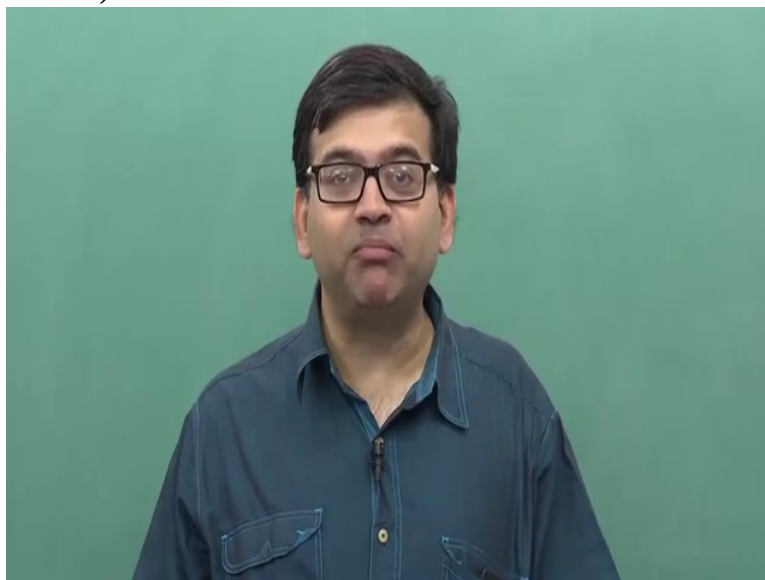


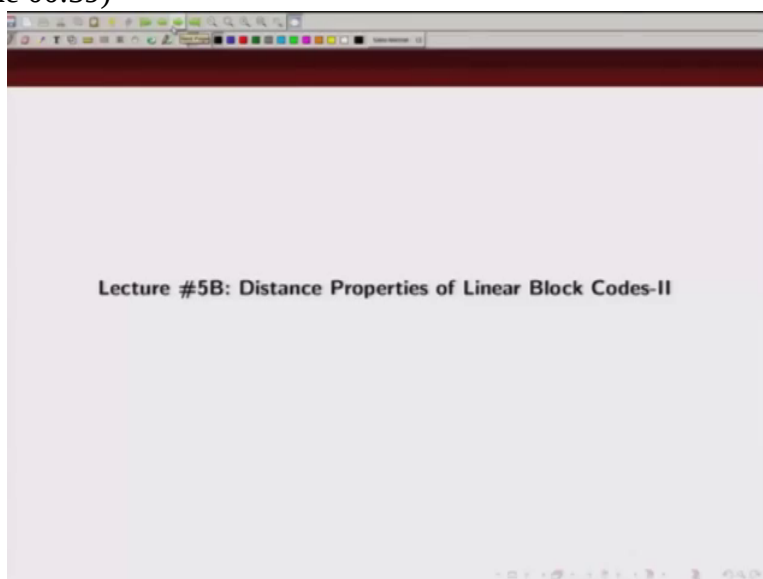
An Introduction to Coding Theory
Professor Adrish Banerji
Department of Electrical Engineering
Indian Institute of Technology, Kanpur
Module 02
Lecture Number 09
Distance Properties of Linear Block Codes-II

(Refer Slide Time 00:18)



In this lecture we are going to talk about what do we mean by weight distribution of a linear block code and then we are going to talk about how is the error correcting capability and error detecting capability of a linear block code dependent on the minimum distance of a code. So we will continue

(Refer Slide Time 00:39)



basically our discussion on distance properties that we have started

(Refer Slide Time 00:43)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

last time. So this is one example of a linear block code where number of information bits is 3

(Refer Slide Time 00:52)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

and number of

(Refer Slide Time 00:55)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

coded bits is 6. This is a list of 2^k codewords which is 8 codewords, message bits and these are their corresponding codewords. So these are the, from 0 0 0 to 1 1 1, these are our 2^k message bits and corresponding to each of our message bits these are the corresponding codewords,

(Refer Slide Time 01:21)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

Ok. Now

(Refer Slide Time 01:27)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

let us look at what is the weight distribution of these codewords. So these codewords, this is all zero codeword, so the weight, Hamming weight for this is basically 0. What about

(Refer Slide Time 01:43)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

This codeword has 3 1's. So Hamming weight is 3,

(Refer Slide Time 01:51)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

this codeword has three 1's. So its Hamming weight is 3.

(Refer Slide Time 01:57)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

This codeword has four 1's. So the Hamming weight is 4.

(Refer Slide Time 02:04)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

This codeword has three 1's so Hamming weight is 3.

(Refer Slide Time 02:10)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

This one similarly has Hamming weight 4,

(Refer Slide Time 02:16)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

Handwritten Hamming weights: 0, 3, 3, 4, 3, 4, 4, 3

this one Hamming weight 4 and this one has

(Refer Slide Time 02:21)

Distance properties of block codes

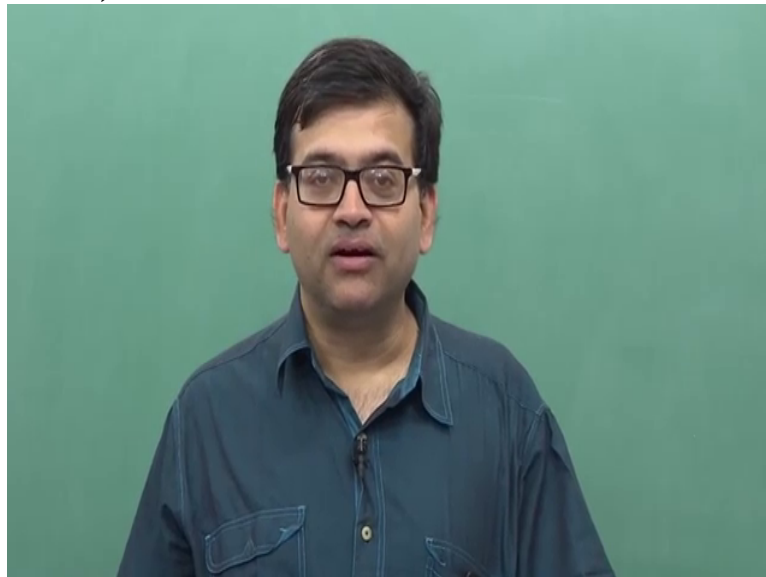
Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

Handwritten Hamming weights: 0, 3, 3, 4, 3, 4, 4, 3

Hamming weight 3.

(Refer Slide Time 02:24)



Now what is the minimum distance of the code? As you recall we define the minimum distance of the code as minimum weight

(Refer Slide Time 02:35)

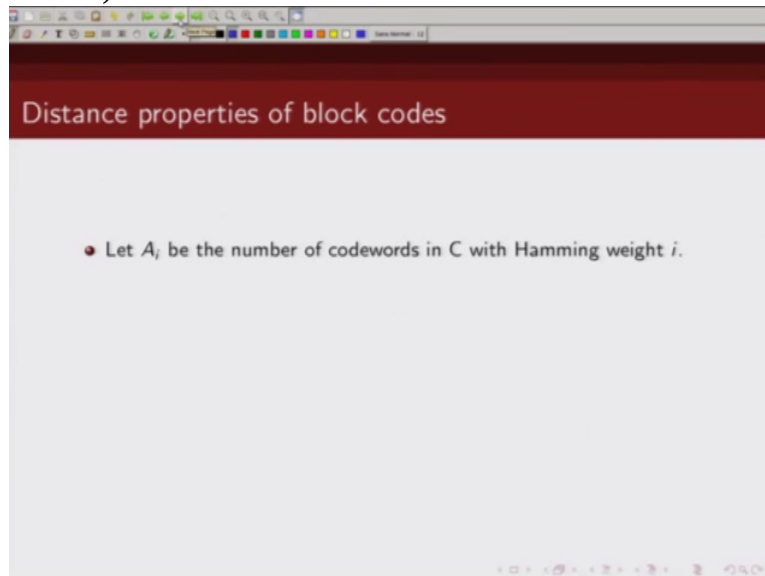
Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

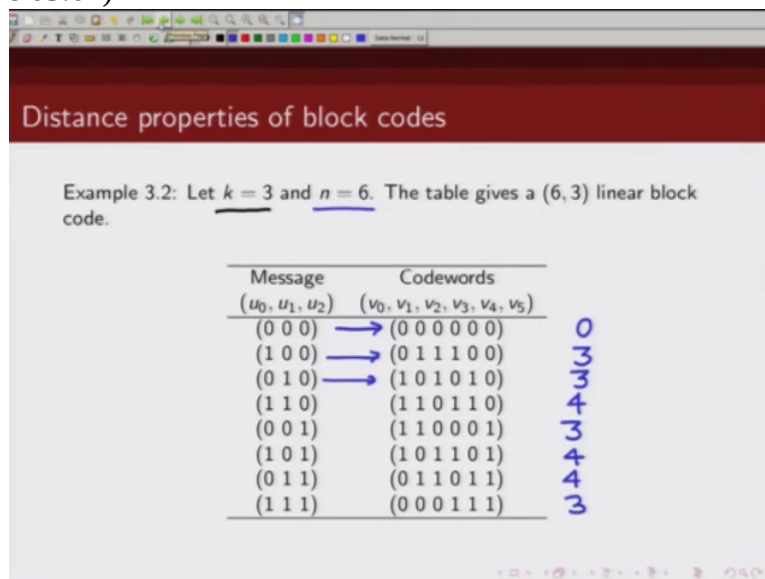
of a non-zero codeword. So what is the minimum weight of the non-zero codeword in this case? Its 3 so minimum distance of this code is 3.

(Refer Slide Time 02:50)



So let a_i denotes the number of codewords in C with Hamming weight i . So if

(Refer Slide Time 03:02)



you look here, if I, so I will use a 0 to denote

(Refer Slide Time 03:09)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

A_0

number of codewords which have Hamming weight 0 and that number is 1. Do we have

(Refer Slide Time 03:20)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

$A_0 = 1$

any codeword with Hamming weight 1? No. So a 1 is going to be 0.

(Refer Slide Time 03:28)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

$A_0 = 1$
 $A_1 = 0$

What about a 2? How many codewords we have with Hamming weight 2? Again that's 0.

(Refer Slide Time 03:39)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

$A_0 = 1$
 $A_1 = 0$
 $A_2 = 0$

What about a 3? That's basically 1, 2, 3, 4. We have 4 codewords with

(Refer Slide Time 03:51)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

Handwritten notes: $A_0 = 1$, $A_1 = 0$, $A_2 = 0$, $A_3 = 4$

Hamming weight 3, a 4, 1, 2, 3, Ok

(Refer Slide Time 04:04)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

Handwritten notes: $A_0 = 1$, $A_1 = 0$, $A_2 = 0$, $A_3 = 4$, $A_4 = 3$

Ok we don't have any codeword with Hamming weight 5 or

(Refer Slide Time 04:10)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

Handwritten notes on the right side of the slide:

- $A_0 = 1$
- $A_1 = 0$
- $A_2 = 0$
- $A_3 = 4$
- $A_4 = 3$
- $A_5 = 0$

Hamming weight 6.

(Refer Slide Time 04:13)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

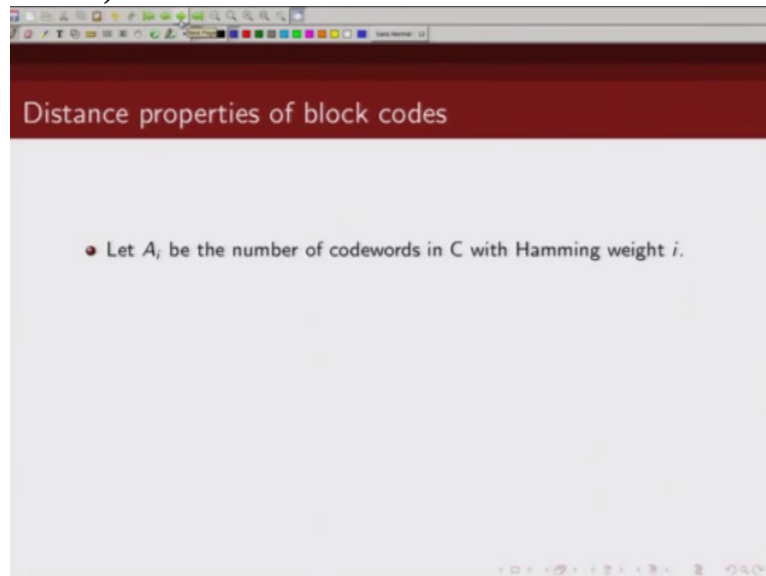
Message (u_0, u_1, u_2)	Codewords ($v_0, v_1, v_2, v_3, v_4, v_5$)	
(0 0 0)	(0 0 0 0 0 0)	0
(1 0 0)	(0 1 1 1 0 0)	3
(0 1 0)	(1 0 1 0 1 0)	3
(1 1 0)	(1 1 0 1 1 0)	4
(0 0 1)	(1 1 0 0 0 1)	3
(1 0 1)	(1 0 1 1 0 1)	4
(0 1 1)	(0 1 1 0 1 1)	4
(1 1 1)	(0 0 0 1 1 1)	3

Handwritten notes on the right side of the slide:

- $A_0 = 1$
- $A_1 = 0$
- $A_2 = 0$
- $A_3 = 4$
- $A_4 = 3$
- $A_5 = 0$
- $A_6 = 0$

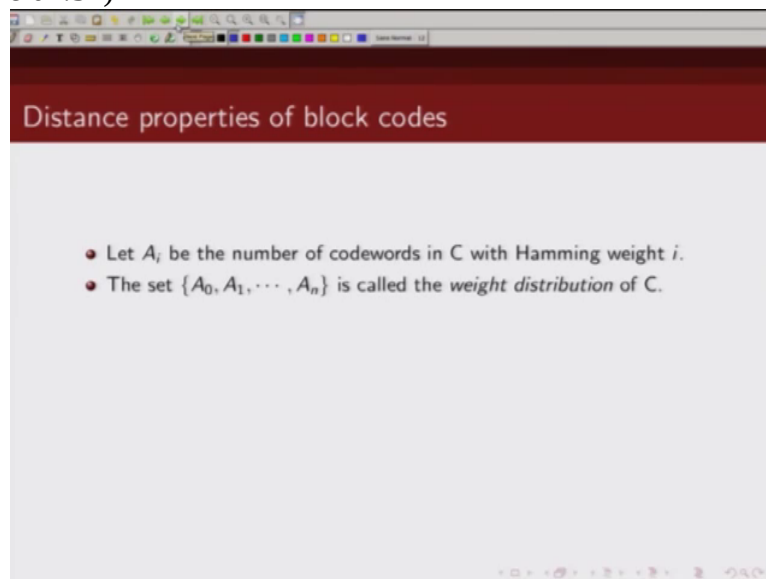
And you can do a quick check, the number of codewords should add up to number of codewords that we have which is 8, 1 plus 4 plus 3, Ok. So we are denoting

(Refer Slide Time 04:24)



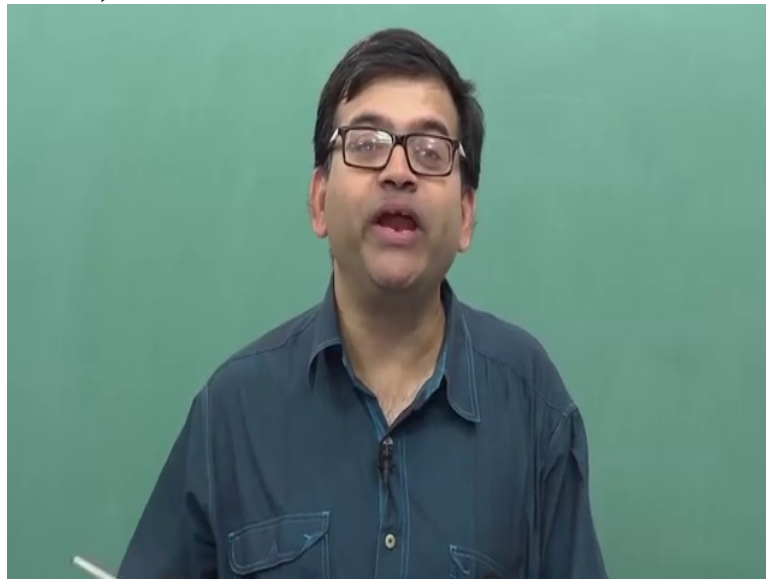
by A_i , the number of codewords in this linear block code with Hamming weight i .

(Refer Slide Time 04:32)



Now this set which describes how many codewords

(Refer Slide Time 04:38)



we have of particular weight, this is basically known as weight distribution of a linear block code, see. So for this

(Refer Slide Time 04:49)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

Handwritten notes on the right side of the slide:

$A_0 = 1$
 $A_1 = 0$
 $A_2 = 0$
 $A_3 = 4$
 $A_4 = 3$
 $A_5 = 0$
 $A_6 = 0$

Vertical handwritten notes on the left side of the table:

0
3
3
4
3
4
4
3

block code, the weight distribution is given by this. This completely specifies the weight distribution

(Refer Slide Time 04:59)

Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

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)

Handwritten notes on the right side of the slide:

- $A_0 = 1$
- $A_1 = 0$
- $A_2 = 0$
- $A_3 = 4$
- $A_4 = 3$
- $A_5 = 0$
- $A_6 = 0$

Vertical numbers next to the codewords: 0, 3, 3, 4, 3, 4, 4, 3

of this particular 6 3 linear block code.

