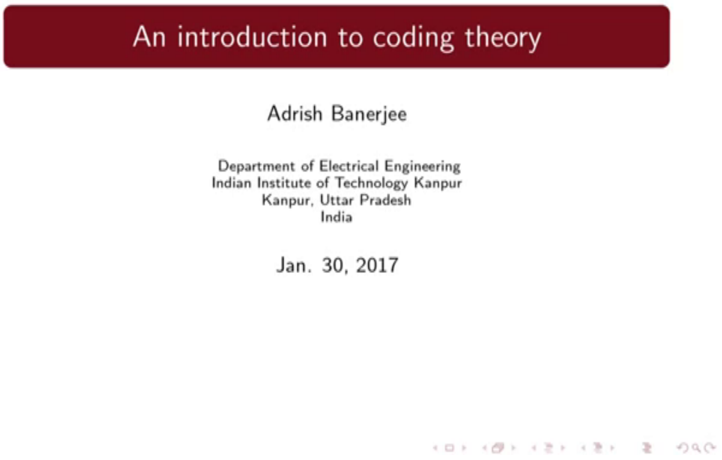
An Introduction to Coding Theory
Professor Adrish Banerji
Department of Electrical Engineering
Indian Institute of Technology, Kanpur
Module 02
Lecture Number 08
Decoding of Linear Block Codes

(Refer Slide Time 00:13)

Welcome to the course on Coding Theory.

(Refer Slide Time 00:15)



An introduction to coding theory

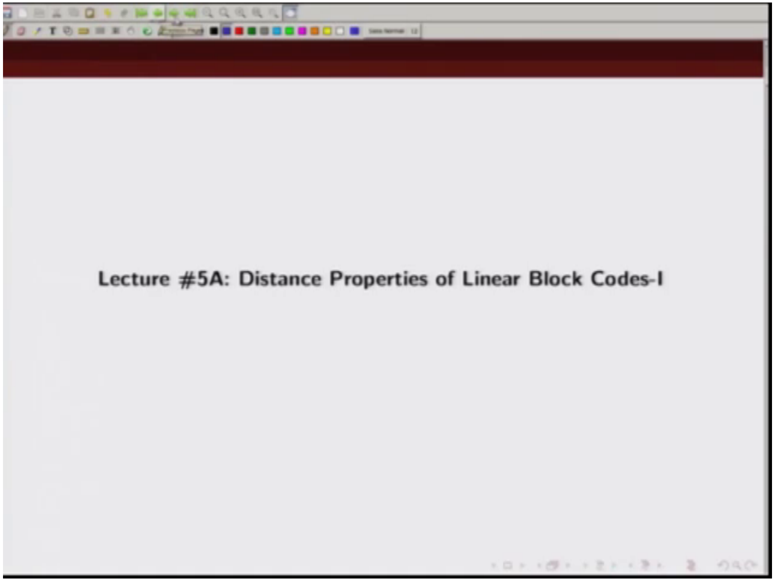
Adrish Banerjee

Department of Electrical Engineering
Indian Institute of Technology Kanpur
Kanpur, Uttar Pradesh
India

Jan. 30, 2017

As we know the error correcting

(Refer Slide Time 00:18)



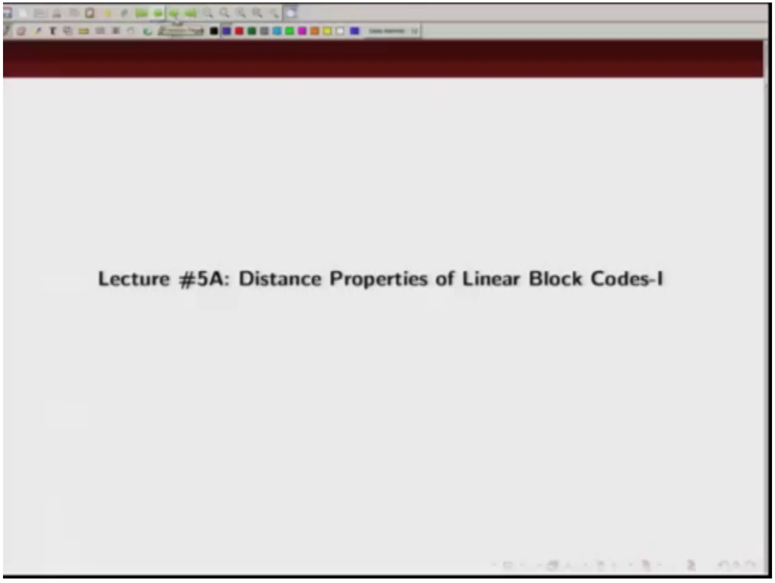
Lecture #5A: Distance Properties of Linear Block Codes-I

and error detecting capability of error correcting codes

(Refer Slide Time 00:21)

depends on the distance profile of these codes so today we are going to talk and, talk about the distance properties

(Refer Slide Time 00:30)



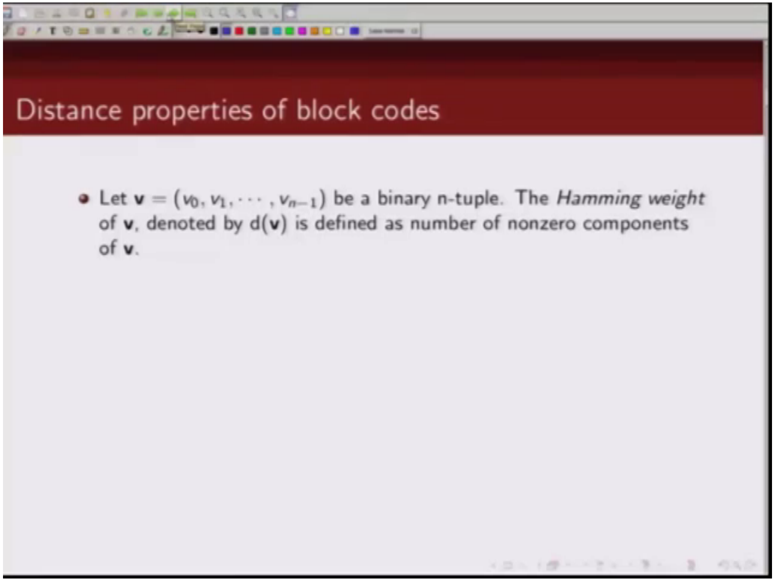
Lecture #5A: Distance Properties of Linear Block Codes-I

of linear block codes. We are going to

(Refer Slide Time 00:34)

describe what we mean by Hamming distance of codes and then we are going to talk about how the minimum Hamming distance of code is related to the columns of parity check matrix.

(Refer Slide Time 00:50)

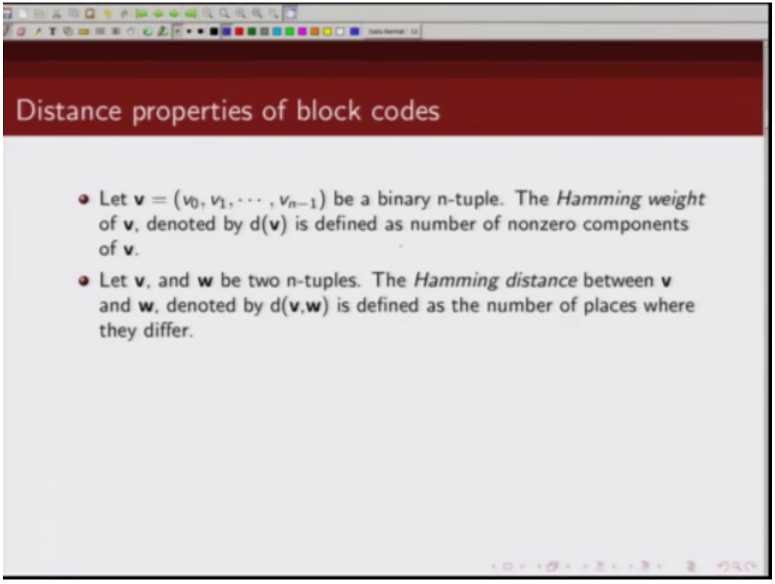


Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.

I am first going to describe what is Hamming weight. So if we have a n-tuple, let's call it v, so v is an n-tuple, and since we are restricting our discussion to binary linear block code. So we consider a binary n-tuple. So this v 0, v 1, v 2, v n minus 1 could be either 0 or 1. So we define the Hamming weight of this vector v as number of non zero components of v. So, for example, let's say

(Refer Slide Time 01:30)

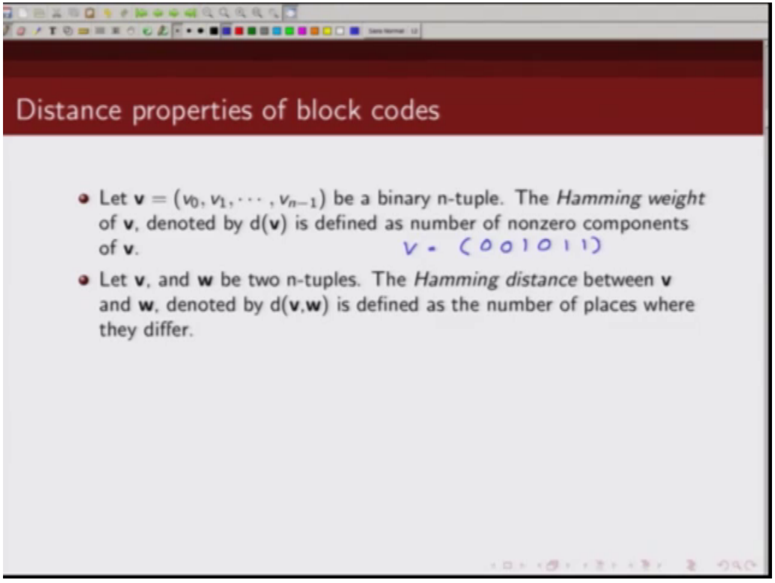


Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.
- Let $\mathbf{v}$, and $\mathbf{w}$ be two n-tuples. The *Hamming distance* between $\mathbf{v}$ and $\mathbf{w}$, denoted by d($\mathbf{v}$,$\mathbf{w}$) is defined as the number of places where they differ.

v is 0 0 1 0 1 1. Let's say

(Refer Slide Time 01:38)

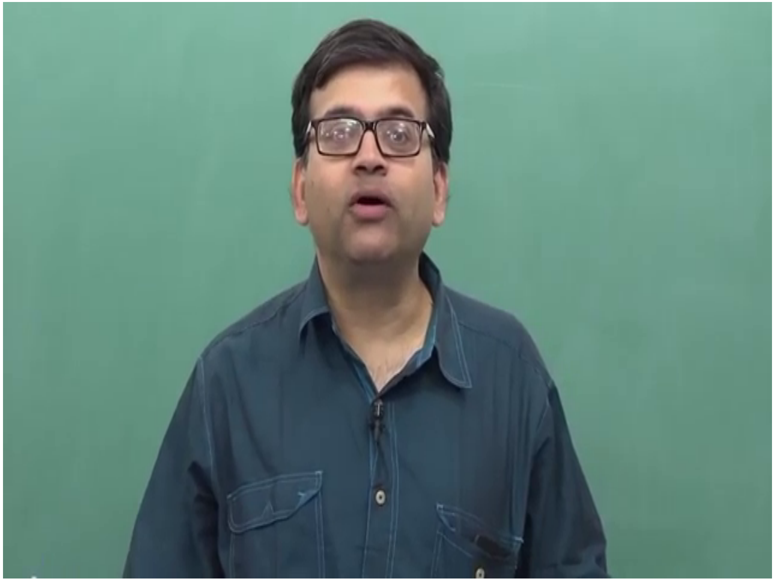


Distance properties of block codes

- Let **v** $= (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of **v**, denoted by d(**v**) is defined as number of nonzero components of **v**. $v = (0010\,11)$
- Let **v**, and **w** be two n-tuples. The *Hamming distance* between **v** and **w**, denoted by d(**v**,**w**) is defined as the number of places where they differ.

