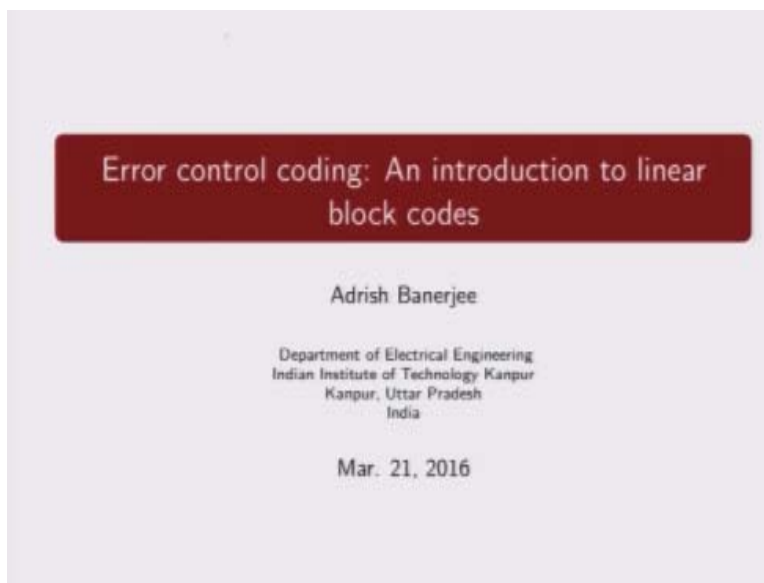


Indian Institute of Technology Kanpur
National Programme on Technology Enhanced Learning (NPTEL)
Course Title
Error Control Coding: An Introduction to Linear Block Codes

Lecture – 5A
Distance Properties of Linear Block Codes - I
by
Prof. Adrish Banerjee
Department of Electrical Engineering, IIT Kanpur

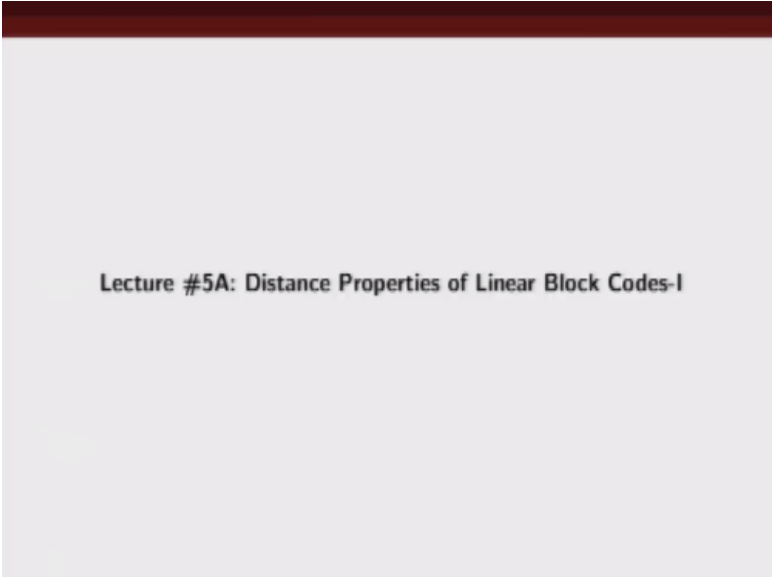
Welcome to the course on error control coding, an introduction to linear block codes.

(Refer Slide Time: 00:20)



As we know the error correcting and error detecting capability of error correcting codes depends on the distance profile of these codes so today we are going to talk and talk about.

(Refer Slide Time: 00:33)



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

The distance properties of linear block codes, we are going to describe what we mean by hamming distance of codes and then we are going to talk about how the minimum hamming distance of a code is related to the columns of a parity check matrix.

(Refer Slide Time: 00:530)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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 us call it \mathbf{v} so \mathbf{v} is an n – tuple and since we are restricting our discussion to binary linear block codes so we consider a binary n – tuple so this $v_0, v_1, v_2, \dots, v_{n-1}$ could be either zero or one, so we define the hamming weight of this vector \mathbf{v} as number of non zero components of \mathbf{v} .

(Refer Slide Time: 01:31)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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.

(Refer Slide Time: 01:33)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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} .
 $\mathbf{v} = (001011)$
- 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.

So for example let us say \mathbf{v} is 001011 let us say this is my \mathbf{v} , so we can see here how many non zero components we have one, two, three. So the hamming weight of \mathbf{v} is in this example three.

(Refer Slide Time: 01:59)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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} .
 $\mathbf{v} = (001011)$
- 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.

Now let \mathbf{v} and \mathbf{w} are two n – tuples so we define the hamming distance between \mathbf{v} and \mathbf{w} which is denoted by $d(\mathbf{v}, \mathbf{w})$ as the number of places where \mathbf{v} and \mathbf{w} are differing.

(Refer Slide Time: 02:19)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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.

So for example if \mathbf{v} is given by this 1001011 and \mathbf{w} is given by 0100011 then what is the hamming distance? Let us look at the first location this is one and this is zero so they are differing in the first location so that is one, similarly the second location this is zero, this is one so they are differing so now its hamming weight is hamming distance two 00.

Both are same the third bit location, fourth bit location this is one and this is zero so they are differing so hamming distance is now three 00 they are same, this bit location both the \mathbf{v} and \mathbf{w} are one, similarly in this location \mathbf{v} and \mathbf{w} are same, so that means our hamming distance between \mathbf{v} and \mathbf{w} is three and these are the three locations where they are differing, one is this.

(Refer Slide Time: 03:31)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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 $\mathbf{v} = (\underline{1} \underline{0} \underline{0} \underline{1} 0 1 1)$ and $\mathbf{w} = (0 1 0 0 0 1 1)$ is 3.

