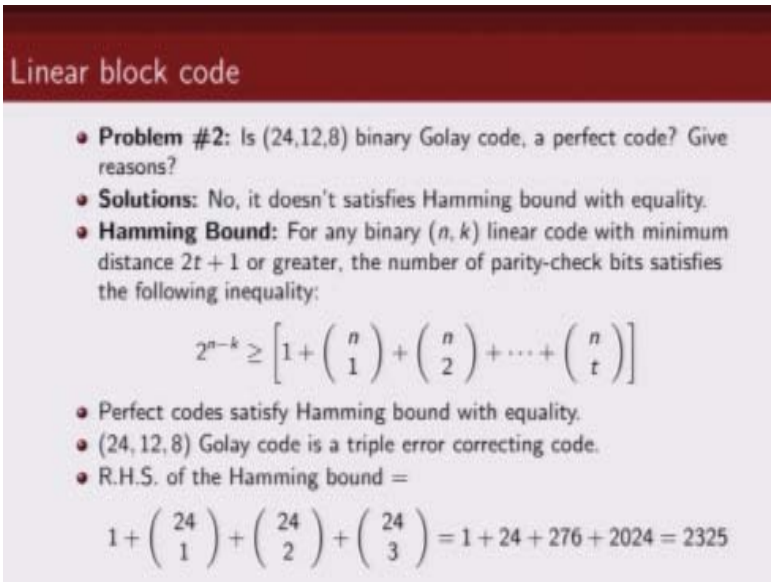


So let us just compute the right end side, this one.

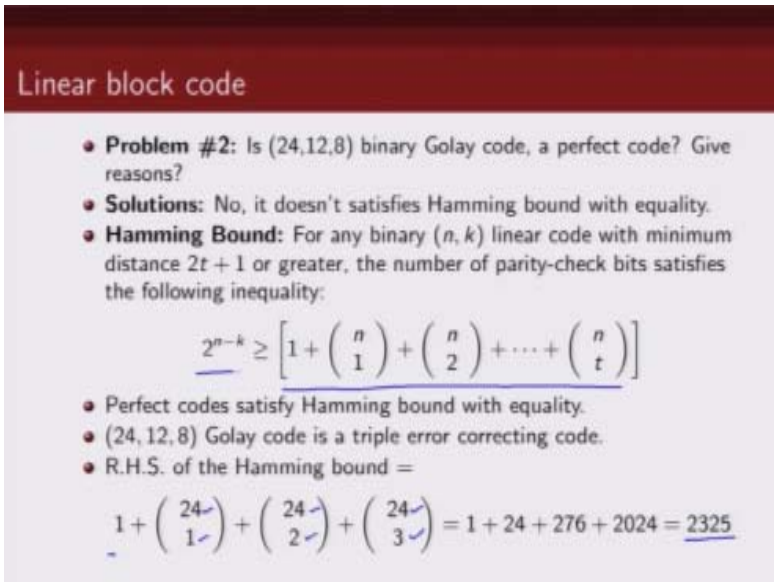
(Refer Slide Time: 04:28)



(Refer Slide Time: 04:31)

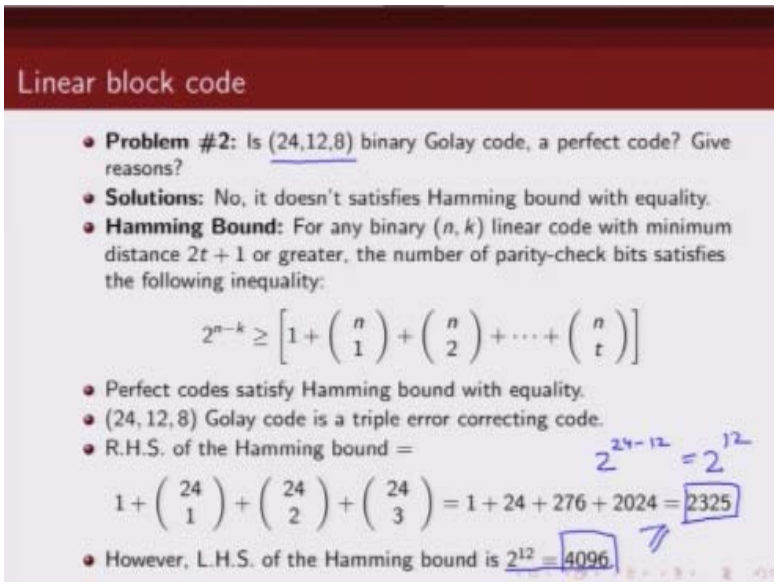


(Refer Slide Time: 04:33)



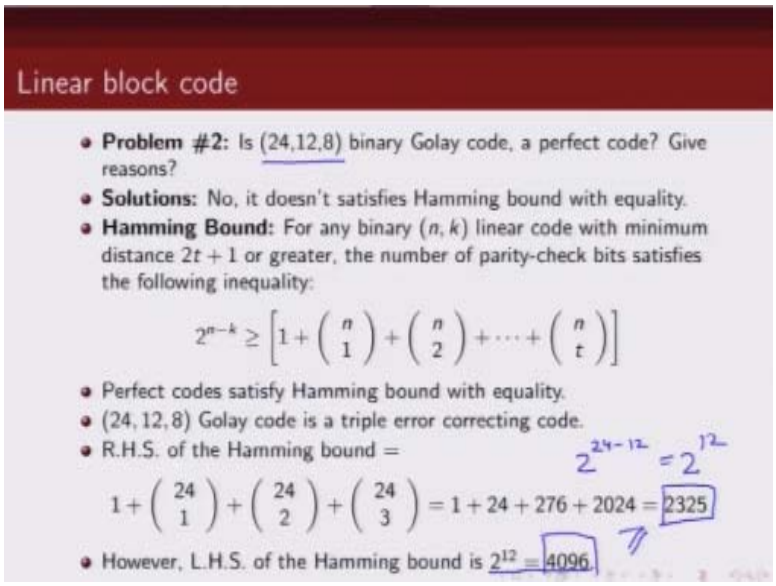
So this will be 1plus n is 24, 24 choose 1, 24 choose 2, plus 24 choose 3 because t is three, so this is 1+24+276+2024 so this will be 2325, so the term that we are getting on the right hand side is 2325, now let us look at the left hand side.

