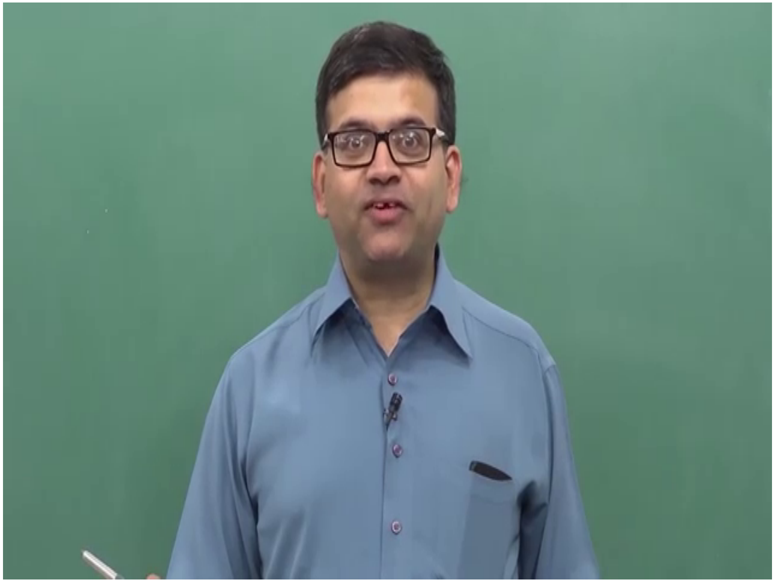
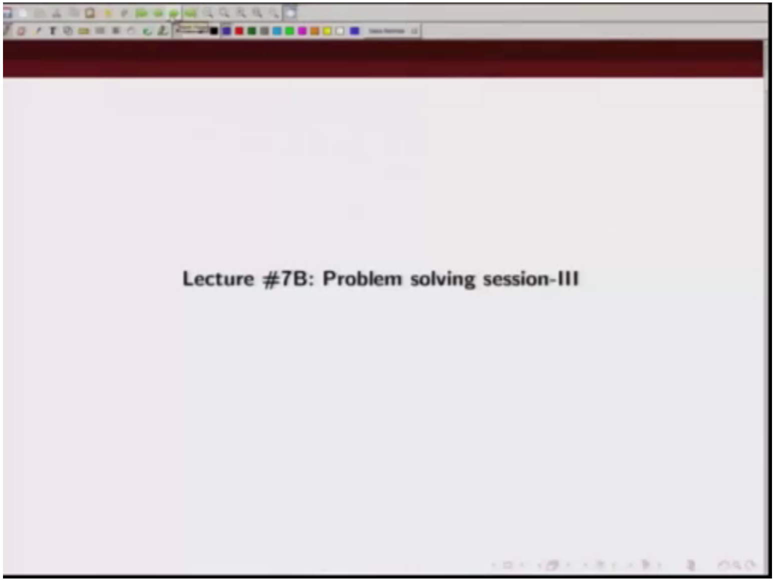
An Introduction to Coding Theory
Professor Adrish Banerji
Department of Electrical Engineering
Indian Institute of Technology, Kanpur
Module 03
Lecture Number 14
Problem Solving Session-II

(Refer Slide Time 00:15)



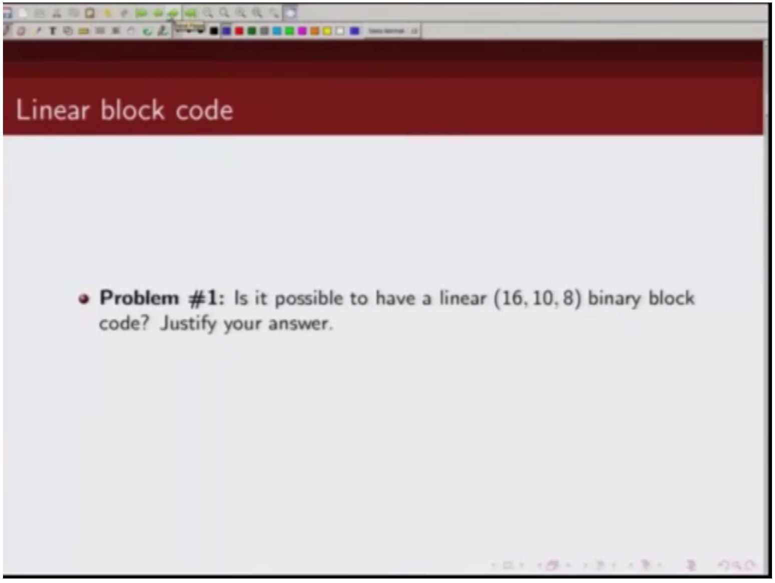
So in the last lecture we discussed about bounds on the size of the code. Now let's solve some problems related to that.

(Refer Slide Time 00:22)



Lecture #7B: Problem solving session-III

(Refer Slide Time 00:23)

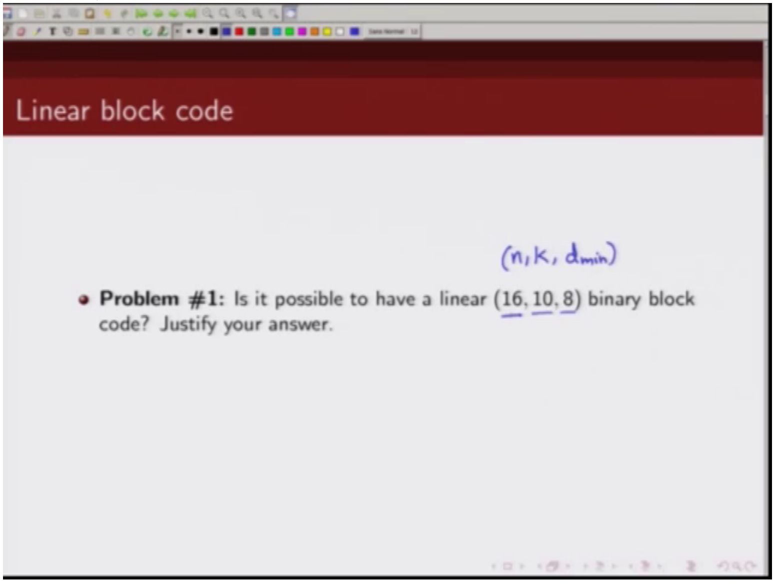


Linear block code

- **Problem #1:** Is it possible to have a linear (16, 10, 8) binary block code? Justify your answer.

So first question is, is it possible to have linear block code, binary block code which has n given by 16, k given by 10 and minimum distance of 8. So when I write it like this, so this stands for

(Refer Slide Time 00:48)



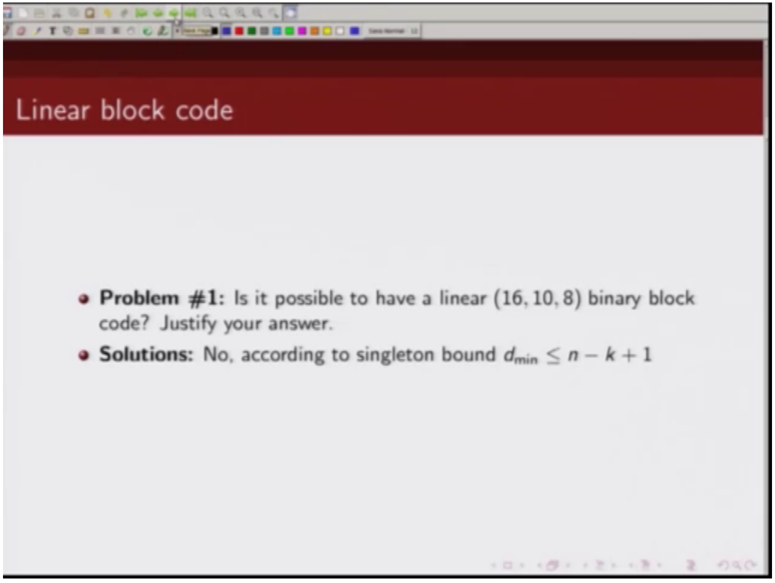
Linear block code

(n, k, d_{min})

- **Problem #1:** Is it possible to have a linear $(\underline{16}, \underline{10}, \underline{8})$ binary block code? Justify your answer.

n and this is k and 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's see whether this satisfies the bounds on minimum distance. So let's start with singleton

(Refer Slide Time 01:17)

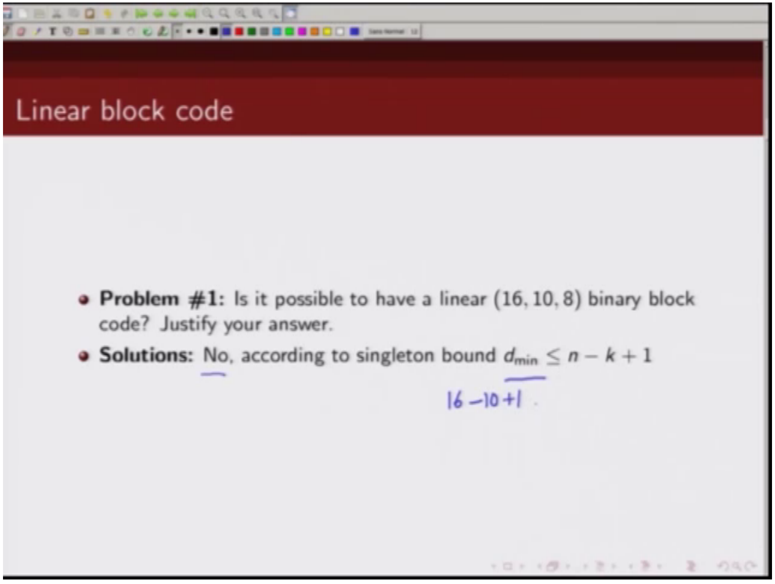


Linear block code

- **Problem #1:** Is it possible to have a linear (16, 10, 8) binary block code? Justify your answer.
- **Solutions:** No, according to singleton bound $d_{min} \leq n - k + 1$

bound. Well, the answer to this question is no. The reason being, for example this does not satisfy the singleton bound. Now what does singleton bound says? The minimum distance of a code has to be less than equal to n minus k plus 1, n here is 16, k is 10 and this is 1 so what singleton bound

(Refer Slide Time 01:45)



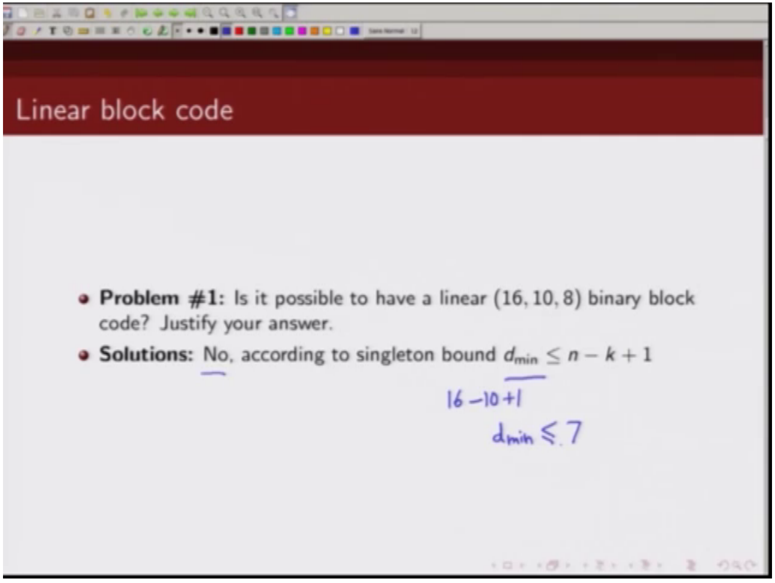
Linear block code

- **Problem #1:** Is it possible to have a linear (16, 10, 8) binary block code? Justify your answer.
- **Solutions:** No, according to singleton bound $d_{min} \leq n - k + 1$

$16 - 10 + 1$

says, that minimum distance of a 16 10 code cannot be more than 7.

(Refer Slide Time 01:52)



Linear block code

- **Problem #1:** Is it possible to have a linear (16, 10, 8) binary block code? Justify your answer.
- **Solutions:** No, according to singleton bound $d_{min} \leq n - k + 1$

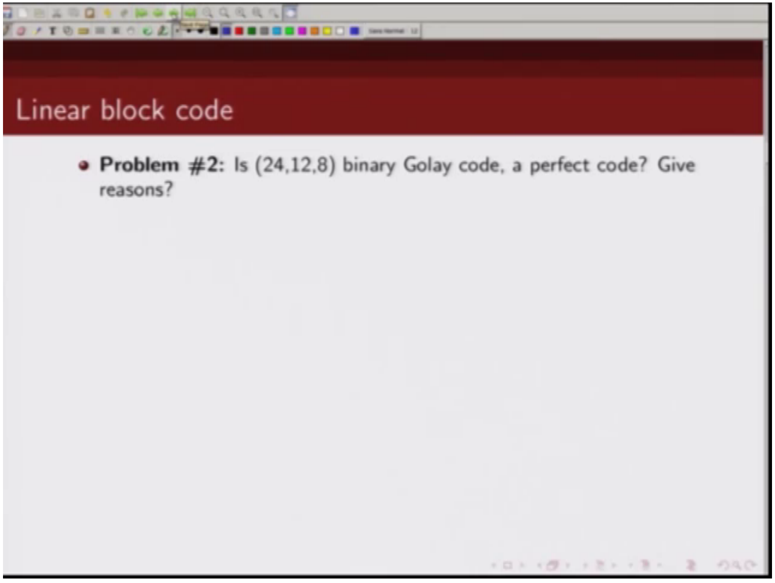
$16 - 10 + 1$

$d_{min} \leq 7$

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 not, are satisfied or not.

The next

(Refer Slide Time 02:18)

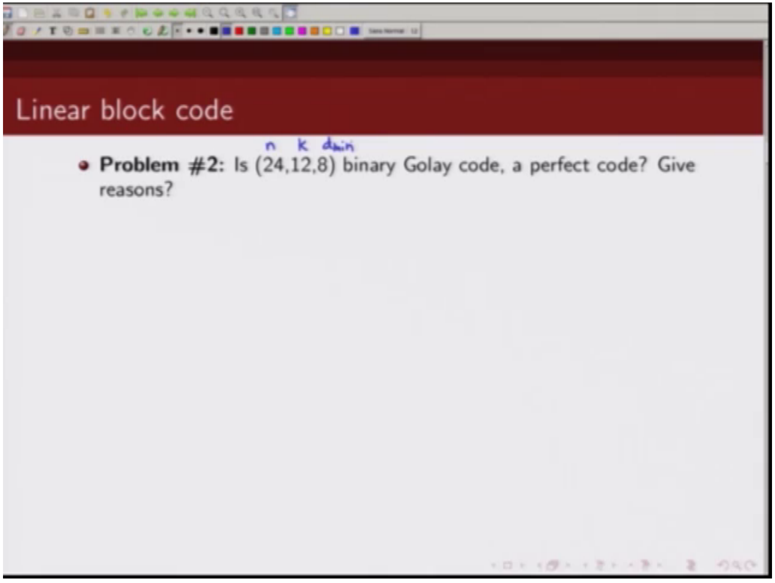


Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?

question is 24 12 8 binary Golay code, is this a perfect code? Now again here n is 24, k is 12 and minimum distance is 8.