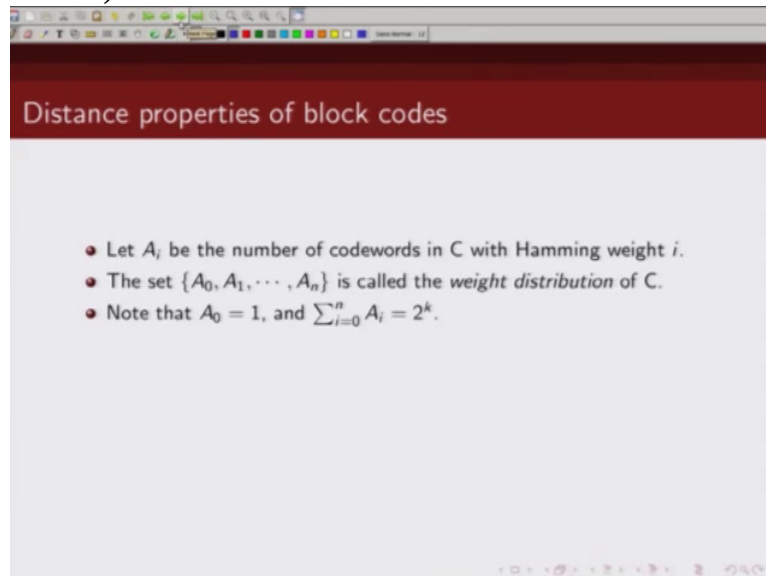
(Refer Slide Time 05:05)

Distance properties of block codes

- Let A_i be the number of codewords in C with Hamming weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the *weight distribution* of C .

And since we have said

(Refer Slide Time 05:07)



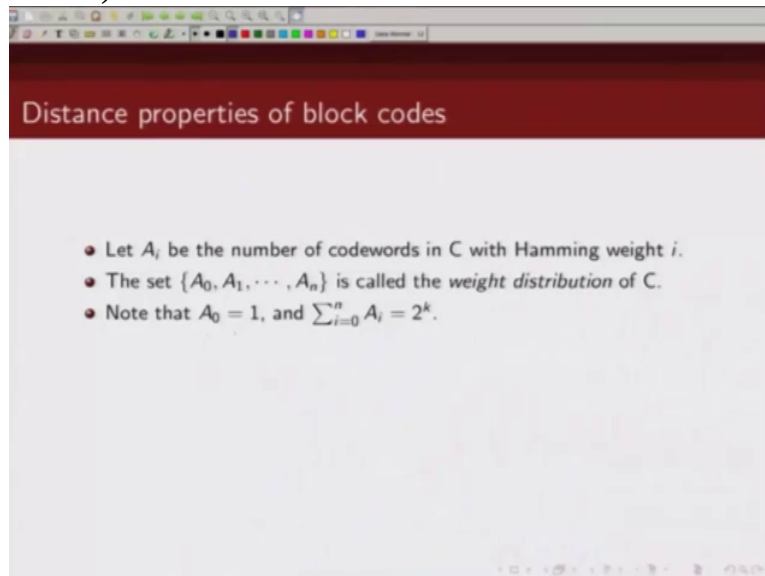
a linear block

(Refer Slide Time 05:08)



code will have an all zero codeword, so a 0 will be

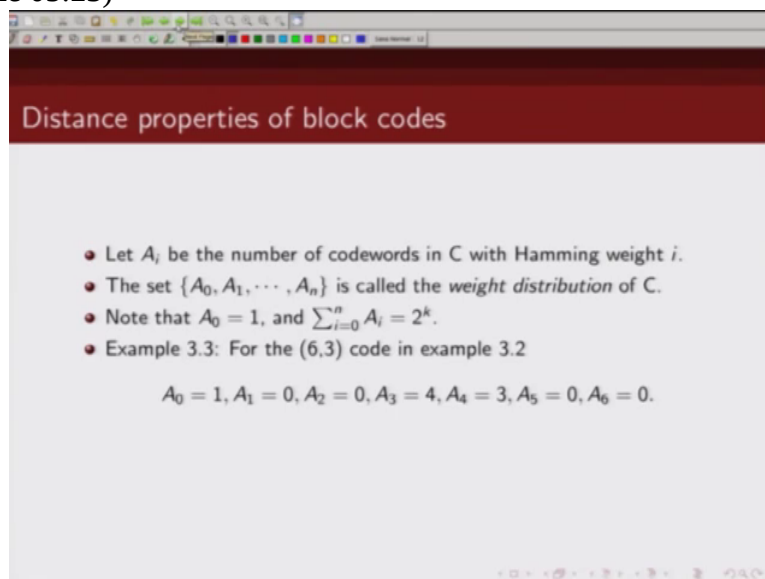
(Refer Slide Time 05:11)



1 and sum of all these codewords, they should all add up to total number of codewords which is 2 to the power k.

I just worked out

(Refer Slide Time 05:23)



this example for the 6 3 code we have shown in the previous slide and I showed you that in this particular example a 0 is 1, a 3 is

(Refer Slide Time 05:35)

Distance properties of block codes

- Let A_i be the number of codewords in C with Hamming weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the *weight distribution* of C .
- Note that $A_0 = 1$, and $\sum_{i=0}^n A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 4, A_4 = 3, A_5 = 0, A_6 = 0.$$

4,

(Refer Slide Time 05:36)

Distance properties of block codes

- Let A_i be the number of codewords in C with Hamming weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the *weight distribution* of C .
- Note that $A_0 = 1$, and $\sum_{i=0}^n A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$\underline{A_0 = 1}, A_1 = 0, A_2 = 0, \underline{A_3 = 4}, A_4 = 3, A_5 = 0, A_6 = 0.$$

a 4 is 3. Rest all others are

(Refer Slide Time 05:39)

Distance properties of block codes

- Let A_i be the number of codewords in C with Hamming weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the *weight distribution* of C .
- Note that $A_0 = 1$, and $\sum_{i=0}^n A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 4, A_4 = 3, A_5 = 0, A_6 = 0.$$

0. And I also showed

(Refer Slide Time 05:43)

Distance properties of block codes

- Let A_i be the number of codewords in C with Hamming weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the *weight distribution* of C .
- Note that $A_0 = 1$, and $\sum_{i=0}^n A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 4, A_4 = 3, A_5 = 0, A_6 = 0.$$

- d_{\min} in the above example is 3.

you that the minimum distance of this code is 3 because minimum weight of a non-zero codeword in this example is 3. Now the probability of

(Refer Slide Time 05:58)

Slide titled "Error detecting properties of block codes". The slide contains a bullet point: "The probability of undetected error on a BSC is given by". Below this is the formula:
$$P_u(E) = \sum_{i=1}^n A_i \rho^i (1 - \rho)^{n-i}$$

undetected error for a linear block code over a binary symmetric channel is basically related to the weight distribution of the code.

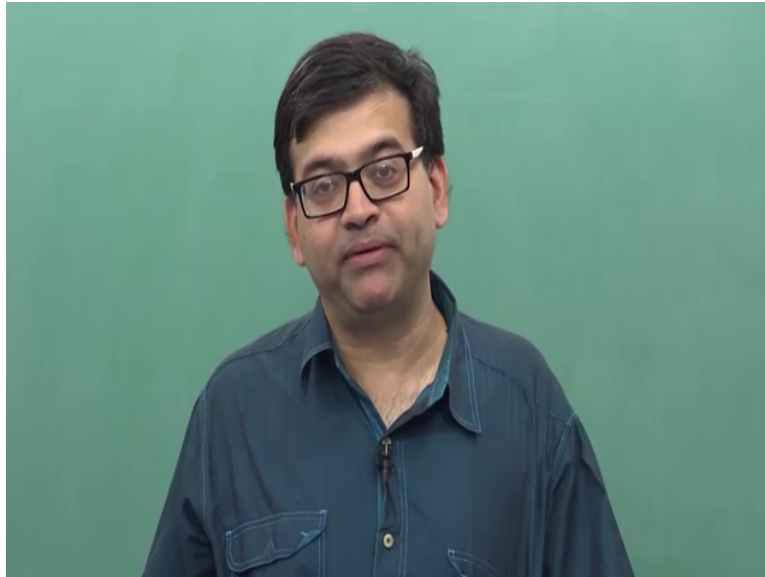
(Refer Slide Time 06:10)

Slide titled "Error detecting properties of block codes". The slide contains a bullet point: "The probability of undetected error on a BSC is given by". Below this is the formula:
$$P_u(E) = \sum_{i=1}^n A_i \rho^i (1 - \rho)^{n-i}$$

Below the formula is another bullet point: "Example 3.4: For the (6, 3) code in example 3.2,". Below this is the formula:
$$P_u(E) = 4\rho^3(1 - \rho)^3 + 3\rho^4(1 - \rho)^2 \approx 4\rho^3 \quad (\text{for small } \rho)$$

So for a 6 3 linear block code and, so when does an, when does a undetected error happens?

(Refer Slide Time 06:22)



An undetected error happens if, let's say you send one particular codeword and at the receiver you receive some other codeword. So without loss of generality let's assume that we sent a all zero codeword. And at the receiver you received any other non-zero codeword. So if I send an all zero codeword

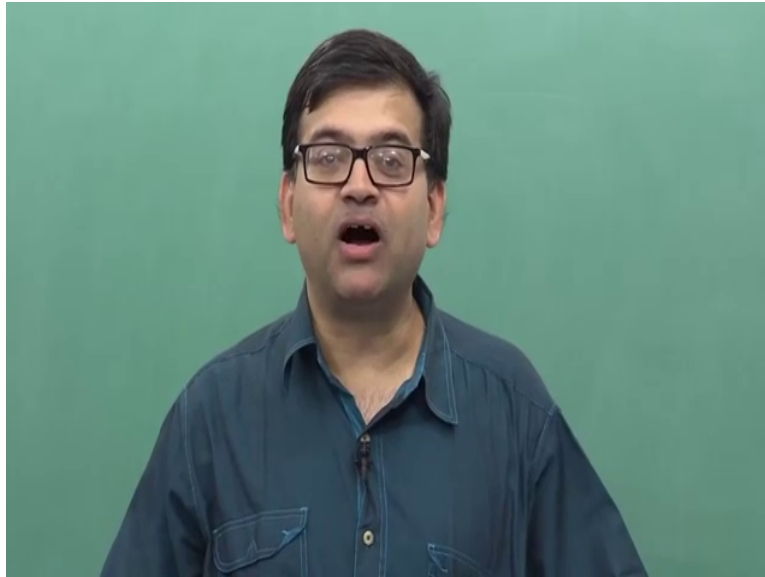
(Refer Slide Time 06:52)

A slide titled "Error detecting properties of block codes" with a red header. The slide contains the following text:

- The probability of undetected error on a BSC is given by
$$P_u(E) = \sum_{i=1}^n A_i \rho^i (1 - \rho)^{n-i}$$
- Example 3.4: For the (6, 3) code in example 3.2,
$$P_u(E) = 4\rho^3(1 - \rho)^3 + 3\rho^4(1 - \rho)^2 \approx 4\rho^3 \quad (\text{for small } \rho)$$

at the transmitter and at the receiver you receive any other non-zero codeword then that will be the case of undetected error. So you can see basically, that's why I have written it as, so what is the probability, when you are sending an all zero codeword, what is the probability of getting another codeword of weight a i or weight i? What is the probability that, when I am sending an all zero codeword and you receive a codeword

(Refer Slide Time 07:32)



which has weight i ? Now that probability is given by,

(Refer Slide Time 07:38)

A screenshot of a presentation slide. The title bar is dark red with the text "Error detecting properties of block codes" in white. The main content area is light gray. It contains a bullet point: "The probability of undetected error on a BSC is given by" followed by the equation
$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$
. Below this is another bullet point: "Example 3.4: For the (6,3) code in example 3.2," followed by the equation
$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$
. The slide has a standard presentation navigation bar at the bottom.

since we are considering a binary symmetric channel, now recall what happens in binary symmetric channel, two inputs 0 and 1,

(Refer Slide Time 07:49)

The slide is titled "Error detecting properties of block codes". It contains the following text and equations:

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

Handwritten blue annotations on the slide include a "0 ." next to the first bullet point, a "1 ." next to the second bullet point, and a "1 ." next to the example text.

two outputs 0 and 1, and what

(Refer Slide Time 07:52)

This slide is identical to the one above, but with additional handwritten blue annotations:

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

Handwritten blue annotations include a "0 ." next to the first bullet point, a ". 0" next to the formula, a "1 ." next to the second bullet point, and a "1" next to the example text.

is the crossover probability? That is basically given by p. So with probability p,

(Refer Slide Time 07:59)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

0 can get flipped to 1, 1 can get flipped to 0. And the probability of correct detection is 1 minus p. So you are sending a

(Refer Slide Time 08:11)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

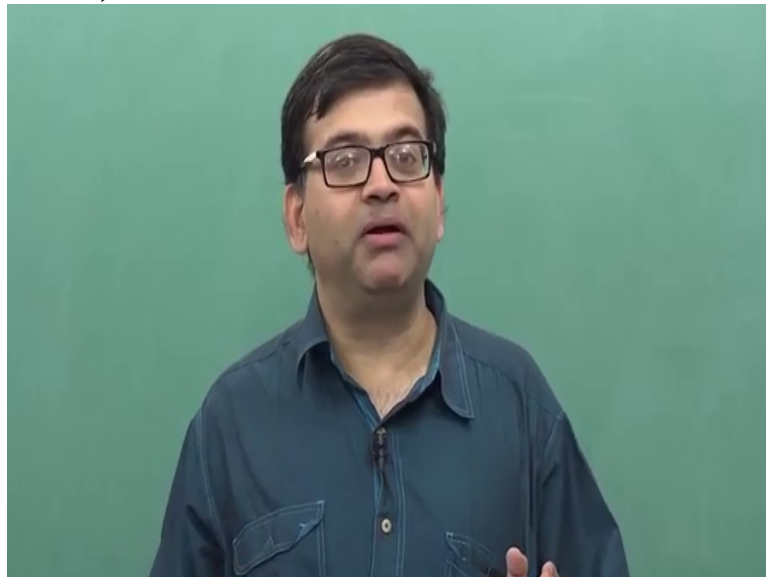
$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

codeword which is an n-bit tuple. Now what's a probability

(Refer Slide Time 08:17)



that you are sending an all zero codeword of all zero bits, you receive another codeword of

(Refer Slide Time 08:28)

The slide is titled "Error detecting properties of block codes" in a red header. It contains the following content:

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

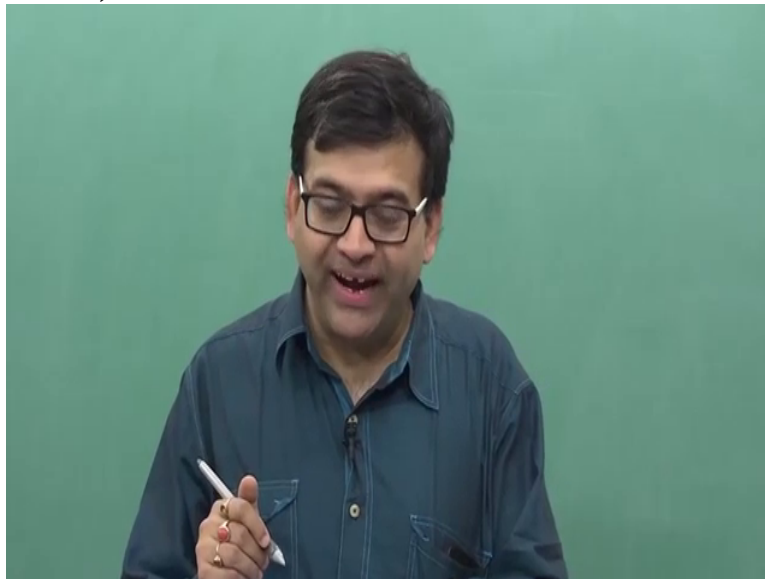
- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

There is a diagram on the right side of the slide showing a square with vertices labeled 0 (top-left), 1 (bottom-left), 1 (bottom-right), and 0 (top-right). The edges are labeled with probabilities: the top edge is labeled $1-p$, the bottom edge is labeled $1-p$, the left edge is labeled p , and the right edge is labeled p . The two diagonals are also labeled with p .

weight i . Now that probability is given by p raised to power i . This will happen when i bits get flipped and n minus i bits do not get flipped. So that probability is given by p raised to power i into 1 minus p raised to power n minus i and how many such codewords exist? That number is given by A_i . So the probability of getting a weight i