(Refer Slide Time: 05:11)



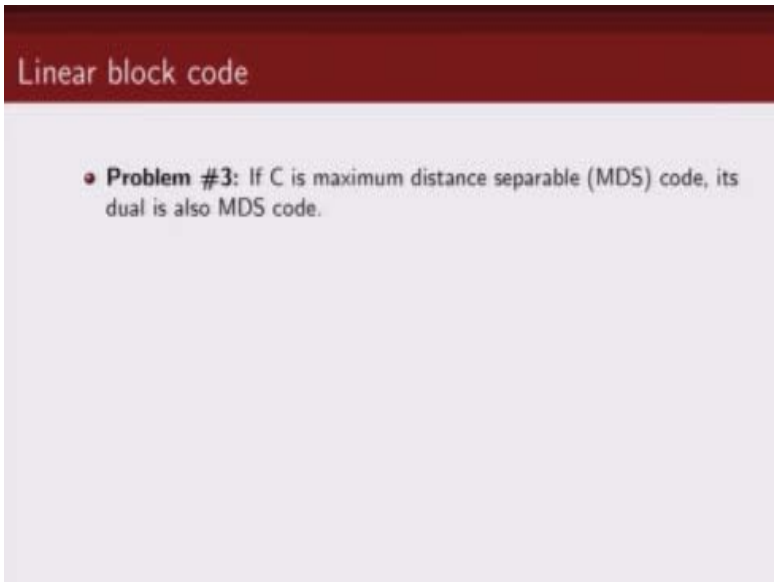
This is 2^{n-k} so n is 24, k is 12 so this will be 2^{12} and this is equal to 4096, now note left hand side is greater than right hand side, left hand side is 4096, right hand side is 2325, so this particular code does not satisfy hamming bound with equality.

(Refer Slide Time: 05:47)



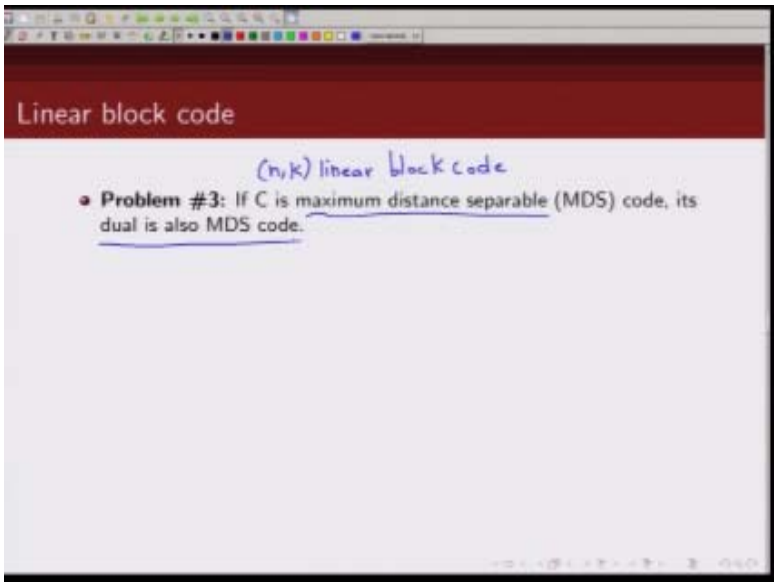
And hence it is not upper fit code.

(Refer Slide Time: 05:51)



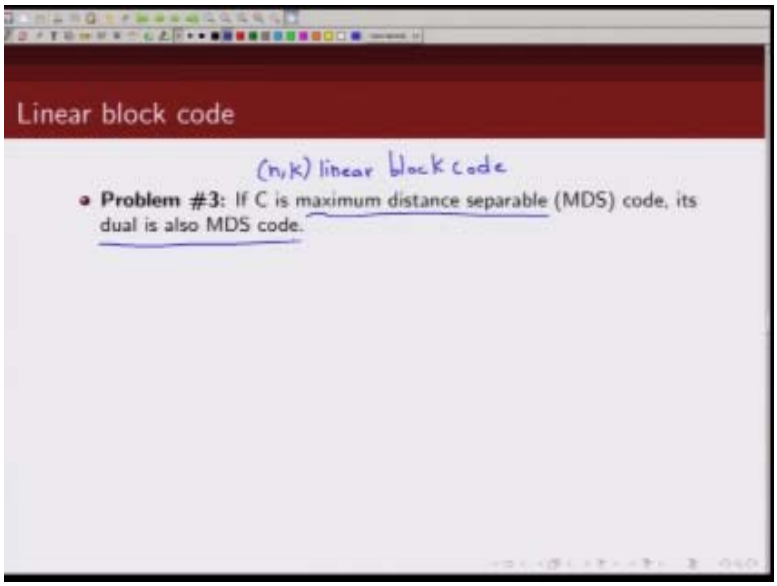
Next, if we are given a linear block code C.