(Refer Slide Time 02:36)

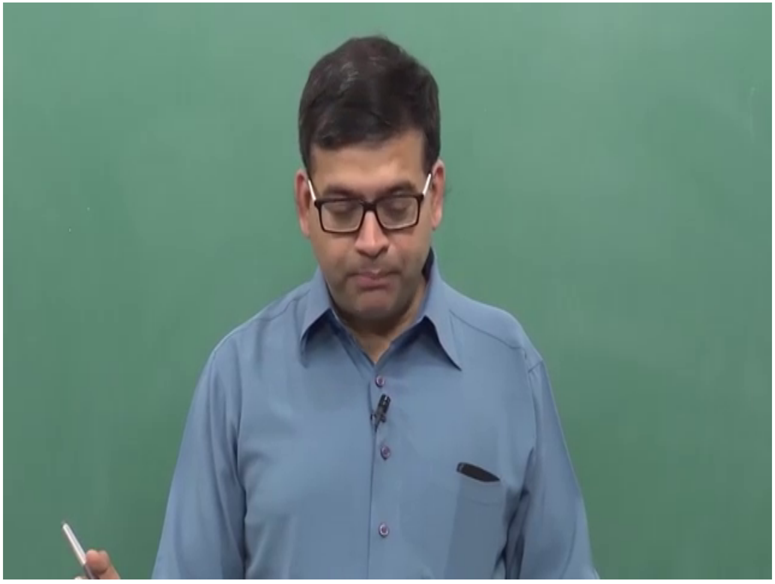


Linear block code

- **Problem #2:** Is $(\overset{n}{24},\overset{k}{12},\overset{d_{min}}{8})$ binary Golay code, a perfect code? Give reasons?

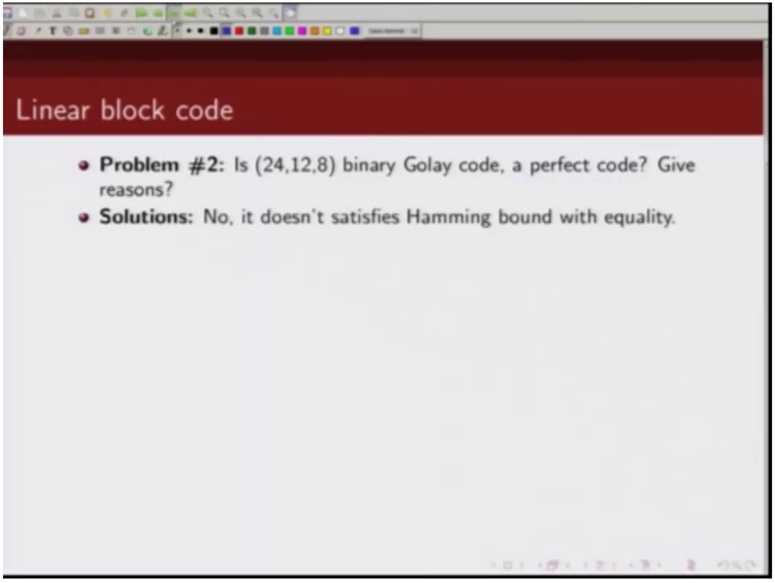
Now what is a perfect code? A code that satisfies Hamming bound with equality is a perfect code.

(Refer Slide Time 02:46)



So we have to check

(Refer Slide Time 02:48)

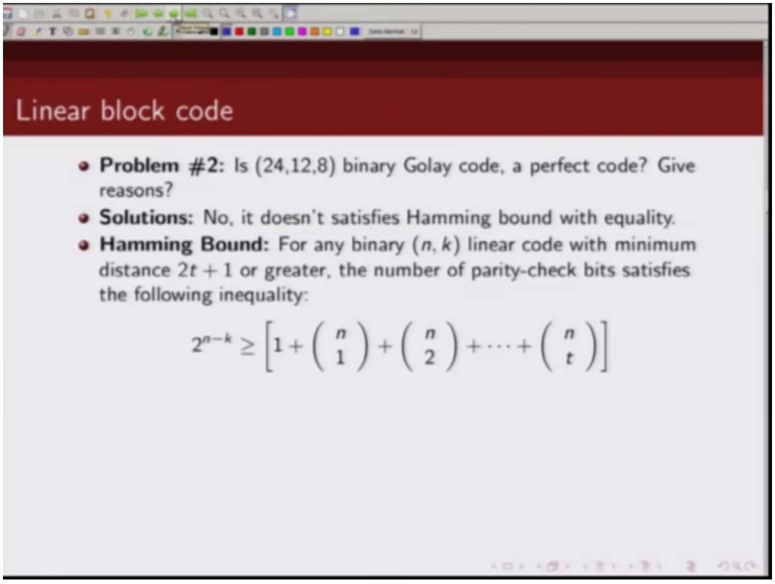


Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.

whether this code satisfies Hamming bound with equality. The answer to this question is no and we will come to that in a minute. It does not satisfy Hamming bound with equality. So what does

(Refer Slide Time 03:05)



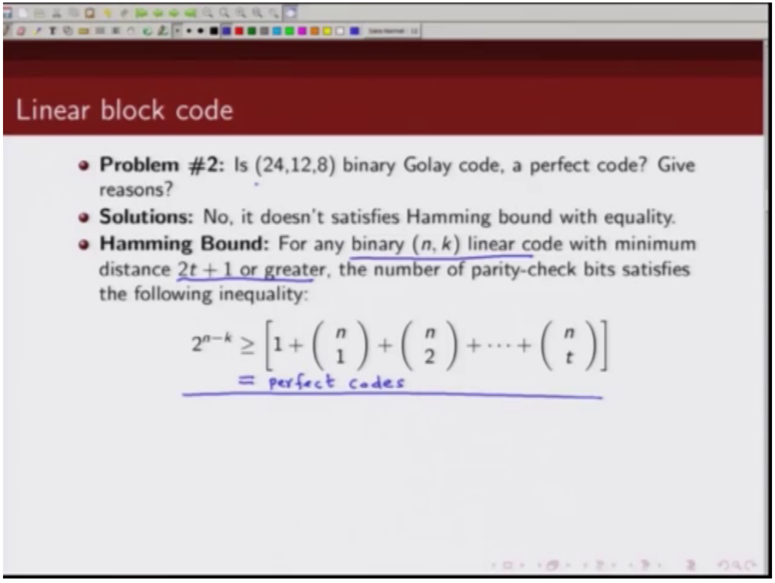
Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

Hamming bound says? If you have a binary n k code whose minimum distance is 2 t or greater then number of priority check bits must satisfy this constraint and codes that satisfy this inequality with equality are known as perfect codes. So we will have to check whether this

(Refer Slide Time 03:35)



Linear block code

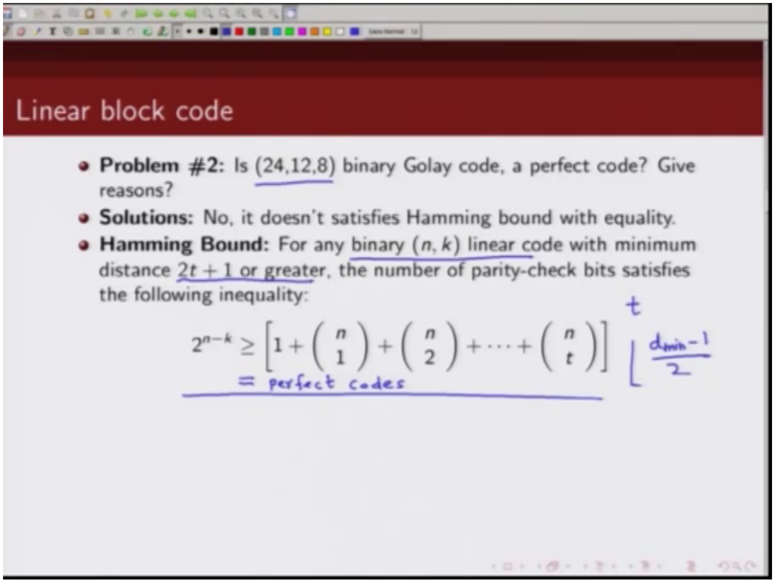
- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

= perfect codes

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 minus 1 by 2 and floor of that.

(Refer Slide Time 03:58)



Linear block code

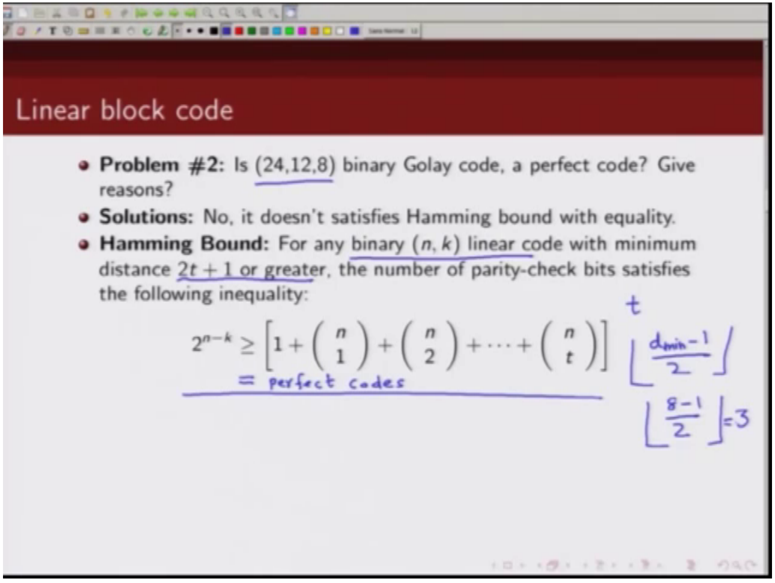
- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right] \quad \overset{t}{\lfloor \frac{d_{min}-1}{2}}$$

= perfect codes

So in this case it's 8 minus 1 by 2 so this is a triple error correcting code, 24 12 8

(Refer Slide Time 04:10)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t+1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

= perfect codes

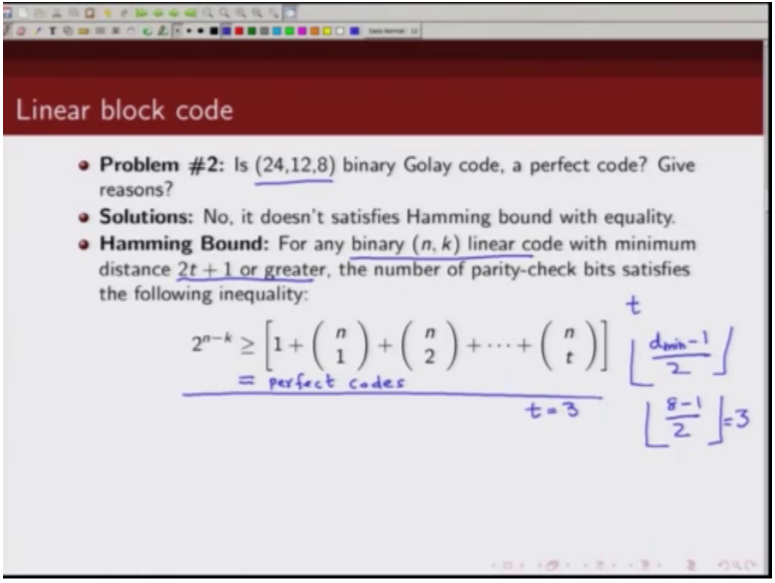
t

$$\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$$

$$\left\lfloor \frac{8-1}{2} \right\rfloor = 3$$

Golay code can correct 3 errors. So t in this, t for this code is 3,

(Refer Slide Time 04:19)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t+1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

= perfect codes

$t = 3$

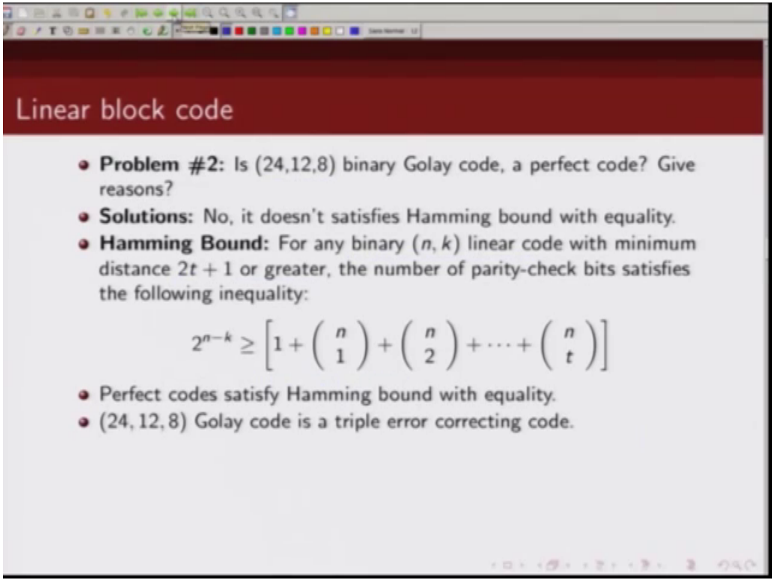
t

$$\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$$

$$\left\lfloor \frac{8-1}{2} \right\rfloor = 3$$

Ok. So

(Refer Slide Time 04:22)



Linear block code

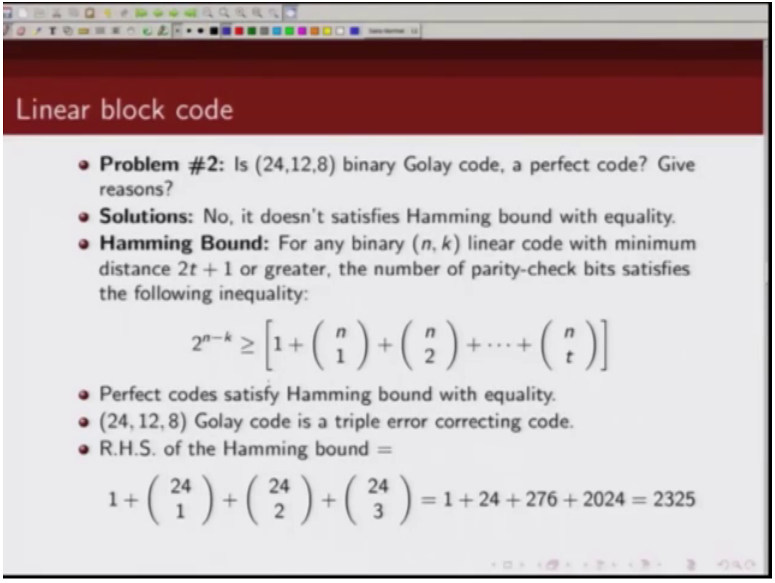
- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

- Perfect codes satisfy Hamming bound with equality.
- $(24, 12, 8)$ Golay code is a triple error correcting code.