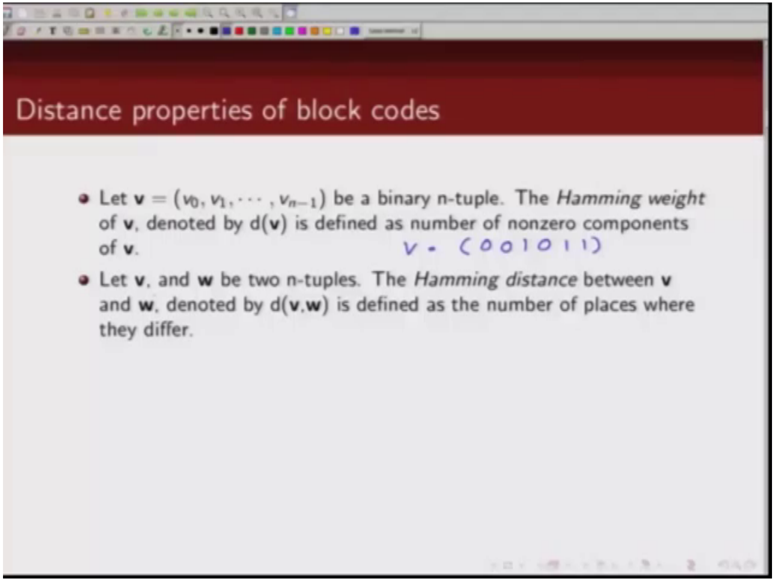
this is my v. So we can see here how many non-zero components we have, 1, 2, 3. So the

(Refer Slide Time 01:48)



Hamming weight of v is in this example is 3. Now let v and w are two

(Refer Slide Time 01:57)

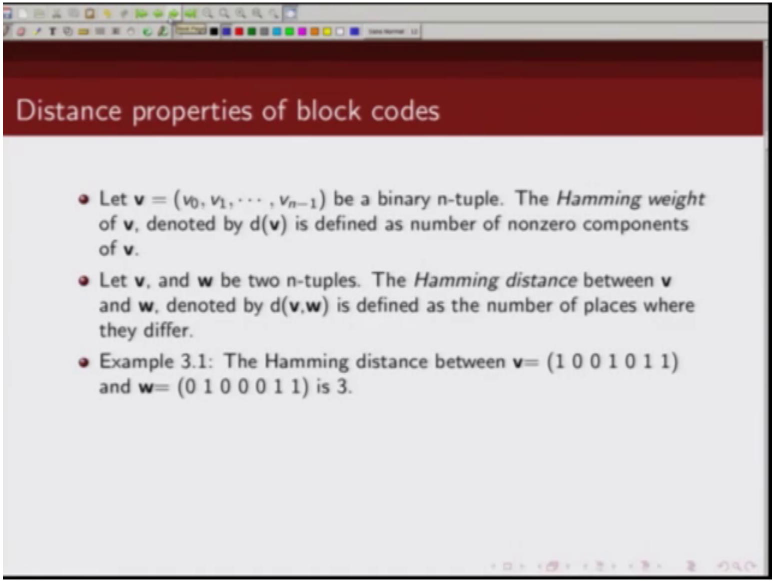


Distance properties of block codes

- Let **v** = $(v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of **v**, denoted by d(**v**) is defined as number of nonzero components of **v**.
  v = (0 0 1 0 1 1)
- Let **v**, and **w** be two n-tuples. The *Hamming distance* between **v** and **w**, denoted by d(**v**,**w**) is defined as the number of places where they differ.

n-tuples. So we define the Hamming distance between v and w which is denoted by d v w as the number of places where v and w are differing. So

(Refer Slide Time 02:16)

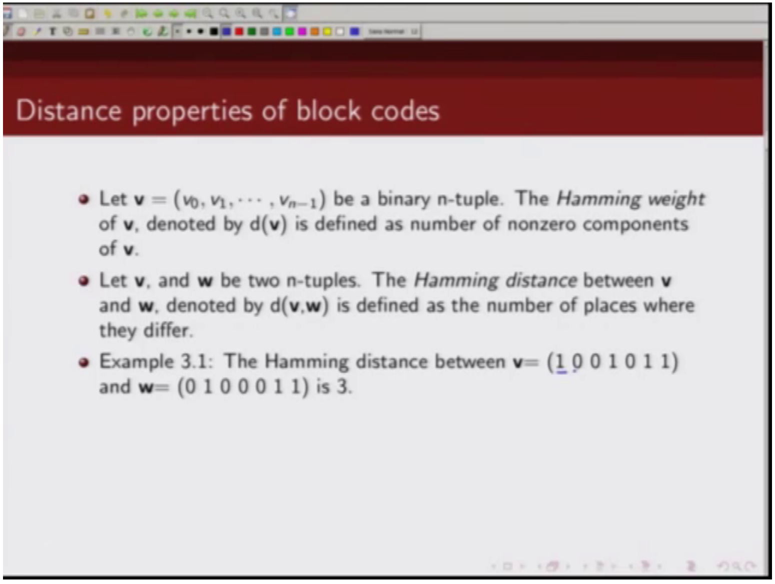


Distance properties of block codes

- Let **v** = $(v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of **v**, denoted by d(**v**) is defined as number of nonzero components of **v**.
- Let **v**, and **w** be two n-tuples. The *Hamming distance* between **v** and **w**, denoted by d(**v**,**w**) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between **v**= (1 0 0 1 0 1 1) and **w**= (0 1 0 0 0 1 1) is 3.

for example, if v is given by this 1 0 0 1 0 1 1, and w is given by 0 1 0 0 0 1 1 then what is the Hamming distance, then let's look at the first location. This is 1 and this is 0. So they are differing in the first location. So that's 1. Similarly the second location, this is 0, this is 1, so they are differing. So now it's Hamming weight is Hamming distance 2, 0 0 both are same, the third bit location, the fourth bit location this is 1 and this is 0, so there are differing, so Hamming distance is now 3, 0 0 they are same, this bit location both the v and w are 1, similarly in this location v and w are same. That means our Hamming distance between v and w is 3. And these are three locations where they are differing. One is this first bit location,

(Refer Slide Time 03:28)

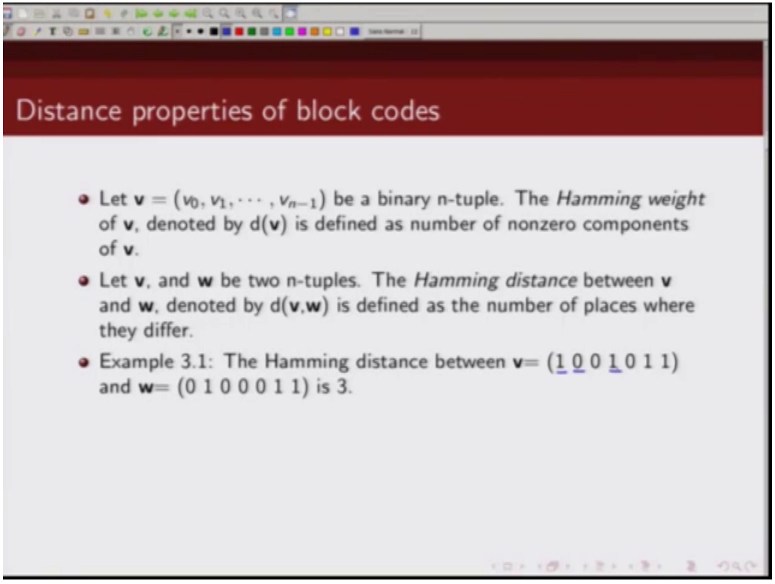


Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of **v**, denoted by d(**v**) is defined as number of nonzero components of **v**.
- Let **v**, and **w** be two n-tuples. The *Hamming distance* between **v** and **w**, denoted by d(**v**,**w**) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between **v**= $(\underline{1}\ \underline{0}\ 0\ 1\ 0\ 1\ 1)$ and **w**= (0 1 0 0 0 1 1) is 3.

second bit location and this fourth bit location,

(Refer Slide Time 03:32)

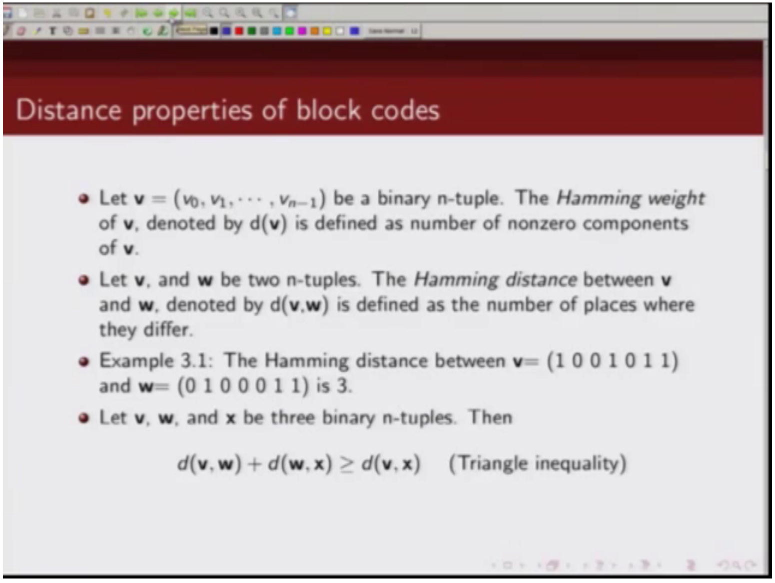


Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of **v**, denoted by d(**v**) is defined as number of nonzero components of **v**.
- Let **v**, and **w** be two n-tuples. The *Hamming distance* between **v** and **w**, denoted by d(**v**,**w**) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between **v**= $(\underline{1}\ \underline{0}\ 0\ \underline{1}\ 0\ 1\ 1)$ and **w**= (0 1 0 0 0 1 1) is 3.

so the Hamming distance between v and w in this example is 3. Now if

(Refer Slide Time 03:40)



Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.
- Let $\mathbf{v}$, and $\mathbf{w}$ be two n-tuples. The *Hamming distance* between $\mathbf{v}$ and $\mathbf{w}$, denoted by d($\mathbf{v}$,$\mathbf{w}$) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between $\mathbf{v}$= (1 0 0 1 0 1 1) and $\mathbf{w}$= (0 1 0 0 0 1 1) is 3.
- Let $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{x}$ be three binary n-tuples. Then

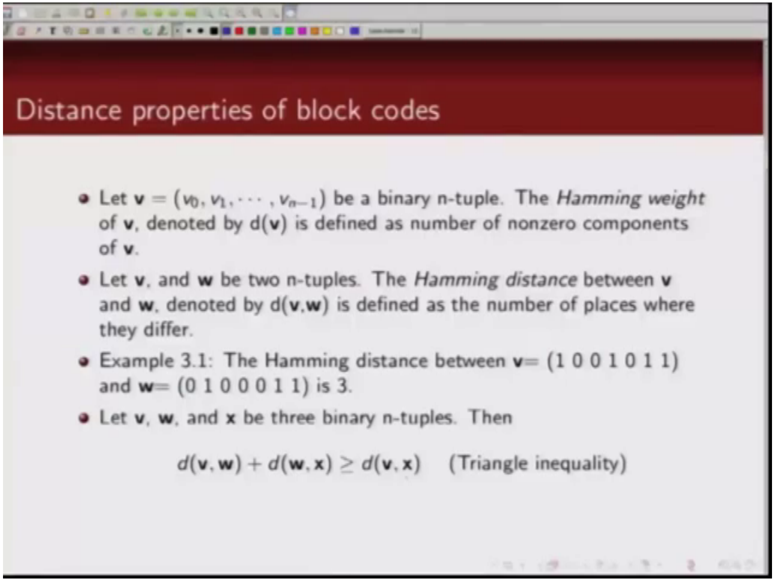
$$d(\mathbf{v},\mathbf{w}) + d(\mathbf{w},\mathbf{x}) \geq d(\mathbf{v},\mathbf{x}) \quad \text{(Triangle inequality)}$$

v, w, x are 3 binary n-tuples, then the Hamming distance between v and w, Hamming distance between w and x and Hamming distance between v and x satisfies this inequality which is known as triangular inequality. So what is triangular inequality? The Hamming distance between v and w

(Refer Slide Time 04:06)

plus the Hamming distance between w and x is greater than equal to Hamming distance between

(Refer Slide Time 04:15)



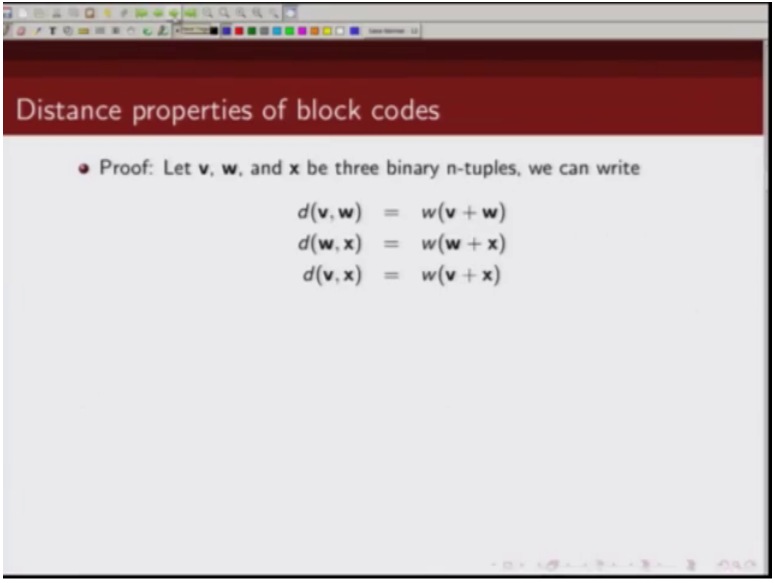
Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of **v**, denoted by d(**v**) is defined as number of nonzero components of **v**.
- Let **v**, and **w** be two n-tuples. The *Hamming distance* between **v** and **w**, denoted by d(**v**,**w**) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between **v**= (1 0 0 1 0 1 1) and **w**= (0 1 0 0 0 1 1) is 3.
- Let **v**, **w**, and **x** be three binary n-tuples. Then

$$d(\mathbf{v},\mathbf{w}) + d(\mathbf{w},\mathbf{x}) \geq d(\mathbf{v},\mathbf{x}) \quad \text{(Triangle inequality)}$$

v and x. So let us

(Refer Slide Time 04:20)



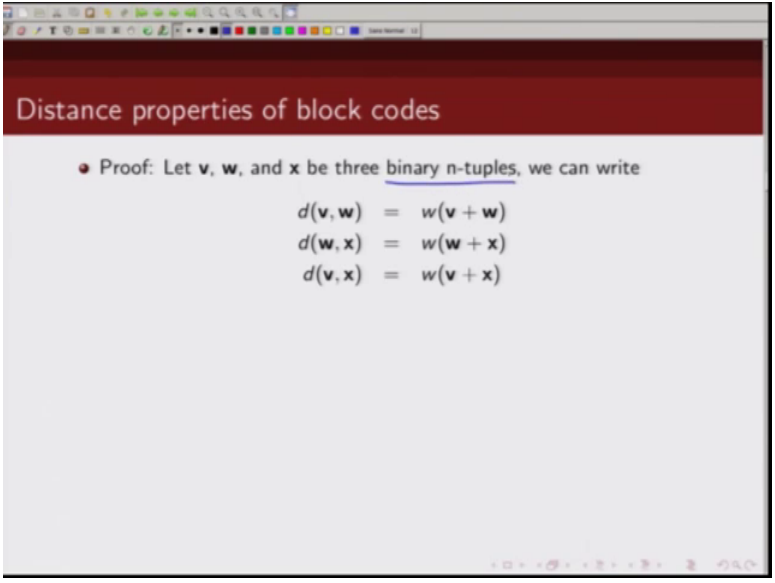
Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

first try to prove this triangular inequality. So let v, w and x are 3 binary n-tuples. So the binary distance between v and w can be defined as Hamming weight of v plus w. Note that we are talking about binary n-tuples.