(Refer Slide Time: 05:57)

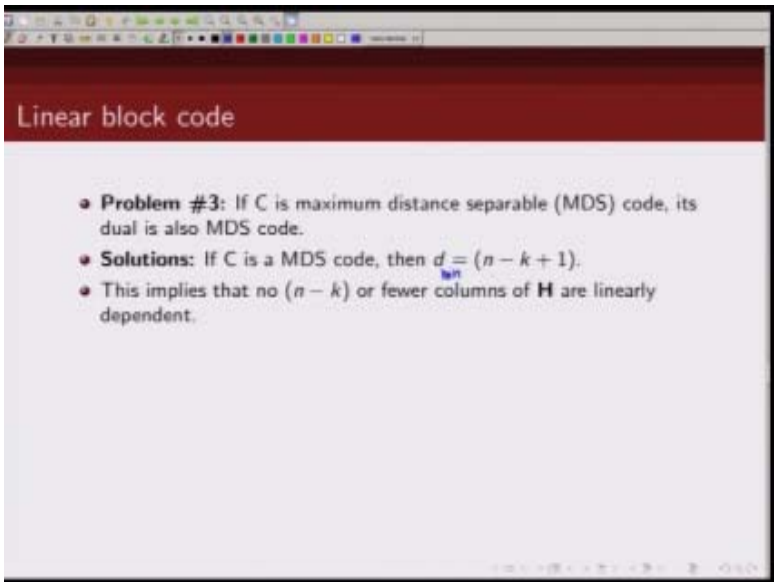


Let us just say an (n, k) linear block code and it is said that this code is maximum distance separable, then show that its a dual code is also maximum distance separable. Now what do we mean by maximum distance separable code, we know the codes that satisfy singleton bound with equality are known as maximum distance separable code.

(Refer Slide Time: 06:30)

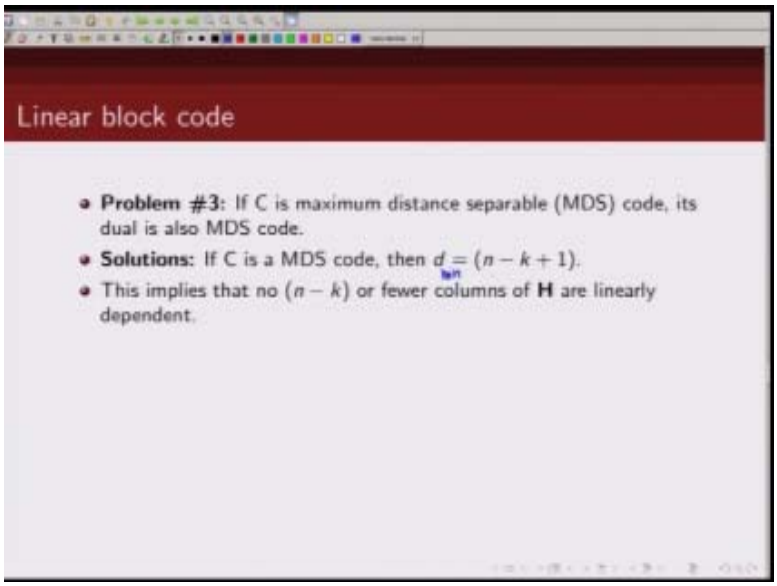


(Refer Slide Time: 06:33)



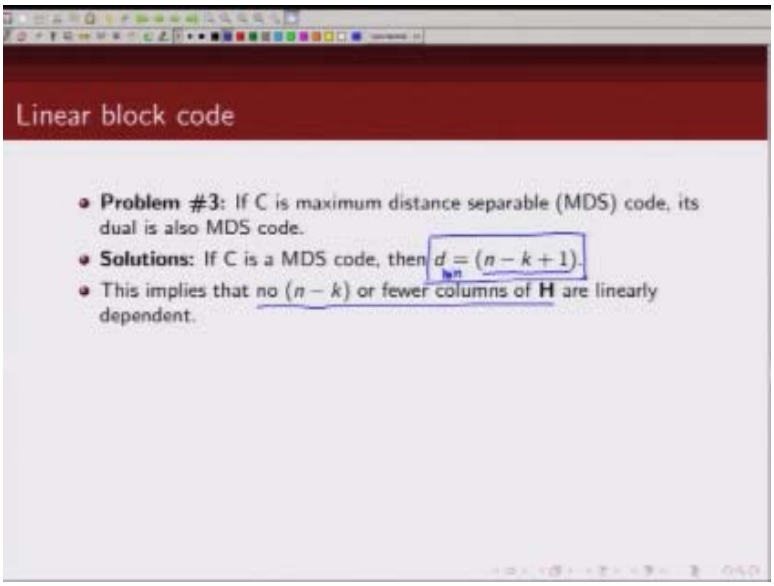
So then if this nk code is maximum distance separable then the minimum distance of this code should be n – k +1 right, this follows from the fact that our given linear block codes C is maximum distance separable. Now if the minimum distance is, if the minimum distance is n – k + 1 it means that there are no n – k or less columns in the parity check matrix of this code which are linearly dependent, if you recall the minimum.