let's just compute the right hand side,

(Refer Slide Time 04:26)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

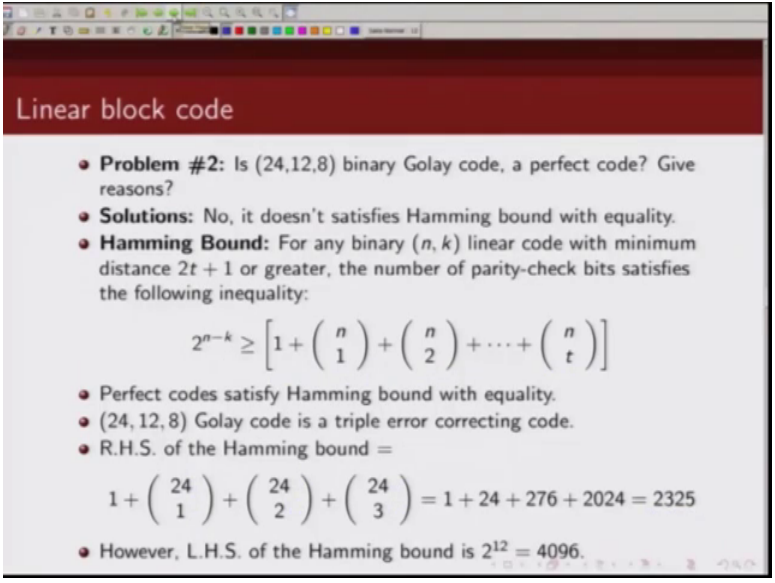
$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

- Perfect codes satisfy Hamming bound with equality.
- $(24, 12, 8)$ Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = 2325$$

this one. So this will be 1 plus n is 24, 24 choose 1 24 choose 2 plus 24 choose 3 because t is 3. So this is 1 plus 24 plus 2 76 plus 20 24 so this will be two thousand three hundred twenty five. So the term that we are getting on the right hand side is two thousand three hundred twenty five. Now let's look at the left hand side. This is 2 raised to power

(Refer Slide Time 05:05)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t+1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

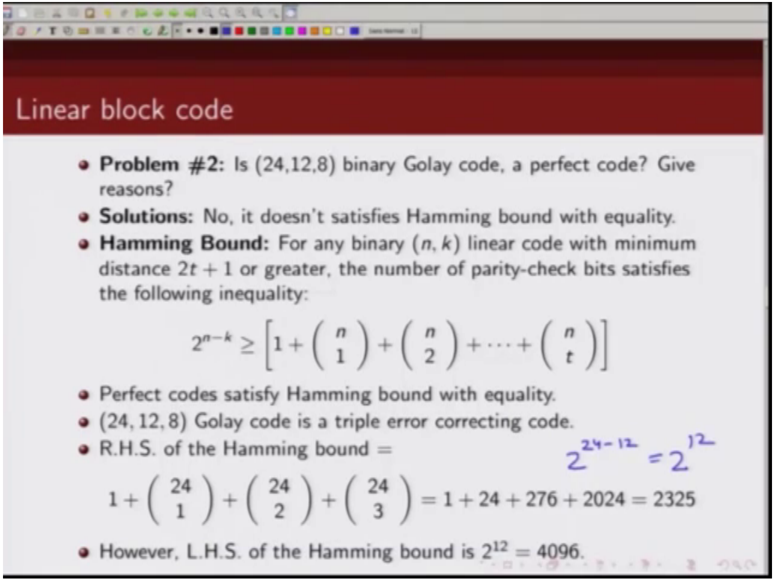
- Perfect codes satisfy Hamming bound with equality.
- $(24, 12, 8)$ Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = 2325$$

- However, L.H.S. of the Hamming bound is $2^{12} = 4096$.

n minus k. So n is 24, k is 12, so this will be 2 raised to power 12. And this is equal to

(Refer Slide Time 05:16)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t+1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

- Perfect codes satisfy Hamming bound with equality.
- $(24, 12, 8)$ Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

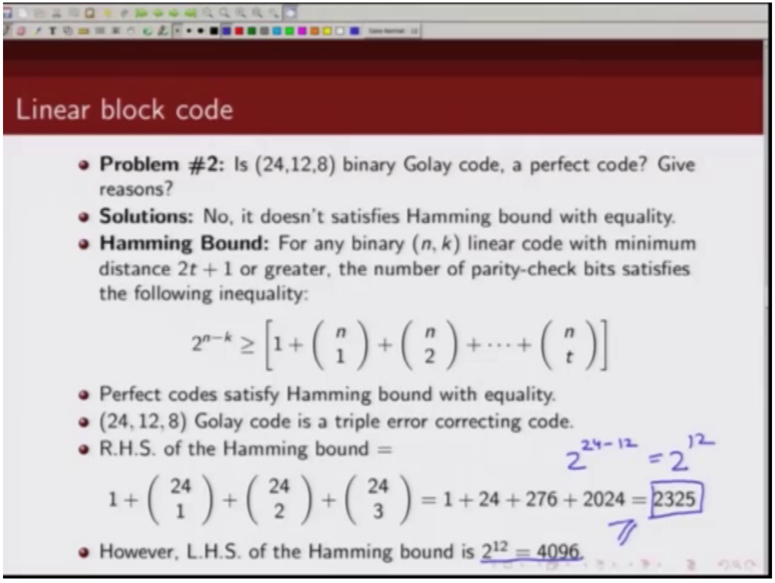
$$2^{24-12} = 2^{12}$$

$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = 2325$$

- However, L.H.S. of the Hamming bound is $2^{12} = 4096$.

4 0 9 6. Now note left hand side is greater than right hand side. Left hand side

(Refer Slide Time 05:27)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t+1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

- Perfect codes satisfy Hamming bound with equality.
- (24, 12, 8) Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

$$2^{24-12} = 2^{12}$$

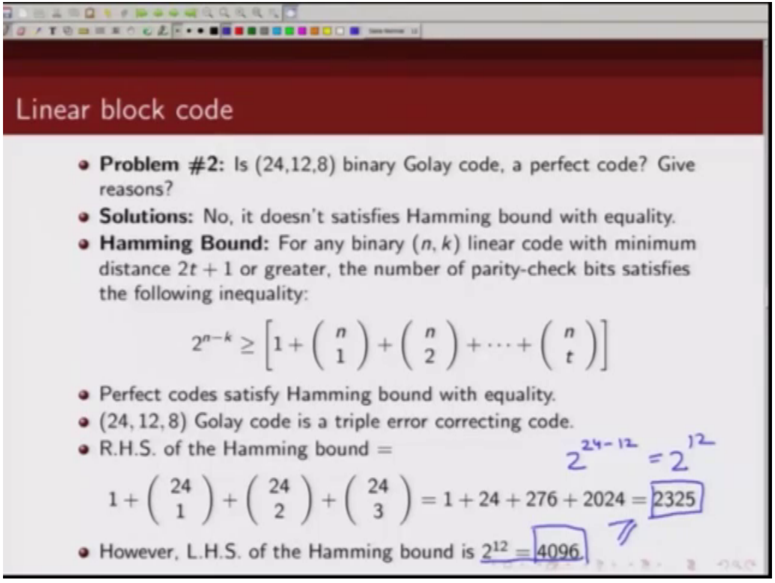
$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = \boxed{2325}$$

$$\ngtr$$

- However, L.H.S. of the Hamming bound is $\underline{2^{12} = 4096}$.

is 4 0 9 6. Right hand side is 2 3 2 5.

(Refer Slide Time 05:30)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t+1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

- Perfect codes satisfy Hamming bound with equality.
- (24, 12, 8) Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

$$2^{24-12} = 2^{12}$$

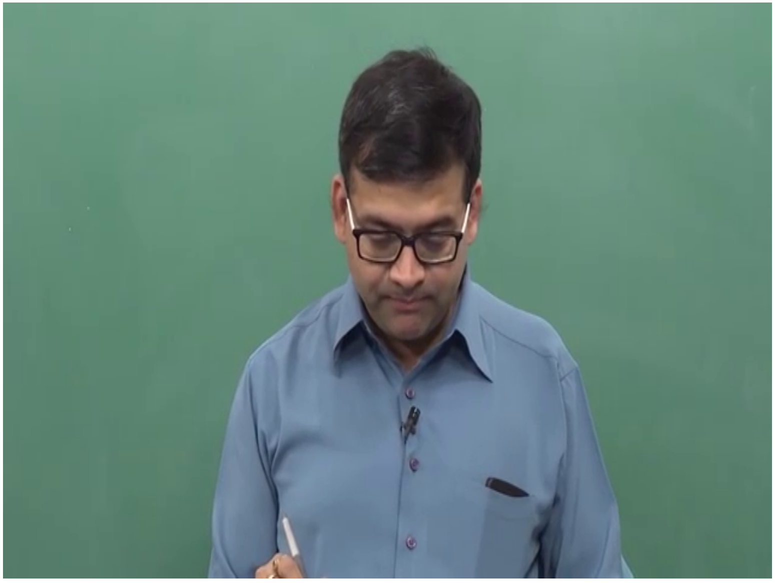
$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = \boxed{2325}$$

$$\ngtr$$

- However, L.H.S. of the Hamming bound is $\underline{2^{12} = \boxed{4096}}$.

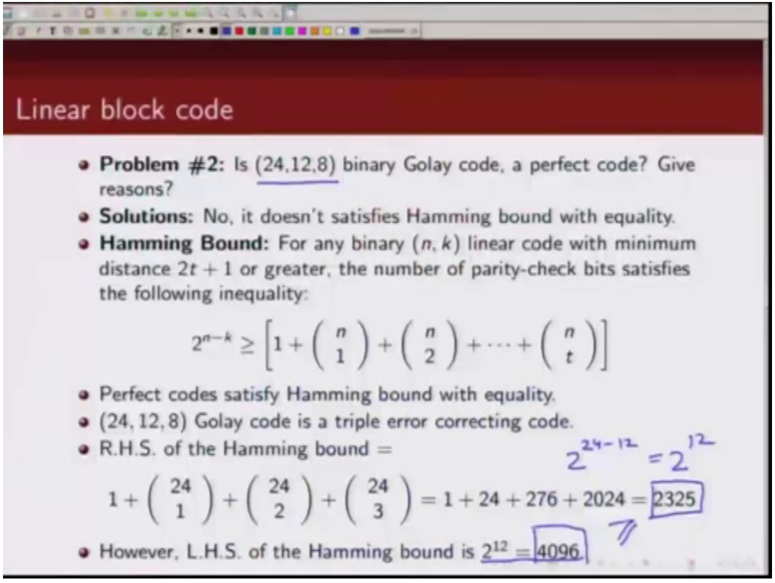
So this particular code does not satisfy Hamming bound with equality and

(Refer Slide Time 05:39)



hence it is not a perfect code.

(Refer Slide Time 05:42)



Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]$$

- Perfect codes satisfy Hamming bound with equality.
- $(24, 12, 8)$ Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

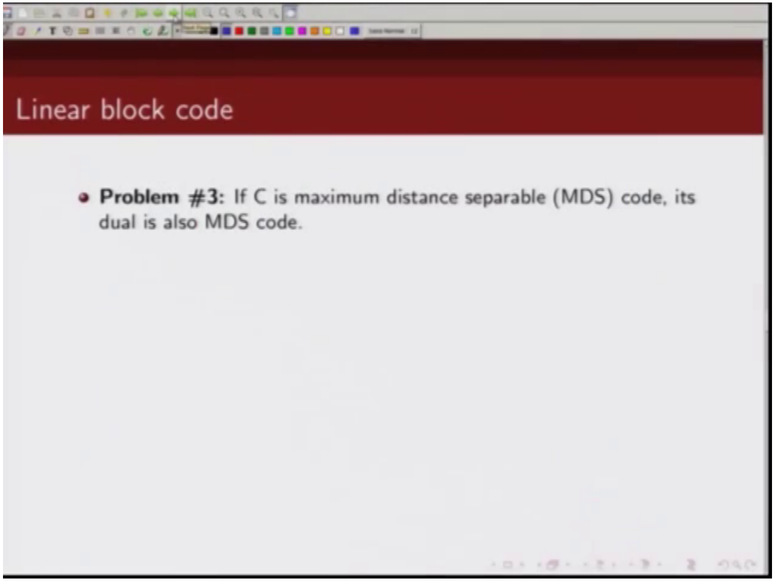
$2^{24-12} = 2^{12}$

$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = \boxed{2325}$$

- However, L.H.S. of the Hamming bound is $2^{12} = \boxed{4096}$.

Next

(Refer Slide Time 05:45)

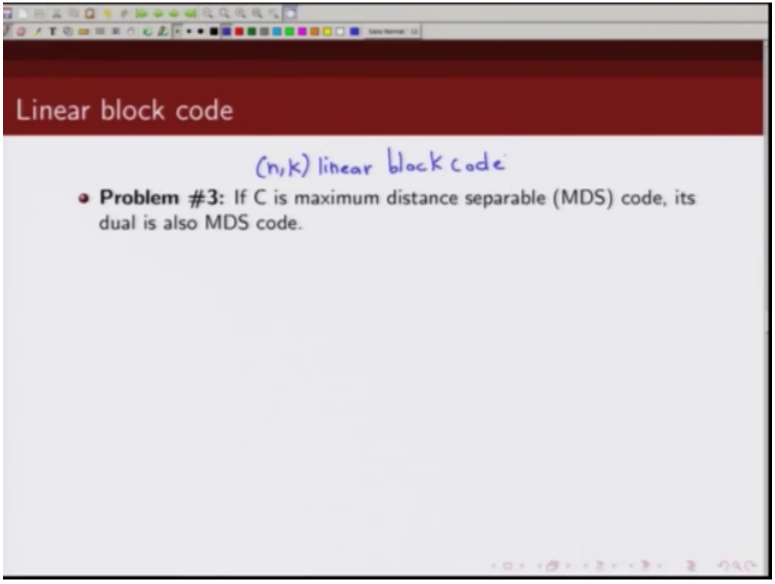


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.

if we are given a linear block code C, let's just say an n k linear block code, it is said that this code

(Refer Slide Time 06:01)



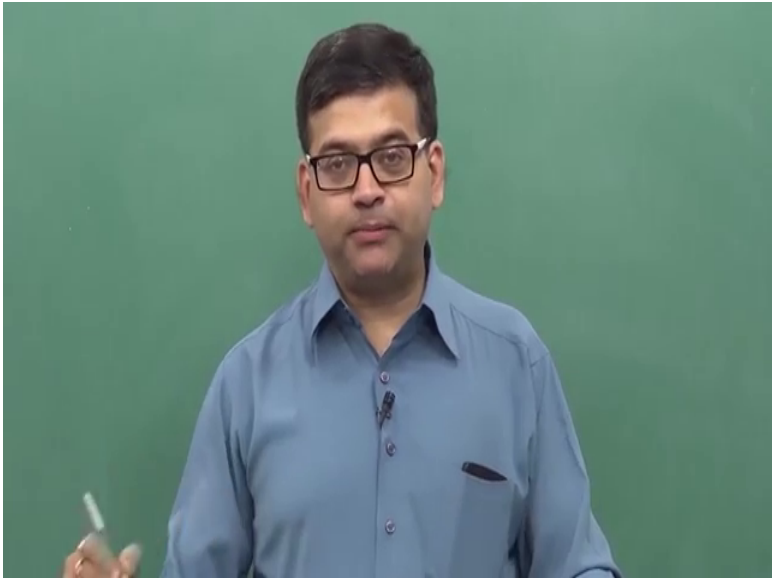
Linear block code

(n,k) linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.