First bit location, second bit location and this fourth bit location, so the hamming distance between \mathbf{v} and \mathbf{w} in this example is three.

(Refer Slide Time: 03:42)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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

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

Now if \mathbf{v} , \mathbf{w} , \mathbf{x} are three binary n – tuples then the hamming distance between \mathbf{v} and \mathbf{w} hamming distance between \mathbf{w} and \mathbf{x} and hamming distance between \mathbf{v} and \mathbf{x} satisfies this inequality which is known as triangle inequality, so what is triangle inequality? The hamming distance between \mathbf{v} and \mathbf{w} plus the hamming distance between \mathbf{w} and \mathbf{x} is greater than equal to hamming distance between \mathbf{v} and \mathbf{x} .

(Refer Slide Time: 04:18)

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ 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

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

(Refer Slide Time: 04:23)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n -tuples, we can write
$$\begin{aligned}d(\mathbf{v}, \mathbf{w}) &= w(\mathbf{v} + \mathbf{w}) \\d(\mathbf{w}, \mathbf{x}) &= w(\mathbf{w} + \mathbf{x}) \\d(\mathbf{v}, \mathbf{x}) &= w(\mathbf{v} + \mathbf{x})\end{aligned}$$

So let us first try to prove this triangular inequality, so let \mathbf{v} , \mathbf{w} and \mathbf{x} are three binary n – tuples so the hamming distance between \mathbf{v} and \mathbf{w} can be defined as hamming weight of $\mathbf{v} + \mathbf{w}$, note that we are talking about.

(Refer Slide Time: 04:48)

Distance properties of block codes

• Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n-tuples, we can write

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

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

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

Binary n – tuples right and what is hamming distance? Hamming distance is number of positions in which \mathbf{v} and \mathbf{w} are differing and since we are talking about binary n – tuples.

(Refer Slide Time: 05:03)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n-tuples, we can write

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

So the number of places where \mathbf{v} and \mathbf{w} are differing can be found if we add \mathbf{v} and \mathbf{w} this modulo two addition of \mathbf{v} and \mathbf{w} and we find out the positions where the sum is one because only in those locations where these bits are differing.

(Refer Slide Time: 05:27)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n-tuples, we can write

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

$\mathbf{v} + \mathbf{w}$ will be one otherwise it will be zero because we know for binary modulo two additions.

(Refer Slide Time: 05:33)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n-tuples, we can write

$d(\mathbf{v}, \mathbf{w})$	$=$	$w(\mathbf{v} + \mathbf{w})$	$0+0=0$
$d(\mathbf{w}, \mathbf{x})$	$=$	$w(\mathbf{w} + \mathbf{x})$	$1+1=0$
$d(\mathbf{v}, \mathbf{x})$	$=$	$w(\mathbf{v} + \mathbf{x})$	$0+1=1$
			$1+0=1$

0+0 is going to 0, 1+1 is going to be 0 only when they are differing, 0+1 in this case it is going to be 1 and if this is 1 and this is 0 in this case also this hamming weight is going to be 1. So we can write down the hamming distance between \mathbf{v} and \mathbf{w} as the hamming weight between $\mathbf{v} + \mathbf{w}$. Similarly we can write the hamming distance between \mathbf{w} and \mathbf{x} as the weight of this vector $\mathbf{w} + \mathbf{x}$ and we can define the hamming distance between \mathbf{v} and \mathbf{x} as the weight of $\mathbf{v} + \mathbf{x}$.

(Refer Slide Time: 06:26)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n -tuples, we can write
$$d(\mathbf{v}, \mathbf{w}) = w(\mathbf{v} + \mathbf{w})$$
$$d(\mathbf{w}, \mathbf{x}) = w(\mathbf{w} + \mathbf{x})$$
$$d(\mathbf{v}, \mathbf{x}) = w(\mathbf{v} + \mathbf{x})$$
- - For any two code vectors \mathbf{a} and \mathbf{b} ,
$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a} + \mathbf{b})$$

So if we have two code vectors \mathbf{a} and \mathbf{b} we know the weight of ' \mathbf{a} ' plus weight of ' \mathbf{b} ' is going to be greater than equal to weight of $\mathbf{a} + \mathbf{b}$. Only when the ones in \mathbf{a} and \mathbf{b} are non overlapping this is going to be equal, otherwise weight of ' \mathbf{a} ' plus weight of ' \mathbf{b} ' will be greater than weight of $\mathbf{a} + \mathbf{b}$.

(Refer Slide Time: 06:50)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{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 \mathbf{a} and \mathbf{b} ,
$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a} + \mathbf{b})$$
- - Let $\mathbf{a} = \mathbf{v} + \mathbf{w}$ and $\mathbf{b} = \mathbf{w} + \mathbf{x}$, we get
$$w(\mathbf{v} + \mathbf{w}) + w(\mathbf{w} + \mathbf{x}) \geq w(\mathbf{v} + \mathbf{w} + \mathbf{w} + \mathbf{x}) = w(\mathbf{v} + \mathbf{x})$$

Now let us choose our 'a' and 'b' wisely, so let us choose a to be $\mathbf{v} + \mathbf{w}$.