(Refer Slide Time 09:02)



codeword at the receiver; when you send an all zero codeword, that probability

(Refer Slide Time 09:08)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

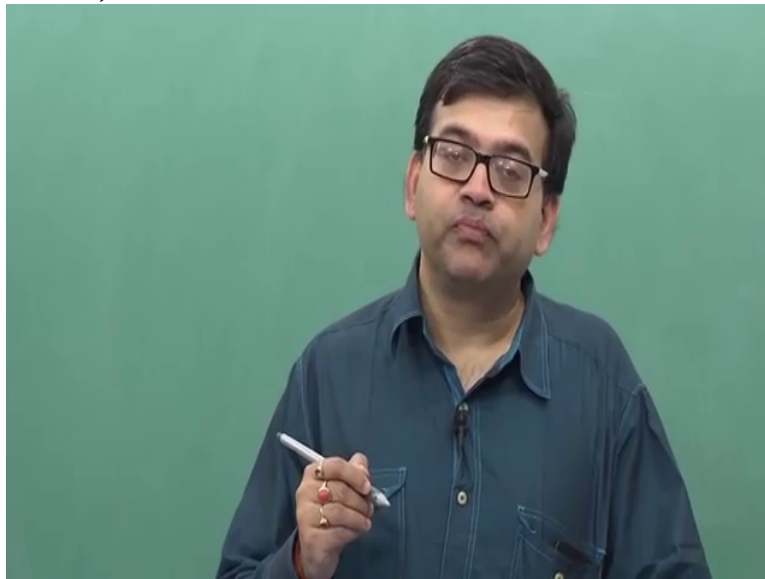
- Example 3.4: For the (6,3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

```
graph TD
    0((0)) -- "1-p" --> 0
    0 -- "p" --> 1((1))
    1 -- "p" --> 0
    1 -- "1-p" --> 1
```

is basically given by this. Ok. Now

(Refer Slide Time 09:13)



an undetected error will happen if the receiver receives any non-zero codeword. So I have to sum up

(Refer Slide Time 09:22)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$

The diagram shows a square with nodes labeled 0 and 1. The top node is 0, the bottom node is 1, the left node is 0, and the right node is 1. There are two diagonal lines crossing in the center. The top-left to bottom-right line is labeled '1-p' at both ends. The top-right to bottom-left line is labeled 'p' at both ends.

this probability

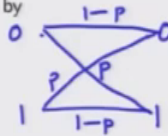
(Refer Slide Time 09:25)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$


for all i going from 1 to n . So this is my overall

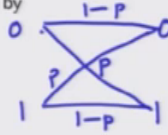
(Refer Slide Time 09:34)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$


undetected error probability if I send a linear block code over a binary symmetric channel. So for the example that I have considered I know the weight distribution, so if I plug that in here what I get is, so there were 4 codewords with weight 3, so this is 4 p raised to power 3. And what was n , n is 6.

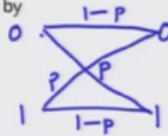
(Refer Slide Time 10:04)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$


So 6 minus i which is 3 in this case, it's 3. So first term that I will get is this.

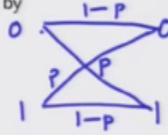
(Refer Slide Time 10:12)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad (\text{for small } p)$$


The next term corresponding to

(Refer Slide Time 10:20)

Distance properties of block codes

- Let A_i be the number of codewords in C with Hamming weight i .
- The set $\{A_0, A_1, \dots, A_n\}$ is called the *weight distribution* of C .
- Note that $A_0 = 1$, and $\sum_{i=0}^n A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 4, A_4 = 3, A_5 = 0, A_6 = 0.$$

- d_{\min} in the above example is 3.

these codewords

(Refer Slide Time 10:23)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

is given, so there are 3 codewords of weight 4

(Refer Slide Time 10:26)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = \underline{4p^3(1-p)^3} + 3p^4(1-p)^2 \approx \underline{4p^3} \quad (\text{for small } p)$$

Probability of 4 bits getting flipped is p raised to power 4 and probability of the other 2 bits not getting flipped is $1 - p$ whole square. And since p is typically small, I mean I can approximate it, for small p I can approximate this undetected error probability

(Refer Slide Time 10:45)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6, 3) code in example 3.2,

$$P_u(E) = \underline{4p^3(1-p)^3} + 3p^4(1-p)^2 \approx \underline{4p^3} \quad (\text{for small } p)$$

as 4 times p^3 , because this will be close to 1 and since p is a small number, p raised to power 4 will be a small number. So this will be roughly equal to 4 into p raised to power 3. This is for the case when p is small.

(Refer Slide Time 11:05)

• There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$

on a BSC.

So you can see in general, so in this particular example

(Refer Slide Time 11:11)

• The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

• Example 3.4: For the $(6,3)$ code in example 3.2,

$$P_u(E) = \underline{4p^3(1-p)^3} + 3p^4(1-p)^2 \approx \underline{4p^3} \quad (\text{for small } p)$$

the undetected probability basically

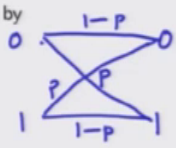
(Refer Slide Time 11:14)

Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the (6,3) code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \text{ (for small } p)$$


varies as p raised to power 3 which is basically same as n minus k . In general we can show that

(Refer Slide Time 11:22)

Error detecting properties of block codes

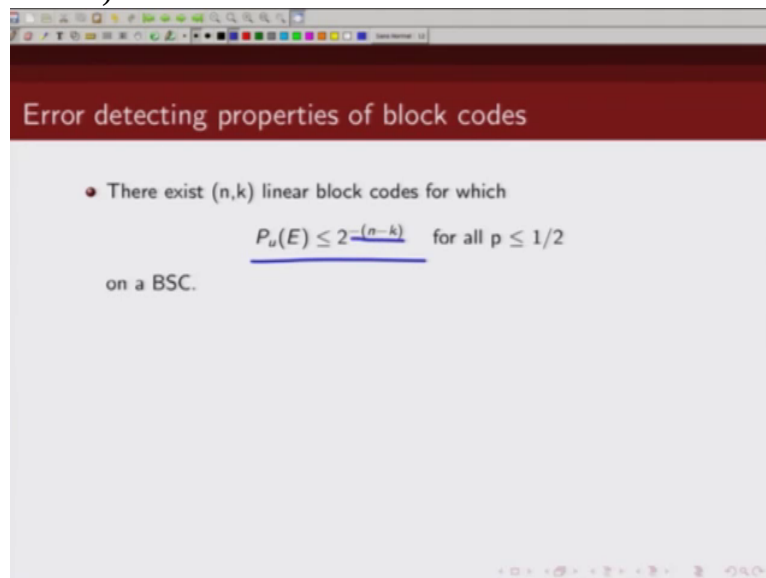
- There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \text{ for all } p \leq 1/2$$

on a BSC.

that undetected probability is dependent on how many

(Refer Slide Time 11:27)



Error detecting properties of block codes

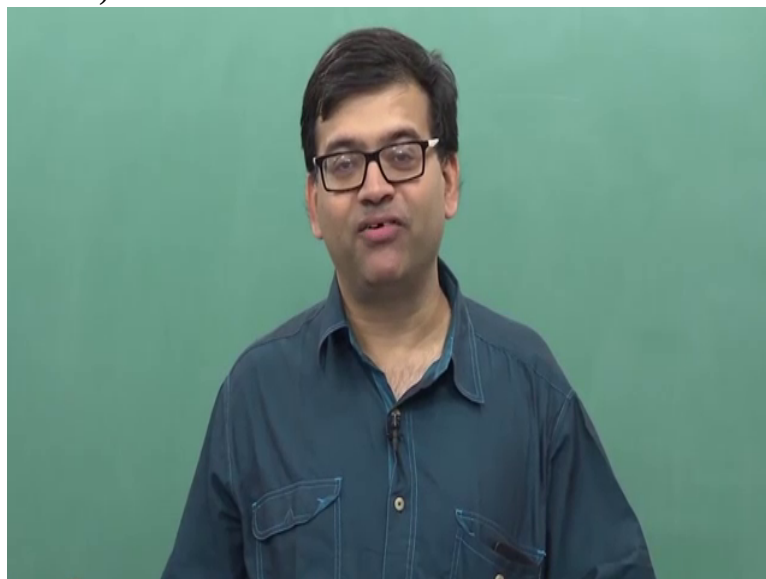
- There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$

on a BSC.

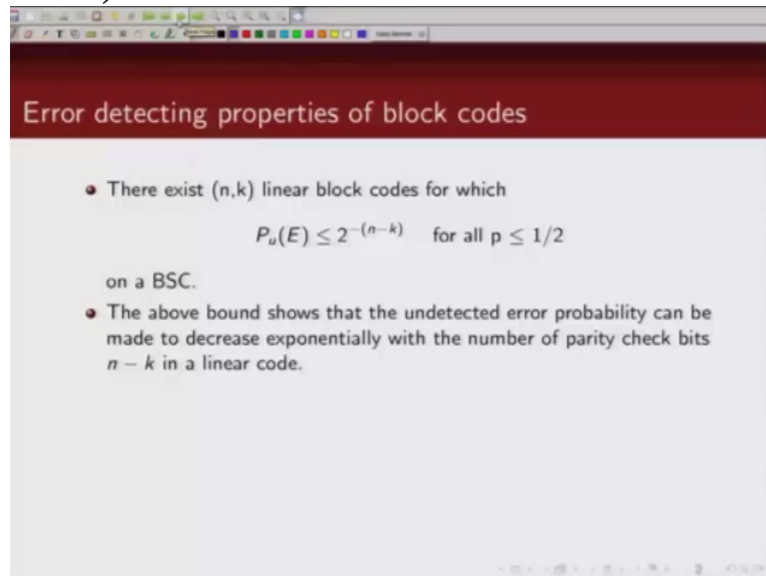
parity bits that we have; so the more

(Refer Slide Time 11:30)



the number of parity bits, lesser will be the undetected error probability. So we can make

(Refer Slide Time 11:37)

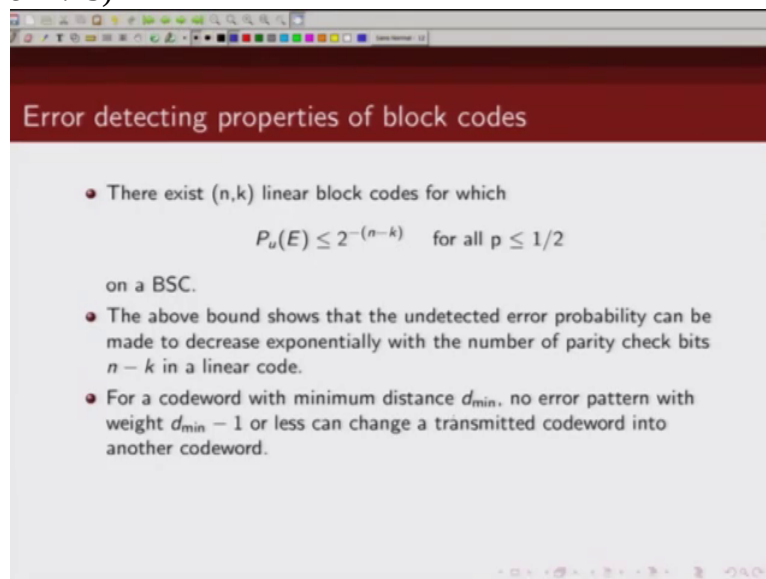


Slide titled "Error detecting properties of block codes".

- There exist (n,k) linear block codes for which
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.

undetected probability go small by increasing the number of parity bits. Now if we have

(Refer Slide Time 11:45)



Slide titled "Error detecting properties of block codes".

- There exist (n,k) linear block codes for which
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.

a codeword with minimum distance d_{\min} , we know that any error pattern or weight less than equal to $d_{\min} - 1$ is not going to change that codeword into any other valid codeword. So in other words, if there is an error pattern of weight

(Refer Slide Time 12:14)

Error detecting properties of block codes

- There exist (n,k) linear block codes for which
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.

$d_{\min} - 1$ or less, then

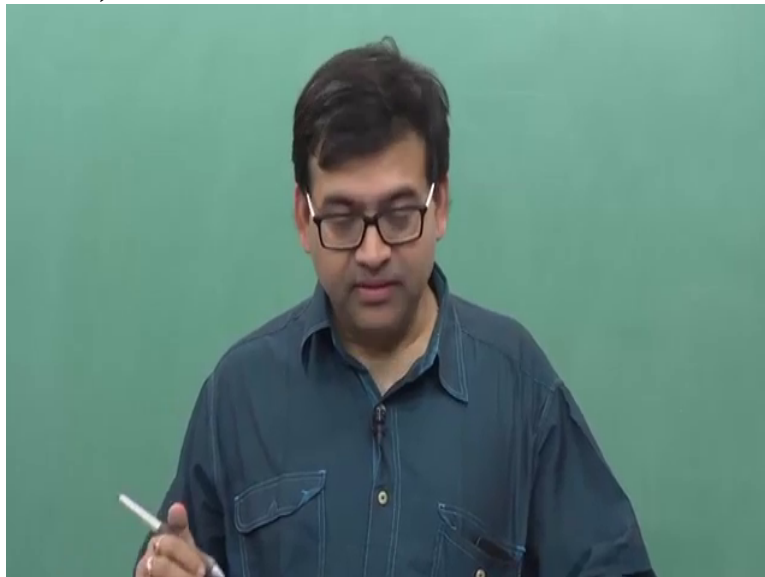
(Refer Slide Time 12:19)

Error detecting properties of block codes

- There exist (n,k) linear block codes for which
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.

it cannot change a

(Refer Slide Time 12:24)



valid codeword into another valid codeword. What does that mean? It means that we can actually detect any error pattern of weight up to $d_{\min} - 1$. So

(Refer Slide Time 12:42)

A slide titled "Error detecting properties of block codes" with a red header. The slide contains the following text:

- There exist (n, k) linear block codes for which
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min} - 1$ or fewer errors are detectable, and $d_{\min} - 1$ is called the *random error detecting capability* of a block code.

all error patterns of weight $d_{\min} - 1$ or fewer errors are basically detectable and this is also known as random error correcting capability of a linear block code.

Now take an example of a repetition code that we did in the first class. So let's say we have a rate one half repetition code.

(Refer Slide Time 13:09)

The slide is titled "Error detecting properties of block codes". It contains a list of four bullet points. The first bullet point is followed by a handwritten note $R = \frac{1}{2}$. The second bullet point is followed by the equation $P_u(E) \leq 2^{-(n-k)}$ for all $p \leq 1/2$. The remaining three bullet points are unchanged.

- There exist (n,k) linear block codes for which $R = \frac{1}{2}$
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min} - 1$ or fewer errors are detectable, and $d_{\min} - 1$ is called the *random error detecting capability* of a block code.

So then for 0, we are sending 0 0

(Refer Slide Time 13:16)

The slide is titled "Error detecting properties of block codes". It contains a list of four bullet points. The first bullet point is followed by a handwritten note $R = \frac{1}{2}$. The second bullet point is followed by the equation $P_u(E) \leq 2^{-(n-k)}$ for all $p \leq 1/2$. The remaining three bullet points are unchanged. There is also a handwritten note $0 \rightarrow \infty$ on the right side of the slide.

- There exist (n,k) linear block codes for which $R = \frac{1}{2}$
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min} - 1$ or fewer errors are detectable, and $d_{\min} - 1$ is called the *random error detecting capability* of a block code.

and for 1 we are sending 1 1.

(Refer Slide Time 13:22)

Error detecting properties of block codes

- There exist (n,k) linear block codes for which $R = \frac{1}{2}$
 $P_u(E) \leq 2^{-(n-k)}$ for all $p \leq 1/2$
on a BSC.
 $0 \rightarrow 00$
 $1 \rightarrow 11$
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min} - 1$ or fewer errors are detectable, and $d_{\min} - 1$ is called the *random error detecting capability* of a block code.

Now let's assume because of error in the channel some of the bits got flipped. So let's say this what we received when we, let's say what we received was 1 0. If you receive 1 0 can you detect?

(Refer Slide Time 13:45)

Error detecting properties of block codes

- There exist (n,k) linear block codes for which $R = \frac{1}{2}$
 $P_u(E) \leq 2^{-(n-k)}$ for all $p \leq 1/2$
on a BSC.
 $0 \rightarrow 00$
 $1 \rightarrow 11$
 10
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min} - 1$ or fewer errors are detectable, and $d_{\min} - 1$ is called the *random error detecting capability* of a block code.

So what is the minimum distance, first answer this question. What is the minimum distance of this code, this rate one half repetition code? We can see the minimum distance is 2. Minimum distance of this code is 2. So

(Refer Slide Time 14:04)

The slide is titled "Error detecting properties of block codes". It contains a list of bullet points and handwritten notes. The handwritten notes include the rate $R = \frac{1}{2}$ and the minimum distance $d_{\min} = 2$. Below these, there are mappings: $0 \rightarrow 00$, $1 \rightarrow 11$, and 10 written below the previous lines. The main text of the slide is as follows:

- There exist (n, k) linear block codes for which
$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$
on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.
- For a codeword with minimum distance d_{\min} , no error pattern with weight $d_{\min} - 1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min} - 1$ or fewer errors are detectable, and $d_{\min} - 1$ is called the *random error detecting capability* of a block code.

according to this, we should be able all error patterns of weight 1. So let's take an example. Let's say we received 1 0, can you detect the error? Yes we can because since it's a rate one half repetition code what we expect to receive

(Refer Slide Time 14:30)



either 0 0 or 1 1 if we

(Refer Slide Time 14:35)

Error detecting properties of block codes

• There exist (n, k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all } p \leq 1/2$$

on a BSC.