(Refer Slide Time 04:45)



Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

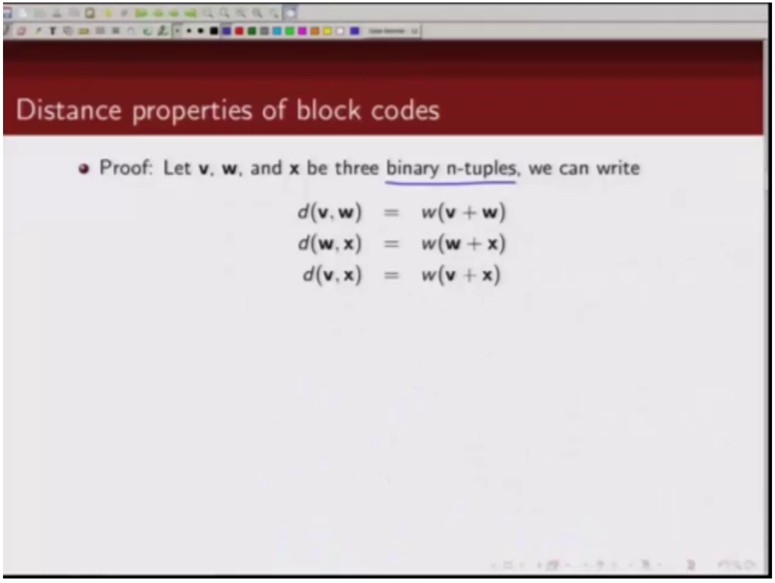
$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

And what is Hamming distance? Hamming distance is number of positions in which v and w

(Refer Slide Time 04:53)

are differing. And since we are talking about binary n-tuples so

(Refer Slide Time 05:00)



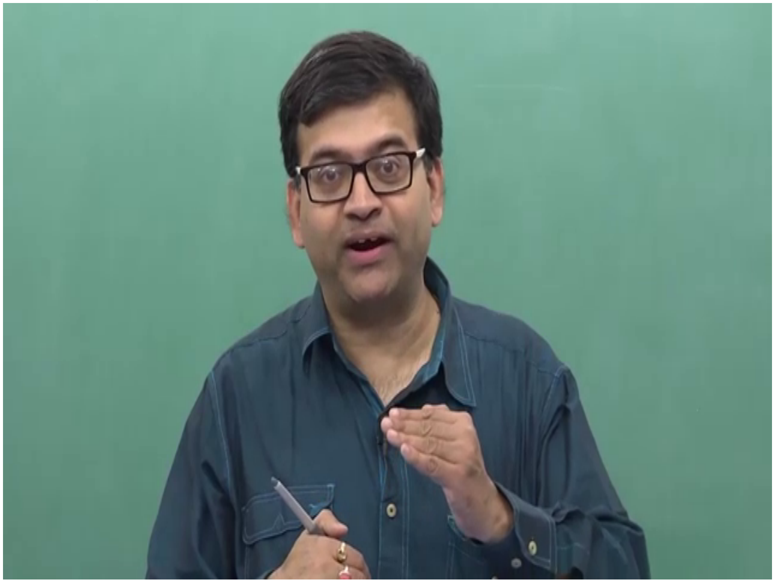
Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

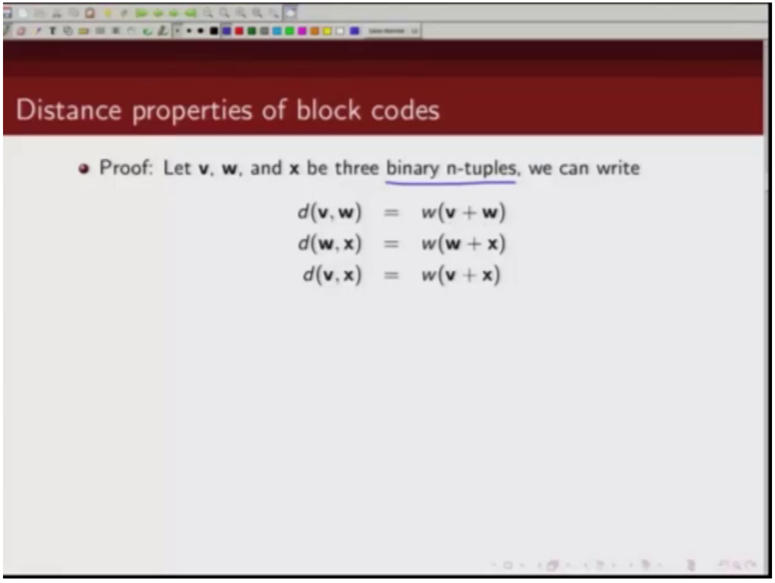
the number of places where v and w are differing can be found if we add v and w, that is modulo 2 addition of v and w and we find out the positions where the sum is 1. Because only in those locations where these

(Refer Slide Time 05:21)



bits are differing v plus w will be

(Refer Slide Time 05:25)



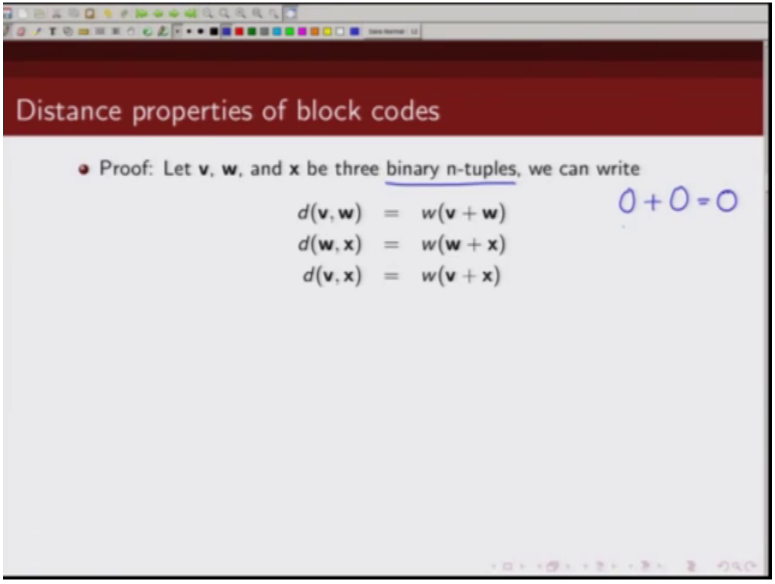
Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

1 otherwise it will be 0 because we know for binary modulo 2 addition 0 plus 0 is going to be 0,

(Refer Slide Time 05:35)



Distance properties of block codes

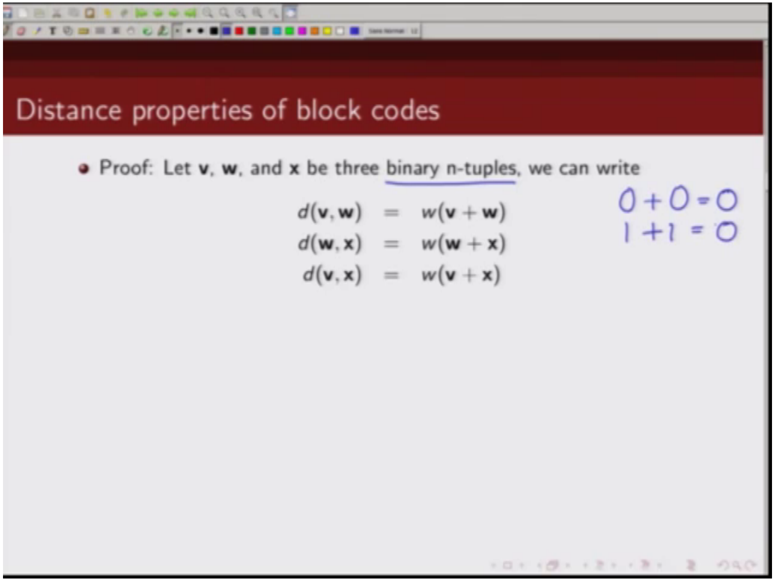
- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$0+0=0$

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

1 plus 1 is going to be 0, only when

(Refer Slide Time 05:39)



Distance properties of block codes

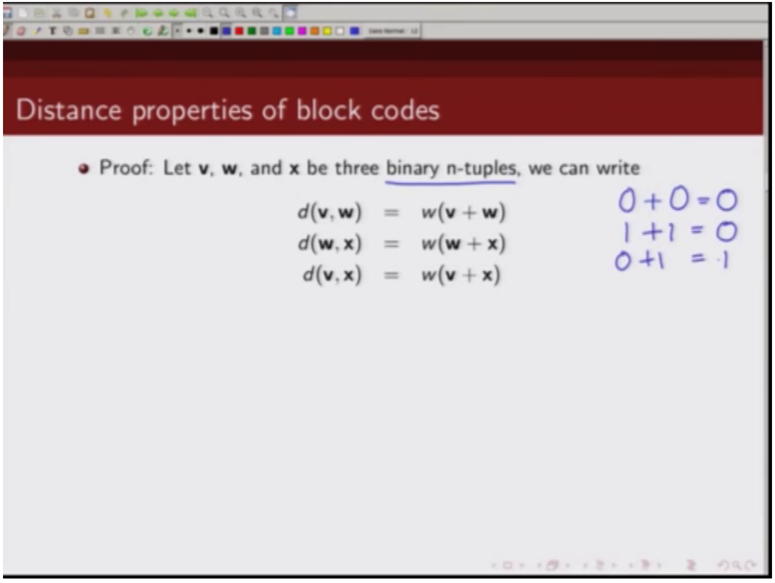
- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$d(\mathbf{v},\mathbf{w}) = w(\mathbf{v}+\mathbf{w})$$
$$d(\mathbf{w},\mathbf{x}) = w(\mathbf{w}+\mathbf{x})$$
$$d(\mathbf{v},\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

$0+0=0$
$1+1=0$

they are differing, 0 plus 1 in this case, it is going to be 1

(Refer Slide Time 05:44)



Distance properties of block codes

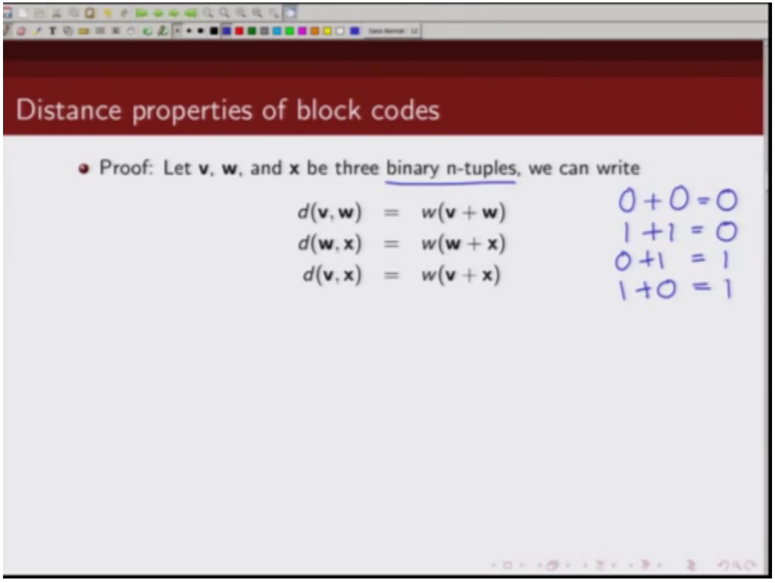
- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$d(\mathbf{v},\mathbf{w}) = w(\mathbf{v}+\mathbf{w})$$
$$d(\mathbf{w},\mathbf{x}) = w(\mathbf{w}+\mathbf{x})$$
$$d(\mathbf{v},\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

$0+0=0$
$1+1=0$
$0+1=1$

and if this is 1 and this is 0, in this case also

(Refer Slide Time 05:49)



Distance properties of block codes

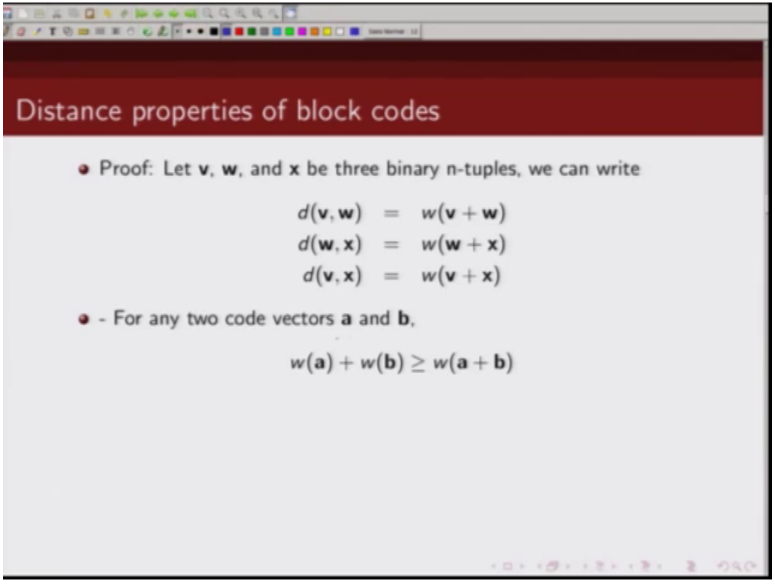
- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