(Refer Slide Time: 06:58)

Distance properties of block codes

- Proof: Let \mathbf{v} , \mathbf{w} , and \mathbf{x} be three binary n -tuples, we can write

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

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

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

- - For any two code vectors \mathbf{a} and \mathbf{b} ,

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

- - Let $\mathbf{a} = \mathbf{v} + \mathbf{w}$ and $\mathbf{b} = \mathbf{w} + \mathbf{x}$, we get

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

And \mathbf{b} to be $\mathbf{w} + \mathbf{x}$, if we choose these values of \mathbf{a} and \mathbf{b} and put it in this inequality what we get is weight of $\mathbf{v} + \mathbf{w}$ + weight of $\mathbf{w} + \mathbf{x}$ is \geq than equal to weight of $\mathbf{v} + \mathbf{w} + \mathbf{w} + \mathbf{x}$. $\mathbf{w} + \mathbf{w}$ is going to be 0 so this will be $\mathbf{v} + \mathbf{x}$ this is going by weight of $\mathbf{v} + \mathbf{x}$ so what we have shown is weight of $\mathbf{v} + \mathbf{w}$ + weight of $\mathbf{w} + \mathbf{x}$ is \geq than equal to hamming weight of $\mathbf{v} + \mathbf{x}$ and weight of $\mathbf{v} + \mathbf{w}$ is nothing but hamming distance between \mathbf{v} and \mathbf{w} so this we can replace by hamming distance between \mathbf{v} and \mathbf{w} this we can replace by hamming distance between.

\mathbf{w} and \mathbf{x} and this we can replace by hamming distance between \mathbf{v} and \mathbf{x} , hence we get the hamming distance between \mathbf{v} and \mathbf{w} + hamming distance \mathbf{w} and \mathbf{x} if \geq than equal to hamming distance between \mathbf{v} and \mathbf{x} .

(Refer Slide Time: 08:28)

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

Now let us define 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 two code words. So we define minimum distance of a linear block code C as minimum hamming distance between \mathbf{v} and \mathbf{w} where \mathbf{v} and \mathbf{w} are code words and \mathbf{v} is obviously not equal to \mathbf{w} . Now this can be 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 \mathbf{v} , non 0 code word \mathbf{v} belonging to this linear block code C . It is easy to show that the minimum distance of a code is nothing but minimum weight code word of a linear block code minimum weight non 0 code word, so let us see how we can show this so minimum distance of a code is defined as hamming, minimum hamming distance between any two code words \mathbf{v} and \mathbf{w} belonging to this linear block code C where \mathbf{v} is not same as \mathbf{w} .

Now we know that hamming distance between \mathbf{v} and \mathbf{w} can be written in terms of hamming weight.

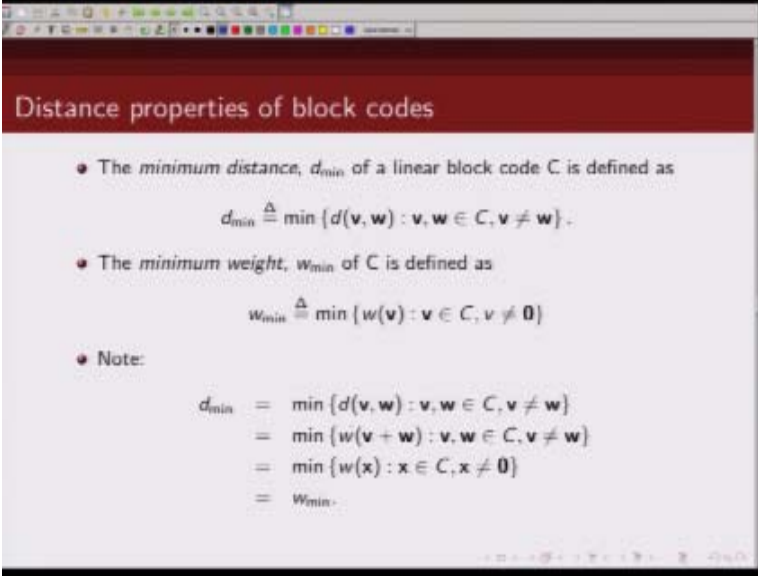
(Refer Slide Time: 10:08)

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

Of $\mathbf{v} + \mathbf{w}$ so this can be written as hamming weight of $\mathbf{v} + \mathbf{w}$ so we can write minimum distance as minimum hamming weight of $\mathbf{v} + \mathbf{w}$ where $\mathbf{v} + \mathbf{w}$ are code words belonging to this linear block code and \mathbf{v} is not same as \mathbf{w} . Now $\mathbf{v} + \mathbf{w}$, $\mathbf{v} +$ since we are talking about linear block codes sum of two code word is also a valid code word.

(Refer Slide Time: 10:45)

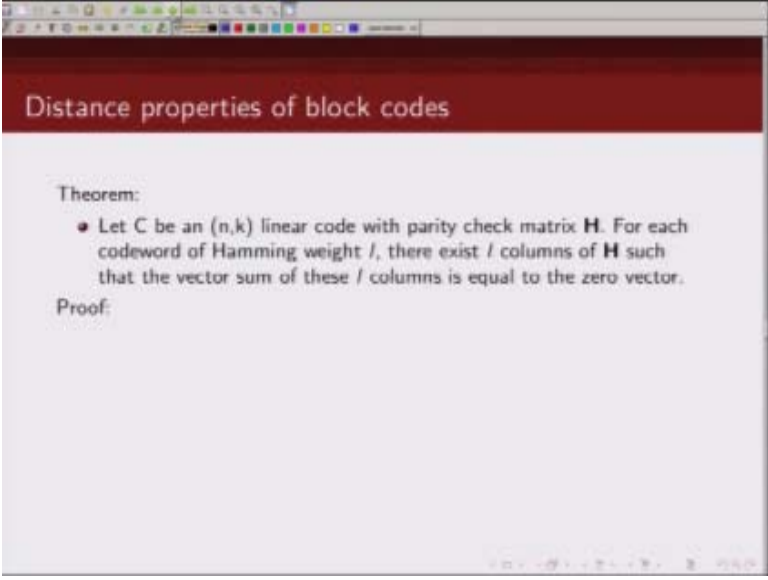


Distance properties of block codes

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

So $\mathbf{v} + \mathbf{x}$, $\mathbf{v} + \mathbf{w}$ is going to be another valid code word belonging to this linear block code C , so we can write this as minimum weight of a code word \mathbf{x} belonging to this linear block code where \mathbf{x} is a non 0 code word. So in another words this is there 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 0 code word belonging to C .