(Refer Slide Time: 07:23)



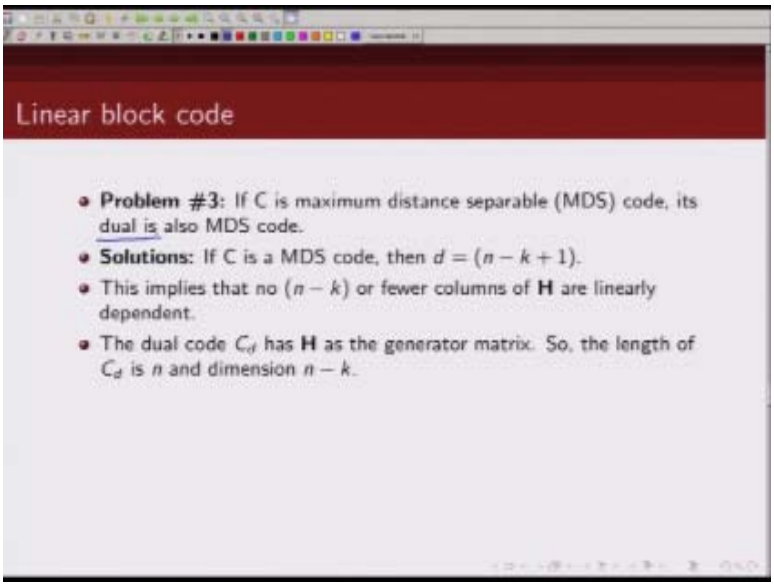
Number of columns of this parity check matrix which are linear lead dependent are basically can be found out from if we look at various, if we add up the columns of the parity check matrix the minimum number of columns that add up to 0 is the minimum distance of the code and if the minimum distance of the code.

(Refer Slide Time: 07:43)



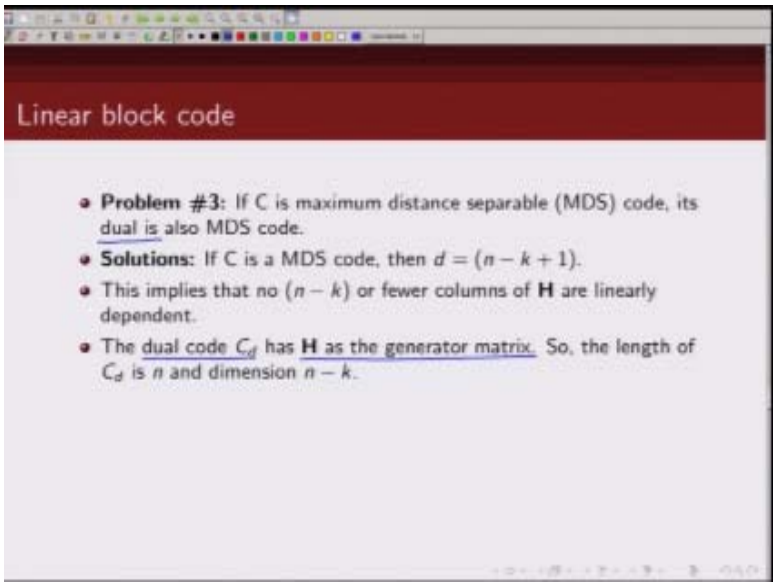
Is n – k + 1 it means no n- k or less columns of this parity check matrix will add up to 0, so that is what we are saying no n- k or fewer columns of this parity check matrix are linearly dependent, that is because the minimum distance of this code is n – k +1.

(Refer Slide Time: 08:16)



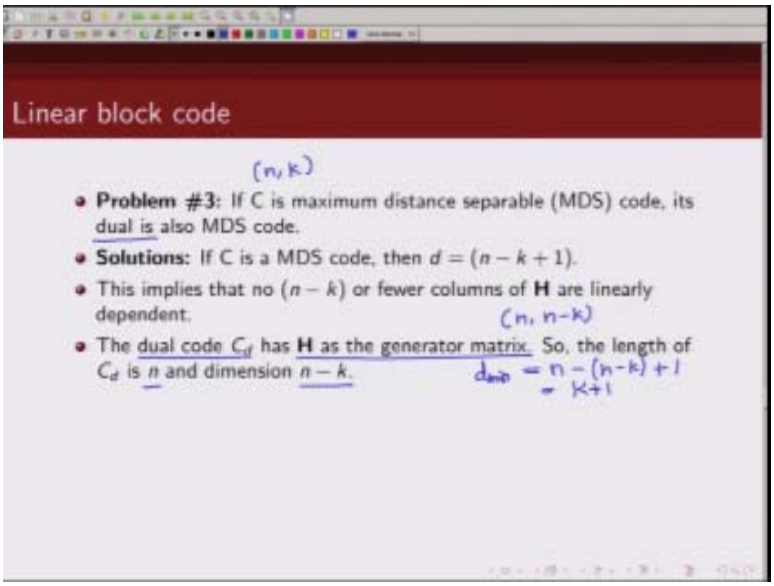
Now let us look at its dual code, now what do we know about the dual code? We know that the generator matrix of a dual code is same as parity check matrix of the original code.

(Refer Slide Time: 08:38)



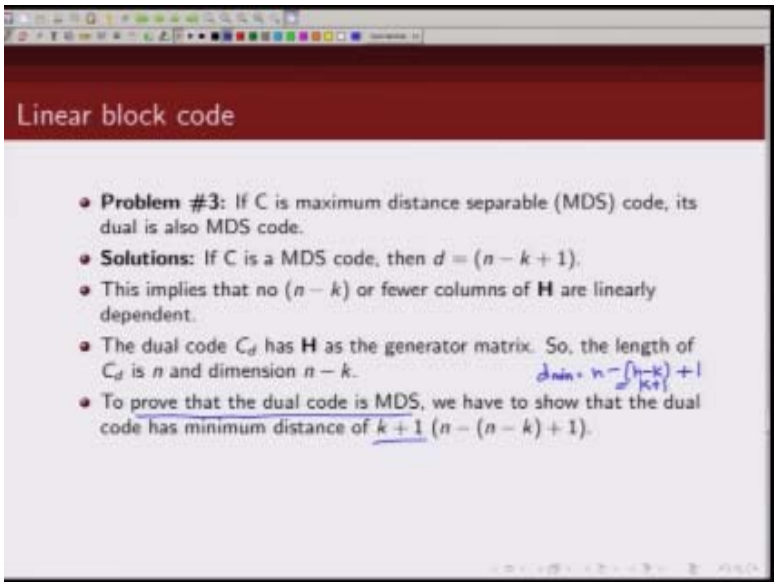
So for this dual code then H will be the generator matrix, this follows from the property of dual code and we also know the dual code.