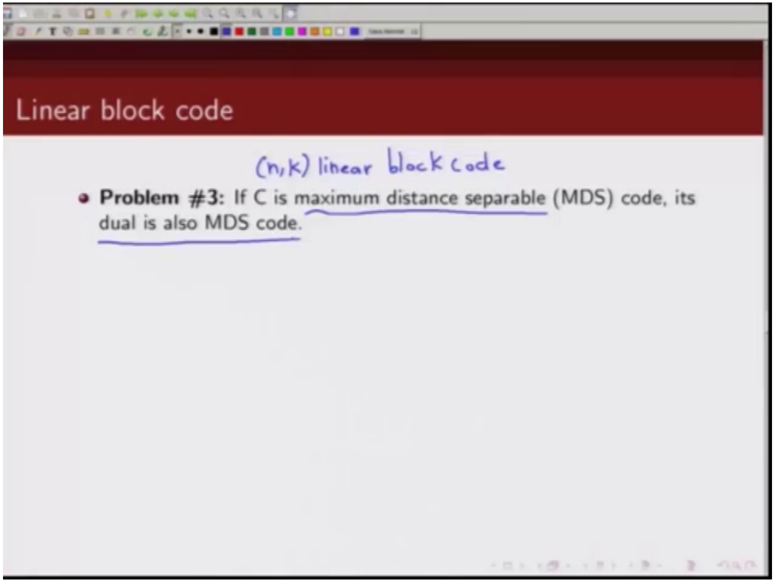
is maximum distance separable. Then show that its dual code is also maximum distance separable.

(Refer Slide Time 06:10)



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

(Refer Slide Time 06:24)



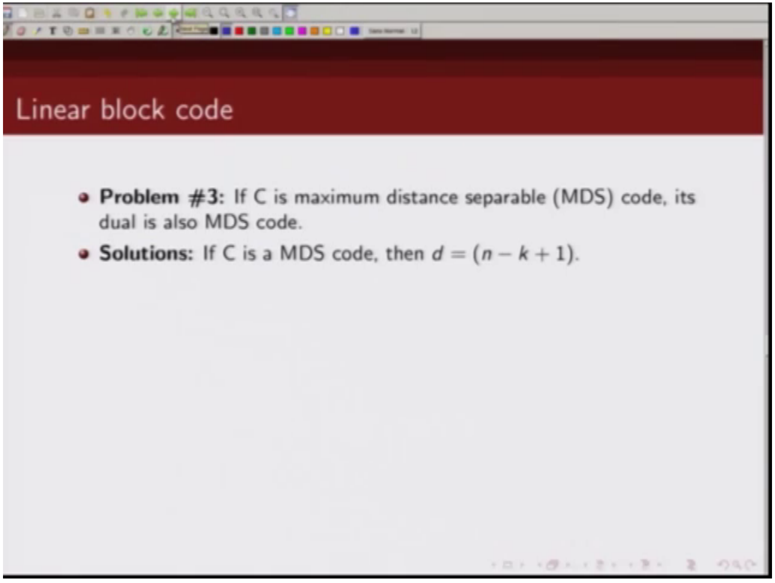
Linear block code

(n,k) linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.

separable code. So then

(Refer Slide Time 06:27)

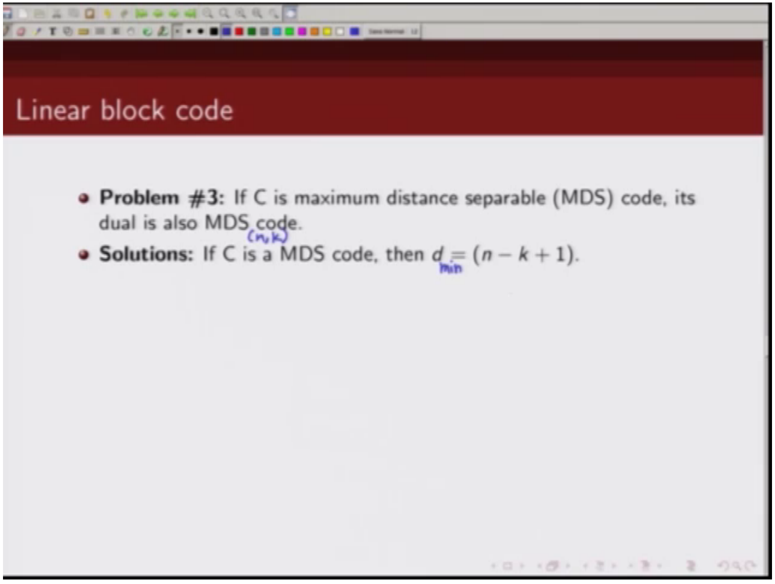


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.

if this n k code is maximum distance separable then minimum distance of this code should be n minus

(Refer Slide Time 06:38)

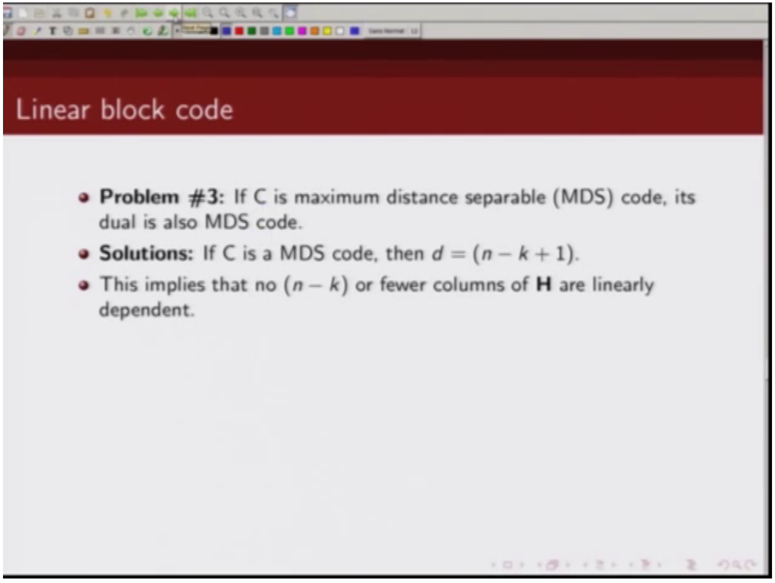


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS $\underset{(n,k)}{\text{code}}$.
- **Solutions:** If C is a MDS code, then $d_{min} = (n - k + 1)$.

k plus 1, right? This follows from the fact that our given linear block code C is maximum distance separable. Now if the minimum

(Refer Slide Time 06:53)



Linear block code

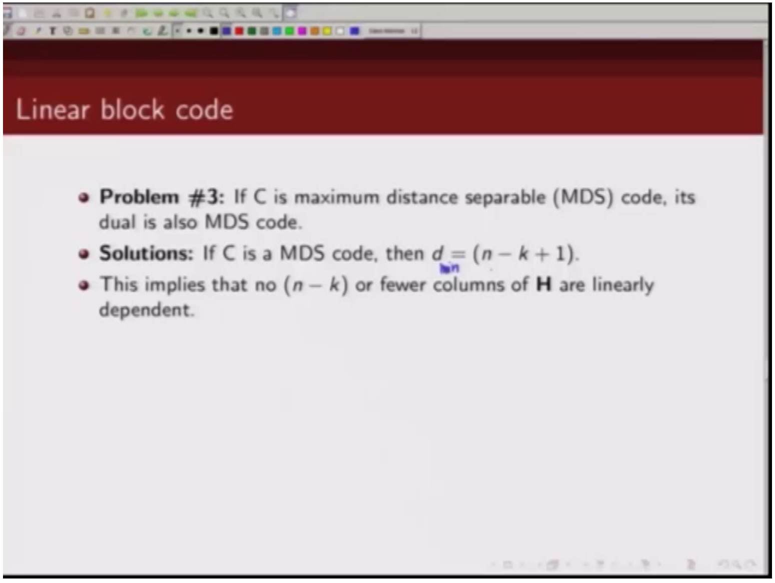
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.

distance is, if the minimum distance is n minus k plus 1, it means that there are no n minus k or less columns in the parity check matrix

(Refer Slide Time 07:10)

of this code which are linearly dependent. If you recall the minimum number of

(Refer Slide Time 07:17)



Linear block code

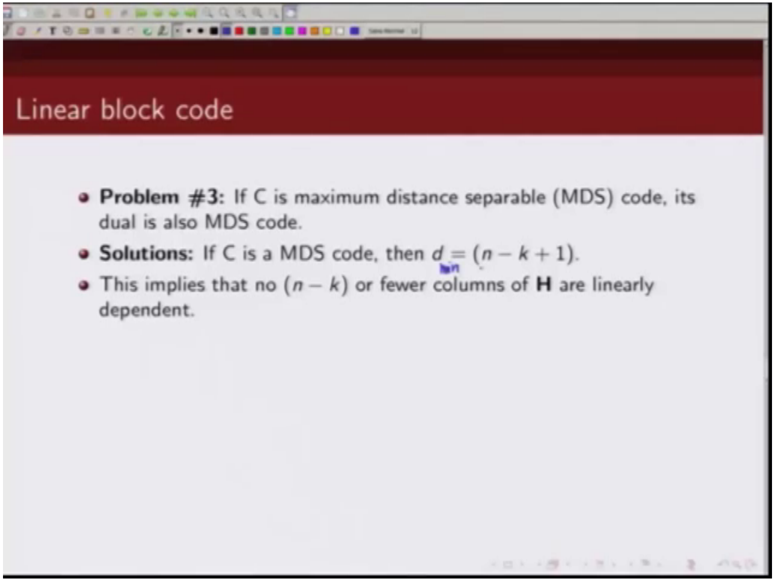
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d_{min} = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.

columns of this parity check matrix which are linearly dependent 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 zero is the

(Refer Slide Time 07:34)

minimum distance of the code. Now if the minimum distance of the code is

(Refer Slide Time 07:38)

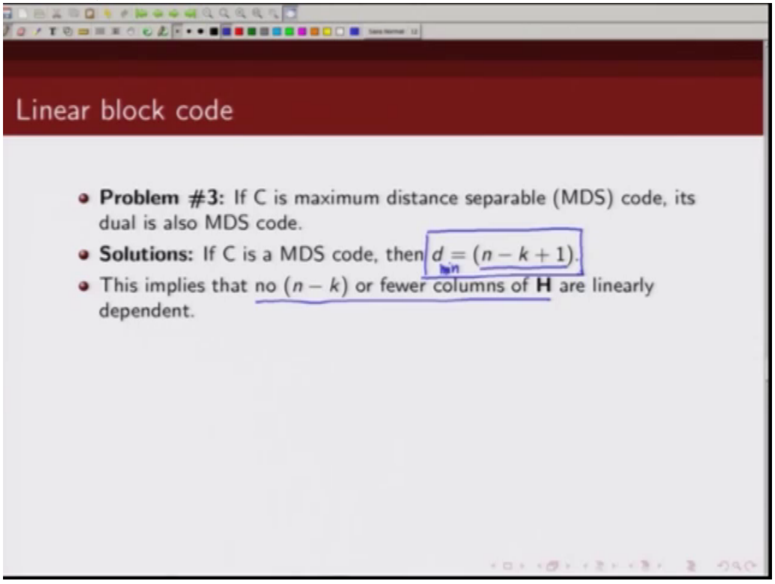


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d_{min} = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.

n minus k plus 1 it means no n minus k or less columns of this parity check matrix will add up to zero. So that's what we are saying, no n minus k or fewer columns of this parity check matrix are linearly dependent. That is because the minimum distance of this code is n minus k

(Refer Slide Time 08:08)

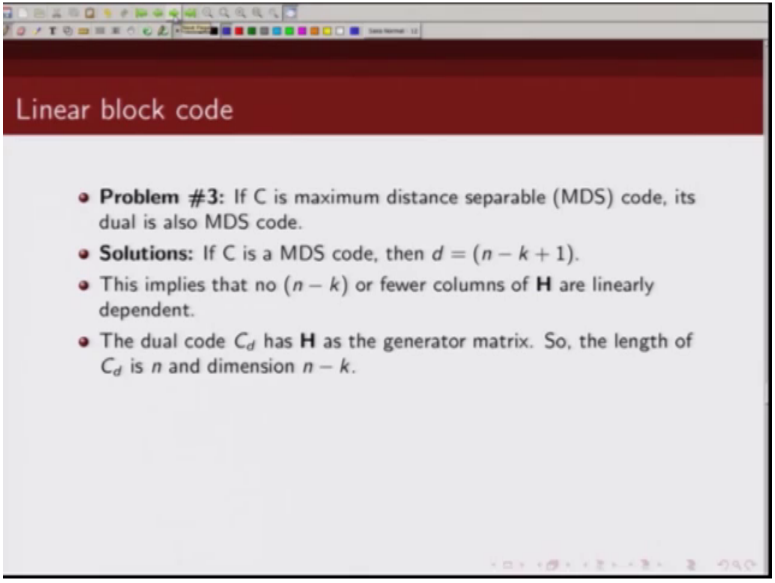


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $\boxed{d_{min} = (n - k + 1)}$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.

plus 1. Now

(Refer Slide Time 08:11)

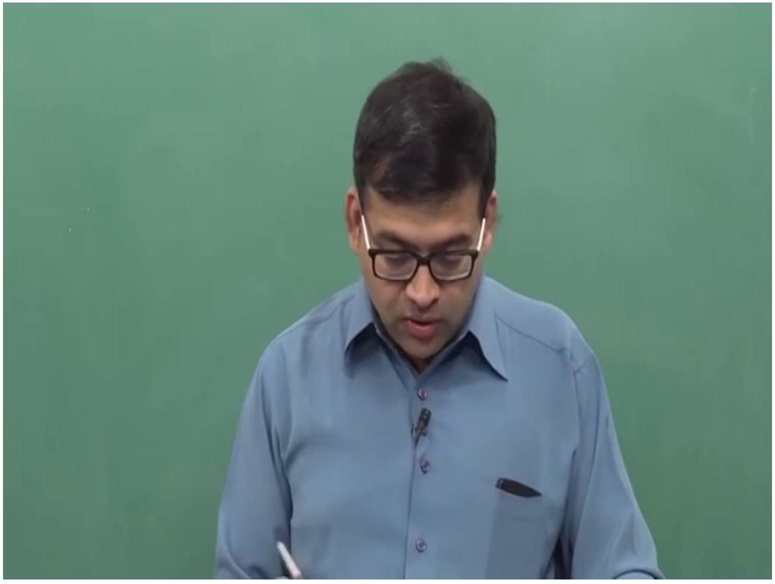


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.