(Refer Slide Time: 11:29)



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:

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

(Refer Slide Time: 11:51)

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

$$H = [h_0, h_1, \dots, h_{n-1}],$$

where h_i represents the i^{th} column of H .

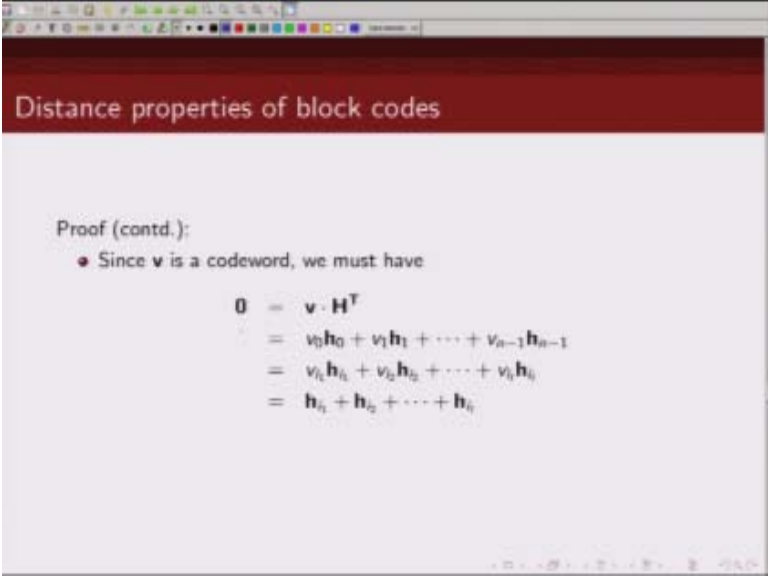
- Let $v_{i_1}, v_{i_2}, \dots, v_{i_l}$ be the l nonzero components of the codeword v , where $0 \leq i_1 \leq i_2 \leq \dots \leq i_l \leq n-1$, then $v_{i_1} = v_{i_2} = \dots = v_{i_l} = 1$.

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 code word of hamming weight L there exist L columns of this parity check matrix h such that the vectors some of these columns is equal to 0 vector. So let us prove this let us say we can write the parity check matrix in this form, note this is a $n - k$ cross n matrix so there are n columns which we are denoting by H_0, H_1, H_2 and h_{n-1} so h_i represent i column of these parity check matrix.

And we said that for each code word of hamming weight L so let us say that at these location I_1, I_2, I_3, I_L these are the locations where the code word is basically has a non zero weight so let the non zero components of this code word v we denoted by $v_{I_1}, v_{I_2}, v_{I_3}$ is and v_{I_L} where we just without laws of generative display I am just writing them as I_1 is less than equal to I_2 is less than equal to I_3 is less than equal to I_L is less than equal to $n - 1$, and since these are the non zero components of the code word .

So at this location we will be 1, at other locations where there are 0 components the values of v at those locations will be zero.

(Refer Slide Time: 13:46)



Distance properties of block codes

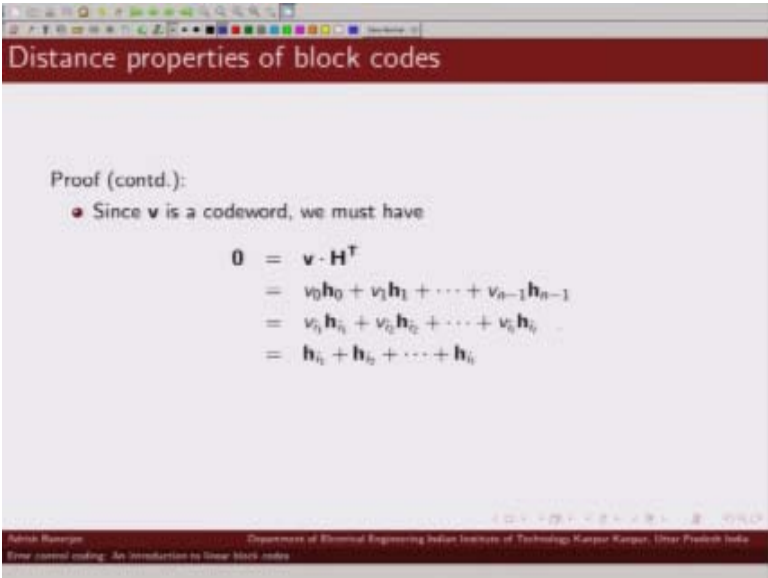
Proof (contd.):

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

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

Now we know that if \mathbf{v} is a valid code word and then \mathbf{vH}^T is equal to zero. So if \mathbf{v} is a valid code word then \mathbf{vH}^T is going to be zero. This we can write as.

(Refer Slide Time: 14:10)



Distance properties of block codes

Proof (contd.):

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

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

Aditya Rauten
Department of Electrical Engineering Indian Institute of Technology Kharagpur, Uttar Pradesh India
Error control coding: An introduction to linear block codes

$v_0h_0 + v_1h_1 + v_2h_2 + \dots + v_{n-1}h_{n-1}$. Now note that among these $v_0, v_1, v_2, \dots, v_{n-1}$, there are l components which are non zero and what are those l components v_{i1}, v_{i2}, v_{i3} upto v_{il} . So all other components of v will be zero.