(Refer Slide Time: 08:50)



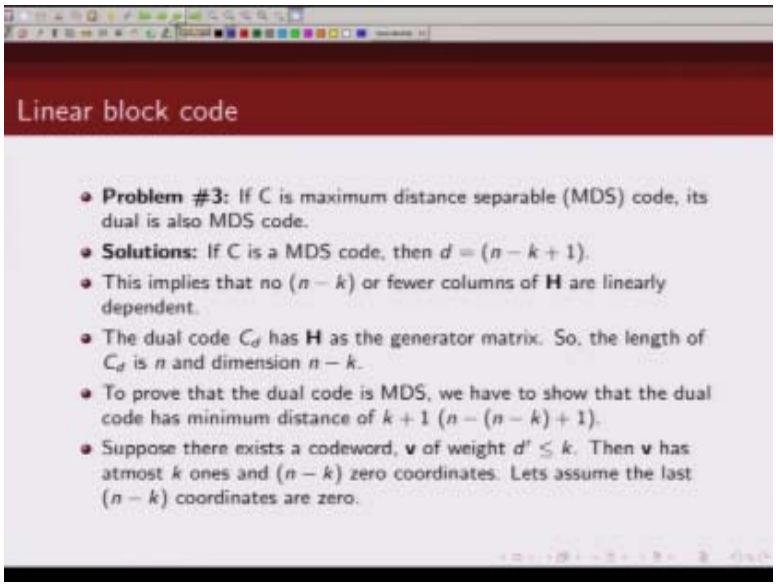
Code word length should be n and since this was an nk code the dual code dimension should be n – k. Now to prove that this dual code which is specified by these parameters length n and dimension n- k to prove that this is maximum distance separable we will have to show that its minimum distance is given by d_{min} is equal to n – dimension is n – k +1, so will have to show that minimum distance of the dual code is k+1.

(Refer Slide Time: 09:42)



So that is what we are going to show now to prove that the dual code is maximum distance separable, the dual code also has to satisfy singleton bound and according to singleton bound the minimum distance should be n- k dimension of the code which is n – k + 1, and this comes out to be k + 1 so we will have to show that the minimum distance of the dual of this code is k + 1.

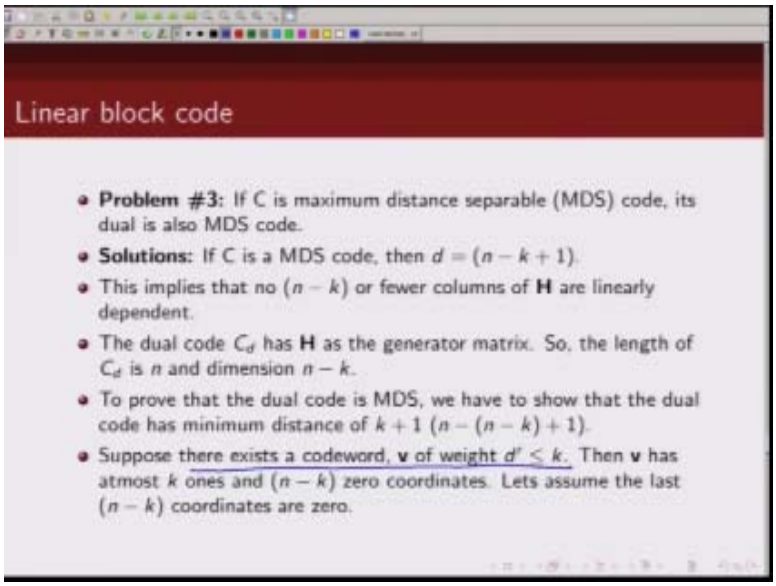
(Refer Slide Time: 10:19)



Now to prove this result we will take help of what we call method of contradiction. So how does the method of contradiction work, we will start off with the assumption that there exists a code word of weight less than equal to k so we will assume that minimum distance is not k + 1, and then we will show that through the properties of this code that this condition is not possible for assumption that there exist a code word of weight k or less is incorrect and hence the minimum distance.

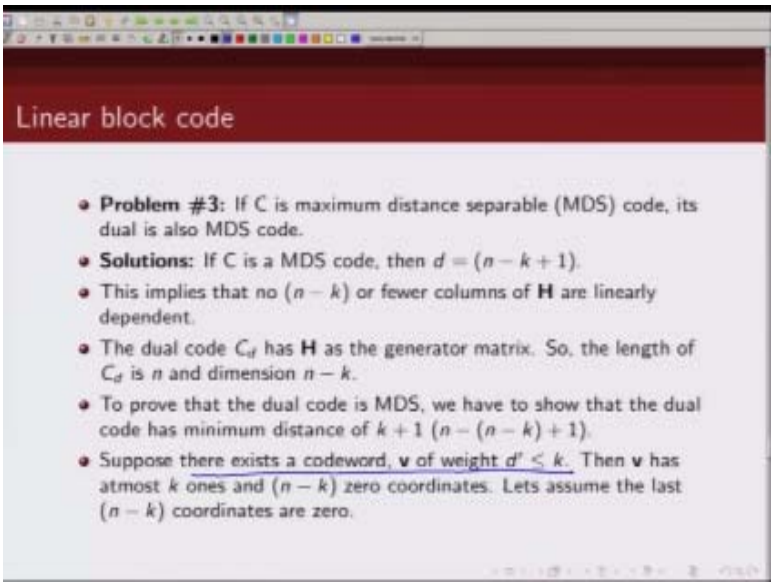
Should be more than k and then we will use singleton bound to show that minimum distance can at most be k + 1 and hence the minimum distance of the dual code is k + 1, so this the approach that we are going to follow.