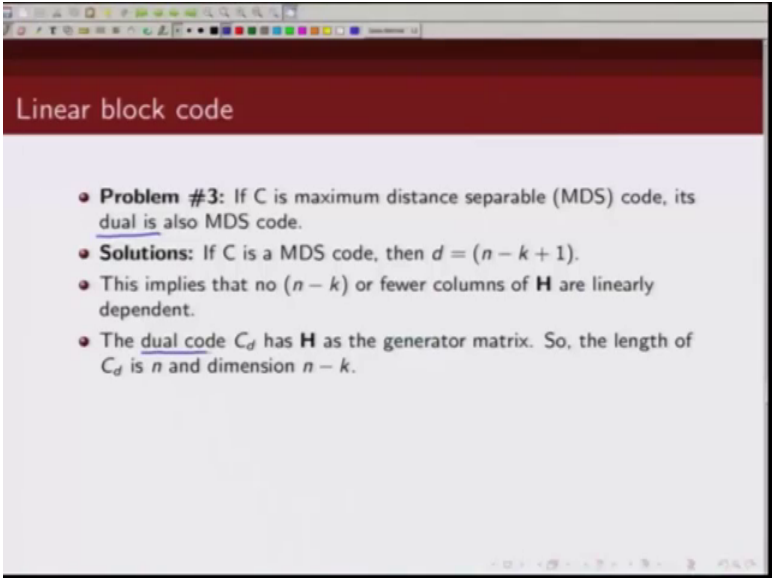
let's look at its dual code. Now what do we know about the dual code? We know that the generator matrix of a dual code is same as parity check matrix of the original code. So

(Refer Slide Time 08:30)



for this dual code

(Refer Slide Time 08:32)

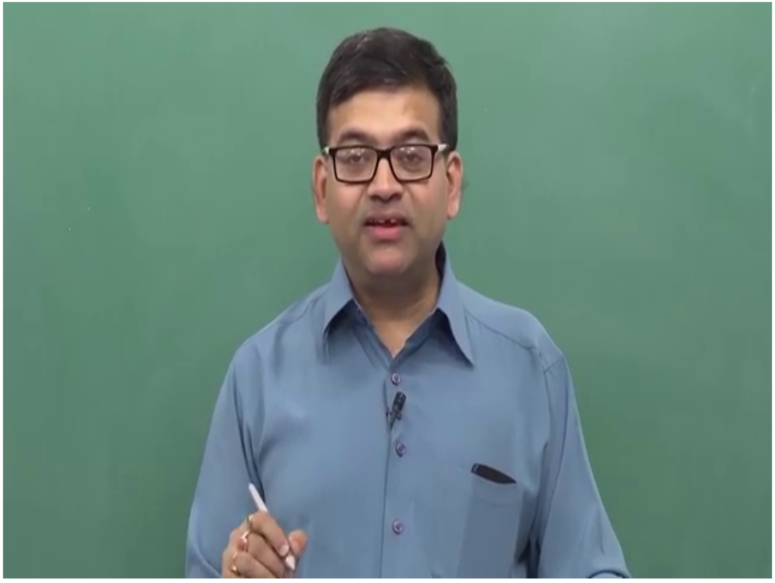


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.

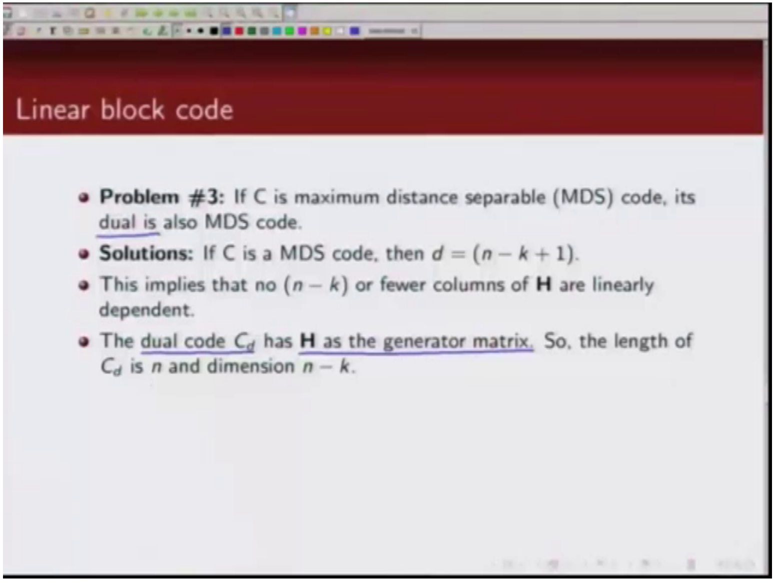
then, H will be the generator matrix. This follows from

(Refer Slide Time 08:37)



the property of dual code. And we also know the dual

(Refer Slide Time 08:43)

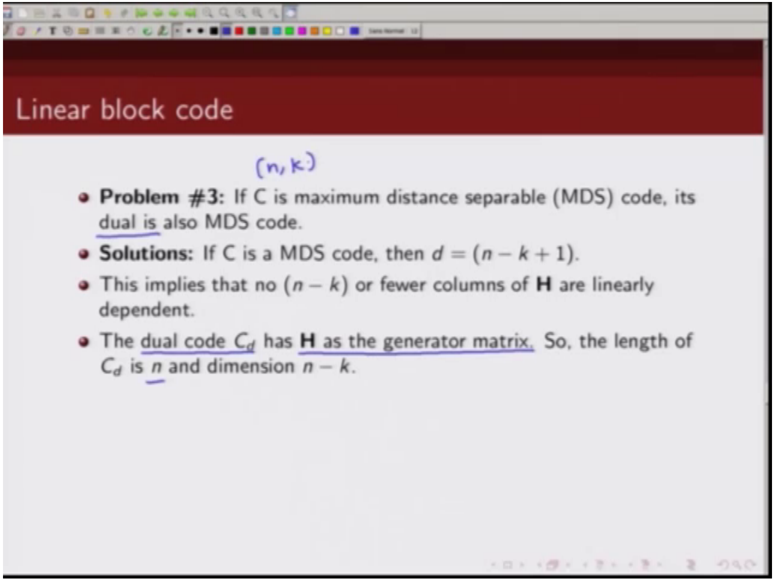


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.

code codeword length should be n and since this was an n k code the dual

(Refer Slide Time 08:50)



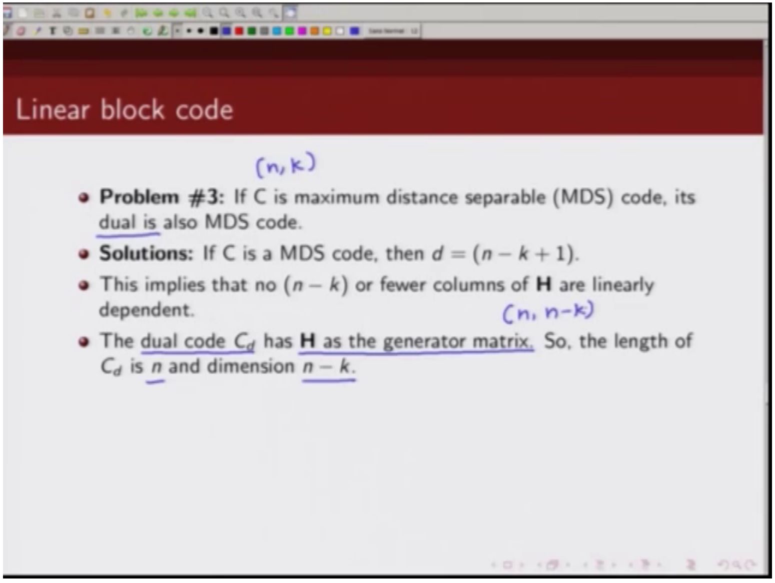
Linear block code

(n, k)

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.

code dimension must be n minus k. Now to prove that this dual code which is specified by these parameters,

(Refer Slide Time 09:03)



Linear block code

(n, k)

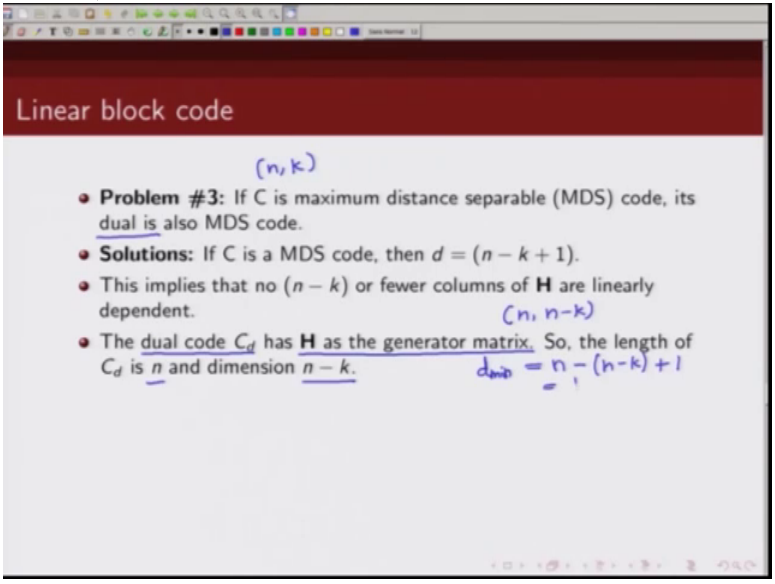
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.

$(n, n-k)$

- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.

length n and dimension n minus 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 minus dimension is n minus k plus 1. So we will have to show that

(Refer Slide Time 09:26)



Linear block code

(n, k)

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.

$(n, n-k)$

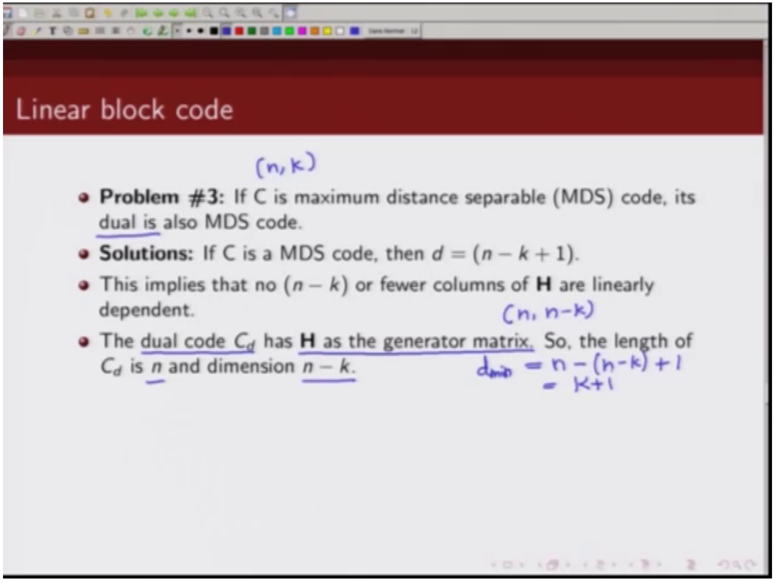
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.

$d_{min} = n - (n-k) + 1$

$=$

minimum distance

(Refer Slide Time 09:28)



Linear block code

(n, k)

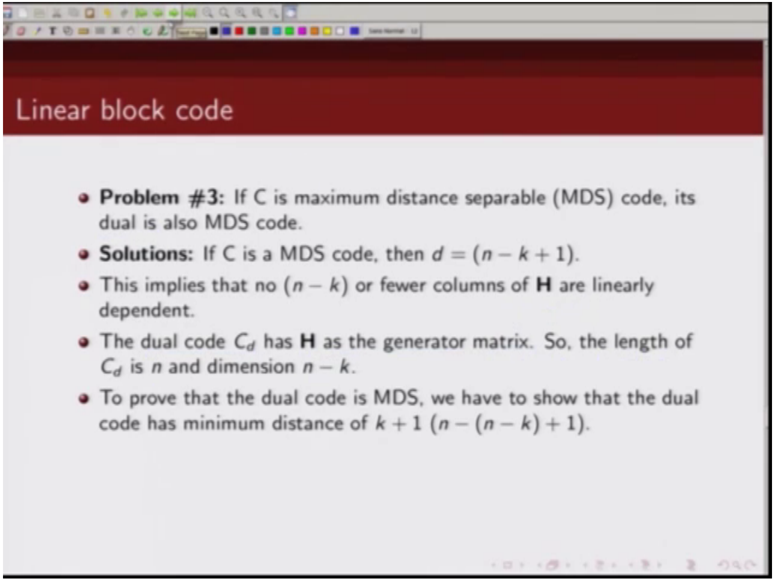
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.

$(n, n-k)$

$$d_{min} = n - (n-k) + 1$$
$$= k+1$$

of the dual code is k plus 1. So that's what

(Refer Slide Time 09:37)

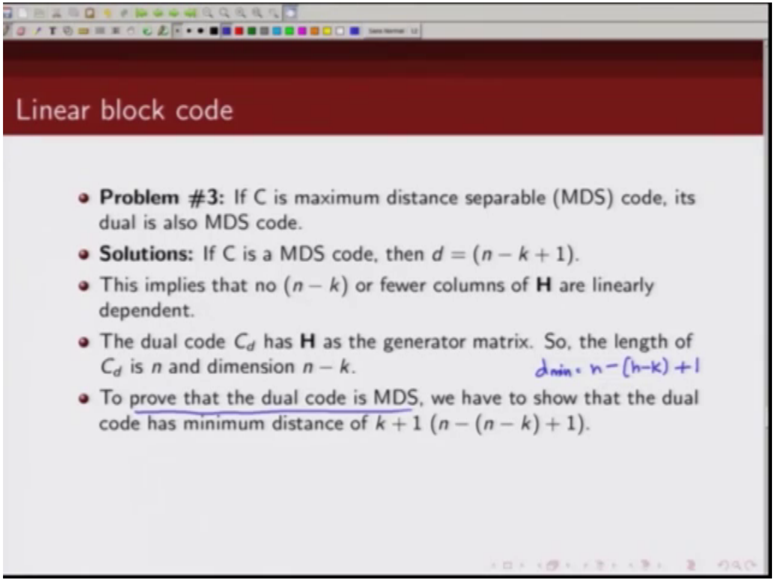


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.

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 minus dimension of the code which is n minus k plus 1 and this comes out to be

(Refer Slide Time 10:00)

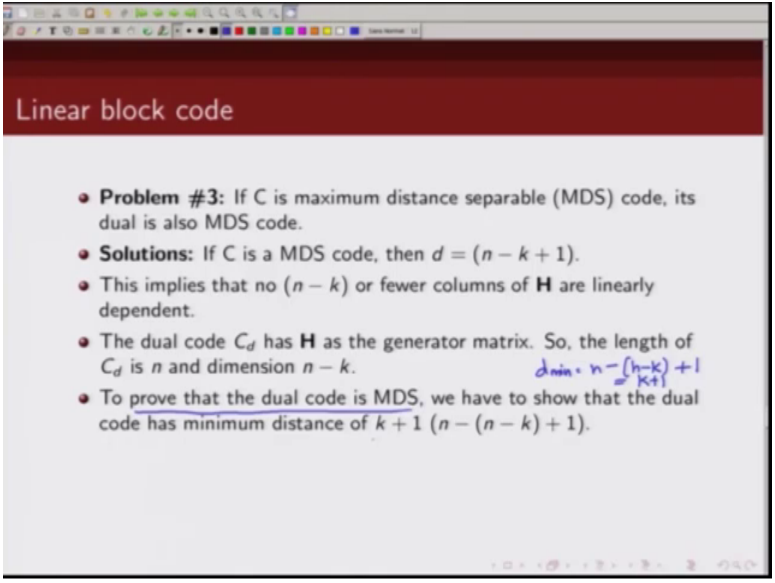


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n-k+1)$.
- This implies that no $(n-k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n-k$. $d_{min} = n-(n-k)+1$
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k+1$ $(n-(n-k)+1)$.

k plus 1. So we will have to show that

(Refer Slide Time 10:04)



Linear block code

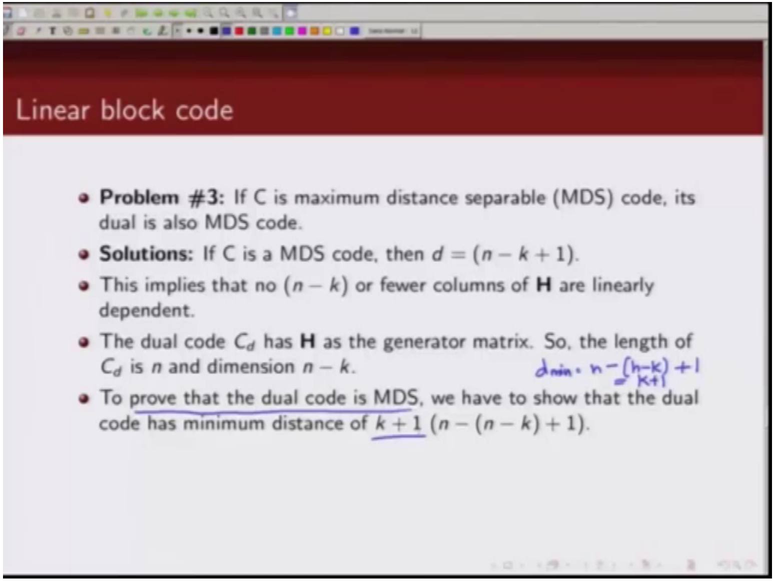
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n-k+1)$.
- This implies that no $(n-k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n-k$. $d_{min} = n-\underbrace{(n-k)+1}_{=k+1}$
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k+1$ $(n-(n-k)+1)$.

the minimum distance of the dual of this code

(Refer Slide Time 10:09)

is k plus 1.