$0+0=0$
$1+1=0$
$0+1=1$
$1+0=1$

this Hamming weight is going to be 1. So we can write down the Hamming distance between v and w as the Hamming weight between v plus w. Similarly we can write the Hamming distance between w and x as the weight of this vector w plus x. And we can define the Hamming distance between v and x as the weight of v plus x. So if we have

(Refer Slide Time 06:24)



Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

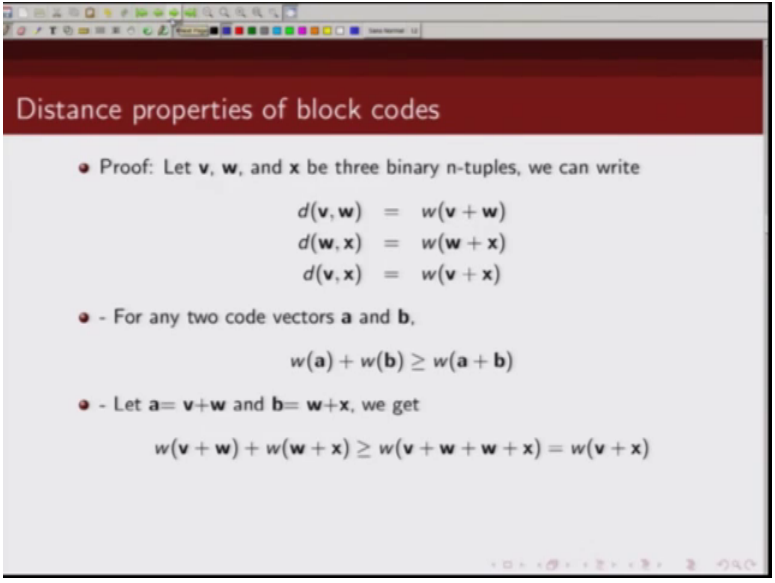
$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors **a** and **b**,

$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

2 code vectors a and b we know the weight of a plus the weight of b is going to be greater than or equal to weight of a plus v. Only when the 1's in a and b are non-overlapping this is going to be equal otherwise weight of a plus weight of b will be greater than weight of a plus b. Now let us

(Refer Slide Time 06:48)



Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors **a** and **b**,

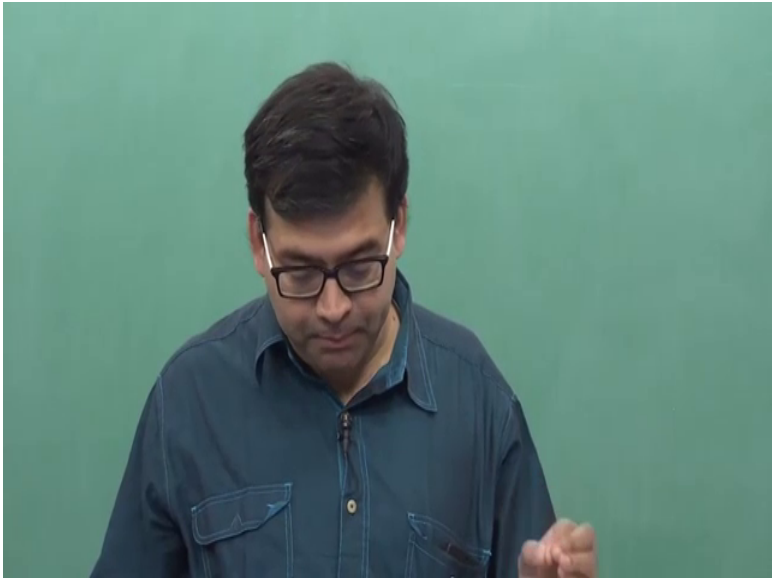
$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

- - Let **a**= **v**+**w** and **b**= **w**+**x**, we get

$$w(\mathbf{v}+\mathbf{w}) + w(\mathbf{w}+\mathbf{x}) \geq w(\mathbf{v}+\mathbf{w}+\mathbf{w}+\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

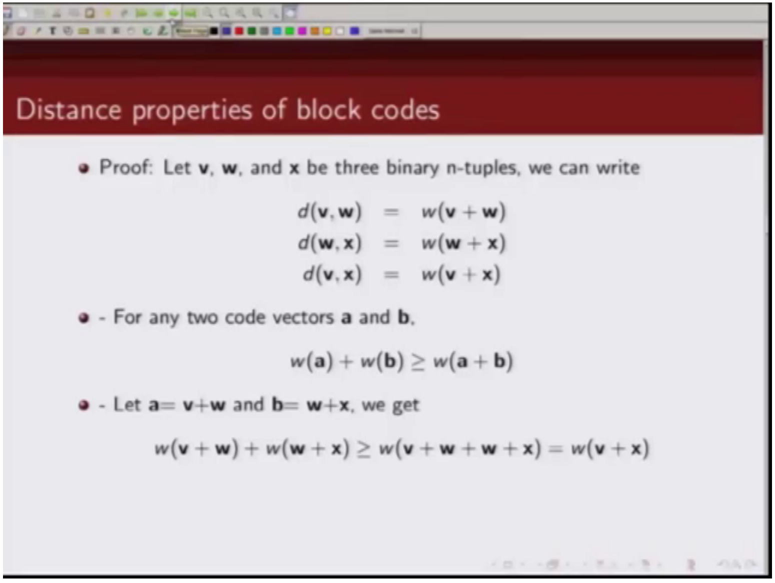
choose our a and

(Refer Slide Time 06:50)



b wisely. So let us choose a to be v plus w and

(Refer Slide Time 06:56)



Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors **a** and **b**,

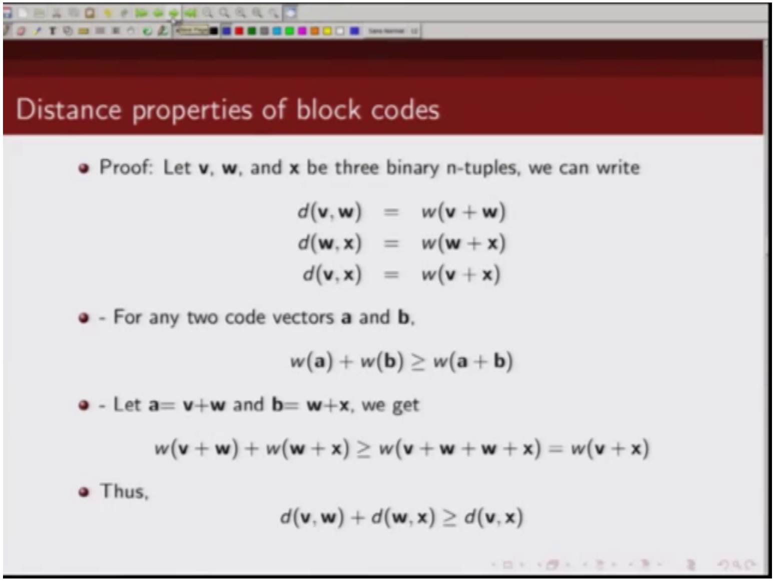
$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

- - Let **a**= **v**+**w** and **b**= **w**+**x**, we get

$$w(\mathbf{v}+\mathbf{w}) + w(\mathbf{w}+\mathbf{x}) \geq w(\mathbf{v}+\mathbf{w}+\mathbf{w}+\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

b to be w plus x. If we choose these values of a and b and put this in this inequality what we get is weight of v plus w plus weight of w plus x is greater than equal to weight of v plus w plus w plus x. w plus w is going to be 0, so this will be v plus x. This is given by weight of v plus x. So what we have shown is weight of v plus w plus weight of w plus x is greater than equal to Hamming weight of v plus x. And weight of v plus w is nothing but Hamming distance between v and w. So this we can replace by Hamming distance between v and w. This we can replace by Hamming distance between w and x. And this we can replace by Hamming distance between v and x. Hence we get

(Refer Slide Time 08:12)



Distance properties of block codes

- Proof: Let **v**, **w**, and **x** be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors **a** and **b**,

$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

- - Let **a**= **v**+**w** and **b**= **w**+**x**, we get

$$w(\mathbf{v}+\mathbf{w}) + w(\mathbf{w}+\mathbf{x}) \geq w(\mathbf{v}+\mathbf{w}+\mathbf{w}+\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

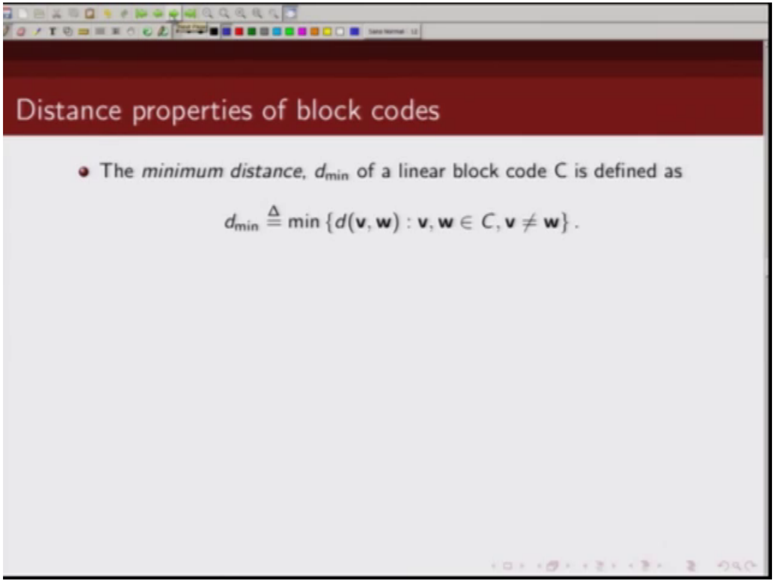
- Thus,

$$d(\mathbf{v},\mathbf{w}) + d(\mathbf{w},\mathbf{x}) \geq d(\mathbf{v},\mathbf{x})$$

the Hamming distance between v and w plus Hamming distance between w and x is greater than equal to Hamming distance between v and x.

Now let us define

(Refer Slide Time 08:26)



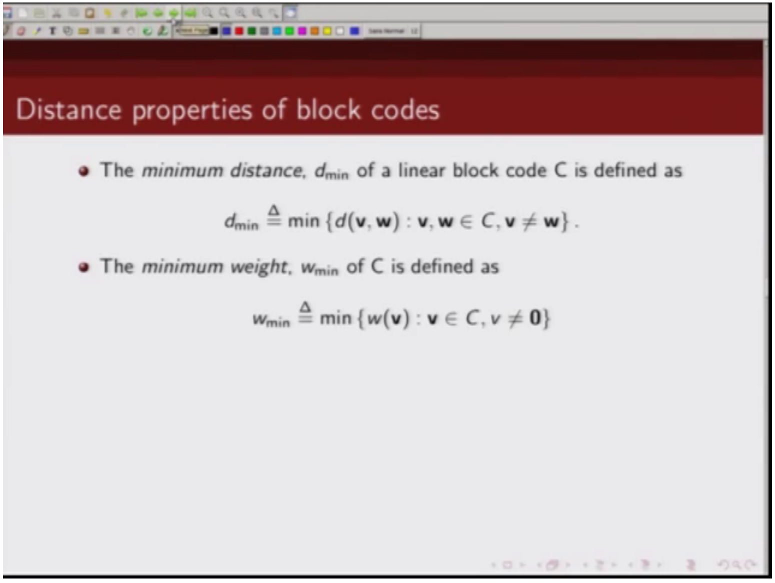
Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \triangleq \min \{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

by what do we mean by minimum distance of a linear block code. So we define a minimum distance of a linear block code in this fashion. It is the minimum Hamming distance between any 2 codewords so we define minimum distance of linear block code C as minimum Hamming distance between v and w where v and w are codewords and v is obviously not equal to w. Now this can be

(Refer Slide Time 09:05)



Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

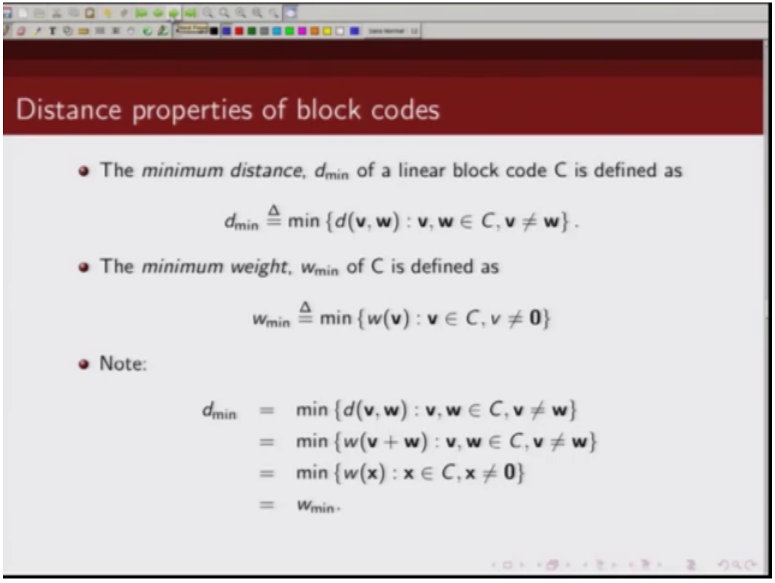
$$d_{\min} \triangleq \min \{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

$$w_{\min} \triangleq \min \{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\}$$

written as, we will come to that. Similarly we will define a minimum weight of a code. A minimum weight of a code is defined as minimum Hamming weight of code v, non zero codeword v belonging to this linear block code C. It's easy to