• The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.

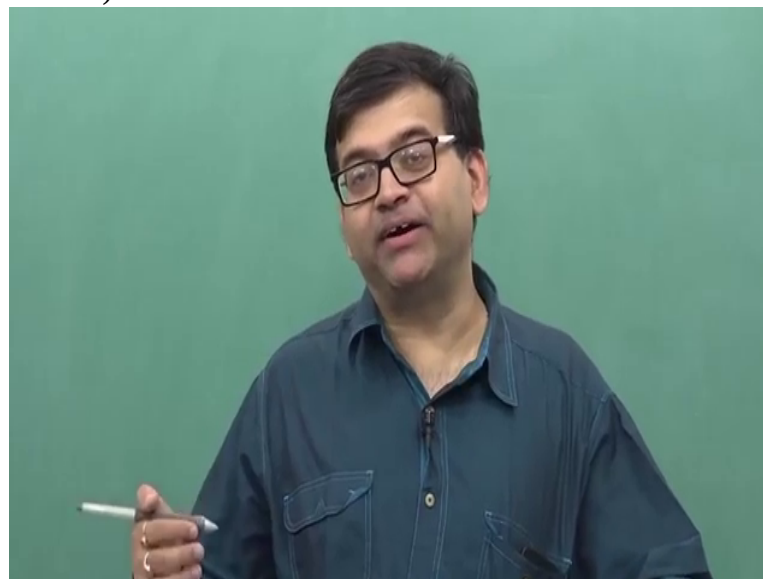
• For a codeword with minimum distance d_{min} , no error pattern with weight $d_{min} - 1$ or less can change a transmitted codeword into another codeword.

• Therefore, all error patterns with $d_{min} - 1$ or fewer errors are detectable, and $d_{min} - 1$ is called the *random error detecting capability* of a block code.

Handwritten notes:
 $R = \frac{1}{2}$ $d_{min} = 2$
 $0 \rightarrow 00$
 $1 \rightarrow 11$
 10

transmit these codewords over a binary symmetric channel. But what we have received is 1 0 which is neither 0 0 nor 1 1. So we are able to detect single error. So to repeat basically, if you have a linear block code whose minimum distance is d_{min} . You will be able to detect all errors, random errors of error pattern up to

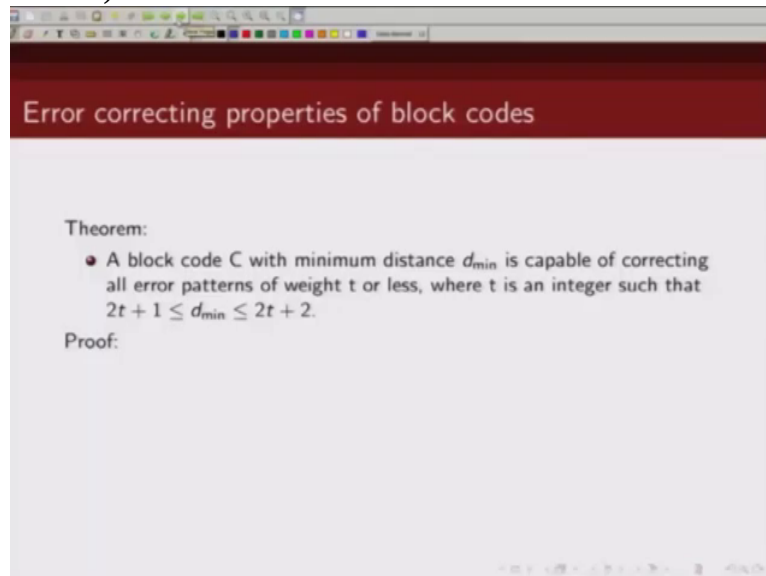
(Refer Slide Time 15:09)



$d_{min} - 1$.

Next we are going to show how is the error detecting capability, error correcting capability of a linear block code related to the minimum distance of a code. So

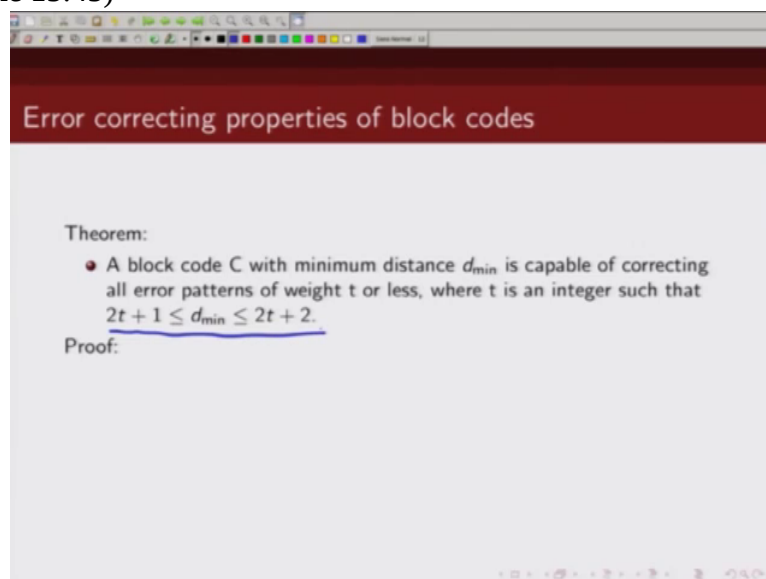
(Refer Slide Time 15:31)



The slide is titled "Error correcting properties of block codes" in a dark red header. Below the header, the text reads: "Theorem: • A block code C with minimum distance d_{min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{min} \leq 2t + 2$." Below the theorem, the word "Proof:" is written.

if we have a linear block code C whose minimum distance is d_{min} where d_{min} satisfies this relation.

(Refer Slide Time 15:45)



The slide is titled "Error correcting properties of block codes" in a dark red header. Below the header, the text reads: "Theorem: • A block code C with minimum distance d_{min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{min} \leq 2t + 2$." Below the theorem, the word "Proof:" is written.

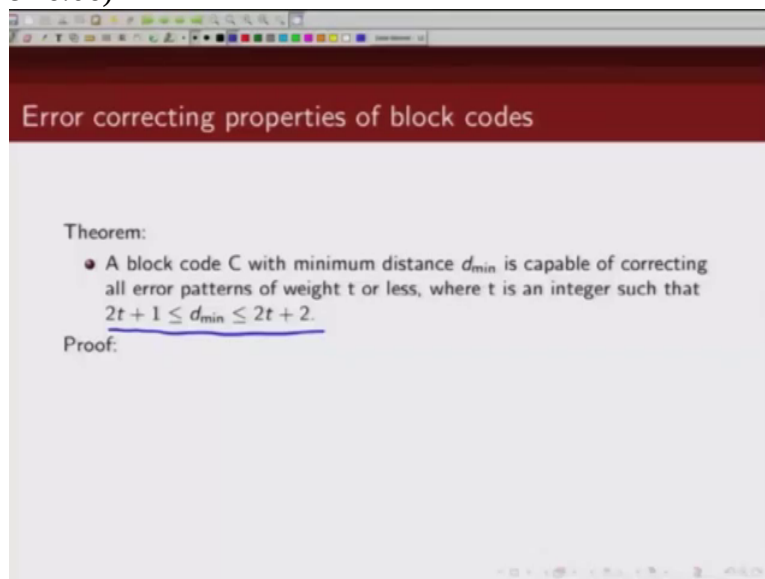
d_{min} is greater than equal to $2t + 1$ where t is an integer and its less than an integer and it is less than equal to $2t + 2$. If d_{min} satisfies this relation

(Refer Slide Time 15:58)



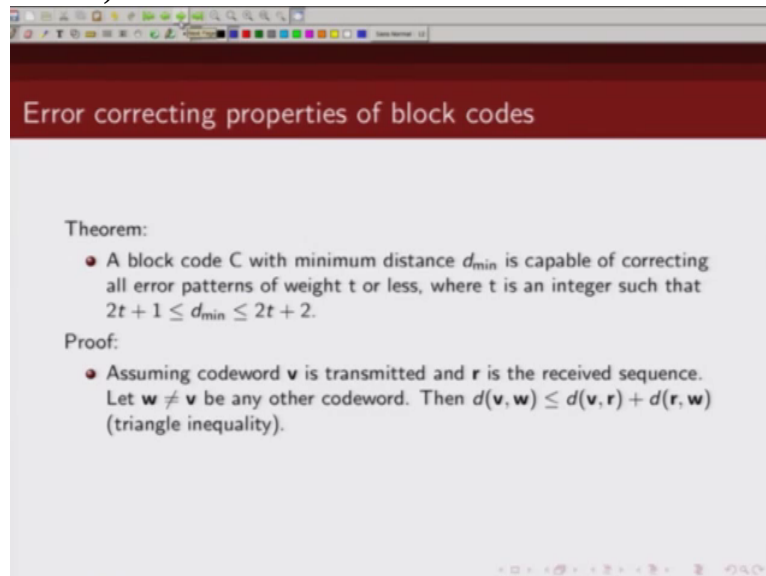
and if we have a linear block code with minimum distance d_{\min} then it is capable

(Refer Slide Time 16:06)



of correcting all error patterns up to weight t. So let us prove this result.

(Refer Slide Time 16:17)



The slide displays the following text:

Theorem:

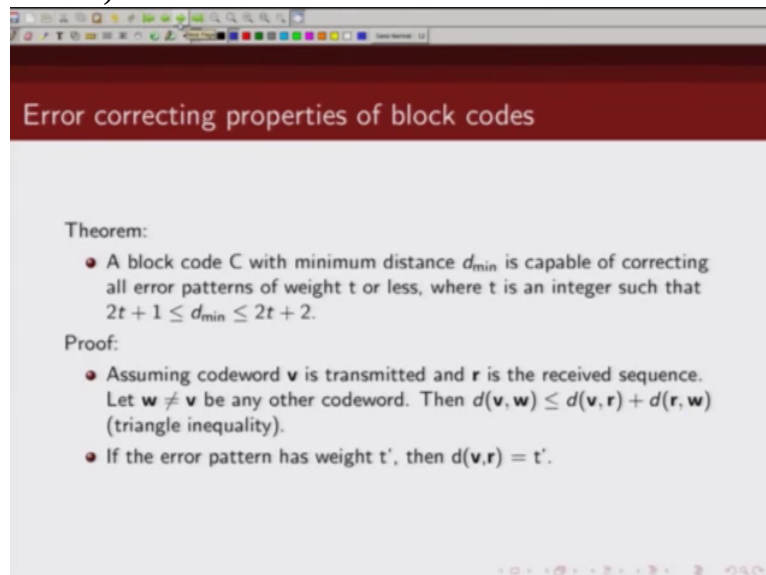
- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).

Let us assume the codeword that is transmitted is given by \mathbf{v} and what we received is say tuple \mathbf{r} . Let us assume there is another codeword \mathbf{w} which is not same as \mathbf{v} . Now we know from triangular inequality that Hamming distance between \mathbf{v} and \mathbf{w} will be less than equal to Hamming distance between \mathbf{v} and \mathbf{r} plus Hamming distance between \mathbf{r} and \mathbf{w} . Now let us assume

(Refer Slide Time 17:00)



The slide displays the following text:

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$.

that the error pattern has weight t hat. And what's \mathbf{r} ; \mathbf{r} is nothing but \mathbf{v} plus this error pattern,

(Refer Slide Time 17:13)

Error correcting properties of block codes

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$. $\mathbf{r} = \mathbf{v} + \mathbf{e}$

correct? So the Hamming distance between \mathbf{v} and \mathbf{r} is going to be the weight of this error pattern and which we are denoting by t' . Now since

(Refer Slide Time 17:29)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

\mathbf{v} and \mathbf{w} are valid codewords, so the Hamming distance between \mathbf{v} and \mathbf{w} will be at least equal to the minimum distance of the code. So the Hamming distance between \mathbf{v} and \mathbf{w} is greater than equal to minimum distance of the code and in the beginning we defined that our minimum distance

(Refer Slide Time 17:53)

The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$. $\mathbf{r} = \mathbf{v} + \mathbf{e}$

is at least $2t + 1$. So from these

(Refer Slide Time 17:58)

The slide is titled "Error correcting properties of block codes". It contains the following text:

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

two, we can write that Hamming distance between \mathbf{v} and \mathbf{w} is greater than equal to $2t + 1$. Now from the triangular inequality we know that Hamming distance between \mathbf{r} and \mathbf{w} , this we can see from here, this relationship

(Refer Slide Time 18:24)

The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$. $\mathbf{r} = \mathbf{v} + \mathbf{e}$

basically triangular inequality

(Refer Slide Time 18:27)

The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$. $\mathbf{r} = \mathbf{v} + \mathbf{e}$

what we have is

(Refer Slide Time 18:29)

The slide displays the following text and equations:

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

the Hamming distance between \mathbf{v} and \mathbf{w} to be less than equal to Hamming distance between \mathbf{r} and \mathbf{w} plus Hamming distance between \mathbf{r} and \mathbf{v} , right.

(Refer Slide Time 18:48)

The slide displays the following text and equations:

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{r}, \mathbf{w}) + d(\mathbf{r}, \mathbf{v})$$
$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

Now this we can write as, we can bring this here and we can bring this here, what we can write this as, let us say we can write this, this relation in this particular form.

(Refer Slide Time 19:11)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{v}, \mathbf{u}) \leq d(\mathbf{r}, \mathbf{u}) + d(\mathbf{r}, \mathbf{v})$$
$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

Ok.

Now what is this quantity, Hamming distance

(Refer Slide Time 19:21)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{v}, \mathbf{u}) \leq d(\mathbf{r}, \mathbf{u}) + d(\mathbf{r}, \mathbf{v})$$
$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

between \mathbf{v} and \mathbf{w} ? The Hamming distance between \mathbf{v} and \mathbf{w} is at least equal to

(Refer Slide Time 19:28)

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{r}, \mathbf{w}) + d(\mathbf{r}, \mathbf{v})$$

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

$2t + 1$. And what is Hamming distance between the transmitted codeword and the received codeword? This is we denote it by t' . So then Hamming distance between \mathbf{r} and \mathbf{w} is given by $2t + 1$ minus t' . Now

(Refer Slide Time 19:54)

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

- If $t' \leq t$, then

$$d(\mathbf{r}, \mathbf{w}) \geq t + 1 > t \text{ and } d(\mathbf{v}, \mathbf{r}) = t' \leq t.$$

as long as your error pattern is

(Refer Slide Time 20:00)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'.$$

- If $t' \leq t$, then

$$d(\mathbf{r}, \mathbf{w}) \geq t + 1 > t \text{ and } d(\mathbf{v}, \mathbf{r}) = t' \leq t.$$

less than equal to t the weight of error pattern is less than equal to t , in that case the Hamming distance between \mathbf{r} and \mathbf{w} will be, you can plug that value of t here and what we will get is Hamming distance between \mathbf{r} and \mathbf{w} is greater than equal to t plus 1 which is greater than equal to t where as the Hamming distance between

(Refer Slide Time 20:34)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'.$$

- If $t' \leq t$, then

$$d(\mathbf{r}, \mathbf{w}) \geq t + 1 > t \text{ and } d(\mathbf{v}, \mathbf{r}) = t' \leq t.$$

transmitted codeword and the received codeword is t hat which is less than equal to t . What does it mean? It means that the received codeword is closer to \mathbf{v} than any other codeword \mathbf{w} . So what will be your maximum likelihood decoder for binary symmetric channel will decide in favor of? It will decide in favor of \mathbf{v} . So you will correctly decode this received sequence to be \mathbf{v} and this was our transmitted codeword. So you will not make an error. So what we

have shown here is, as long as your error pattern has weight up to t , those error patterns are correctable provided

(Refer Slide Time 21:36)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{v}, \mathbf{u}) \leq d(\mathbf{r}, \mathbf{u}) + d(\mathbf{r}, \mathbf{v})$$

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

the minimum distance of

(Refer Slide Time 21:38)

Error correcting properties of block codes

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$.

$$\mathbf{r} = \mathbf{v} + \mathbf{e}$$

your code is d_{\min}

(Refer Slide Time 21:42)

Error correcting properties of block codes

Theorem:

- A block code C with minimum distance d_{\min} is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword \mathbf{v} is transmitted and \mathbf{r} is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t' , then $d(\mathbf{v}, \mathbf{r}) = t'$. $\mathbf{r} = \mathbf{v} + \mathbf{e}$

and it satisfies this relationship. So the minimum distance of the code is at least $2t + 1$, and it is less than equal to $2t + 2$, then it can correct all error patterns of weight t or less. So as

(Refer Slide Time 22:03)

Error correcting properties of block codes

Proof (contd):

- Since \mathbf{v} , and \mathbf{w} are codewords,
$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

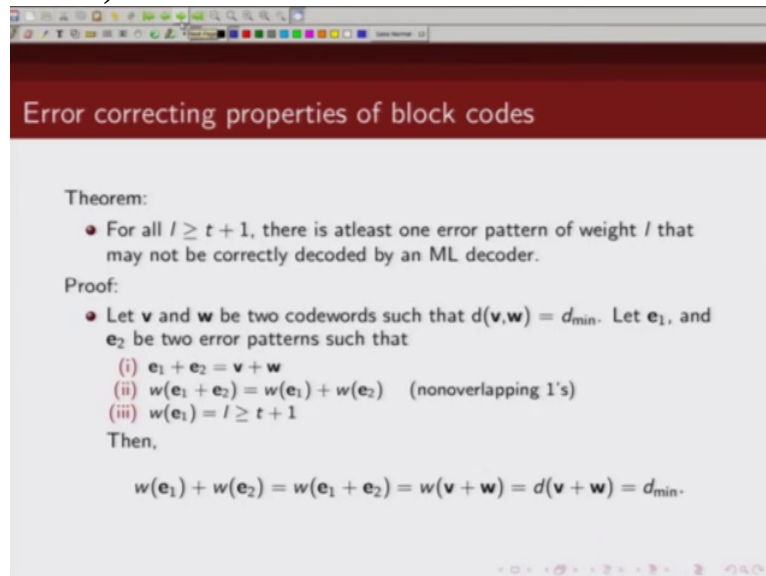
$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'$$

- If $t' \leq t$, then
$$d(\mathbf{r}, \mathbf{w}) \geq t + 1 > t \text{ and } d(\mathbf{v}, \mathbf{r}) = t' \leq t.$$
- Hence \mathbf{r} is closer to \mathbf{v} than any other codeword \mathbf{w} , and an ML decoder will decode correctly.

we can see here, the received codeword is closer to \mathbf{v} than any other codeword \mathbf{w} so it will decide in favor of \mathbf{v} and this \mathbf{r} will be decoded as \mathbf{v} .