(Refer Slide Time 10:11)



Linear block code

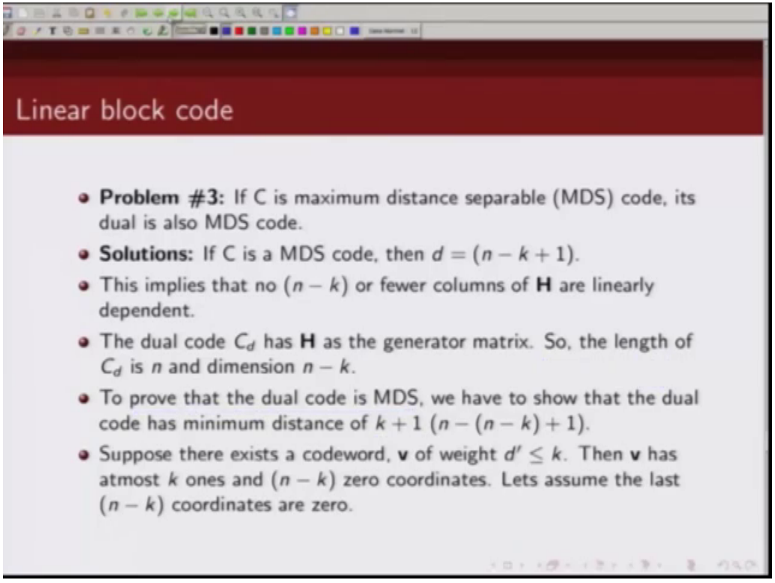
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.

$d_{min} = n - (n-k) + 1$
$= k+1$

- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $\underline{k + 1}$ $(n - (n - k) + 1)$.

Now

(Refer Slide Time 10:14)



Linear block code

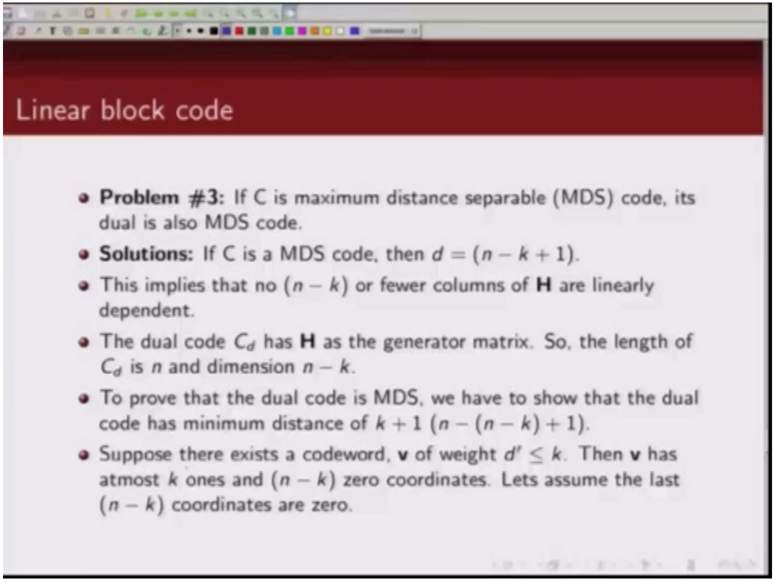
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.
- Suppose there exists a codeword, $\mathbf{v}$ of weight $d' \leq k$. Then $\mathbf{v}$ has atmost k ones and $(n - k)$ zero coordinates. Lets assume the last $(n - k)$ coordinates are zero.

to prove this result we will take help of what we call method of contradiction. So how does method of contradiction work? We will start off with the assumption that there exists a codeword of weight

(Refer Slide Time 10:30)

less than equal to k. So we will assume that minimum distance is not k plus 1. And then we will show that, through the properties of this code that this condition is not possible, for assumption that there exists a codeword 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 plus 1 and hence the minimum distance of the dual code is k plus 1. So this is the approach that we are going to follow. So as we said

(Refer Slide Time 11:15)



Linear block code

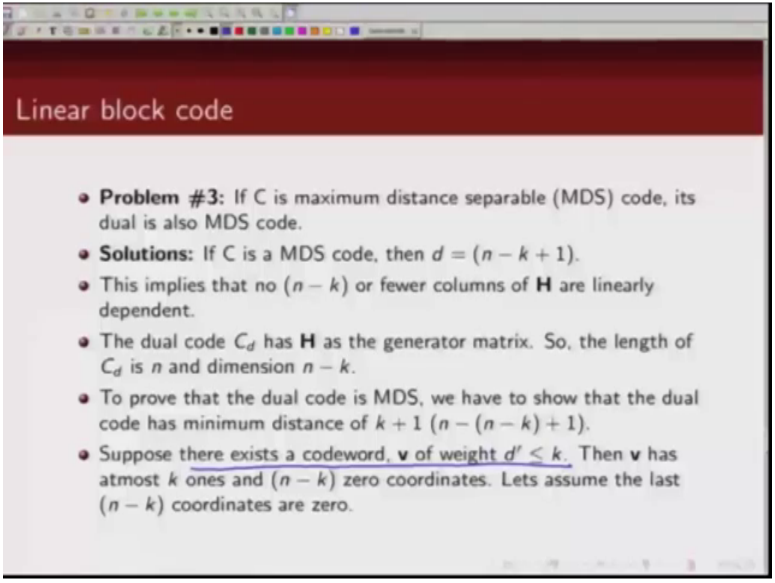
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of **H** are linearly dependent.
- The dual code C_d has **H** as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.
- Suppose there exists a codeword, **v** of weight $d' \leq k$. Then **v** has atmost k ones and $(n - k)$ zero coordinates. Lets assume the last $(n - k)$ coordinates are zero.

in method of contradiction we will first assume that, let's assume that there exists the codeword of weight less than k plus 1. So we assume that there exists a codeword v of weight d prime which is less than equal to k. Now if there exists a codeword

(Refer Slide Time 11:40)

of weight less than equal to k, then what does it mean? That means that codeword weight will at most have k once right, so

(Refer Slide Time 11:51)



Linear block code

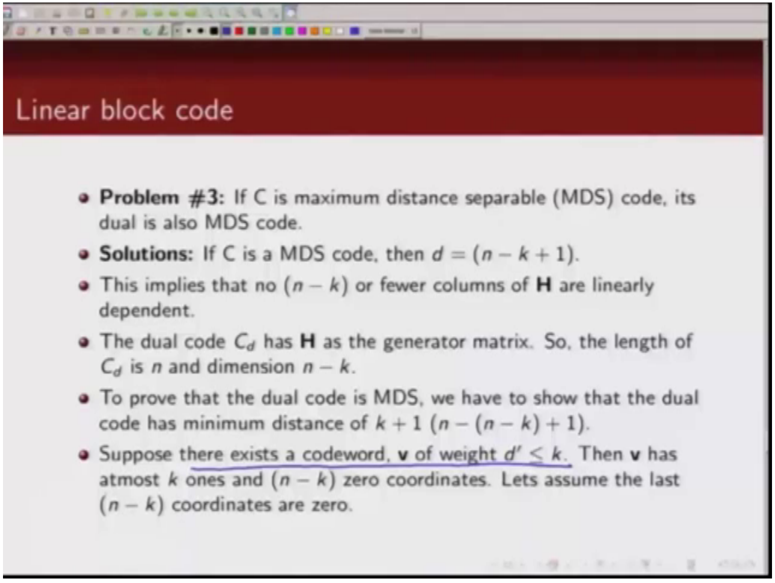
- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.
- Suppose there exists a codeword, $\mathbf{v}$ of weight $d' \leq k$. Then $\mathbf{v}$ has atmost k ones and $(n - k)$ zero coordinates. Lets assume the last $(n - k)$ coordinates are zero.

our codeword be the n bit codeword, so out of this at most k bits are 1. Remaining n minus k

(Refer Slide Time 12:01)

bits are zero.

(Refer Slide Time 12:04)

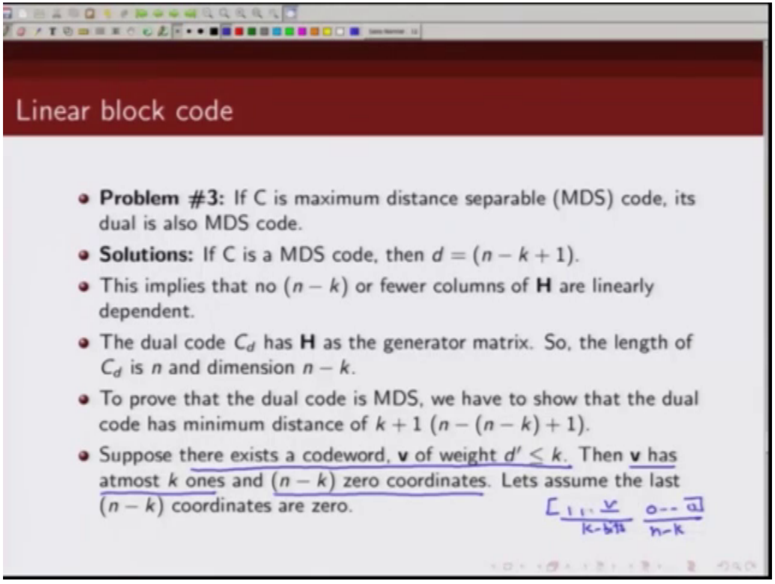


Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.
- Suppose there exists a codeword, $\mathbf{v}$ of weight $d' \leq k$. Then $\mathbf{v}$ has atmost k ones and $(n - k)$ zero coordinates. Lets assume the last $(n - k)$ coordinates are zero.

So we can at most have k 1s and n minus k or more bits are zero. Without loss of generality let's assume that those bits which are zero are towards the end. So what we are assuming is, let's say this is our codeword v. So first k bits have 1's and these, these remaining bits have zeroes. So these are, these bits have zeroes and these bits have 1s,

(Refer Slide Time 12:37)



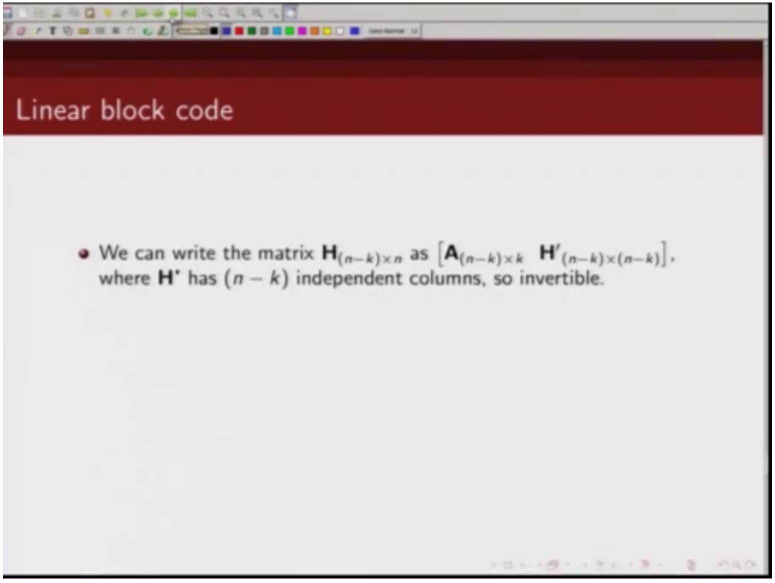
Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.
- Suppose there exists a codeword, $\mathbf{v}$ of weight $d' \leq k$. Then $\mathbf{v}$ has atmost k ones and $(n - k)$ zero coordinates. Lets assume the last $(n - k)$ coordinates are zero.

$$[\underbrace{1\,1\cdots v}_{k\text{-bits}}\ \underbrace{0\cdots 0}_{n-k}]$$

Ok let’s assume that. Now

(Refer Slide Time 12:43)

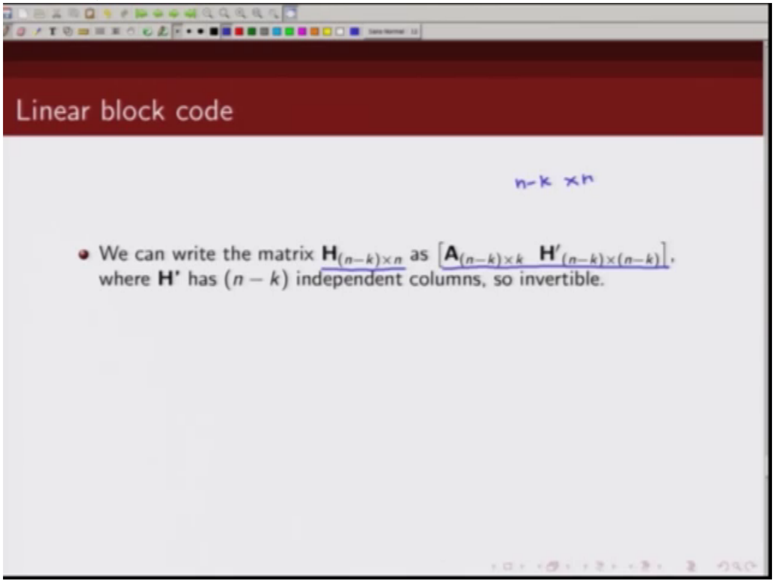


Linear block code

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $\left[\mathbf{A}_{(n-k)\times k} \;\; \mathbf{H}'_{(n-k)\times(n-k)}\right]$, where $\mathbf{H}'$ has $(n-k)$ independent columns, so invertible.

the parity check matrix of the original code which is the generator matrix of our dual code can be written in this particular form. Now please note this parity check matrix is n minus k cross n matrix so this I am writing as

(Refer Slide Time 13:03)