(Refer Slide Time 09:25)



Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \triangleq \min\left\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\right\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

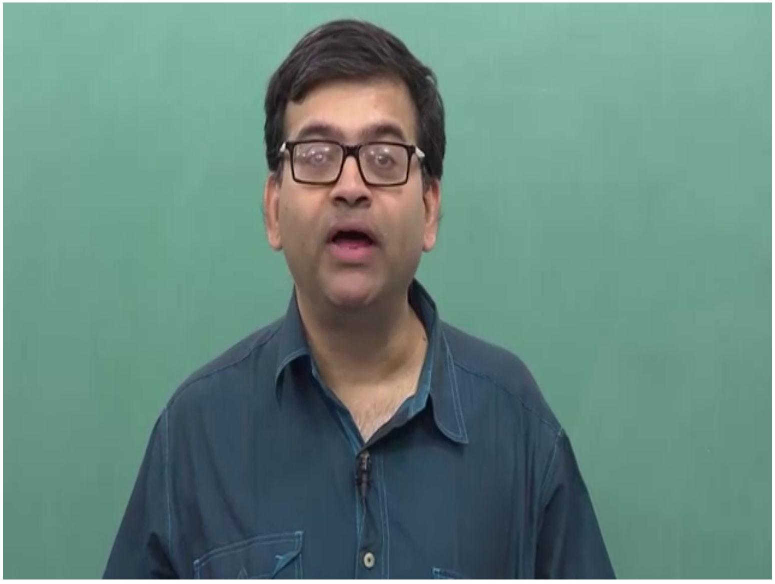
$$w_{\min} \triangleq \min\left\{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\right\}$$

- Note:

$$\begin{aligned} d_{\min} &= \min\left\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\right\} \\ &= \min\left\{w(\mathbf{v}+\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\right\} \\ &= \min\left\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\right\} \\ &= w_{\min}. \end{aligned}$$

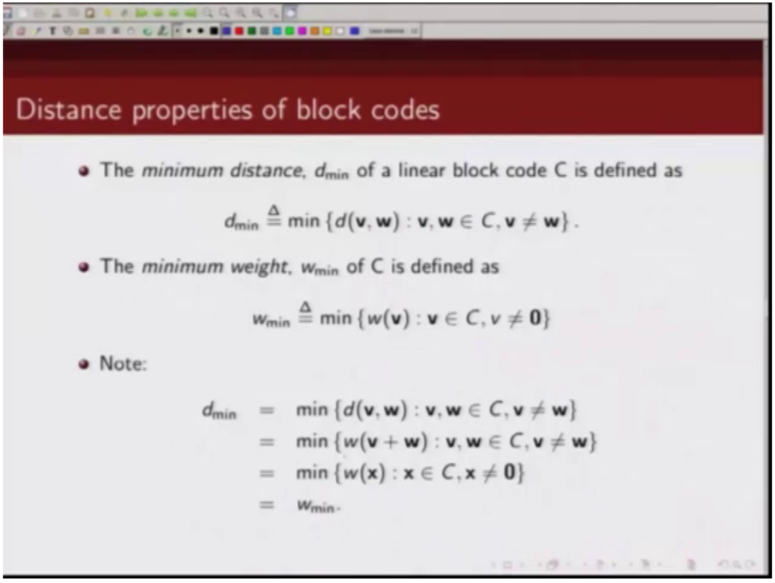
show that the minimum distance of a code is nothing but minimum weight codeword of a linear block code, minimum weight non zero codeword. So let's see how we can show this. So minimum distance of a code is defined as Hamming, minimum Hamming distance between any two 2 codewords v and w belonging to this linear block code C where v is not same as w. Now we know that Hamming distance between v and w

(Refer Slide Time 10:02)



can be written in terms of

(Refer Slide Time 10:04)



Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \triangleq \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

$$w_{\min} \triangleq \min\{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\}$$

- Note:

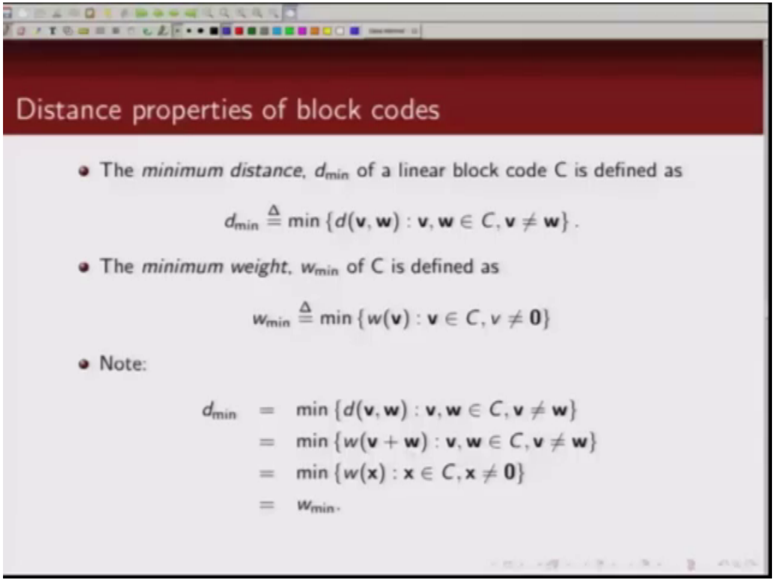
$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min\{w(\mathbf{v}+\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\} \\ &= w_{\min}. \end{aligned}$$

Hamming weight of v plus w. So this can be written as Hamming weight of v plus w. So we can write minimum distance as minimum Hamming weight of v plus w where v plus w are codewords belonging to this linear block code and v is not same as w. Now v plus w, now since we are talking about linear block codes,

(Refer Slide Time 10:35)

sum of 2 codewords is also a valid codeword. So v plus x,

(Refer Slide Time 10:42)



Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \triangleq \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

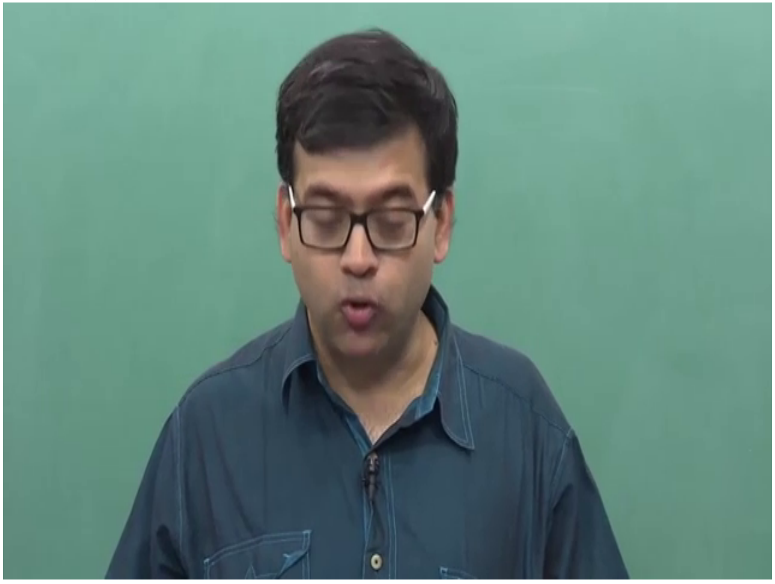
$$w_{\min} \triangleq \min\{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\}$$

- Note:

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min\{w(\mathbf{v}+\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\} \\ &= w_{\min}. \end{aligned}$$

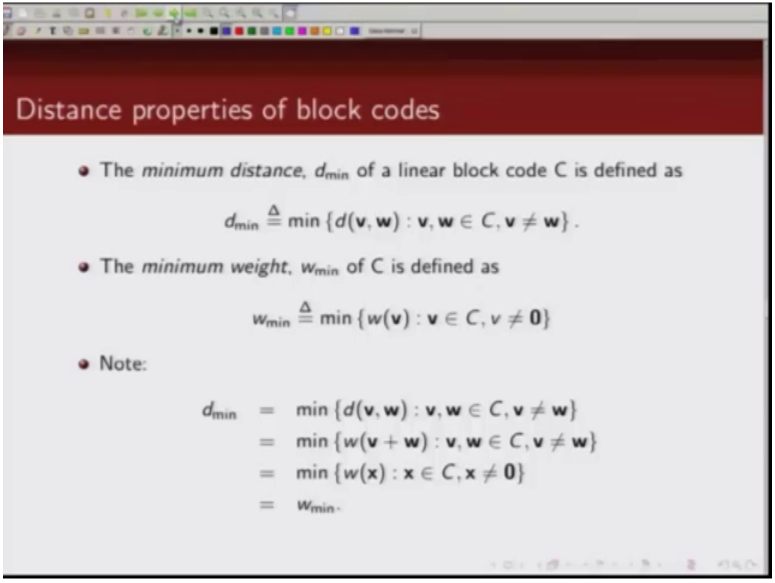
v plus w is going to be another valid codeword belonging to this linear block code C. So we can write this as minimum weight of a codeword x belonging to this linear block code where x is a non-zero codeword. So in other words, this is then nothing but minimum weight of linear block code C, so we can write then minimum distance of a linear block code to be equal to the minimum weight of a non-zero codeword

(Refer Slide Time 11:22)



belonging to C.

(Refer Slide Time 11:26)



Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \triangleq \min \{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

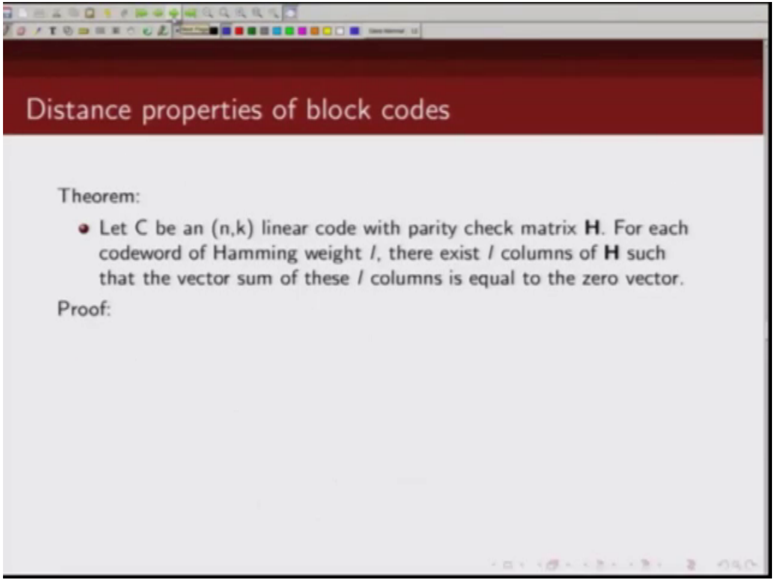
$$w_{\min} \triangleq \min \{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\}$$

- Note:

$$\begin{aligned} d_{\min} &= \min \{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min \{w(\mathbf{v} + \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min \{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\} \\ &= w_{\min}. \end{aligned}$$

Next we are

(Refer Slide Time 11:27)



Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight *l*, there exist *l* columns of **H** such that the vector sum of these *l* columns is equal to the zero vector.

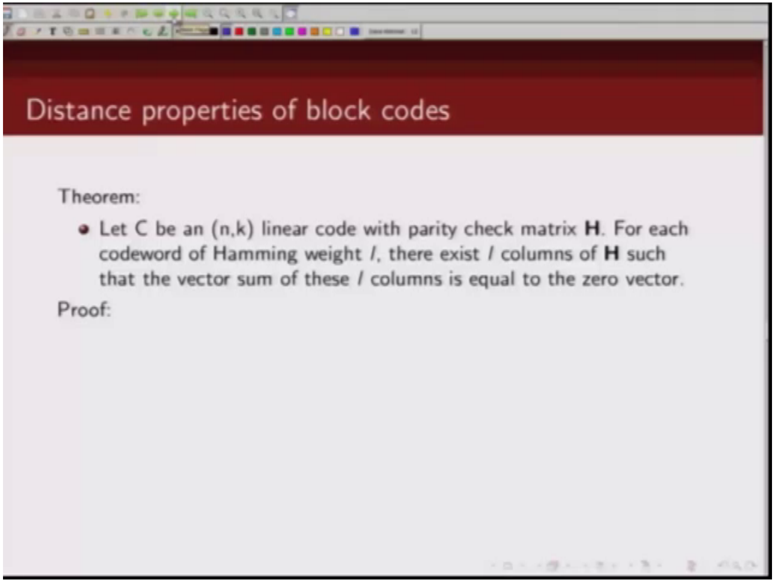
Proof:

going to show how is

(Refer Slide Time 11:31)

minimum distance of a linear block code related to columns of a parity check matrix and how from the columns we can find out what is the minimum distance of a linear block code.

(Refer Slide Time 11:48)



Distance properties of block codes

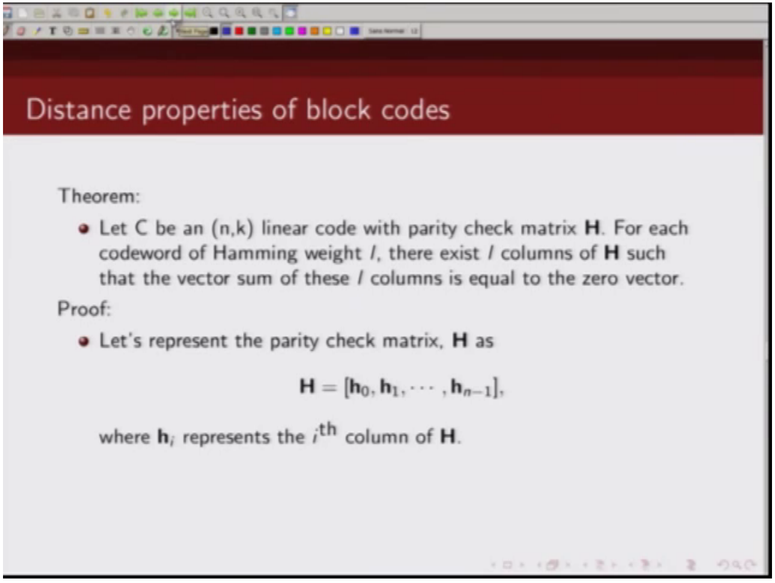
Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight *l*, there exist *l* columns of **H** such that the vector sum of these *l* columns is equal to the zero vector.