Next we are

(Refer Slide Time 22:18)



Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

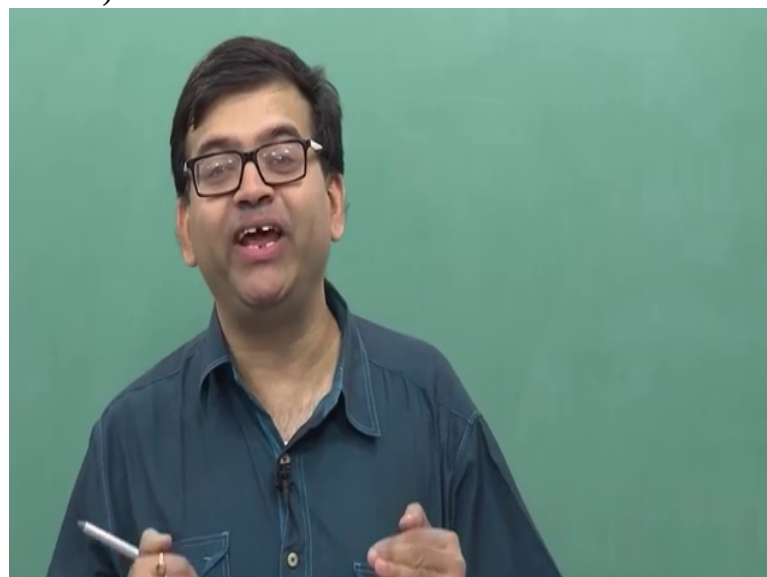
- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v} + \mathbf{w}) = d_{\min}.$$

going to show that if there exists an error pattern of weight greater than equal to $t + 1$ then our decoder whose minimum distance is at least $2t + 1$ but less than $2t + 2$, this decoder will make an error. In other words, it would not be able to correct this error pattern of weight $t + 1$. So for all error patterns of weight l , if l is at least $t + 1$, then our maximum likelihood decoder may not be able to correctly decode or correct that error. So let's prove this. If \mathbf{v} and \mathbf{w} are 2 codewords and let's assume that the Hamming distance between \mathbf{v} and \mathbf{w} is equal to the minimum distance of the code which is denoted by t_{\min} . And let \mathbf{e}_1 and \mathbf{e}_2 are two error patterns which satisfies these 3 properties, and what are these 3 properties? The sum of \mathbf{e}_1 and \mathbf{e}_2 is the same as \mathbf{v} plus \mathbf{w} . The second property is, \mathbf{e}_1 and \mathbf{e}_2 , they do not have any overlapping

(Refer Slide Time 23:50)



1s. So weight of e_1 plus e_2 can be written as weight of e_1

(Refer Slide Time 23:56)

Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v} + \mathbf{w}) = d_{\min}.$$

plus weight of e_2 . And we will show that if there is an error pattern of weight l where l is at least t plus 1 then our maximum likelihood decoder will make an error in decoding. So the way we have chosen our error pattern, weight of e_1 plus weight of e_2 is given by weight of e_1 plus e_2 , this is from 2 and from 1 we know e_1 plus e_2 is nothing but \mathbf{v} plus \mathbf{w} so this is same as weight of \mathbf{v} plus \mathbf{w} and this is nothing but this is Hamming distance between \mathbf{v} and \mathbf{w}

(Refer Slide Time 24:49)

Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v}, \mathbf{w}) = d_{\min}.$$

and we have said the Hamming distance between \mathbf{v} and \mathbf{w} is the minimum distance. So this is equal to the minimum distance. Now let us assume that

(Refer Slide Time 25:02)

• Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1)$$
$$< 2t + 2 - (t + 1) = t + 1$$

we transmitted this codeword \mathbf{v} and what we received is \mathbf{r} . So this \mathbf{v} got corrupted by this error pattern \mathbf{e}_1 which has

(Refer Slide Time 25:15)

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - (i) $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - (ii) $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - (iii) $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v}, \mathbf{w}) = d_{\min}.$$

Hamming weight of at least

(Refer Slide Time 25:18)

Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v}, \mathbf{w}) = d_{\min}.$$

t plus 1. Now

(Refer Slide Time 25:21)

Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - (t + 1) = t + 1 \end{aligned}$$

we will repeat the same exercise, we will try to find out the Hamming distance of this received codeword from the correct transmitted codeword \mathbf{v} and Hamming distance between the received codeword and any other codeword \mathbf{w} . So if we calculate the Hamming distance between \mathbf{w} and the received codeword we know that Hamming distance between \mathbf{w} and \mathbf{r} is nothing but Hamming weight of \mathbf{w} and \mathbf{r} . And what is \mathbf{r} ? \mathbf{r} is my received codeword, \mathbf{v} plus \mathbf{e}_1 . So I can write this as \mathbf{w} plus \mathbf{v} plus \mathbf{e}_1 . Now what is $w(\mathbf{w} + \mathbf{v})$? From 1,

(Refer Slide Time 26:11)

Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v}, \mathbf{w}) = d_{\min}.$$

I have w plus v is same as e_1 plus e_2 . So then this is

(Refer Slide Time 26:17)

Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1)$$

$$< 2t + 2 - (t + 1) = t + 1$$

e_1 plus e_2 plus e_1 . So e_1 plus e_1 will be 0. So this will be e_2 , weight of e_2 . And what is weight of e_2 ? From this relation

(Refer Slide Time 26:31)

Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v}, \mathbf{w}) = d_{\min}.$$

we can see weight of \mathbf{e}_1 plus weight of \mathbf{e}_2 is d_{\min} . So weight of \mathbf{e}_2 is d_{\min} minus weight of \mathbf{e}_1 . So this we can

(Refer Slide Time 26:44)

Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - (t + 1) = t + 1 \end{aligned}$$

write as weight of \mathbf{e}_2 as d_{\min} minus weight of \mathbf{e}_1 . So d_{\min} is less than equal to $2t + 1$

(Refer Slide Time 26:53)

• Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = \underline{d_{\min}} - w(\mathbf{e}_1)$$
$$< 2t + 2 - (t + 1) = t + 1$$

and weight of \mathbf{e}_1 is at least t plus 1. So

(Refer Slide Time 26:58)

• Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = \underline{d_{\min}} - w(\mathbf{e}_1)$$
$$< 2t + 2 - \underline{(t + 1)} = t + 1$$

weight of \mathbf{e}_2 will be less than $2t$ plus 2 minus t plus 1 which is t plus 1. So the Hamming distance between \mathbf{w} and \mathbf{r} is less than t plus 1. And

(Refer Slide Time 27:15)

Slide titled "Error correcting properties of block codes".

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) < 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.

what is the Hamming distance between \mathbf{v} and \mathbf{r} ? This is weight of \mathbf{e}_1 ,

(Refer Slide Time 27:28)

Slide titled "Error correcting properties of block codes".

$d(\mathbf{v}, \mathbf{r}) = w(\mathbf{e}_1)$

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) < 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.

Ok and what is weight of \mathbf{e}_1 ? Weight of \mathbf{e}_1 is given by l , which is

(Refer Slide Time 27:36)

Error correcting properties of block codes

Theorem:

- For all $l \geq t + 1$, there is atleast one error pattern of weight l that may not be correctly decoded by an ML decoder.

Proof:

- Let \mathbf{v} and \mathbf{w} be two codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$. Let \mathbf{e}_1 , and \mathbf{e}_2 be two error patterns such that
 - $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
 - $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
 - $w(\mathbf{e}_1) = l \geq t + 1$

Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v}, \mathbf{w}) = d_{\min}.$$

at least $t + 1$. So what we

(Refer Slide Time 27:40)

Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - \underline{(t + 1)} = t + 1 \end{aligned}$$

have shown here is

(Refer Slide Time 27:43)

The slide is titled "Error correcting properties of block codes". It contains the following text:

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) < 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance d_{\min} , an ML decoder will correctly decode any error pattern of weight $t \triangleq \lfloor \frac{d_{\min} - 1}{2} \rfloor$ or less.

weight of \mathbf{w} , Hamming distance between \mathbf{w} and \mathbf{r} is

(Refer Slide Time 28:01)

The slide is titled "Error correcting properties of block codes". It contains the following text:

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) < 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance d_{\min} , an ML decoder will correctly decode any error pattern of weight $t \triangleq \lfloor \frac{d_{\min} - 1}{2} \rfloor$ or less.

less than t plus 1 where as Hamming distance between \mathbf{v} and \mathbf{r} is greater than equal to t plus 1. So what we have shown is Hamming distance between \mathbf{w} and \mathbf{r} is less than equal to Hamming distance between received codeword \mathbf{r} and the true codeword which was actually transmitted which is \mathbf{v} . So in this case the maximum likelihood decoder will decode in favor of \mathbf{w} and not \mathbf{v} and will make a mistake. So through this construction

(Refer Slide Time 28:23)



we have shown that if your error pattern is of weight $t + 1$, then you are not guaranteed to correct that error. So from this and the previous result we can conclude

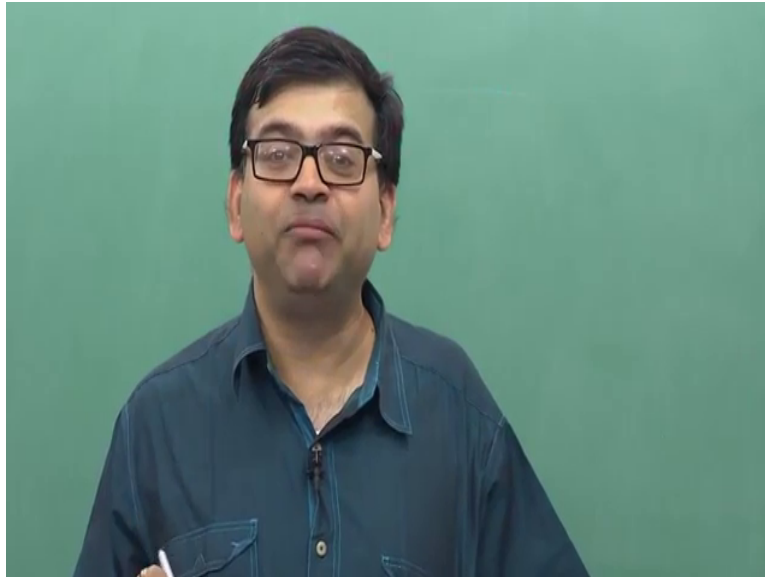
(Refer Slide Time 28:36)

The slide is titled "Error correcting properties of block codes" and contains the following content:

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) < 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance d_{\min} , an ML decoder will correctly decode any error pattern of weight $t \triangleq \lfloor \frac{d_{\min} - 1}{2} \rfloor$ or less.

that if we have a block code with minimum distance d_{\min} which satisfies relationship that d_{\min}

(Refer Slide Time 28:45)



lies between $2t + 1$ and $2t + 2$ then this linear block code with minimum distance d_{\min} should be able to correct

(Refer Slide Time 28:56)

Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) < 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance d_{\min} , an ML decoder will correctly decode any error pattern of weight $t \triangleq \lfloor \frac{d_{\min} - 1}{2} \rfloor$ or less.

all error patterns up to weight t where t is given by

(Refer Slide Time 29:03)

Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1)$$
$$< 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance d_{\min} , an ML decoder will correctly decode any error pattern of weight $t \triangleq \lfloor \frac{d_{\min} - 1}{2} \rfloor$ or less.

this. So this t is

(Refer Slide Time 29:06)

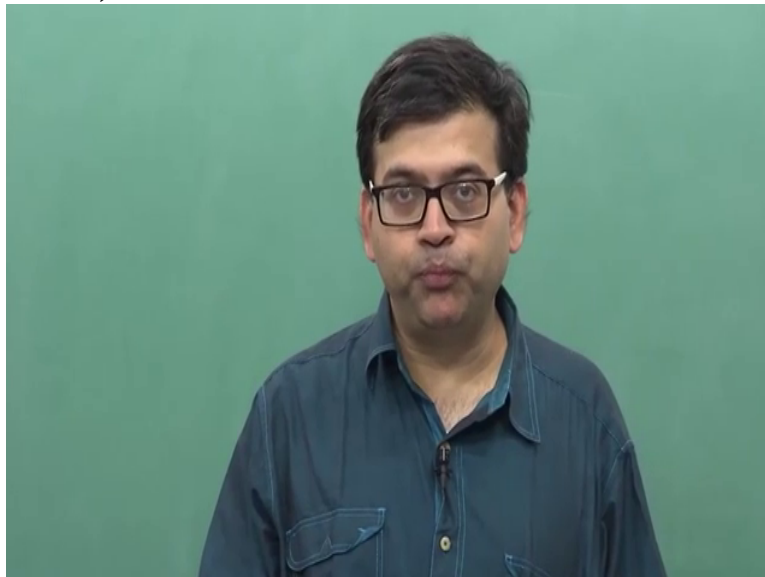
Error correcting properties of block codes

- Assuming \mathbf{v} is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1)$$
$$< 2t + 2 - (t + 1) = t + 1$$
- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance d_{\min} , an ML decoder will correctly decode any error pattern of weight $t \triangleq \lfloor \frac{d_{\min} - 1}{2} \rfloor$ or less.
- t is called the random error correcting capability of the code.

known as random error correcting capability of the linear block code.