(Refer Slide Time: 14:45)

Distance properties of block codes

Proof (contd.):

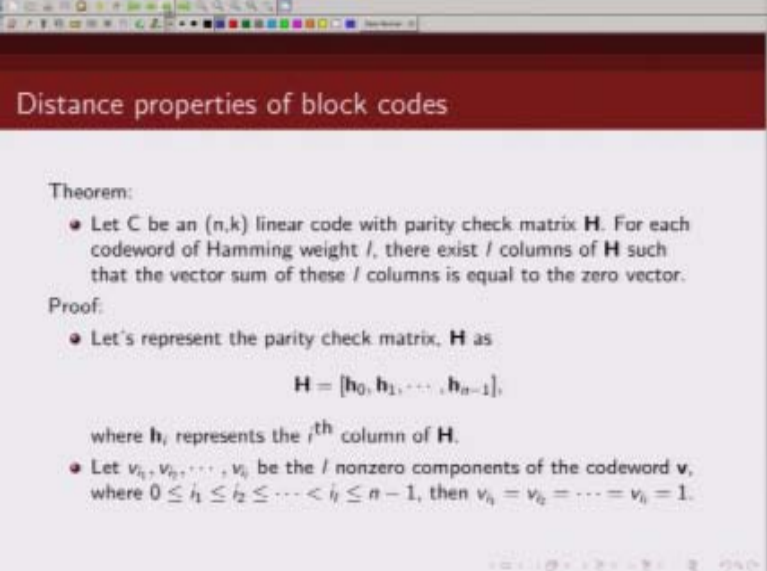
- Since v is a codeword, we must have

$$\begin{aligned}
 0 &= v \cdot H^T \\
 &= v_0h_0 + v_1h_1 + \dots + v_{n-1}h_{n-1} \\
 &= v_{i1}h_{i1} + v_{i2}h_{i2} + \dots + v_{il}h_{il} \\
 &= h_{i1} + h_{i2} + \dots + h_{il}
 \end{aligned}$$

Aditya Ranjan
Department of Electrical Engineering Indian Institute of Technology Kharagpur, West Bengal India
Error control coding: An introduction to linear block codes

So here then only terms that will be left we are left with is basically this $v_{i1}h_{i1} + v_{i2}h_{i2} + \dots + v_{il}h_{il}$. Now since $v_{i1}, v_{i2}, v_{i3}, \dots, v_{il}$ is one, we can write this as $h_{i1} + h_{i2} + h_{i3} + \dots + h_{il}$ is going to be zero. And what are these h_{i1}, h_{i2}, h_{i3} , 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 zero.

(Refer Slide Time: 15:44)



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

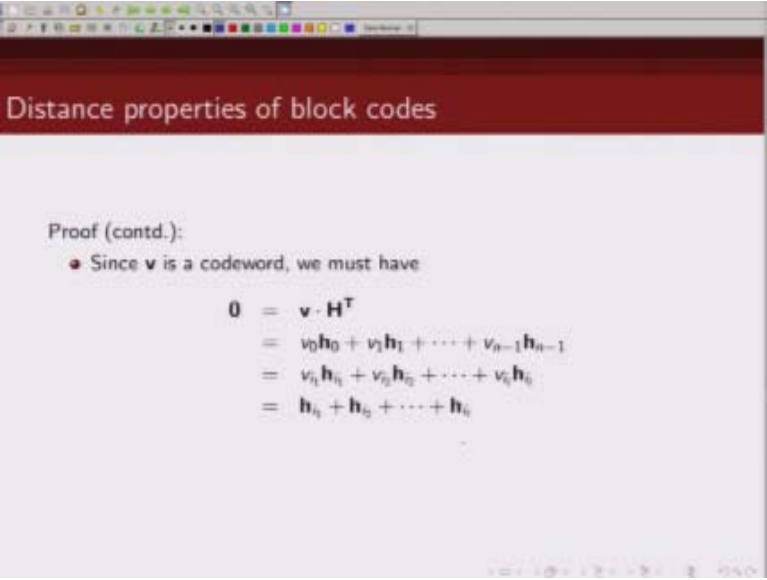
$$H = [h_0, h_1, \dots, h_{n-1}],$$

where h_i represents the i^{th} column of H .

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

And that is what the theorem is about that if there exists a code word for each code word of Hamming weight l , there exist l columns of parity check matrix whose vector sum is equal to 1. So we showed that if l components of these code word \mathbf{v} are non zero.

(Refer Slide Time: 16:09)



Distance properties of block codes

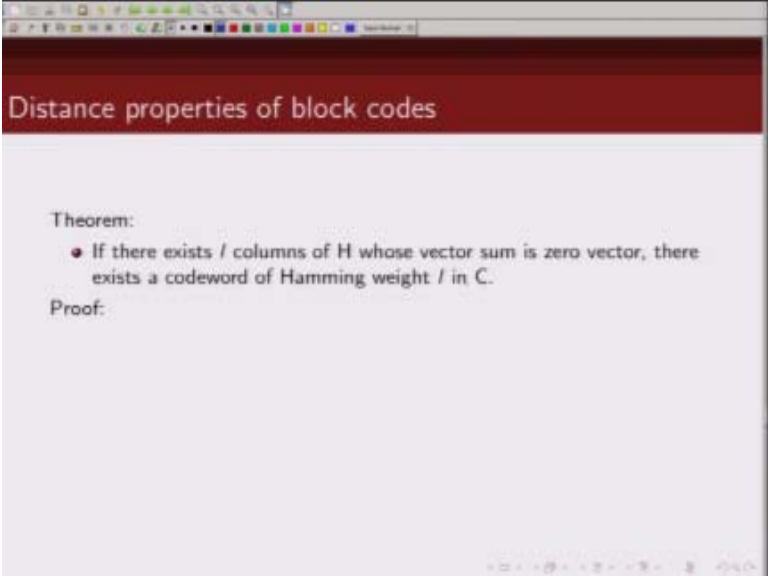
Proof (contd.):

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

$$\begin{aligned} \mathbf{0} &= \mathbf{v} \cdot H^T \\ &= v_0 h_0 + v_1 h_1 + \dots + v_{n-1} h_{n-1} \\ &= v_{i_1} h_{i_1} + v_{i_2} h_{i_2} + \dots + v_{i_l} h_{i_l} \\ &= h_{i_1} + h_{i_2} + \dots + h_{i_l} \end{aligned}$$

Then this relation follows.