Proof:

So the result which I am going to show you is as follows. If C is an n k linear block code whose parity check matrix is given by H, so for each codeword of Hamming weight l there exist l columns of this parity check matrix H such that the vector sum of these columns is equal to zero vector. So let's prove this. Let's say

(Refer Slide Time 12:19)



Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight l, there exist l columns of **H** such that the vector sum of these l columns is equal to the zero vector.

Proof:

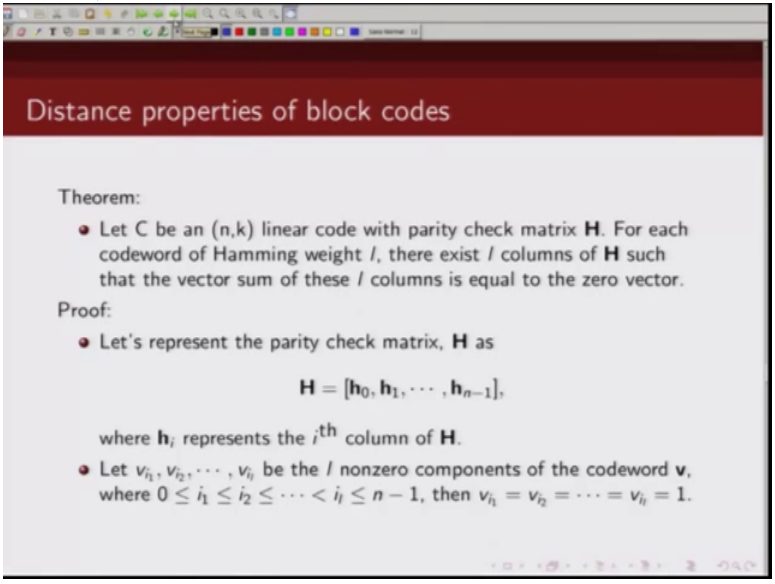
- Let's represent the parity check matrix, **H** as

$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}],$$

where $\mathbf{h}_i$ represents the i^{th} column of **H**.

we can write the parity check matrix in this form. Note this is n minus k cross n matrix so there are n columns which we are denoting by h 0, h 1, h 2 and h n minus 1 so h i represents the ith column of these parity check matrix. And we said that

(Refer Slide Time 12:41)



Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight l, there exist l columns of **H** such that the vector sum of these l columns is equal to the zero vector.

Proof:

- Let's represent the parity check matrix, **H** as

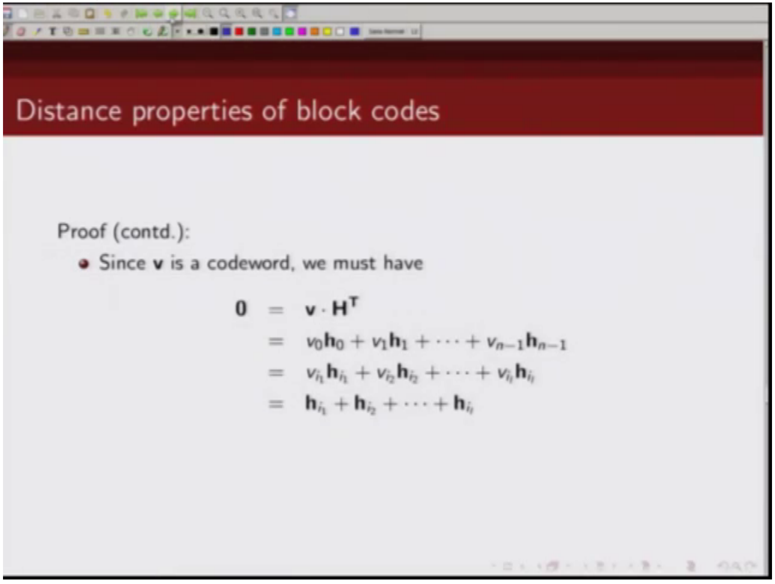
$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}],$$

where $\mathbf{h}_i$ represents the i^{th} column of **H**.

- Let $v_{i_1}, v_{i_2}, \cdots, v_{i_l}$ be the l nonzero components of the codeword $\mathbf{v}$, where $0 \le i_1 \le i_2 \le \cdots < i_l \le n-1$, then $v_{i_1} = v_{i_2} = \cdots = v_{i_l} = 1$.

for each codeword of Hamming weight l, so let us say that at this location i 1, i 2, i 3, i l these are the locations where the codeword basically has a non-zero weight. So the let the non-zero components of the codeword v be denoted by v i 1, v i 2, v i 3 and v i l where we just, without loss of generality we are just writing as i 1 is less than equal to i 2 is less than equal to i 3 is less than equal to i 3 is less than equal to i l is less than equal to n minus 1. And since these are the non-zero components of the codeword, at this location v will be 1, at other locations where are 0 components, the values of v at those locations will be 0.

(Refer Slide Time 13:44)



Distance properties of block codes

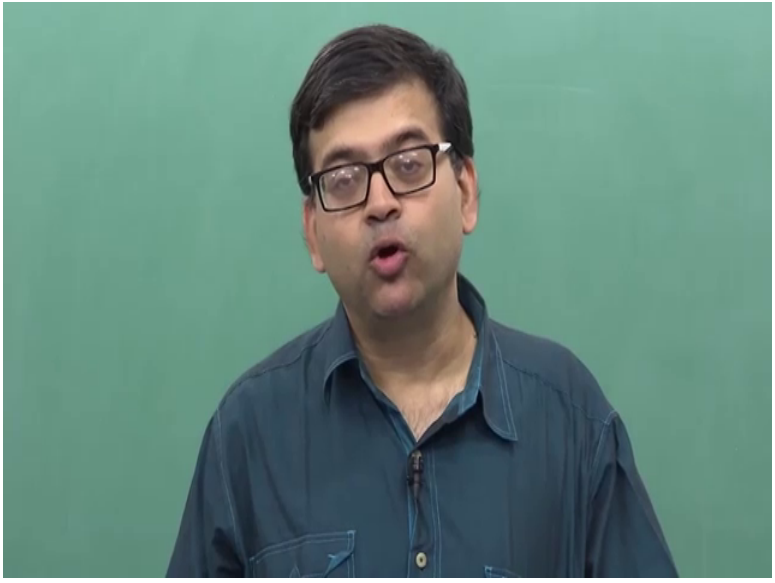
Proof (contd.):

- Since $\mathbf{v}$ is a codeword, we must have

$$\begin{aligned} \mathbf{0} &= \mathbf{v} \cdot \mathbf{H}^{\mathbf{T}} \\ &= v_0\mathbf{h}_0 + v_1\mathbf{h}_1 + \cdots + v_{n-1}\mathbf{h}_{n-1} \\ &= v_{i_1}\mathbf{h}_{i_1} + v_{i_2}\mathbf{h}_{i_2} + \cdots + v_{i_l}\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} \end{aligned}$$

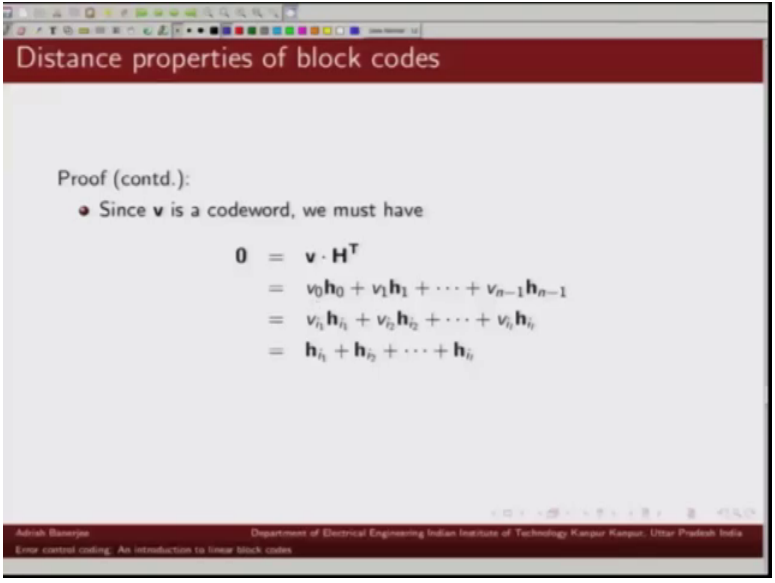
Now we know that if v is a valid codeword then v H transpose is equal to 0. So if v is a valid codeword then v H transpose is going to be 0. This we can write as v naught times h 0 plus v 1 times h 1 plus v 2 times h 2 plus plus plus v n minus 1 h n minus 1. Now note that among these, v 0, v 1, v 2 v n minus 1, there are l components which are

(Refer Slide Time 14:27)



non-zero. And what are those l components? v i 1, v i 2, v i 3 up to v i l so all other components of v will be 0. So here then

(Refer Slide Time 14:43)



Distance properties of block codes

Proof (contd.):

- Since **v** is a codeword, we must have

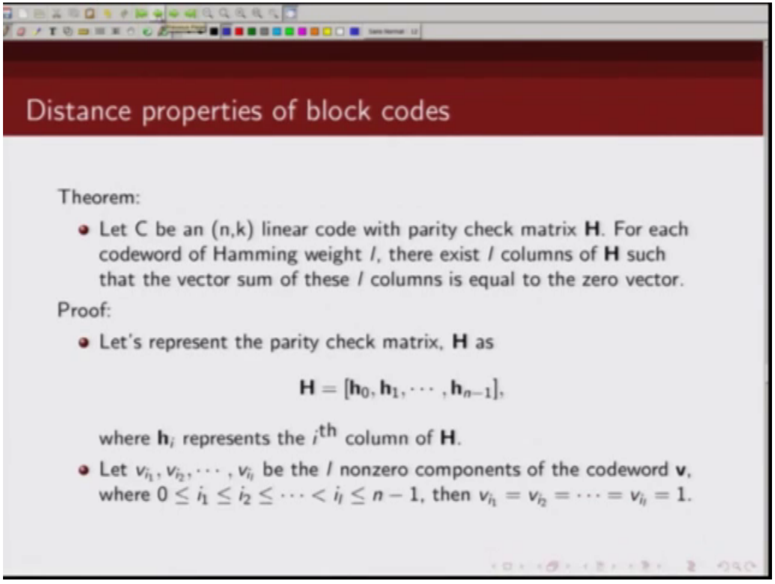
$$\begin{aligned} \mathbf{0} &= \mathbf{v} \cdot \mathbf{H}^T \\ &= v_0\mathbf{h}_0 + v_1\mathbf{h}_1 + \cdots + v_{n-1}\mathbf{h}_{n-1} \\ &= v_{i_1}\mathbf{h}_{i_1} + v_{i_2}\mathbf{h}_{i_2} + \cdots + v_{i_l}\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} \end{aligned}$$

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India

Error control coding: An introduction to linear block codes

only terms that will be left, we are left with is basically v i 1, h i 1 plus v i 2 h i 2 plus up to v i l h i l. Now since v i 1 v i 2 v i 3 v i l is 1 we can write this as h i 1 plus h i 2 plus h i 3 up to h i l is going to be 0 and what are these h i 1, h i 2, h i 3. These are columns of your parity check matrix H. So what does this say? It says that if we do vector sum of these l columns of parity check matrix then basically their vector sum is 0 and that's what the theorem

(Refer Slide Time 15:42)



Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight *l*, there exist *l* columns of **H** such that the vector sum of these *l* columns is equal to the zero vector.

Proof:

- Let's represent the parity check matrix, **H** as

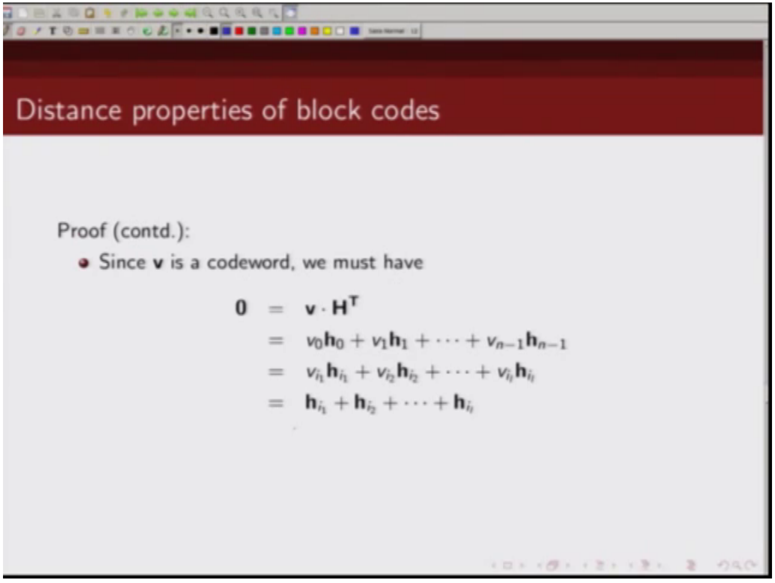
$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}],$$

where $\mathbf{h}_i$ represents the i^{th} column of **H**.