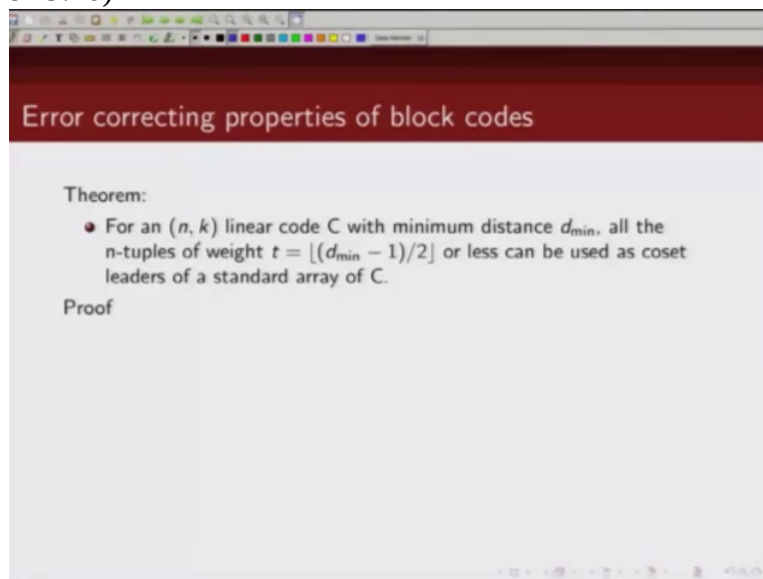
Next we are going to prove a result

(Refer Slide Time 29:15)



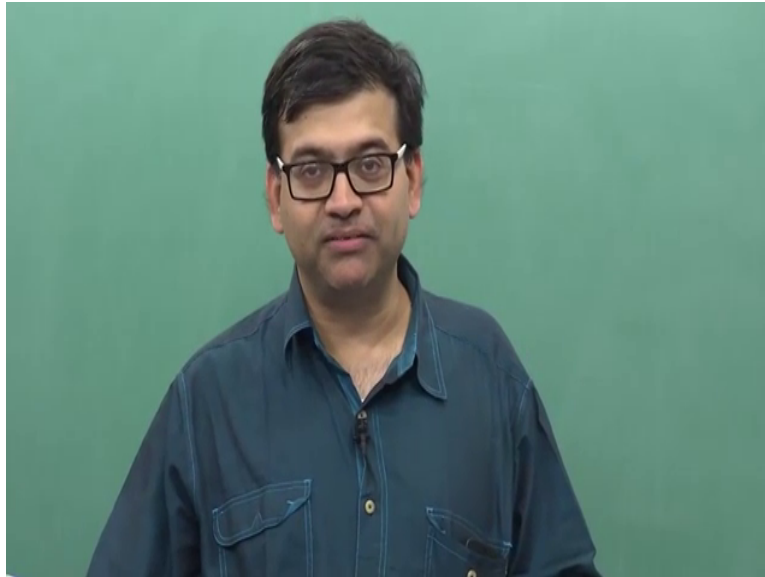
which is as follows. So if we have an $n \times k$ linear block

(Refer Slide Time 29:20)



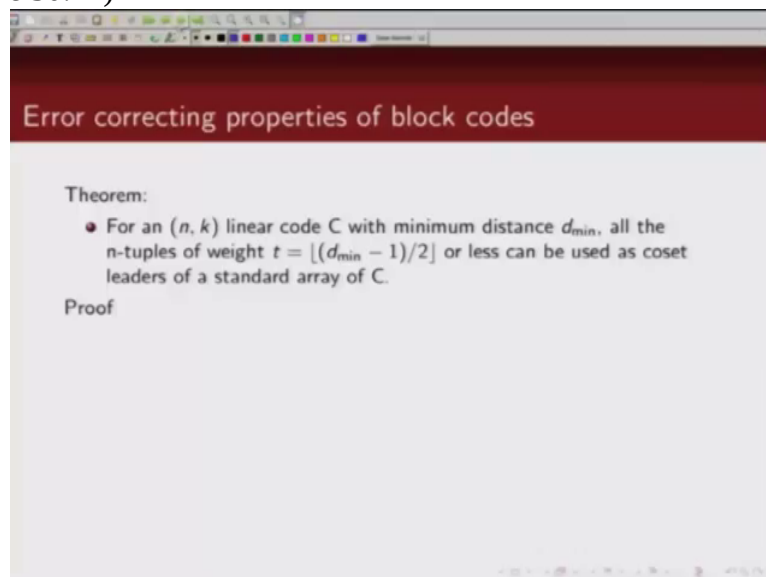
code whose minimum distance is given by t_{min} then we can show where d_{min} lies between $2t + 1$ and $2t + 2$, then we can show that all n -tuples of weight t or less can be used as coset leader in our standard array. So we are going to prove this result using method of contradiction.

(Refer Slide Time 29:50)



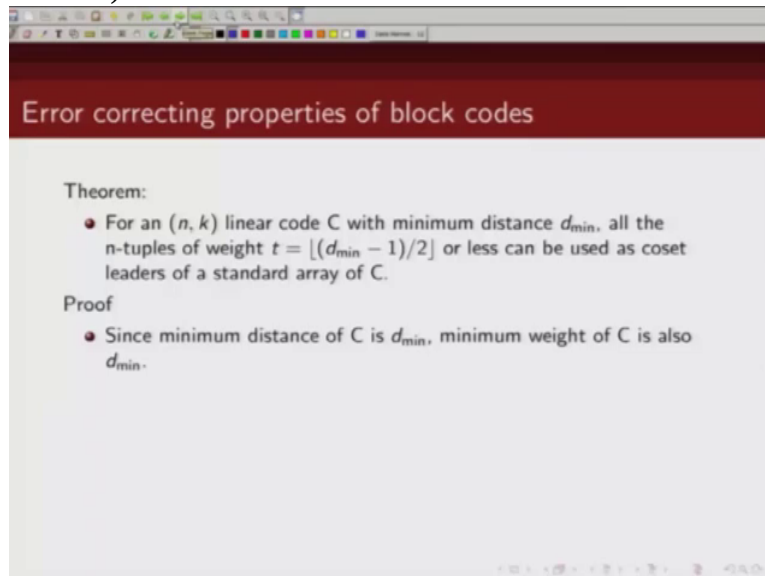
Now let's say, so how method of contradiction work. We will say, let's say they are all error patterns or weight up to t ; let's say they are not coset leaders. Let's say, we will assume a scenario where there are 2 such end tuples with weight up to t which are not coset leaders. In other words they lie in the same coset or same row. And then later on we will show that that is not possible. So that's how this method of contradiction will work

(Refer Slide Time 30:27)



will work

(Refer Slide Time 30:28)



The slide is titled "Error correcting properties of block codes" in a dark red header. Below the header, the text is as follows:

Theorem:

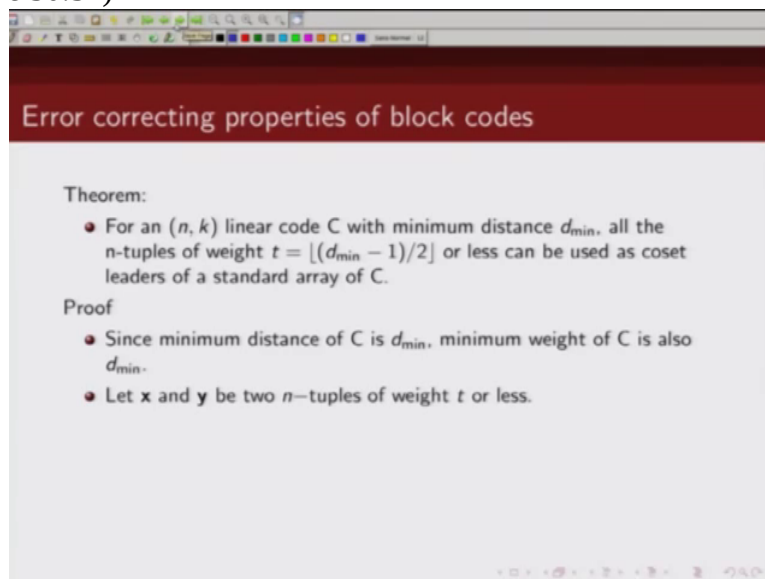
- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .

so minimum distance of the code is d_{\min} so minimum weight of the code is also d_{\min} .

(Refer Slide Time 30:37)



The slide is titled "Error correcting properties of block codes" in a dark red header. Below the header, the text is as follows:

Theorem:

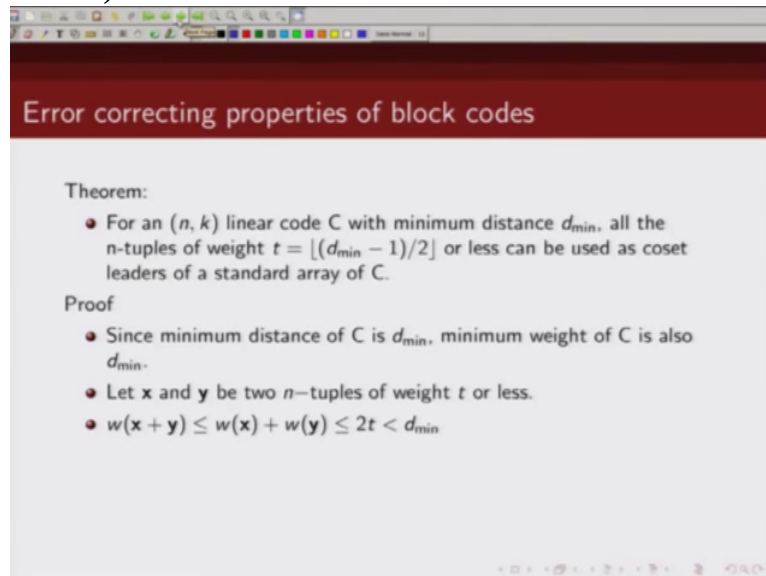
- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.

Let \mathbf{x} and \mathbf{y} are 2 n -tuples of weight t or less. Now

(Refer Slide Time 30:45)



Error correcting properties of block codes

Theorem:

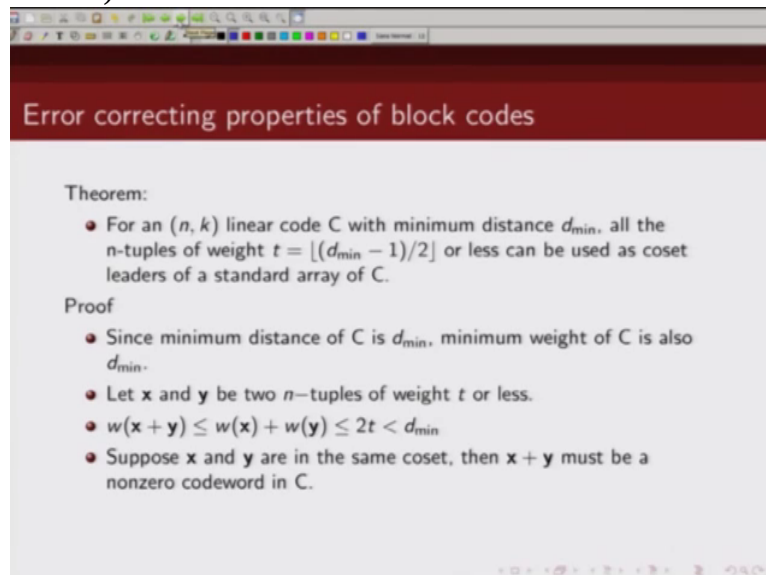
- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$

weight of \mathbf{x} plus \mathbf{y} will be less than equal to weight of \mathbf{x} plus weight of \mathbf{y} . Why, because there might be some overlapping 1s at some locations of this n -tuple \mathbf{x} and \mathbf{y} and we are given that the weight of \mathbf{x} and weight of \mathbf{y} is at most t so then weight of \mathbf{x} plus weight of \mathbf{y} will be less than equal to $2t$ and this is less than minimum distance because minimum distance of code is at least $2t + 1$. Now let us assume

(Refer Slide Time 31:25)



Error correcting properties of block codes

Theorem:

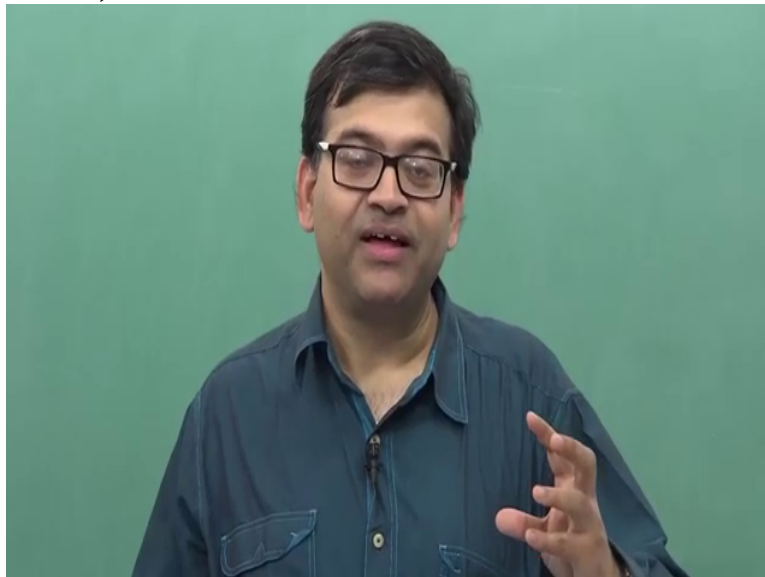
- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .

that these \mathbf{x} and \mathbf{y} which are

(Refer Slide Time 31:29)



error patterns of weight t or less, let us assume that they are not coset leaders. If they are not coset leaders, let us assume they are in the same coset; they are in the same row. So if we assume \mathbf{x} and \mathbf{y} are in

(Refer Slide Time 31:45)

A screenshot of a presentation slide with a red header. The header text is "Error correcting properties of block codes". The main content is as follows:

Theorem:

- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .

the same row or same coset, then \mathbf{x} plus \mathbf{y} must be a codeword. Why this is so? If you recall your standard array we had something like this. First row first column was all zero vector and then we had other codewords. And then we had error pattern, let's say \mathbf{e}_2 . This was \mathbf{e}_2 plus \mathbf{v}_2 . Like, like this was \mathbf{e}_2 plus \mathbf{v}_2 . If you look at

(Refer Slide Time 32:27)

Error correcting properties of block codes

Theorem:

- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .

any 2 elements in the same coset or same row and if you add them up what do you get? Let's add this and this, what do we get? e_2 plus e_2 plus v_2 ,

(Refer Slide Time 32:41)

Error correcting properties of block codes

Theorem:

- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .

we will get v_2 . If we add this and this we will get v_2 plus v_2 which is another codeword v_2 . So if we take any two elements in the same coset and we add them up we are going to get a

(Refer Slide Time 33:01)

Error correcting properties of block codes

Theorem:

- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .

Handwritten notes: A vertical line separates the proof steps. To the right of the line, the top row contains $v_2 \dots v_2^k$ and the bottom row contains $e_2 + v_2 \dots e_2 + v_2^k$.

non zero codeword.

(Refer Slide Time 33:03)

Error correcting properties of block codes

Theorem:

- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .

Handwritten notes: A vertical line separates the proof steps. To the right of the line, the top row contains $v_2 \dots v_2^k$ and the bottom row contains $e_2 + v_2 \dots e_2 + v_2^k$.

So if \mathbf{x} and \mathbf{y} are in the same coset then $\mathbf{x} + \mathbf{y}$ must be a codeword. This is impossible.

(Refer Slide Time 33:15)

Error correcting properties of block codes

Theorem:

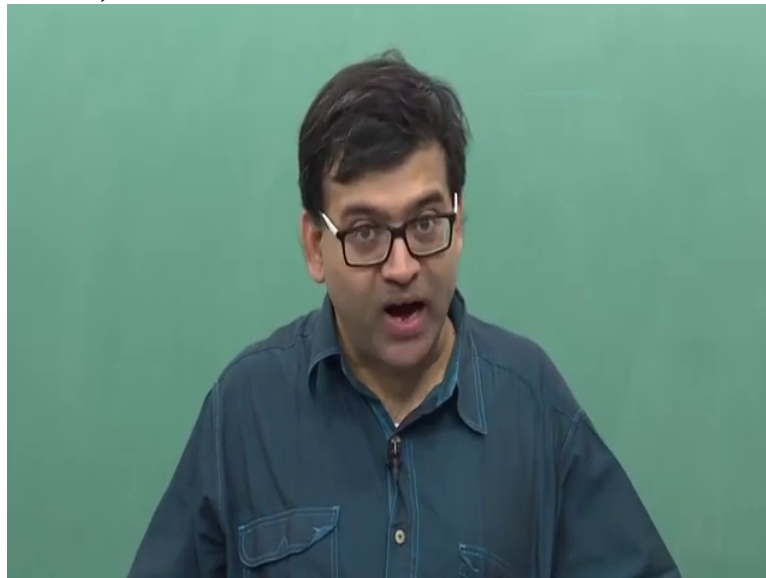
- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .
- This is impossible as weight of $\mathbf{x} + \mathbf{y} < d_{\min}$.

Why? Because if \mathbf{x} plus \mathbf{y} is a

(Refer Slide Time 33:19)



codeword then what is the minimum distance of \mathbf{x} plus \mathbf{y} ? \mathbf{x} plus \mathbf{y} , minimum distance of that must be d_{\min} .

(Refer Slide Time 33:28)

The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .
- This is impossible as weight of $\mathbf{x} + \mathbf{y} < d_{\min}$.

But what is the, what is the weight of \mathbf{x} plus \mathbf{y} , we just showed in this bullet that weight of \mathbf{x} plus \mathbf{y} is less than d_{\min} . That means weight of \mathbf{x} plus \mathbf{y} is less than d_{\min} .

(Refer Slide Time 33:44)

The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

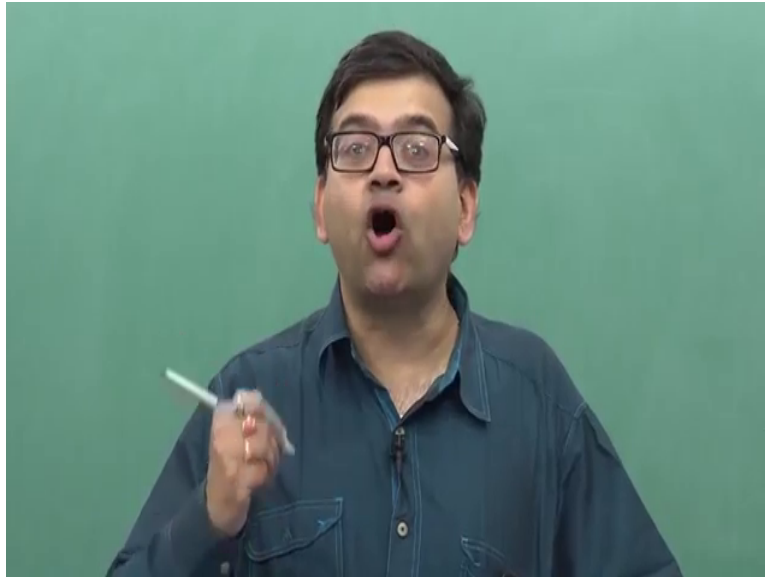
- For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C .