(Refer Slide Time: 16:11)



Distance properties of block codes

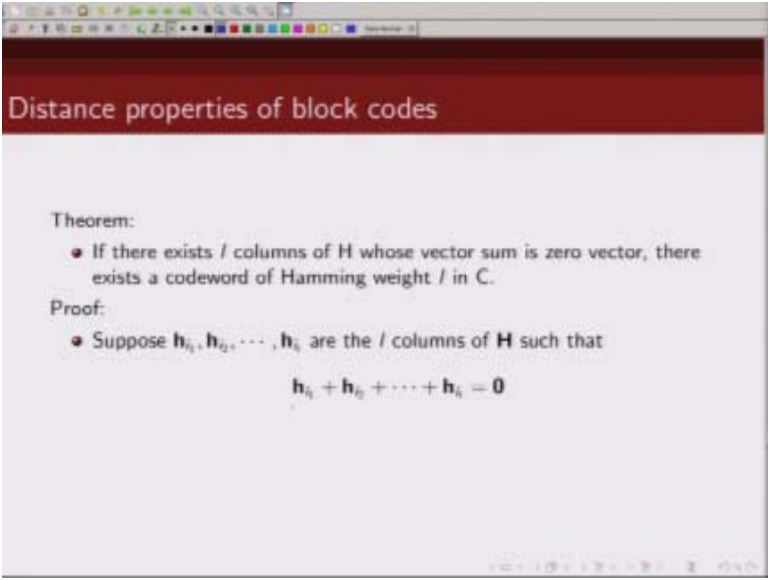
Theorem:

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

Proof:

Next we show another result which says if there exist l columns of parity check matrix whose vector sum is zero, vector then there exist a code word of hamming weight l in this linear block code C . So let us see.

(Refer Slide Time: 16:35)



Distance properties of block codes

Theorem:

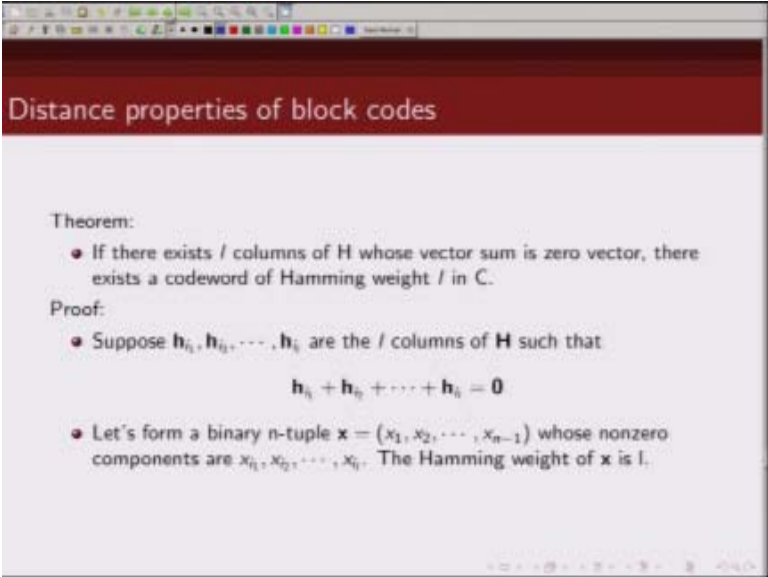
- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C .

Proof:

- Suppose $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_l$ are the l columns of H such that
$$\mathbf{h}_1 + \mathbf{h}_2 + \dots + \mathbf{h}_l = \mathbf{0}$$

So suppose these l columns of parity check matrix H whose vector sum is zero are given by h_{i1} h_{i2} h_{i3} upto h_{il} . Then what we have is $h_{i1}+h_{i2}+h_{i3}$ upto h_{il} is going to be zero.

(Refer Slide Time: 17:04)



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 $h_{i1}, h_{i2}, \dots, h_{il}$ are the l columns of H such that

$$h_{i1} + h_{i2} + \dots + h_{il} = 0$$
- Let's form a binary n -tuple $\mathbf{x} = (x_1, x_2, \dots, x_n)$ whose nonzero components are $x_{i1}, x_{i2}, \dots, x_{il}$. The Hamming weight of \mathbf{x} is l .

Now let us consider an n -tuple we denoted by \mathbf{x} whose non zero components are given by x_{i1} , x_{i2} upto x_{il} , In other word, at l locations this n -tuple is non zero so the hamming weight of \mathbf{x} is l . Now we want to show that if there exist l columns of these parity check matrix H whose vector sum is zero then there exist a code word 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 \mathbf{x} has to be a code word. So how do we show \mathbf{x} is a code word, well if \mathbf{x} is a code word $\mathbf{x} \cdot H^T$ will be zero.