(Refer Slide Time: 11:21)



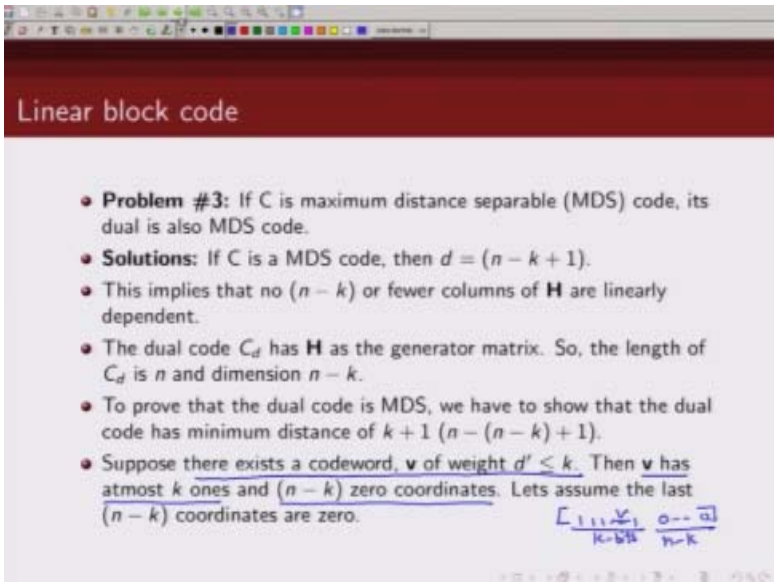
So as we said in method of contradiction we will first assume that let us assume that there exists a code word of weight less than k + 1, so we assume that there exists a code word v of weight d prime which is less than equal to k. Now if there exists a code word of weight less than equal to k what does it mean, that the code word v will at most have k once right.

(Refer Slide Time: 11:57)



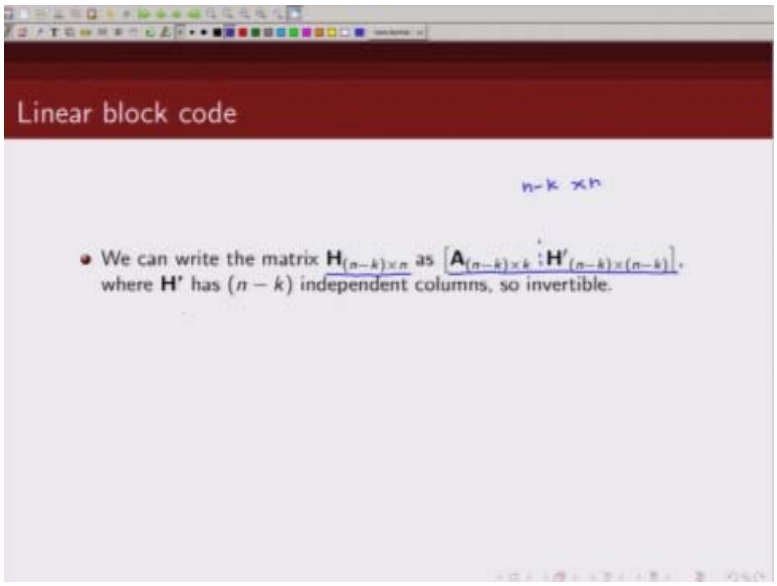
So our code word v is a n bit code word, so out of this at most k bits are one, remaining (n-k) bits are zero.

(Refer Slide Time: 12:09)



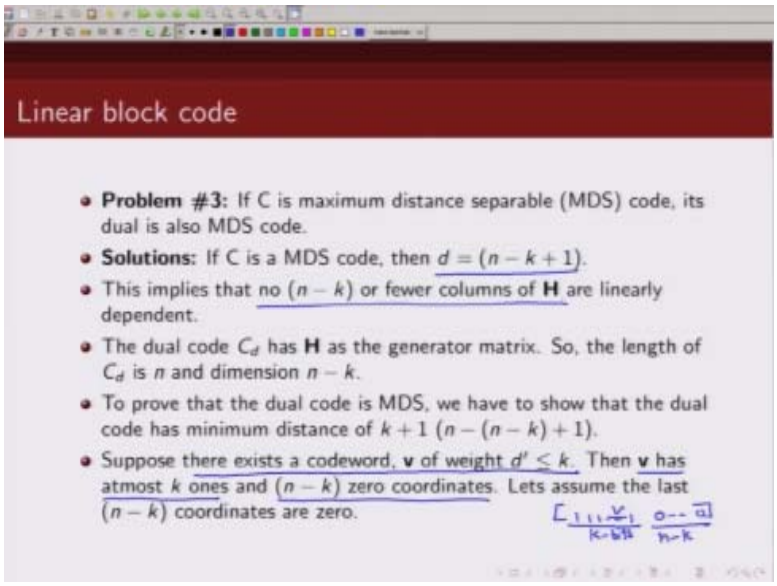
So we can at most have k ones and (n-k) or more bits are zero. Without loss of generality let us assume that those bits which are zero are towards the end so what we are assuming is let us say if this is our code word v, so first k bits have ones and this these remaining bits have zeros. So these are, these bits have zeros and these bits have one okay. Let us assume that.