- Let $v_{i_1}, v_{i_2}, \cdots, v_{i_l}$ be the *l* nonzero components of the codeword **v**, where $0 \le i_1 \le i_2 \le \cdots < i_l \le n-1$, then $v_{i_1} = v_{i_2} = \cdots = v_{i_l} = 1$.

is about. That if there exists a codeword, for each codeword of Hamming weight l there exist l columns of parity check matrix whose vector sum is equal to l. So we showed that if l components of this codeword v are non zero then this relation follows.

(Refer Slide Time 16:06)



Distance properties of block codes

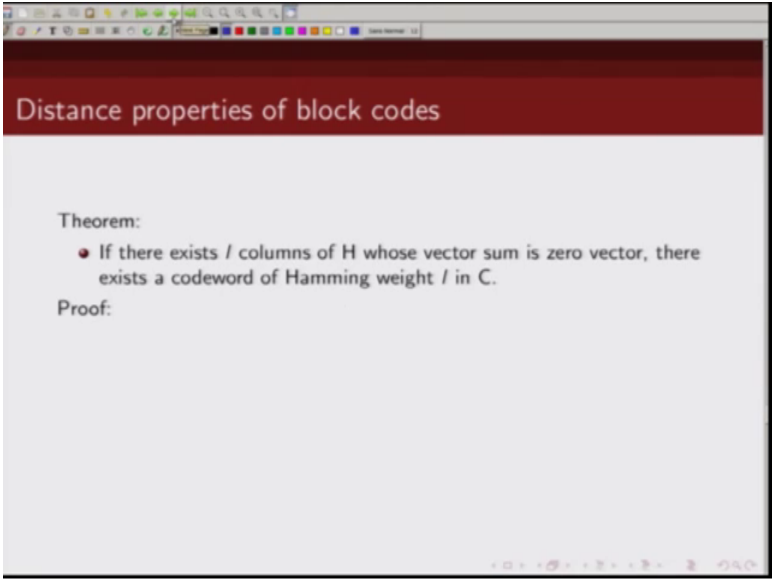
Proof (contd.):

- Since **v** is a codeword, we must have

$$\begin{aligned} \mathbf{0} &= \mathbf{v} \cdot \mathbf{H}^{\mathbf{T}} \\ &= v_0\mathbf{h}_0 + v_1\mathbf{h}_1 + \cdots + v_{n-1}\mathbf{h}_{n-1} \\ &= v_{i_1}\mathbf{h}_{i_1} + v_{i_2}\mathbf{h}_{i_2} + \cdots + v_{i_l}\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} \end{aligned}$$

Next

(Refer Slide Time 16:08)



Distance properties of block codes

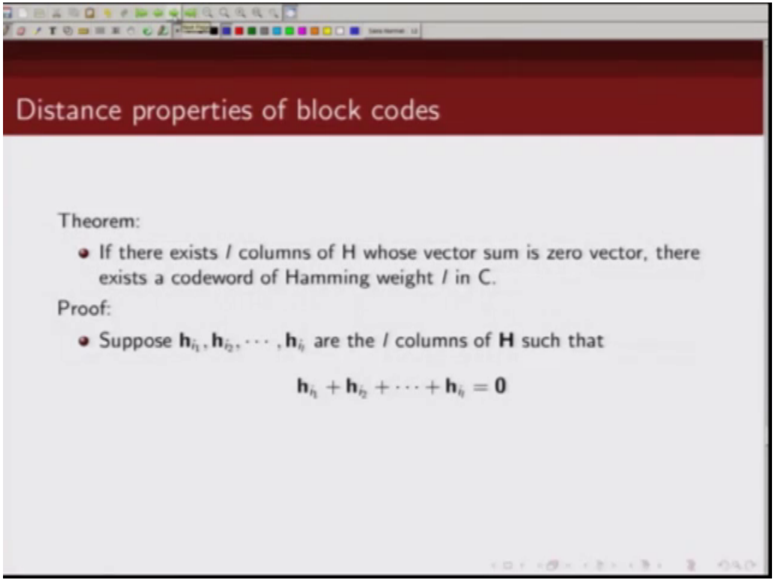
Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

we show another result which says of l columns of parity check matrix whose vector sum is 0 vector then there exists a codeword of Hamming weight l in this linear block code C. So let's see.

(Refer Slide Time 16:33)



Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

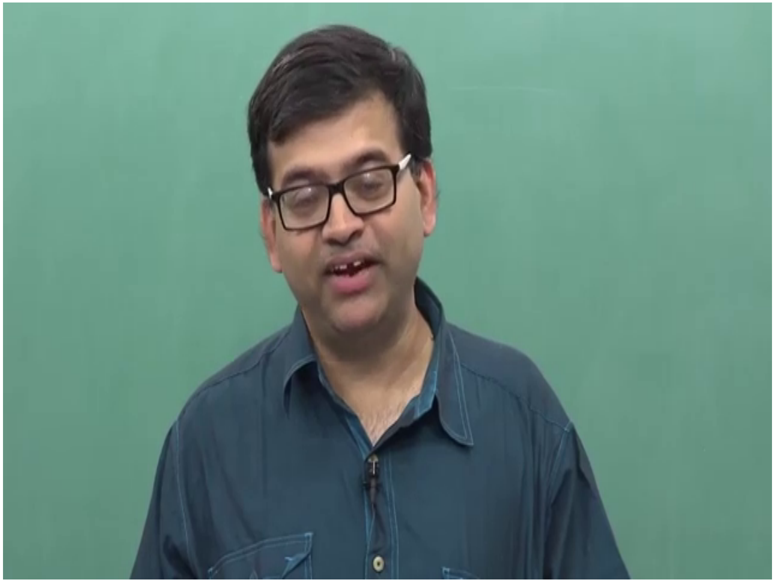
Proof:

- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

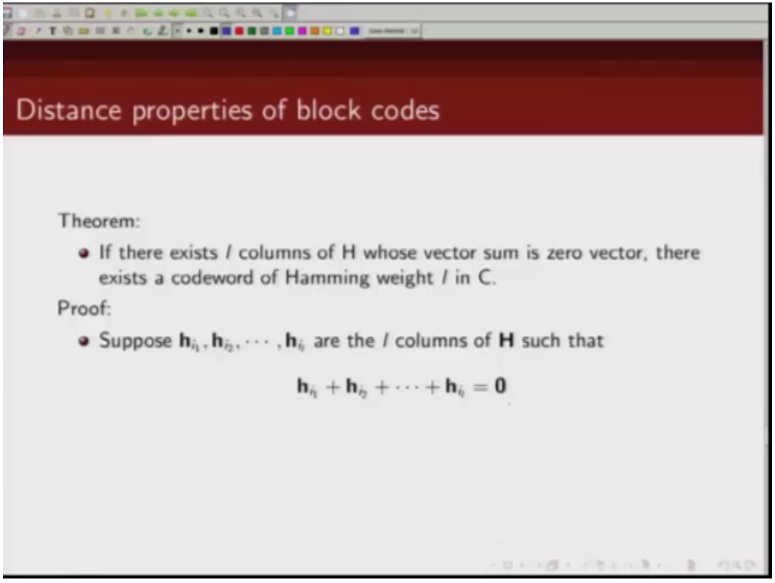
So suppose the l columns of parity check matrix H whose vector sum is zero are given by h i 1, h i 2, h i 3 up to h i l,

(Refer Slide Time 16:55)



then what we have is h i 1 plus h i 2 plus h i 3 up to h i l is going to 0.

(Refer Slide Time 17:01)



Distance properties of block codes

Theorem:

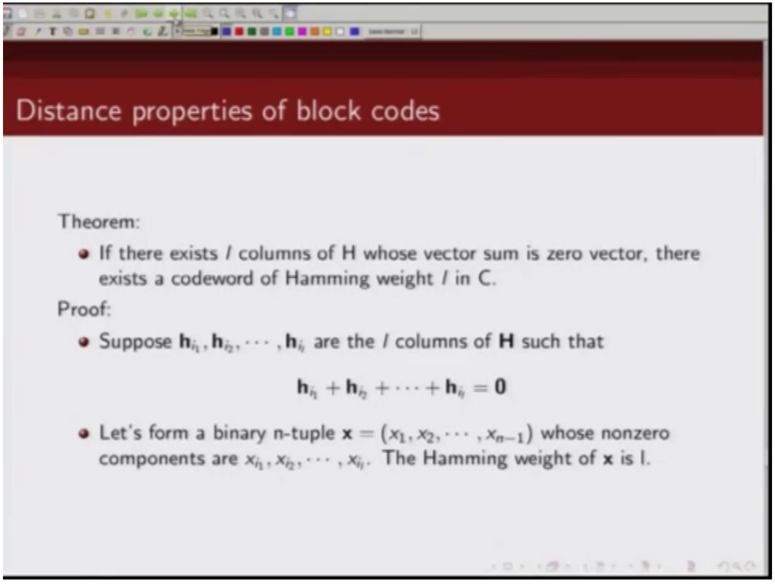
- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

(Refer Slide Time 17:02)



Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

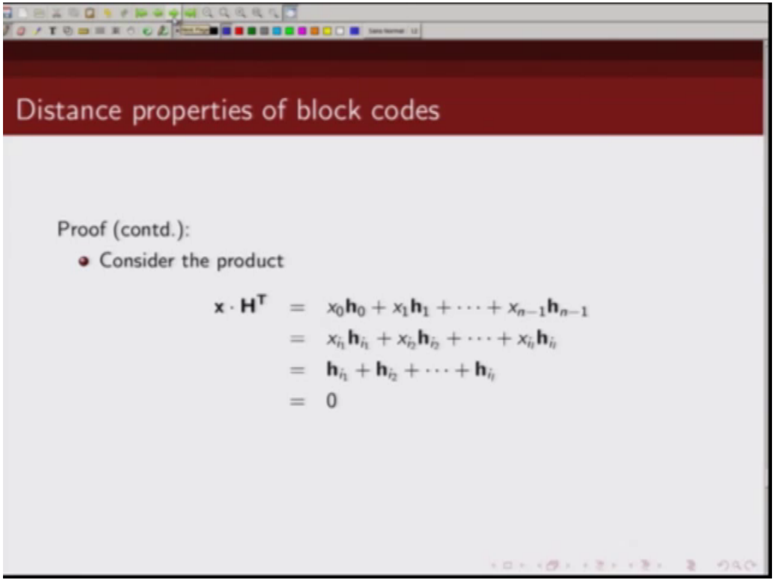
- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

- Let's form a binary n-tuple $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1})$ whose nonzero components are $x_{i_1}, x_{i_2}, \cdots, x_{i_l}$. The Hamming weight of $\mathbf{x}$ is l.

Now let us consider an n-tuple, we denote it by x whose non-zero components are given by x i 1, x i 2 up to x i l. In other words, at l locations this n-tuple is non zero so the Hamming weight of x is l. Now we want to show that if there exist l columns of these parity check matrix H whose vector sum is 0, then there exist a codeword whose Hamming weight is l. So next we are going to show that if this condition happens and if there is an n-tuple whose Hamming weight is l then this x has to be a codeword. So how do we show x is a codeword? Well if x is a codeword, x H transpose will be 0. So let us

(Refer Slide Time 18:09)



Distance properties of block codes

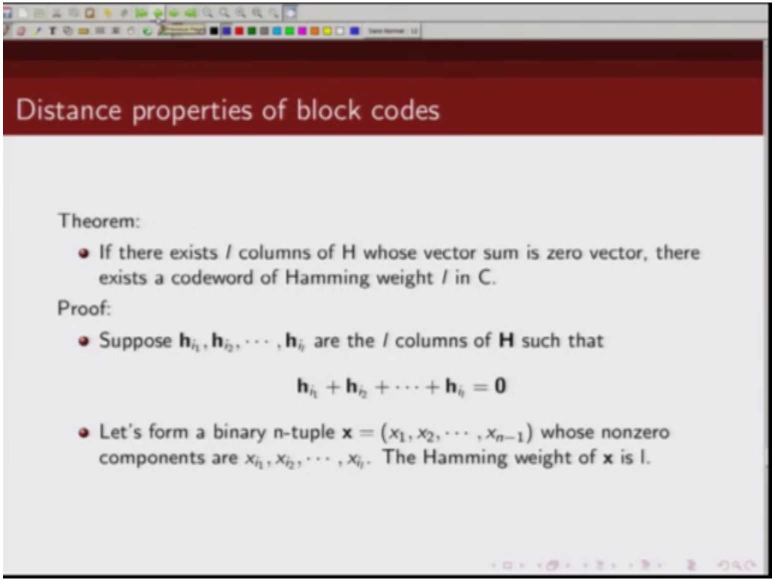
Proof (contd.):

- Consider the product

$$\begin{aligned}\mathbf{x}\cdot\mathbf{H}^T &= x_0\mathbf{h}_0 + x_1\mathbf{h}_1 + \cdots + x_{n-1}\mathbf{h}_{n-1}\\ &= x_{i_1}\mathbf{h}_{i_1} + x_{i_2}\mathbf{h}_{i_2} + \cdots + x_{i_l}\mathbf{h}_{i_l}\\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l}\\ &= 0\end{aligned}$$

evaluate x H transpose. So what is x H transpose? It's given by x 0 h 0 plus x 1 h 1 plus x 2 h 2 plus up to x n minus 1 h n minus 1. Now since we know that l elements of these n-tuple x are non-zero and they are given by x i 1, x i 2, x i 3, x i n l so we can write this as x i 1 h i 1 plus x i 2 h i 2 up to x i l h i l. Now since x i 1, x i 2, x i 3, x i l they are all 1, we can write this as h i 1 plus h i 2 plus h i 3 plus h i l. Now what did we say about vector sum of these l columns? We say