Proof

- Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} .
- Let \mathbf{x} and \mathbf{y} be two n -tuples of weight t or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose \mathbf{x} and \mathbf{y} are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C .
- This is impossible as weight of $\mathbf{x} + \mathbf{y} < d_{\min}$.

If weight of \mathbf{x} plus \mathbf{y} is less than d_{\min} then \mathbf{x} plus \mathbf{y} cannot

(Refer Slide Time 33:50)



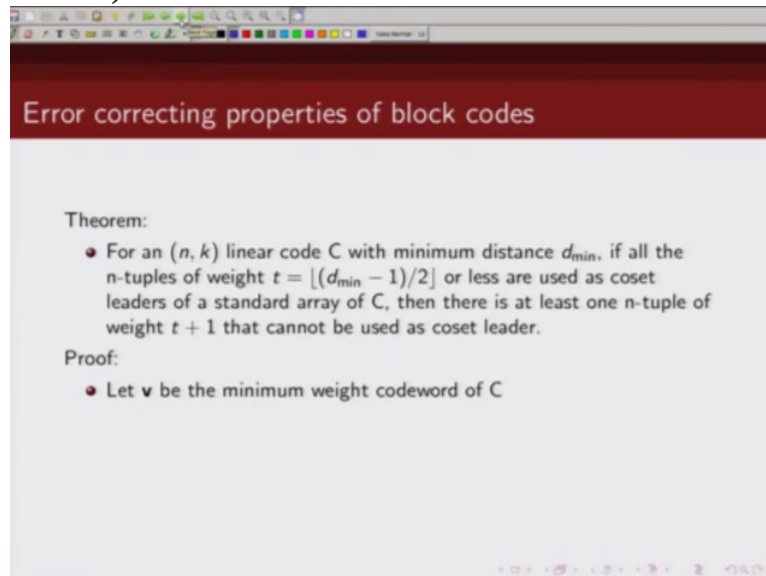
be a non zero codeword because the weight of a non-zero codeword should be at least d_{\min} . So our assumption that x and y are in the same coset is wrong. In other words then x and y must be in different cosets, different rows and we can always make these x and y as coset leaders. So this proves our result that

(Refer Slide Time 34:27)

A screenshot of a presentation slide. The title is "Error correcting properties of block codes" in white text on a dark red background. Below the title, the text "Theorem:" is followed by a bullet point: "For an (n, k) linear code C with minimum distance d_{\min} , all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C ." Below this, the text "Proof" is followed by four bullet points: "Since minimum distance of C is d_{\min} , minimum weight of C is also d_{\min} ." "Let x and y be two n -tuples of weight t or less." " $w(x + y) \leq w(x) + w(y) \leq 2t < d_{\min}$ " "Suppose x and y are in the same coset, then $x + y$ must be a nonzero codeword in C ." "This is impossible as weight of $x + y < d_{\min}$." The slide has a standard presentation navigation bar at the bottom.

all n -tuples of weight n , of weight t or less can be used as coset leaders in the standard array and we know that uh if we use them as coset leaders, we, those are our correctable error patterns.

(Refer Slide Time 34:46)



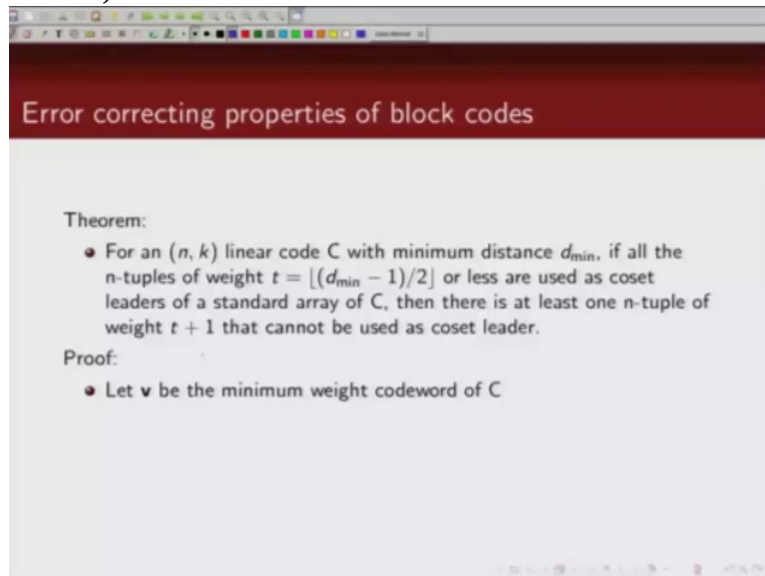
Next I am going to show you a result which is as follows. So if you have a $n \times k$ linear block code whose minimum distance is d_{\min} and if all n -tuples of weight t or less are already used as coset leader then there is at least 1 n -tuple of weight $t + 1$ which cannot be used as coset leader. So this essentially is going to show us again the same result that

(Refer Slide Time 35:21)



any weight pattern of, error pattern of weight $t + 1$ is not guaranteed to be corrected. So how do we

(Refer Slide Time 35:31)



The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

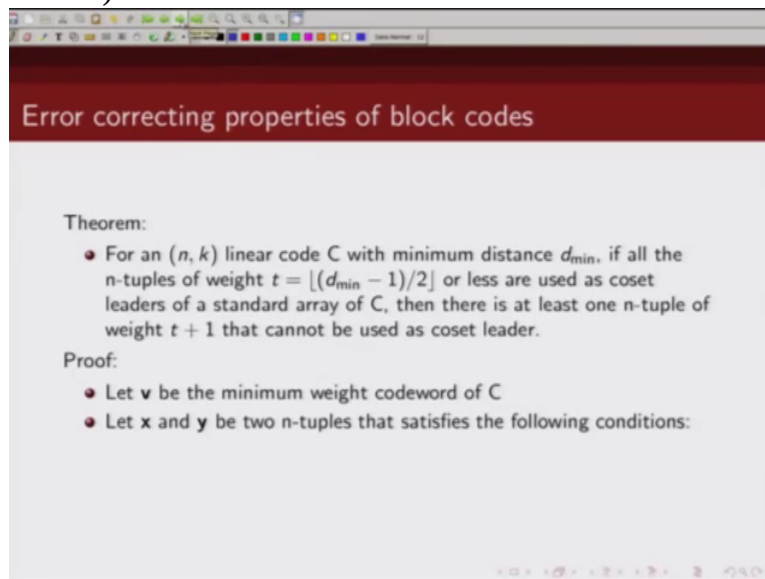
- For an (n, k) linear code C with minimum distance d_{\min} , if all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C , then there is at least one n -tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let \mathbf{v} be the minimum weight codeword of C

prove it? So let's assume \mathbf{v} is the minimum weight codeword of C

(Refer Slide Time 35:38)



The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

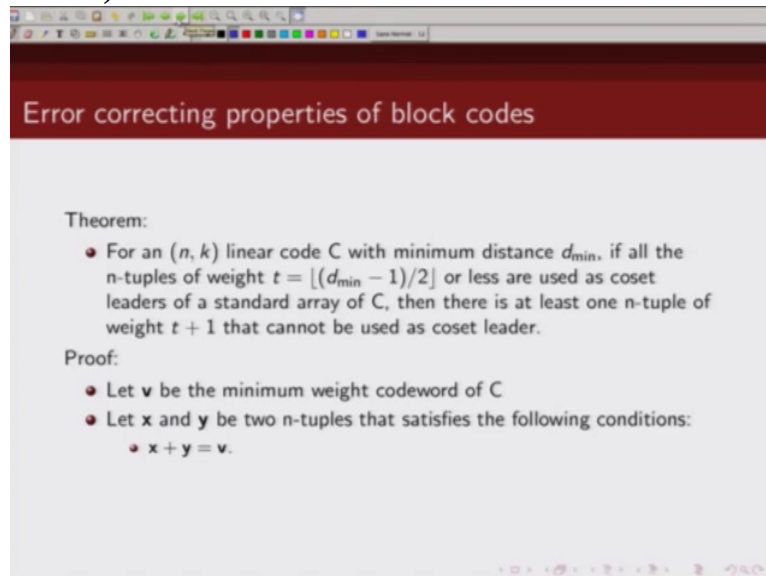
- For an (n, k) linear code C with minimum distance d_{\min} , if all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C , then there is at least one n -tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let \mathbf{v} be the minimum weight codeword of C
- Let \mathbf{x} and \mathbf{y} be two n -tuples that satisfies the following conditions:

and we have 2 n -tuples \mathbf{x} and \mathbf{y} which satisfies these following conditions.

(Refer Slide Time 35:45)



The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

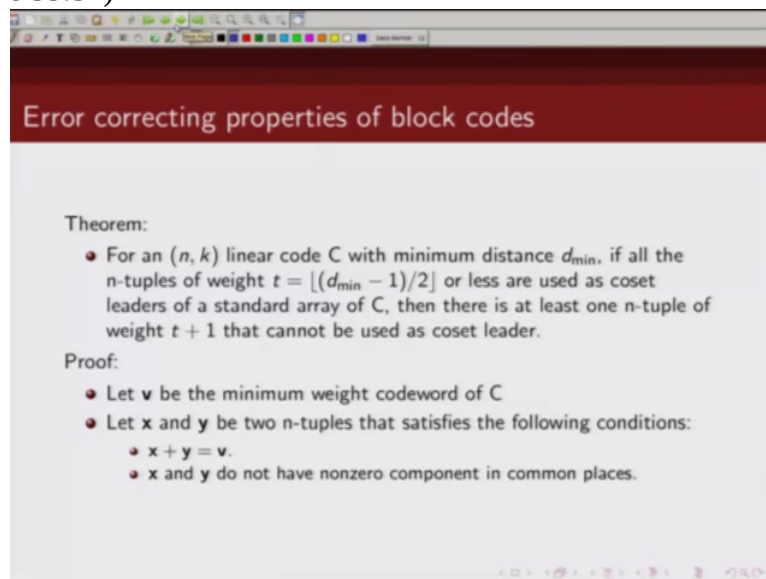
- For an (n, k) linear code C with minimum distance d_{\min} , if all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C , then there is at least one n -tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let \mathbf{v} be the minimum weight codeword of C
- Let \mathbf{x} and \mathbf{y} be two n -tuples that satisfies the following conditions:
 - $\mathbf{x} + \mathbf{y} = \mathbf{v}$.

First, \mathbf{x} plus \mathbf{y} is equal to \mathbf{v} , and \mathbf{x} and \mathbf{y} do not

(Refer Slide Time 35:54)



The slide is titled "Error correcting properties of block codes". It contains the following text:

Theorem:

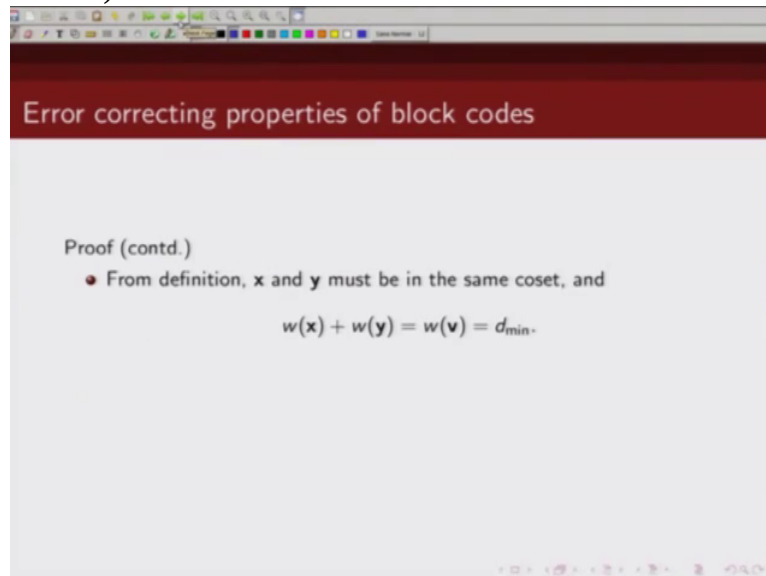
- For an (n, k) linear code C with minimum distance d_{\min} , if all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C , then there is at least one n -tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let \mathbf{v} be the minimum weight codeword of C
- Let \mathbf{x} and \mathbf{y} be two n -tuples that satisfies the following conditions:
 - $\mathbf{x} + \mathbf{y} = \mathbf{v}$.
 - \mathbf{x} and \mathbf{y} do not have nonzero component in common places.

have any component common. So they do not have 1s common in same position. So

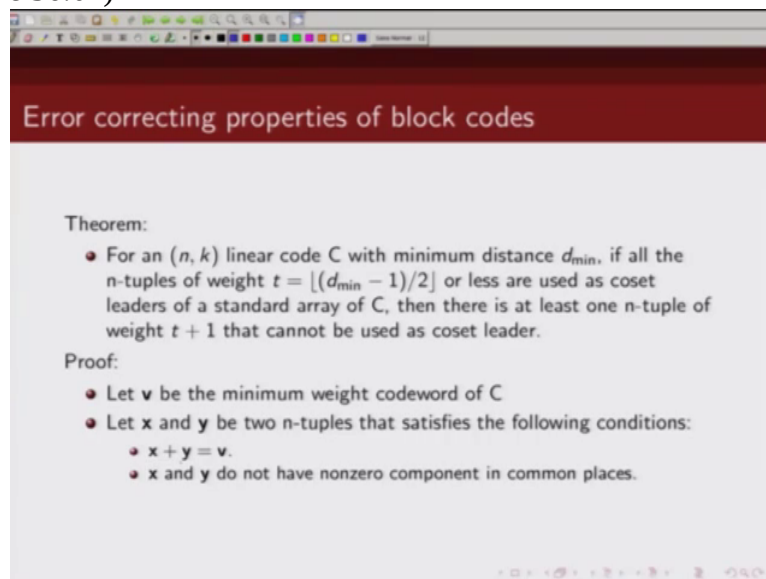
(Refer Slide Time 36:04)



The slide has a dark red header with the text "Error correcting properties of block codes". Below the header, the text "Proof (contd.)" is followed by a bullet point: "From definition, x and y must be in the same coset, and". Below this, the equation $w(x) + w(y) = w(v) = d_{\min}$ is displayed.

from the definition x and y

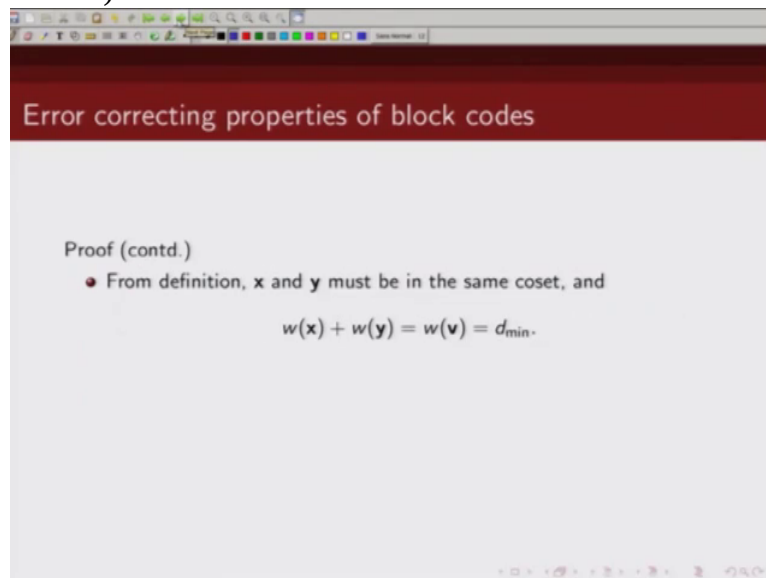
(Refer Slide Time 36:07)



The slide has a dark red header with the text "Error correcting properties of block codes". Below the header, the text "Theorem:" is followed by a bullet point: "For an (n, k) linear code C with minimum distance d_{\min} , if all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C , then there is at least one n -tuple of weight $t + 1$ that cannot be used as coset leader." Below this, the text "Proof:" is followed by two bullet points: "Let v be the minimum weight codeword of C " and "Let x and y be two n -tuples that satisfies the following conditions:". The second bullet point has two sub-bullets: " $x + y = v$." and " x and y do not have nonzero component in common places."