(Refer Slide Time: 12:49)



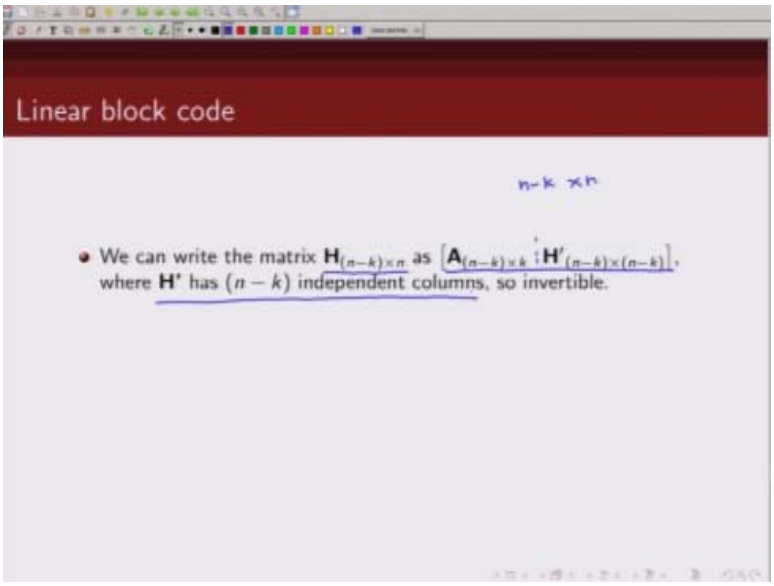
Now the parity check matrix of the original code which is the generator matrix of a dual code can be written in this particular form. Now please note this parity check matrix is n-k x n matrix so this I am writing as one matrix which is A matrix n-k x k and then there is an invertible matrix which I call H prime which is n-k x n-k. Now what was the rank of this matrix H, remember we have.

(Refer Slide Time: 13:31)



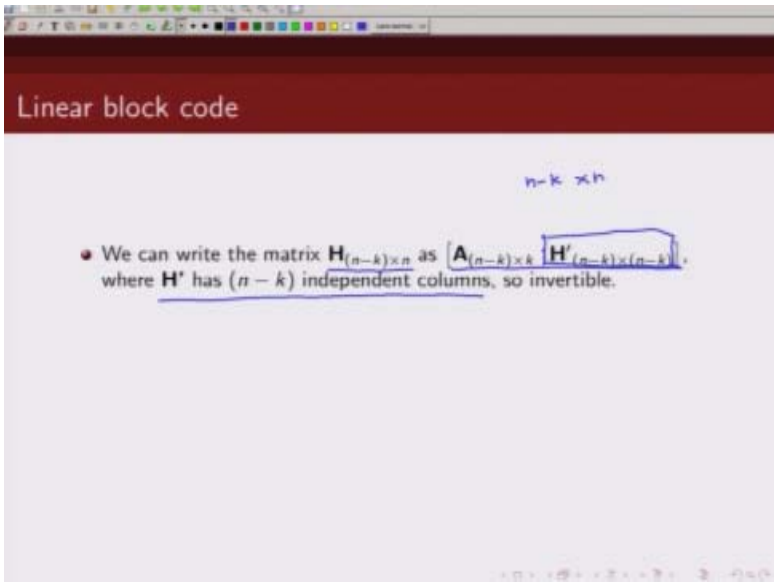
Because minimum distance of the code was n-k+1 so no (n-k) or fewer columns of H were linearly dependent.

(Refer Slide Time: 13:42)



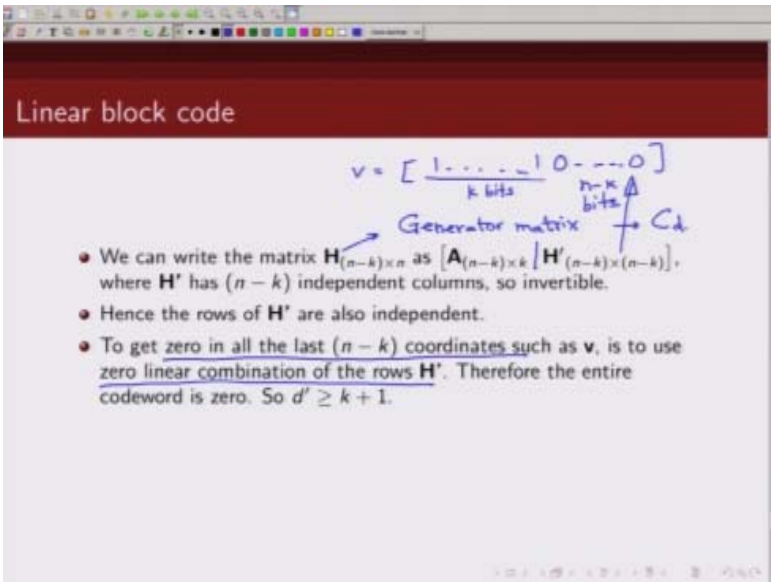
So the row rank was (n-k) so column rank is also (n-k), what does it mean it means that (n-k) there are (n-k) independent columns in this matrix and let us say those.

(Refer Slide Time: 13:58)



(n-k) independent columns are this, given by this H′ okay. So this is, so since this has independent column this can be inverted also.