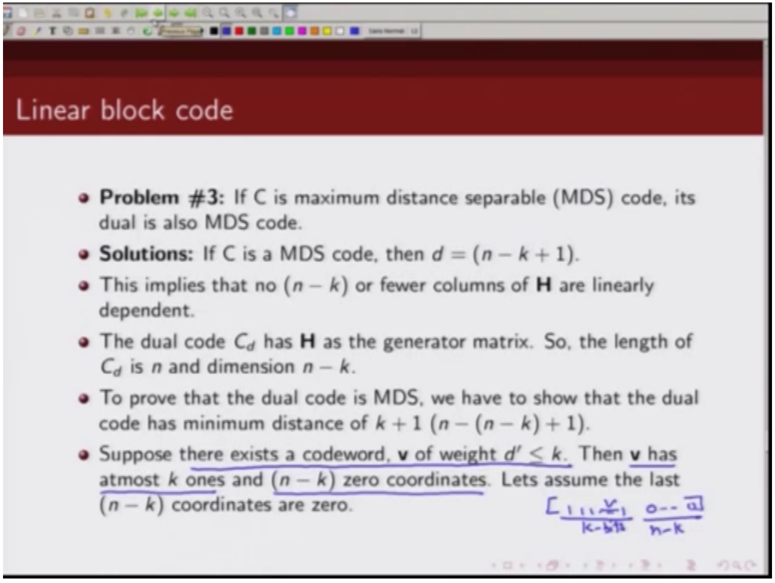
Linear block code

$n-k \times n$

- We can write the matrix $\underline{\mathbf{H}_{(n-k)\times n}}$ as $\left[\underline{\mathbf{A}_{(n-k)\times k} \;\; \mathbf{H}'_{(n-k)\times(n-k)}}\right]$, where $\mathbf{H}'$ has $(n-k)$ independent columns, so invertible.

one matrix which is a matrix, n minus k cross k and then there is an invertible matrix which I call H prime which is n minus k cross n minus k. Now what was the rank of this matrix H? Remember we have,

(Refer Slide Time 13:25)



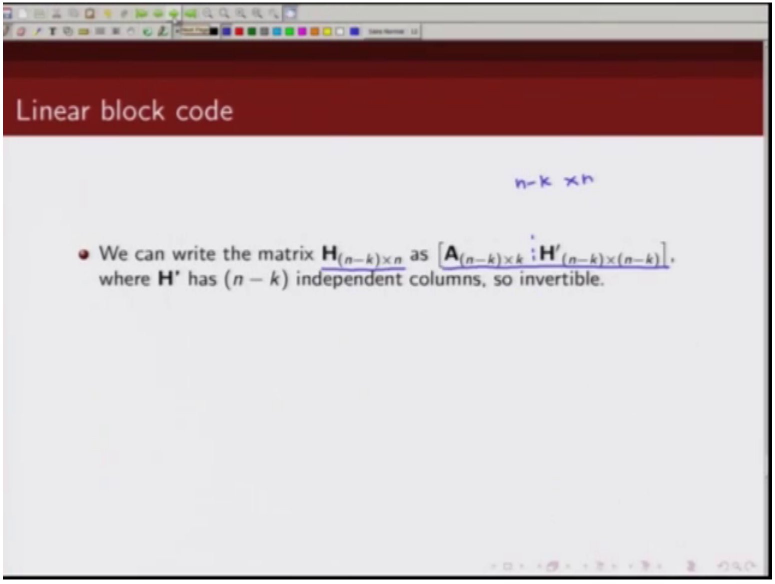
Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ $(n - (n - k) + 1)$.
- Suppose there exists a codeword, $\mathbf{v}$ of weight $d' \leq k$. Then $\mathbf{v}$ has atmost k ones and $(n - k)$ zero coordinates. Lets assume the last $(n - k)$ coordinates are zero.

$$[\underbrace{1\,1\,1 \ldots 1}_{k\text{-wt}}\ \underbrace{0 \cdots 0}_{n-k}]$$

because minimum distance of the code was n minus k plus 1, so no n minus k or fewer columns of H were linearly dependent. So the row rank was

(Refer Slide Time 13:37)



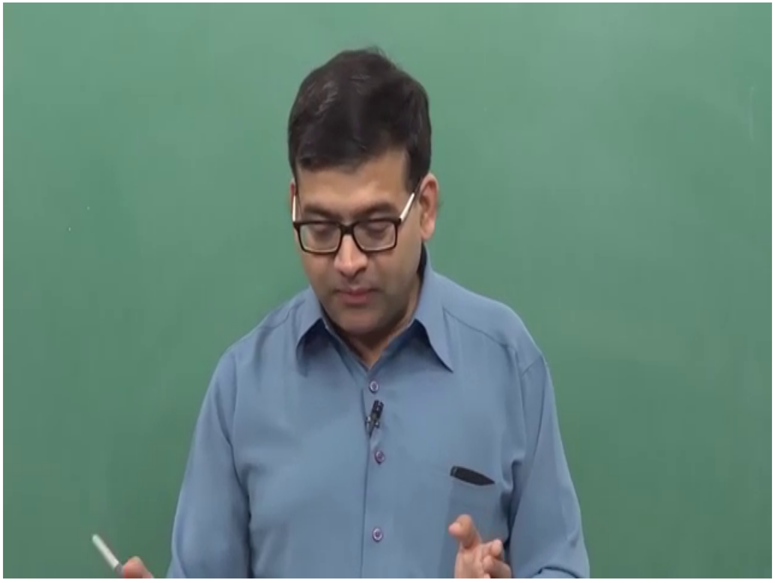
Linear block code

$n-k \times n$

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k} \vdots \mathbf{H}'_{(n-k)\times(n-k)}]$, where $\mathbf{H}'$ has $(n - k)$ independent columns, so invertible.

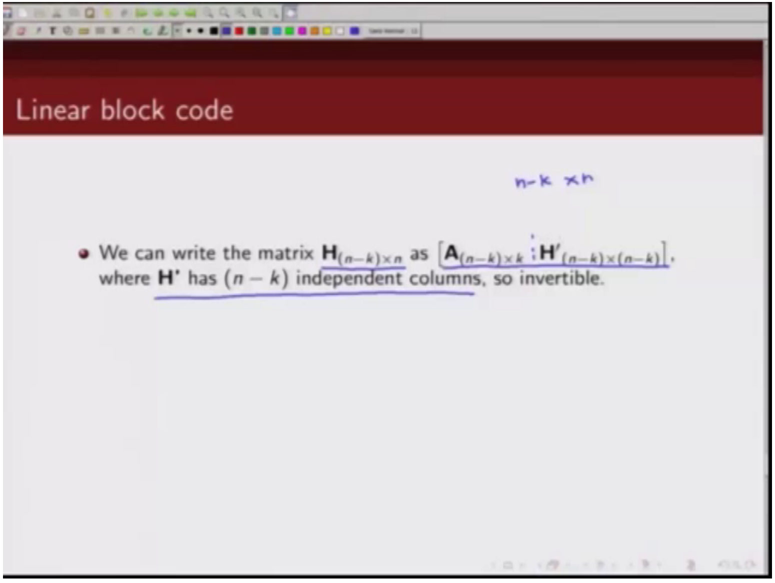
n minus k. So column rank is also n minus k. What does it mean? It means that n minus k, there are n minus k independent columns in this matrix and let's say

(Refer Slide Time 13:50)



those n minus k independent columns are

(Refer Slide Time 13:52)



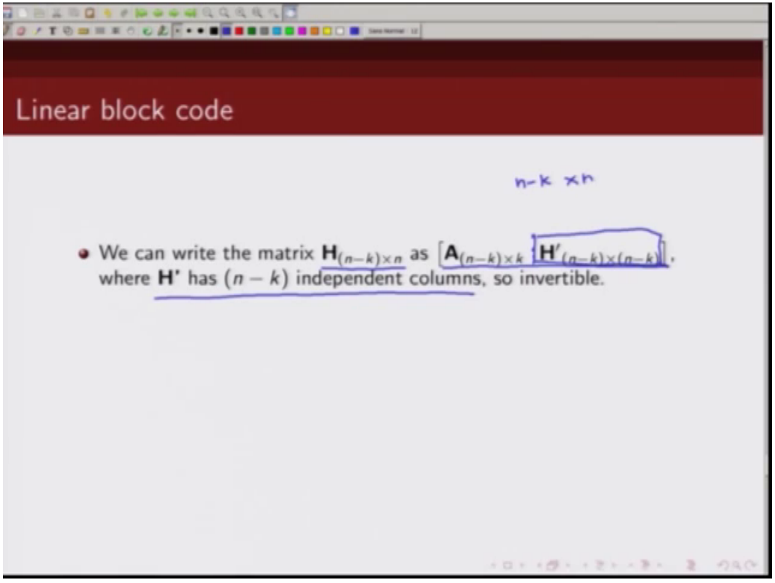
Linear block code

n-k ×n

- We can write the matrix $\underline{\mathbf{H}_{(n-k)\times n}}$ as $\underline{[\mathbf{A}_{(n-k)\times k} \vdots \mathbf{H}'_{(n-k)\times(n-k)}]}$, where $\underline{\mathbf{H}' \text{ has } (n-k) \text{ independent columns}}$, so invertible.

these, given by this H hat, Ok.

(Refer Slide Time 13:57)



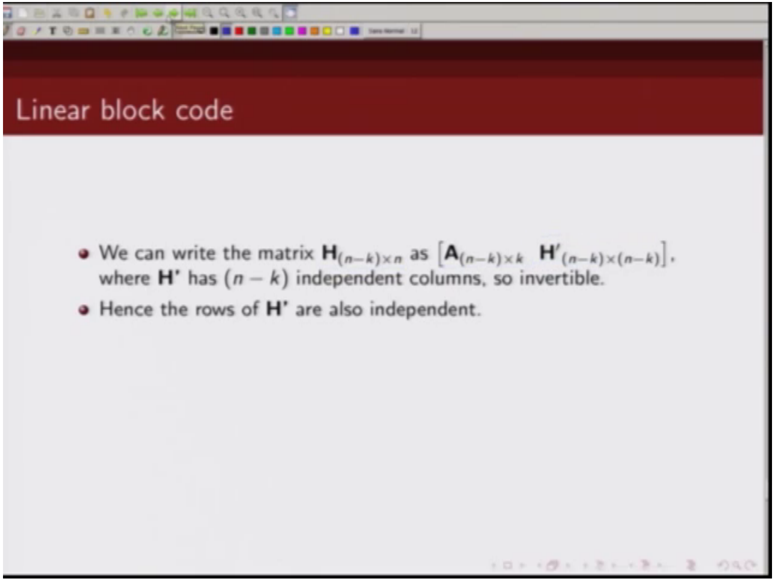
Linear block code

$n-k \times n$

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k}\ \ \boxed{\mathbf{H}'_{(n-k)\times(n-k)}}]$, where **H'** has $(n-k)$ independent columns, so invertible.

This is, so since this has independent columns this can be inverted also.

(Refer Slide Time 14:05)

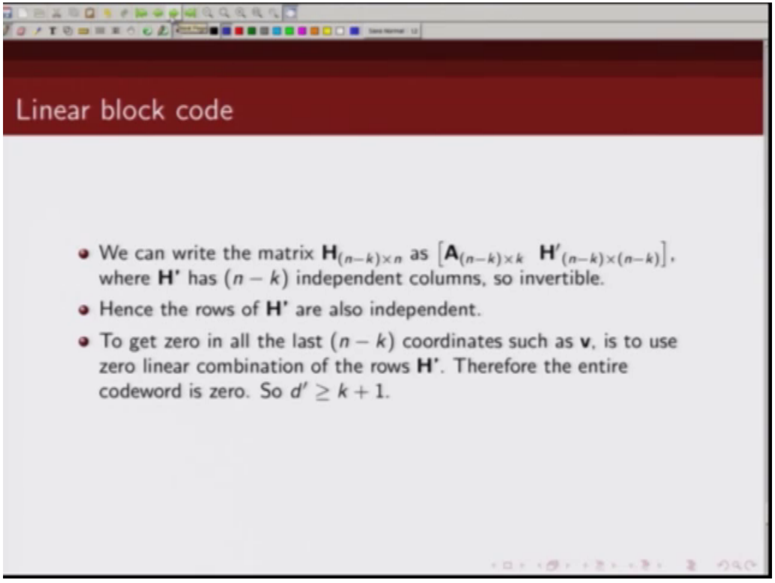


Linear block code

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k}\ \ \mathbf{H}'_{(n-k)\times(n-k)}]$, where **H'** has $(n-k)$ independent columns, so invertible.
- Hence the rows of **H'** are also independent.

And rows of this matrix H hat is also independent because it is ranked

(Refer Slide Time 14:11)

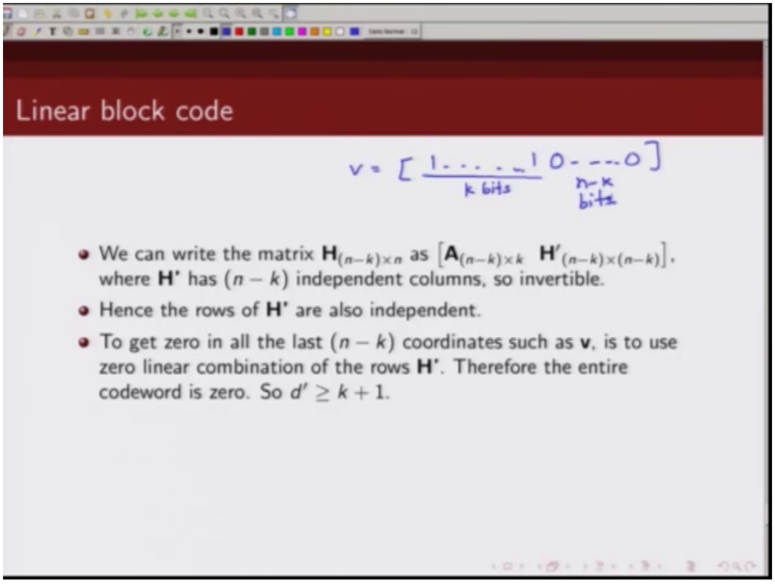


Linear block code

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $\left[\mathbf{A}_{(n-k)\times k} \;\; \mathbf{H}'_{(n-k)\times(n-k)}\right]$, where $\mathbf{H'}$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H'}$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H'}$. Therefore the entire codeword is zero. So $d' \geq k+1$.

n minus k as well. Now remember what did we say about our codeword v? We said our codeword v, the first k bits at most first k bits are 1, so these first k bits can at most be 1 and these are all zeroes. So remaining n minus k bits are all

(Refer Slide Time 14:35)



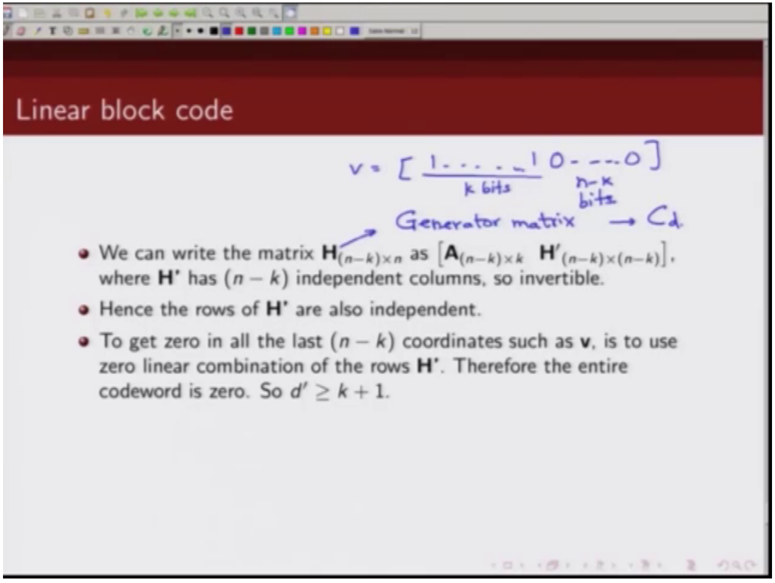
Linear block code

$$v = [\underbrace{1 \cdots\cdots 1}_{k \text{ bits}} \underbrace{0 \cdots 0}_{\substack{n-k \\ \text{bits}}}]$$