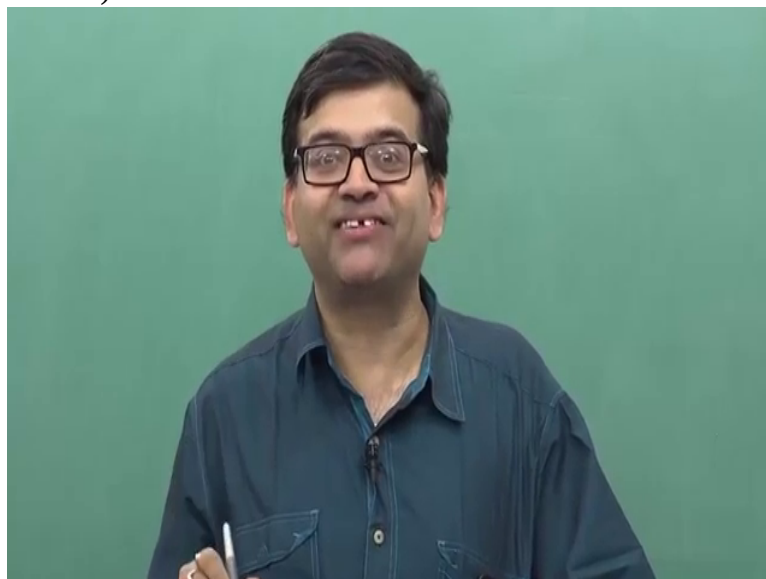
must be in the same coset. Why? Because we know if two elements are in the same coset and if we add them sum is a valid codeword. So x plus y is equal to v which is a valid codeword, then x and y must be in the same coset.

(Refer Slide Time 36:32)



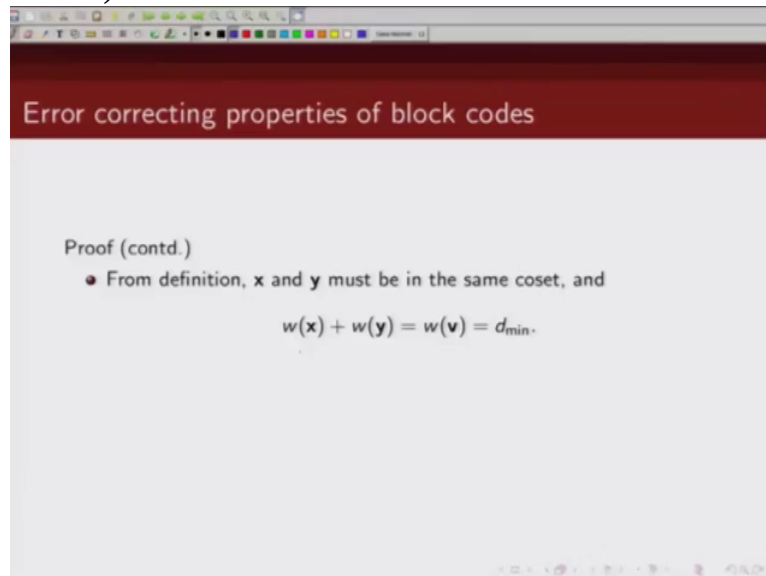
So that's what I said from definition x and y must be in the same coset because x plus y

(Refer Slide Time 36:42)



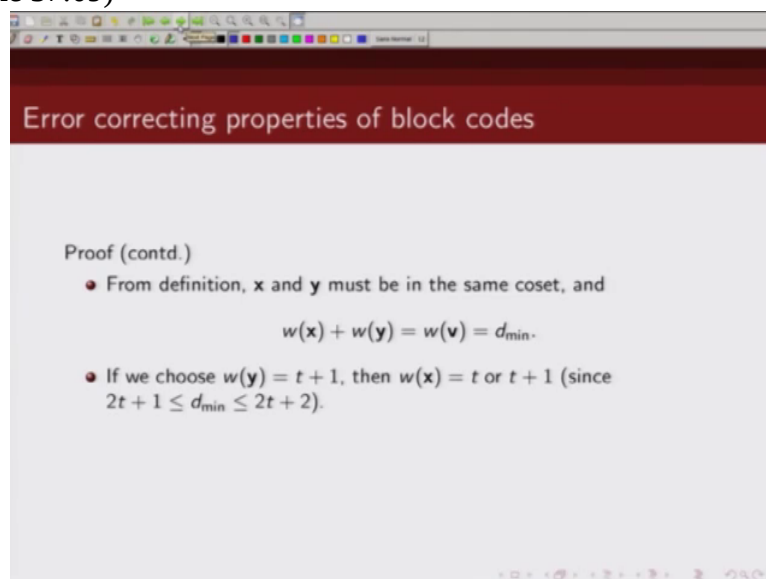
is v which is a valid codeword. And we know that if we add any two elements in a coset their sum is a valid codeword. And

(Refer Slide Time 36:54)



similarly weight of x plus weight of y is equal to weight of v. And we have chosen v to be the minimum distance codeword, so this is given by d min. Now if we choose

(Refer Slide Time 37:09)



our y to have a weight of t plus 1, then we can see from here d min is greater than equal to 2 t plus 1 but less than equal to 2 t plus 2. So from this and using the fact that d min lies between 2 t plus 1 and 2 t plus 2,

(Refer Slide Time 37:39)

Error correcting properties of block codes

Proof (contd.)

- From definition, x and y must be in the same coset, and
$$w(x) + w(y) = w(v) = d_{\min}. \quad 2t+1 \leq d_{\min} \leq 2t+2$$
- If we choose $w(y) = t + 1$, then $w(x) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).

using these 2 results what we get is weight of x

(Refer Slide Time 37:45)

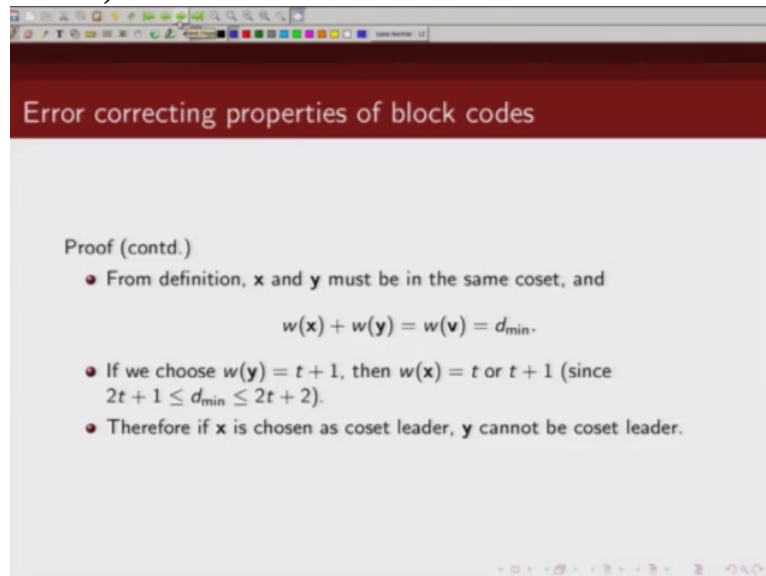
Error correcting properties of block codes

Proof (contd.)

- From definition, x and y must be in the same coset, and
$$w(x) + w(y) = w(v) = d_{\min}. \quad 2t+1 \leq d_{\min} \leq 2t+2$$
- If we choose $w(y) = t + 1$, then $w(x) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).

can be t or t plus 1.

(Refer Slide Time 37:53)



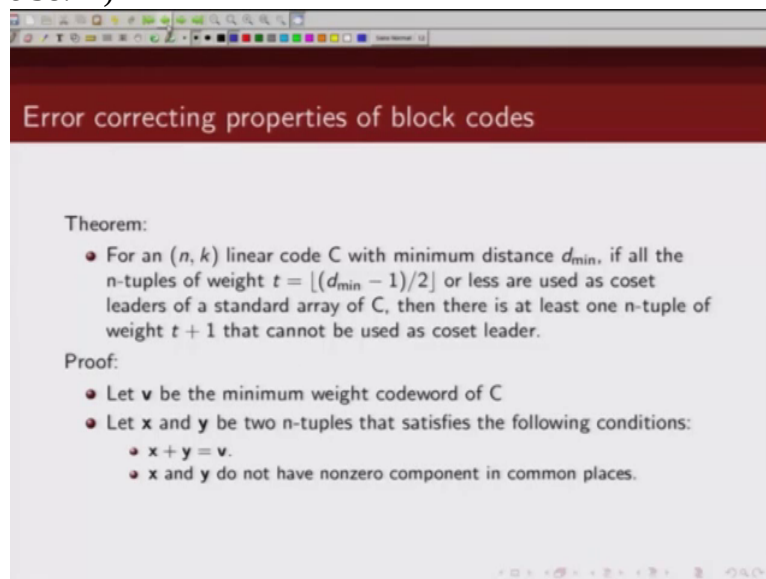
Slide titled "Error correcting properties of block codes". The content is as follows:

Proof (contd.)

- From definition, \mathbf{x} and \mathbf{y} must be in the same coset, and
$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$
- If we choose $w(\mathbf{y}) = t + 1$, then $w(\mathbf{x}) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).
- Therefore if \mathbf{x} is chosen as coset leader, \mathbf{y} cannot be coset leader.

So therefore if we choose \mathbf{x} to be our coset leader then we cannot choose \mathbf{y} as our coset leader. You can see, because \mathbf{x} and \mathbf{y} are in the same coset and weight of \mathbf{x} is t or $t + 1$ whereas weight of \mathbf{y} is $t + 1$. So I will choose \mathbf{x} as my coset leader. And if I choose \mathbf{x} as my coset leader then I cannot choose \mathbf{y} as my coset leader which proves my result

(Refer Slide Time 38:27)



Slide titled "Error correcting properties of block codes". The content is as follows:

Theorem:

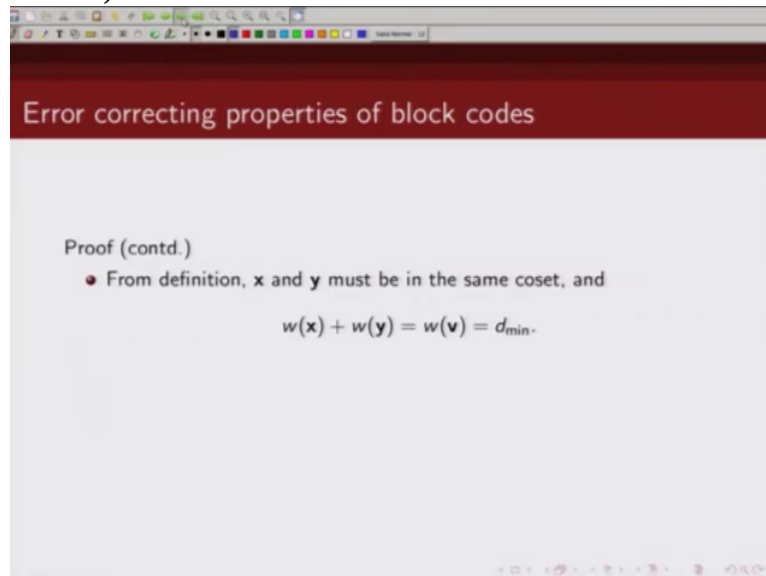
- For an (n, k) linear code C with minimum distance d_{\min} , if all the n -tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C , then there is at least one n -tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let \mathbf{v} be the minimum weight codeword of C
- Let \mathbf{x} and \mathbf{y} be two n -tuples that satisfies the following conditions:
 - $\mathbf{x} + \mathbf{y} = \mathbf{v}$.
 - \mathbf{x} and \mathbf{y} do not have nonzero component in common places.

which says that if all n -tuples of weight t or less are used as coset leaders then there exist at least one error pattern of weight $t + 1$ which cannot be used as coset leader and if this error pattern

(Refer Slide Time 38:44)



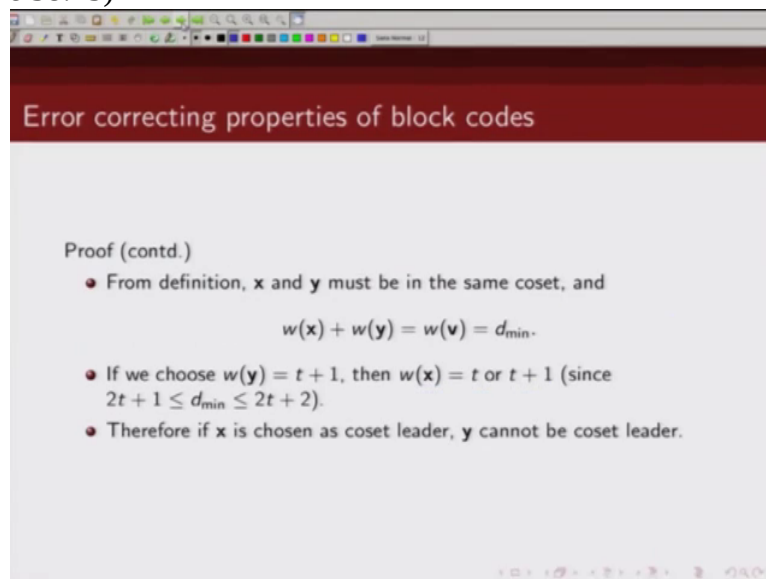
Slide 38:44: Error correcting properties of block codes. Proof (contd.)

- From definition, \mathbf{x} and \mathbf{y} must be in the same coset, and

$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$

pattern

(Refer Slide Time 38:45)



Slide 38:45: Error correcting properties of block codes. Proof (contd.)

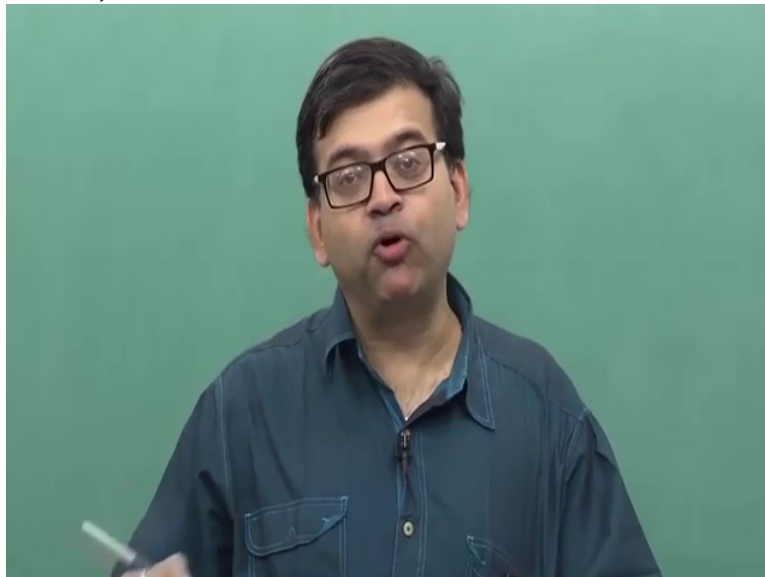
- From definition, \mathbf{x} and \mathbf{y} must be in the same coset, and

$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$

- If we choose $w(\mathbf{y}) = t + 1$, then $w(\mathbf{x}) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).
- Therefore if \mathbf{x} is chosen as coset leader, \mathbf{y} cannot be coset leader.

of weight t plus 1 cannot be put

(Refer Slide Time 38:49)



as coset leader then this is not a correctable error pattern.

(Refer Slide Time 38:54)

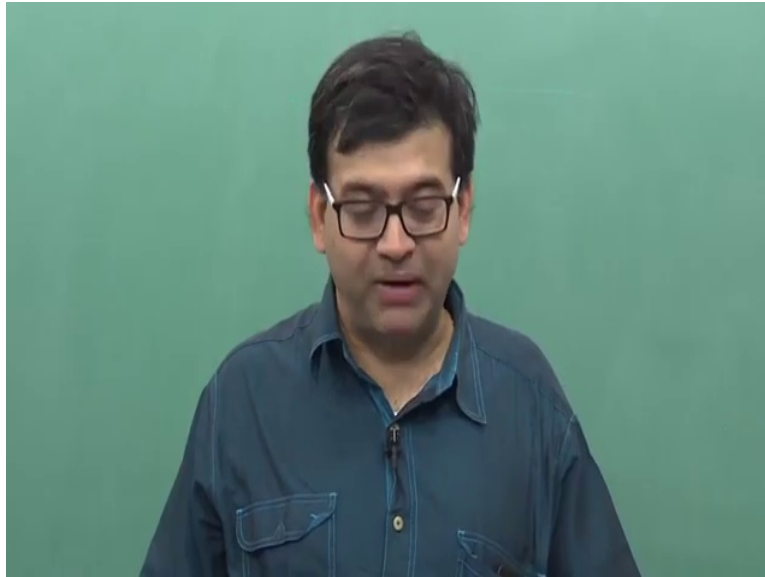
A slide titled "Error correcting properties of block codes" with a red header. The slide contains a proof (contd.) with three bullet points and a mathematical equation. The text is as follows:

Proof (contd.)

- From definition, \mathbf{x} and \mathbf{y} must be in the same coset, and
$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$
- If we choose $w(\mathbf{y}) = t + 1$, then $w(\mathbf{x}) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).
- Therefore if \mathbf{x} is chosen as coset leader, \mathbf{y} cannot be coset leader.

So with this, I will conclude my

(Refer Slide Time 38:57)



lecture on random error correcting and random error detecting properties of block codes.

Thank you