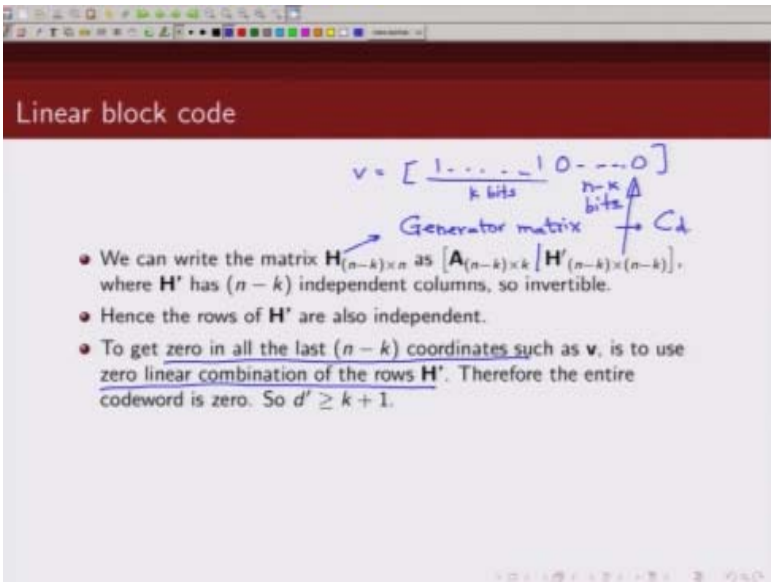
(Refer Slide Time: 14:11)



And rows of this matrix H′ is also independent because it has rank (n-k) as well. Now remember what did we say about our code word v, we said our code word v the first k bits at most first k bits are one so these first k bits can at most be one and these are all zeros. So remaining (n-k) bits are all zero. Now this H matrix is the generator matrix, this is a generator matrix for dual code C_d. So if we have to generate a code word like this from this generator matrix given by this we will have to use this matrix. Now remember to get zero in the last (n-k) coordinates. Now this consists of (n-k) linearly independent columns and rows.

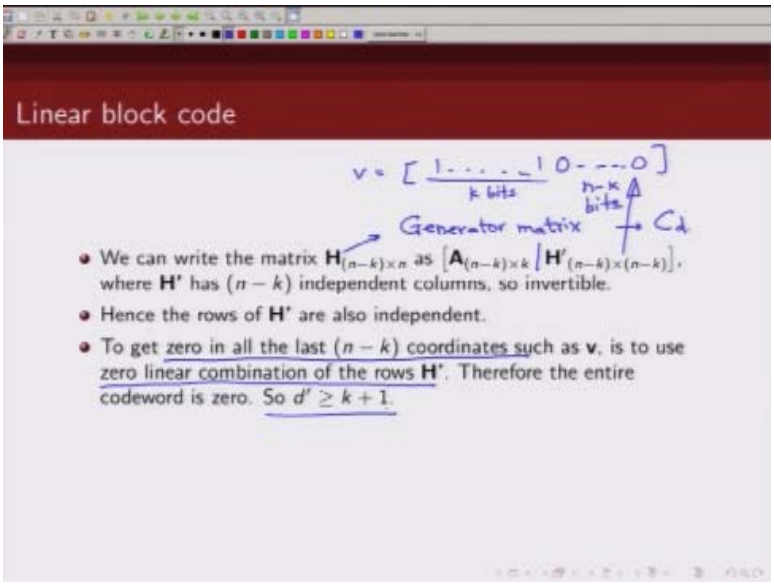
Now to get zero in last (n-k) coordinates the only way we can get it is if we use a zero linear combinations of, of all rows. So if we do zero times all the rows that is the only way we can get this condition. Why because this is, remember this is a linearly independent columns and rows so only ways we can get all zero here is if we take zero linear combination so we multiply all the rows of these generator matrix by zero, but if we do that what is the minimum distance that we get? If, if we do that the code word that we get is all zero code word. So what it means then that our assumption

(Refer Slide Time: 16:12)



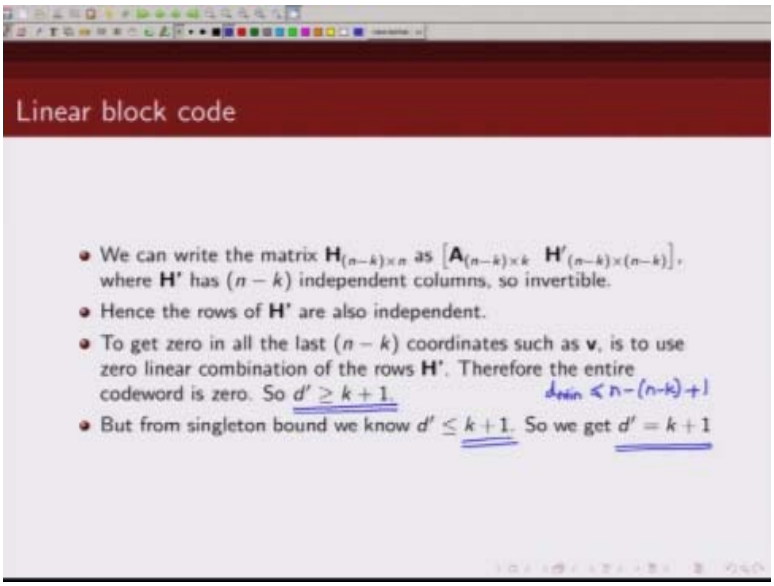
That there exists a code word of weight upto k is incorrect. Because we are not able to construct that code word using the generator matrix of the dual code. Hence our assumption that minimum distance of the code there exists a code word of weight less than equal to k was incorrect.

(Refer Slide Time: 16:39)



So we can conclude or say that the minimum distance of the code is atleast k+1 okay. Now how do we show that it is exactly k+1?

(Refer Slide Time: 16:51)



Now we know that minimum distance of the code must satisfy the bounds. Now it should satisfy for example singleton bound; now what does singleton bound says? Singleton bound says minimum distance of the code is upper bounded by n-dimension of the code is in this case (n-k)+1. So from singleton bound we get the condition that minimum distance should be less than equal to k+1.

And from this we get the condition that minimum distance is atleast k+1. So if we combine these two we get the condition that minimum distance of this code is k+1. Hence, it is proved that the dual code is also maximum distance separable. Because it satisfies singleton bound with equality. With this we conclude this lecture. 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