(Refer Slide Time: 18:12)

Distance properties of block codes

Proof (contd.):

- Consider the product

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

So let us evaluate $\mathbf{x} \cdot \mathbf{H}^T$, so what is $\mathbf{x} \cdot \mathbf{H}^T$ it is given by $x_0 \mathbf{h}_0 + x_1 \mathbf{h}_1 + x_2 \mathbf{h}_2 + \dots + x_{n-1} \mathbf{h}_{n-1}$. Now since we know that l elements of these n -tuple \mathbf{x} are non zero and they are given by $x_{i_1} \ x_{i_2} \ x_{i_3} \dots x_{i_l}$ so then we can write this as $x_{i_1} \mathbf{h}_{i_1} + x_{i_2} \mathbf{h}_{i_2} + \dots + x_{i_l} \mathbf{h}_{i_l}$. Now since $x_{i_1} \ x_{i_2} \ x_{i_3} \dots x_{i_l}$ they are all one, we can write this as $\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \mathbf{h}_{i_3} + \dots + \mathbf{h}_{i_l}$. Now what did we say about vector sum of these l columns?

(Refer Slide Time: 19:22)

Distance properties of block codes

Theorem:

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

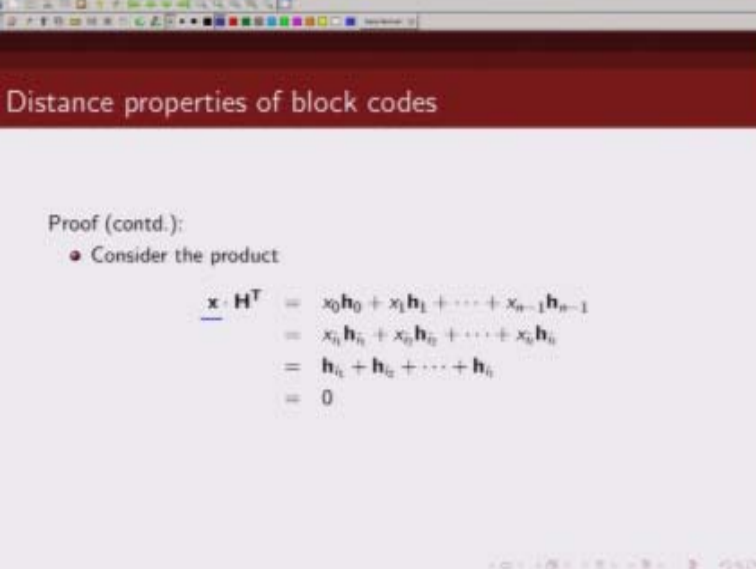
Proof:

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

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \dots + \mathbf{h}_{i_l} = \mathbf{0}$$
- Let's form a binary n -tuple $\mathbf{x} = (x_1, x_2, \dots, x_{n-1})$ whose nonzero components are $x_{i_1}, x_{i_2}, \dots, x_{i_l}$. The Hamming weight of \mathbf{x} is l .

We said the vector sum of these l columns is zero. If that is the case.

(Refer Slide Time: 19:29)



Distance properties of block codes

Proof (contd.):

- Consider the product

$$\begin{aligned}\underline{x} \cdot H^T &= x_0 h_0 + x_1 h_1 + \dots + x_{n-1} h_{n-1} \\ &= x_{i_1} h_{i_1} + x_{i_2} h_{i_2} + \dots + x_{i_r} h_{i_r} \\ &= h_{i_1} + h_{i_2} + \dots + h_{i_r} \\ &= 0\end{aligned}$$

Then this is equal to zero. So what we have shown now is $x \cdot H^T$ is zero. Now if $x \cdot H^T$ is zero then x has to be a valid code word. So we have shown that if

(Refer Slide Time: 19:50)

Distance properties of block codes

Theorem:

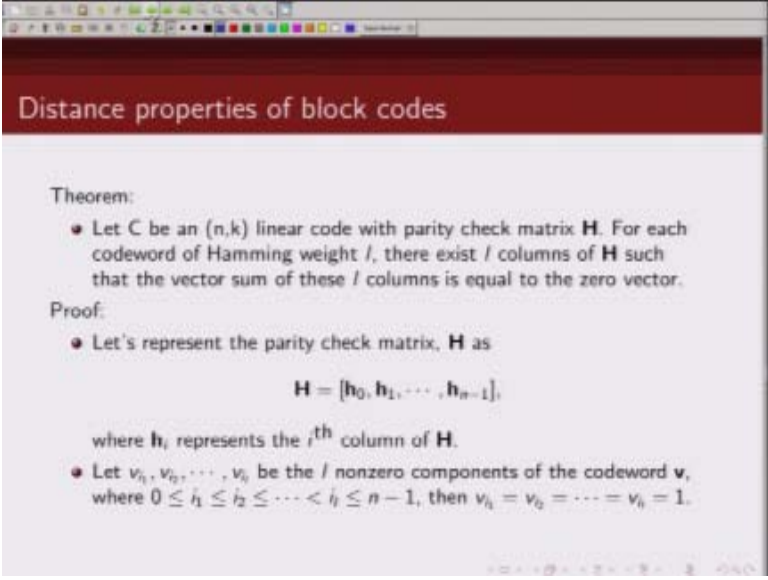
- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C .

Proof:

- Suppose $h_{i_1}, h_{i_2}, \dots, h_{i_l}$ are the l columns of H such that
$$h_{i_1} + h_{i_2} + \dots + h_{i_l} = \mathbf{0}$$
- Let's form a binary n -tuple $\mathbf{x} = (x_1, x_2, \dots, x_{n-1})$ whose nonzero components are $x_{i_1}, x_{i_2}, \dots, x_{i_l}$. The Hamming weight of \mathbf{x} is l .

Vector sum of l columns of parity check matrix H sum up to zero then there exist a code word of hamming weight l . Now using these two theorems this theorem.