(Refer Slide Time 19:20)



Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

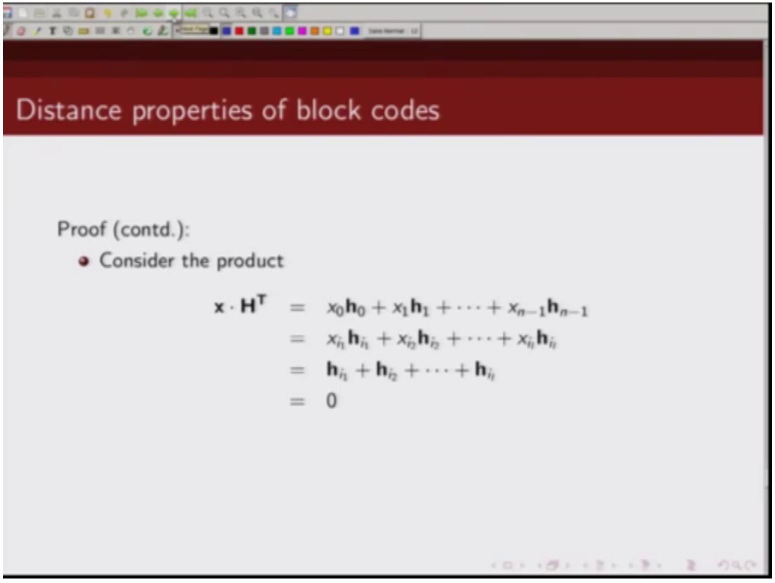
- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

- Let's form a binary n-tuple $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1})$ whose nonzero components are $x_{i_1}, x_{i_2}, \cdots, x_{i_l}$. The Hamming weight of $\mathbf{x}$ is l.

the vector sum of these l columns is 0. If that's the case, then this

(Refer Slide Time 19:26)



Distance properties of block codes

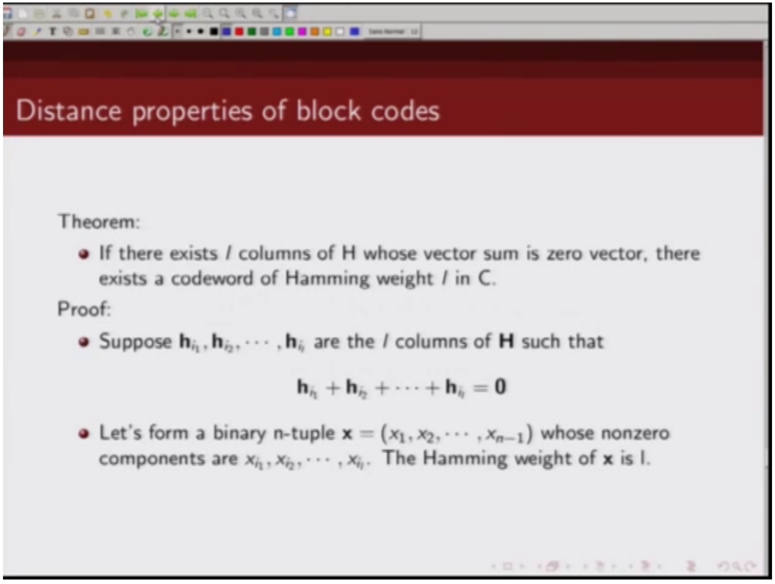
Proof (contd.):

- Consider the product

$$\begin{aligned}\mathbf{x} \cdot \mathbf{H}^{\mathbf{T}} &= x_0\mathbf{h}_0 + x_1\mathbf{h}_1 + \cdots + x_{n-1}\mathbf{h}_{n-1} \\ &= x_{i_1}\mathbf{h}_{i_1} + x_{i_2}\mathbf{h}_{i_2} + \cdots + x_{i_l}\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} \\ &= 0\end{aligned}$$

is equal to 0. So what we have shown now is x H transpose is 0. Now if x H transpose is 0, then x has to be a valid codeword. So we have shown that if

(Refer Slide Time 19:48)



Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

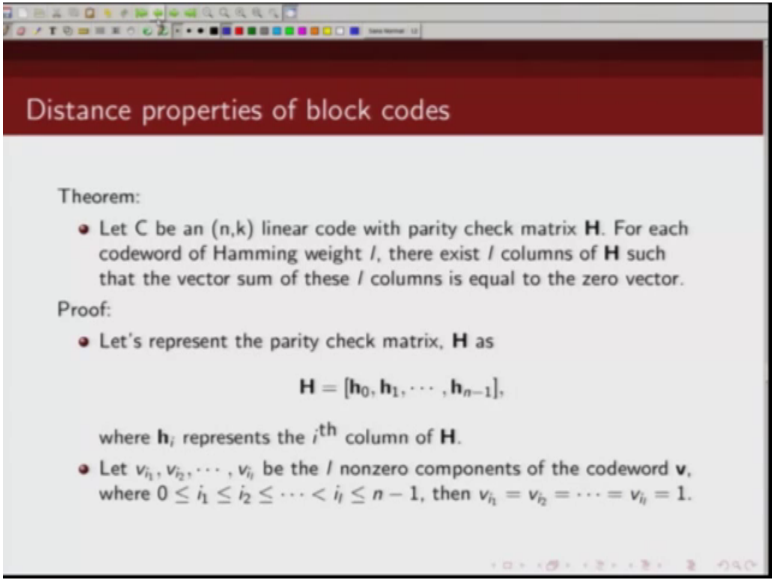
$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

- Let's form a binary n-tuple $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1})$ whose nonzero components are $x_{i_1}, x_{i_2}, \cdots, x_{i_l}$. The Hamming weight of $\mathbf{x}$ is l.

vector sum of l columns of parity check matrix H sum up to 0, then there exist a codeword of Hamming weight l.

Now using these 2 theorems, this theorem and

(Refer Slide Time 20:09)



Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight l, there exist l columns of **H** such that the vector sum of these l columns is equal to the zero vector.

Proof:

- Let's represent the parity check matrix, **H** as

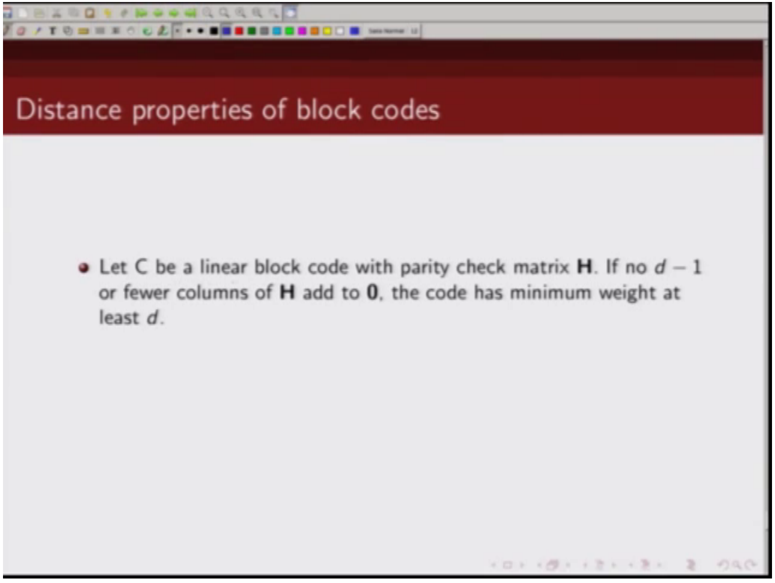
$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}],$$

where $\mathbf{h}_i$ represents the i^{th} column of **H**.

- Let $v_{i_1}, v_{i_2}, \cdots, v_{i_l}$ be the l nonzero components of the codeword **v**, where $0 \leq i_1 \leq i_2 \leq \cdots < i_l \leq n-1$, then $v_{i_1} = v_{i_2} = \cdots = v_{i_l} = 1$.

this theorem, we can make these following observations. If C is a linear

(Refer Slide Time 20:15)

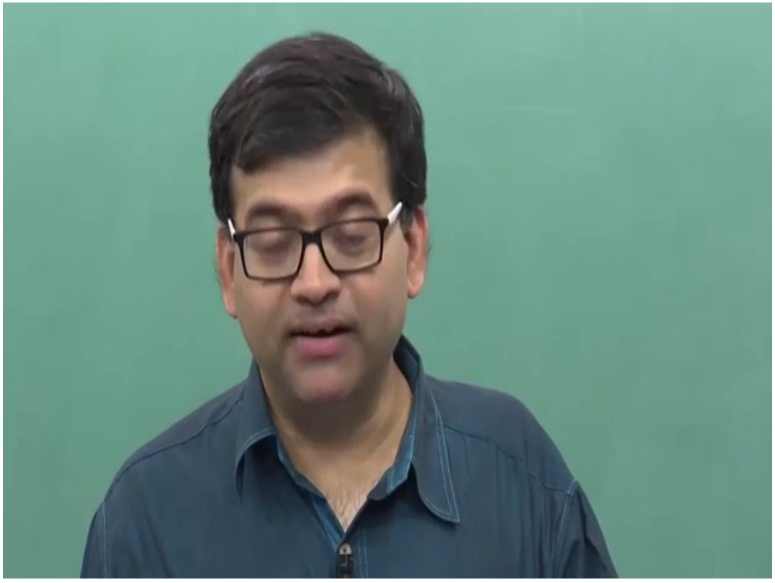


Distance properties of block codes

- Let C be a linear block code with parity check matrix **H**. If no $d-1$ or fewer columns of **H** add to **0**, the code has minimum weight at least d.

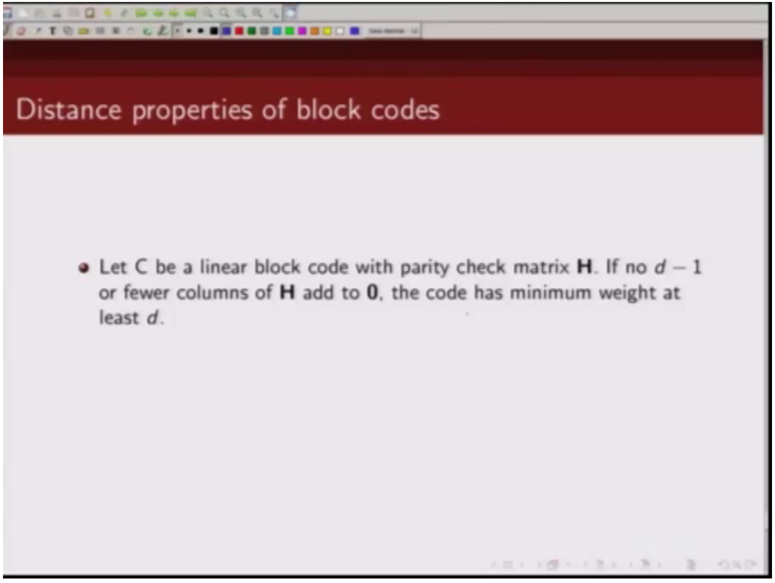
block code with parity check matrix given by H and if no d minus 1 or fewer columns of parity check matrix add up to 0, then the code has a minimum weight of at least d. So minimum distance of code is at least d if no d minus 1 columns of this H matrix, the vector sum of these d minus 1 columns or fewer columns of this H matrix, if they do not add up to 0, it means the

(Refer Slide Time 20:52)



linear block code has at least minimum distance of d.

(Refer Slide Time 20:57)

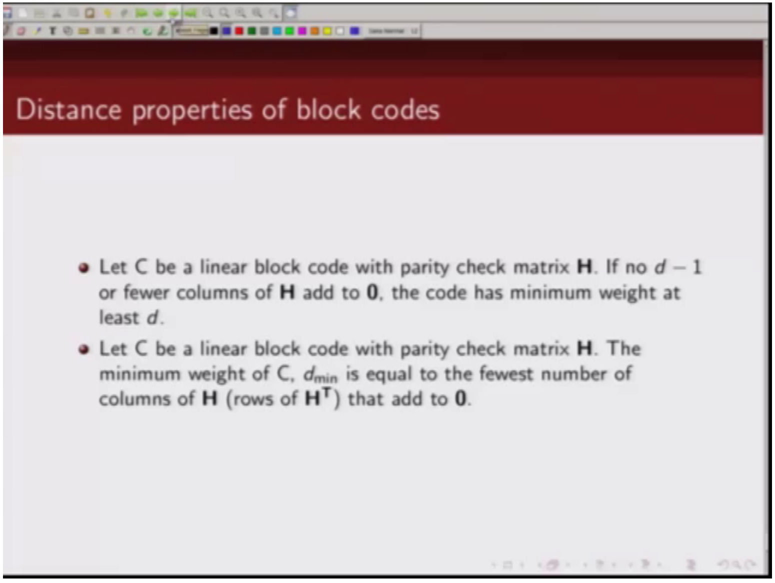


Distance properties of block codes

- Let C be a linear block code with parity check matrix **H**. If no $d-1$ or fewer columns of **H** add to **0**, the code has minimum weight at least d.

The second

(Refer Slide Time 20:59)



Distance properties of block codes

- Let C be a linear block code with parity check matrix $\mathbf{H}$. If no $d-1$ or fewer columns of $\mathbf{H}$ add to $\mathbf{0}$, the code has minimum weight at least d.
- Let C be a linear block code with parity check matrix $\mathbf{H}$. The minimum weight of C, $d_{\min}$ is equal to the fewest number of columns of $\mathbf{H}$ (rows of $\mathbf{H}^{\mathbf{T}}$) that add to $\mathbf{0}$.

statement we can make is if there is a linear block code C with parity check matrix H then minimum weight of this linear block code C d min is basically equal to the smallest number of columns of this H matrix whose vector sum add up to 0. Thank you.