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $\left[\mathbf{A}_{(n-k)\times k} \;\; \mathbf{H}'_{(n-k)\times(n-k)}\right]$, where $\mathbf{H'}$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H'}$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H'}$. Therefore the entire codeword is zero. So $d' \geq k+1$.

zero. Now this H matrix is the generator matrix, this is a generator matrix for dual code C d. So

(Refer Slide Time 14:51)



Linear block code

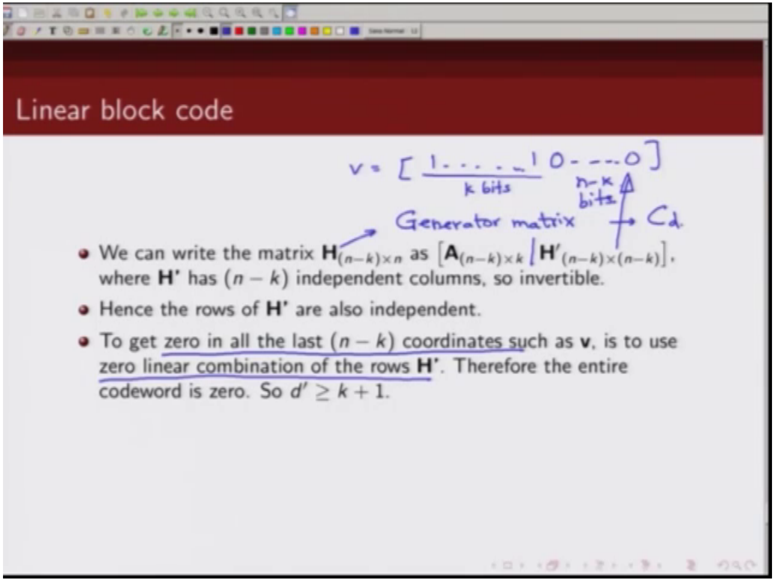
$v = [\underbrace{1 \ldots\ldots 1}_{k \text{ bits}} \underbrace{0 \ldots 0}_{n-k \text{ bits}}]$

Generator matrix → C_d

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k} \;\; \mathbf{H'}_{(n-k)\times(n-k)}]$, where $\mathbf{H'}$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H'}$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H'}$. Therefore the entire codeword is zero. So $d' \geq k+1$.

if we have to generate a codeword 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 minus k coordinates, now this consists of n minus k linearly independent columns and rows. Now to get zeroes in last n minus k coordinates the only way we can get it is if we use a zero linear combination 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

(Refer Slide Time 15:35)



Linear block code

$v = [\underbrace{1 \ldots\ldots 1}_{k \text{ bits}} \underbrace{0 \ldots 0}_{n-k \text{ bits}}]$

Generator matrix → C_d

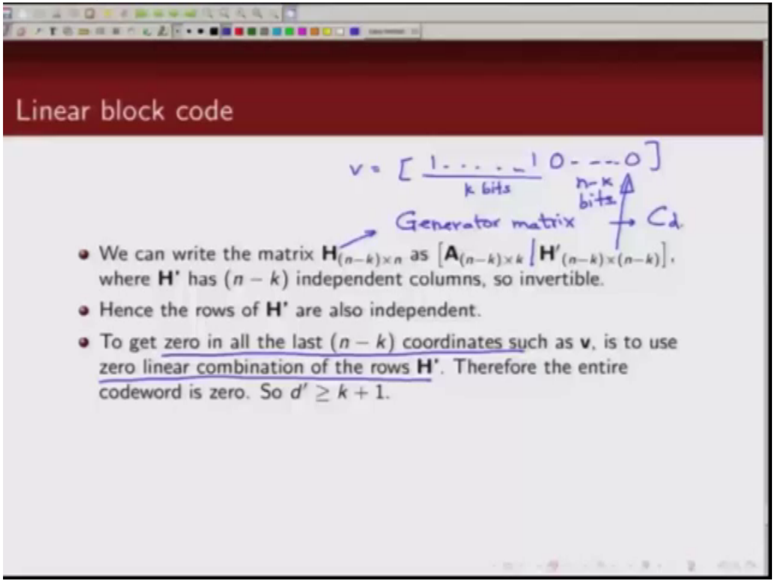
- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k} \mid \mathbf{H'}_{(n-k)\times(n-k)}]$, where $\mathbf{H'}$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H'}$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H'}$. Therefore the entire codeword is zero. So $d' \geq k+1$.

is a linear independent columns and rows, so only way we can get all zeroes here is if we take zero linear combination. So we multiply all the rows of this generator matrix by zero but if we do that what is the minimum distance that we get? If we do that the codeword that we get is

(Refer Slide Time 15:58)

all zero codeword. So what it means then that our assumption

(Refer Slide Time 16:05)



Linear block code

$v = [\underbrace{1 \cdots\cdots 1}_{k \text{ bits}}\ \underbrace{0 - - - 0}_{n-k \text{ bits}}]$

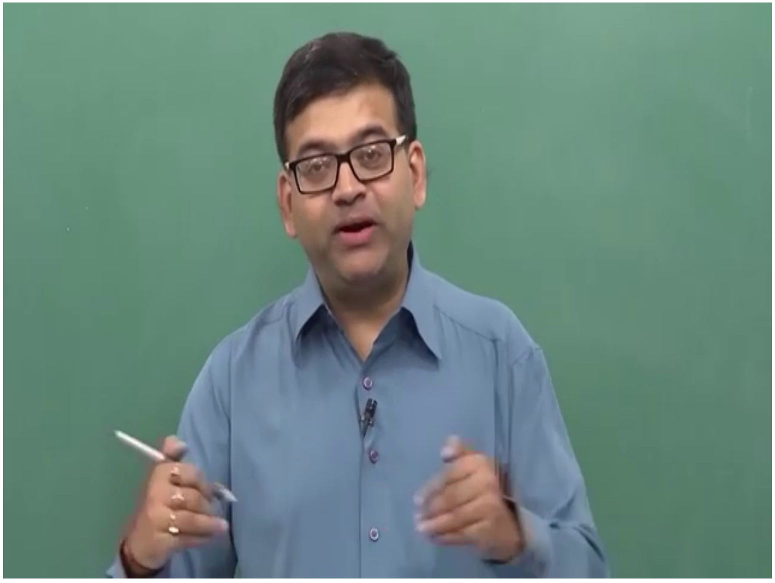
Generator matrix

C_d

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k} | \mathbf{H'}_{(n-k)\times(n-k)}]$, where $\mathbf{H'}$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H'}$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H'}$. Therefore the entire codeword is zero. So $d' \geq k+1$.

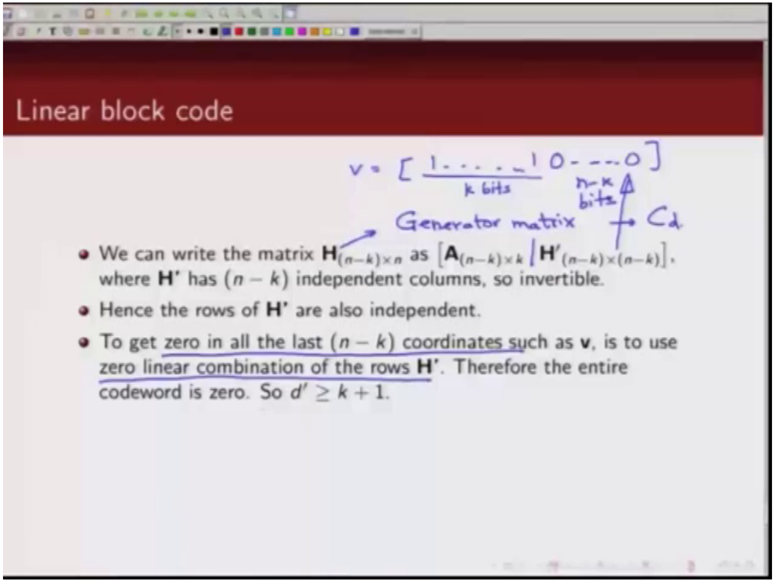
that there exists a codeword of weight up to k is incorrect because we are not able to construct that codeword using the generator matrix

(Refer Slide Time 16:18)



of the dual code. Hence our assumption that minimum distance of the code, there exists a codeword of weight less than equal to k was incorrect, so we can conclude

(Refer Slide Time 16:33)



Linear block code

$$v = [\underbrace{1 \ldots\ldots 1}_{k \text{ bits}} \underbrace{0 \ldots 0}_{n-k \text{ bits}}]$$

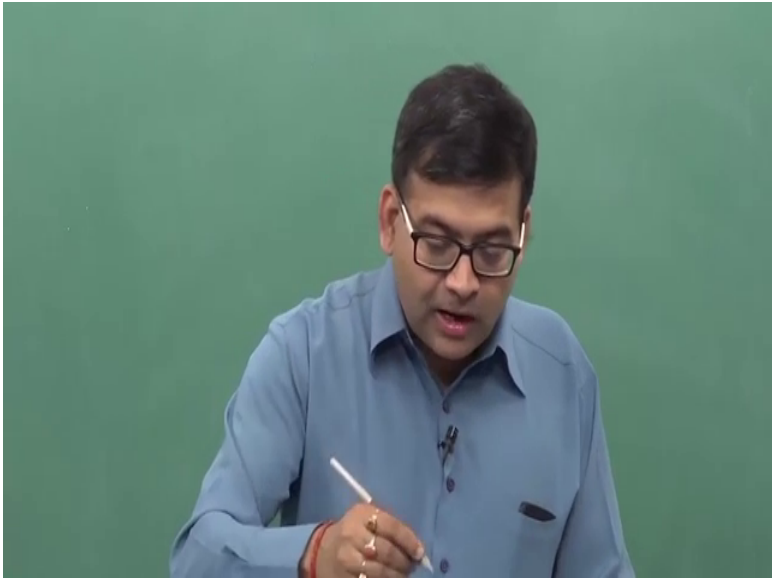
Generator matrix

C_d

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $[\mathbf{A}_{(n-k)\times k} | \mathbf{H'}_{(n-k)\times(n-k)}]$, where **H'** has $(n-k)$ independent columns, so invertible.
- Hence the rows of **H'** are also independent.
- To get zero in all the last $(n-k)$ coordinates such as **v**, is to use zero linear combination of the rows **H'**. Therefore the entire codeword is zero. So $d' \geq k+1$.

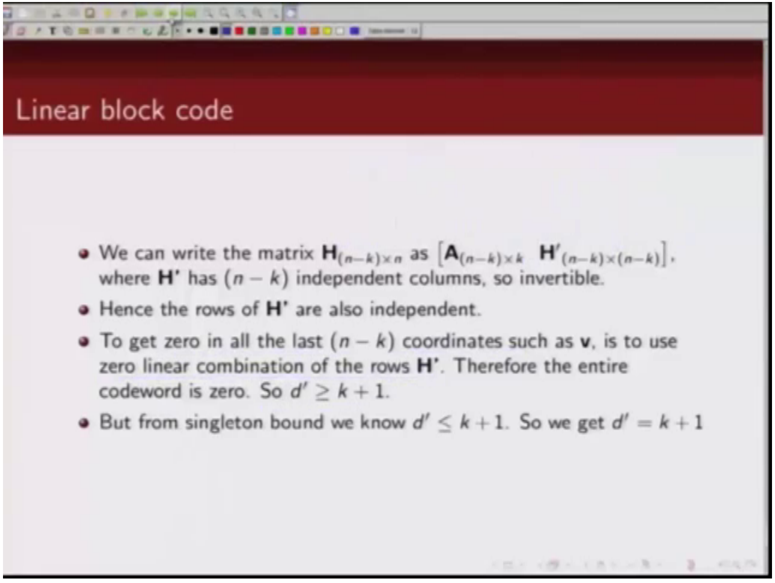
or say that the minimum distance of the code is at least k plus 1. Ok now how

(Refer Slide Time 16:41)



do we show that it is exactly k plus 1? Now we know

(Refer Slide Time 16:45)

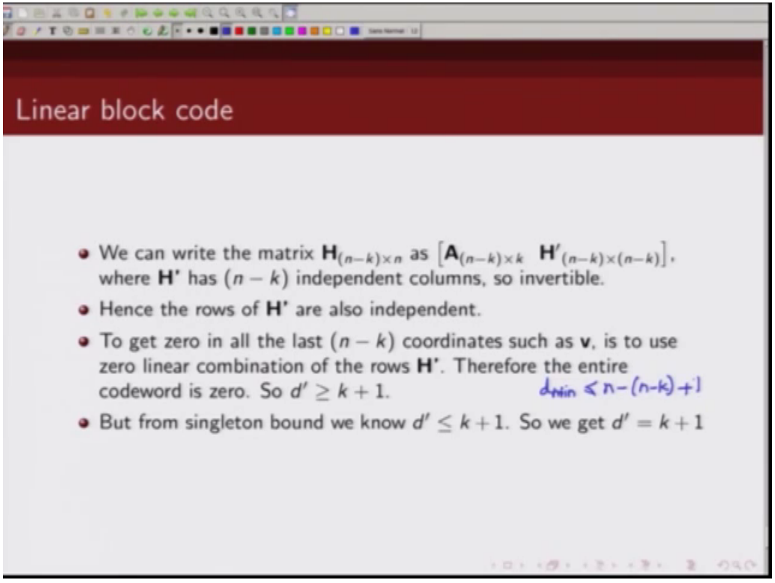


Linear block code

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $\left[\mathbf{A}_{(n-k)\times k} \quad \mathbf{H'}_{(n-k)\times(n-k)}\right]$, where $\mathbf{H'}$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H'}$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H'}$. Therefore the entire codeword is zero. So $d' \geq k+1$.
- But from singleton bound we know $d' \leq k+1$. So we get $d' = k+1$

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 minus dimension of the code is in this case, n minus k plus 1. So from singleton

(Refer Slide Time 17:11)



Linear block code

- We can write the matrix $\mathbf{H}_{(n-k)\times n}$ as $\left[\mathbf{A}_{(n-k)\times k} \;\; \mathbf{H}'_{(n-k)\times(n-k)}\right]$, where $\mathbf{H}'$ has $(n-k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H}'$ are also independent.
- To get zero in all the last $(n-k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H}'$. Therefore the entire codeword is zero. So $d' \geq k+1$. $d_{min} \leq n-(n-k)+1$
- But from singleton bound we know $d' \leq k+1$. So we get $d' = k+1$

bound we get the condition that minimum distance should be less than equal to k plus 1. And from this we get the condition that minimum distance is at least k plus 1. So if we combine these two we will get the condition that minimum distance of this code is k plus 1. Hence it is proved that dual code is also maximum distance separable because it satisfies singleton bound with equality. With this we conclude

(Refer Slide Time 17:47)

this lecture, thank you