(Refer Slide Time: 20:12)



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

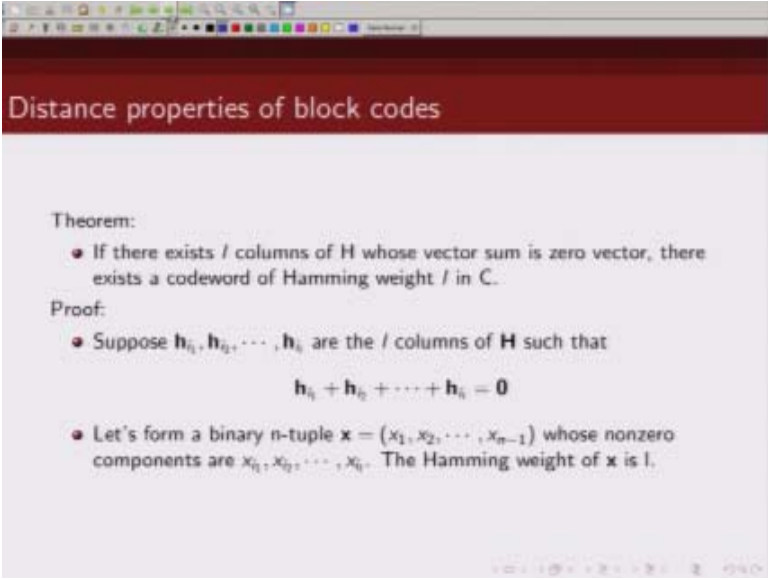
$$H = [h_0, h_1, \dots, h_{n-1}],$$

where h_i represents the i^{th} column of H .

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

And this theorem we can make.

(Refer Slide Time: 20:14)



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:

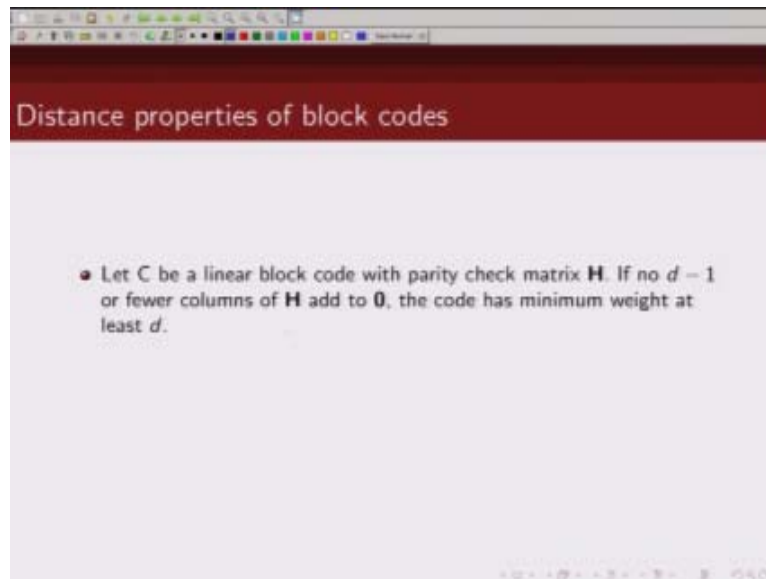
- Suppose $h_{i_1}, h_{i_2}, \dots, h_{i_l}$ are the l columns of H such that

$$h_{i_1} + h_{i_2} + \dots + h_{i_l} = \mathbf{0}$$

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

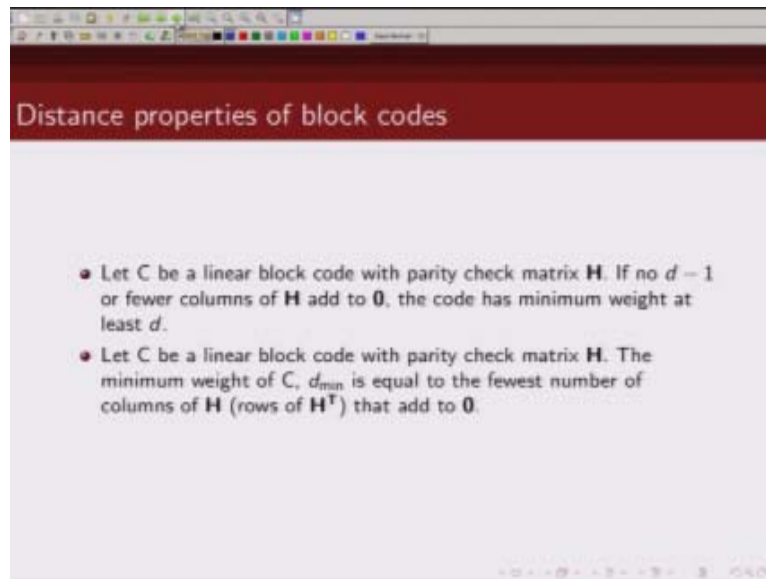
These following observations.

(Refer Slide Time: 20:17)



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

(Refer Slide Time: 21:00)



The second statement that we can make is if there is a linear block code C with parity check matrix H , then the minimum weight of this linear block code C d_{\min} is basically equal to the smallest number of columns of these H matrix whose vector sum add up to zero. Thank you.

Acknowledgement

Ministry of Human Resource & Development

Prof. Satyaki Roy

Co-ordinator, NPTEL IIT Kanpur

NPTEL Team

Sanjay Pal

Ashish Singh

Badal Pradhan

Tapabrata Das

Ram Chandra

Dilip Tripathi

Manoj Shrivastava

Padam Shukla

Sanjay Mishra

Shubham Rawat

Shikha Gupta

K. K. Mishra

Aradhana Singh

**Sweta
Ashutosh Gairola
Dilip Katiyar
Sharwan
Hari Ram
Bhadra Rao
Puneet Kumar Bajpai
Lalty Dutta
Ajay Kanaujia
Shivendra Kumar Tiwari**

an IIT Kanpur Production

©copyright reserved