An introduction to coding theory

Adrish Banerjee

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

Feb. 6, 2017

Lecture #6A: Some simple linear block codes -I

Outline of the lecture

- Dual code.

Outline of the lecture

- Dual code.
- Examples of linear block codes

Outline of the lecture

- Dual code.
- Examples of linear block codes
  - Repetition code

Outline of the lecture

- Dual code.
- Examples of linear block codes
  - Repetition code
  - Single parity check code

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to coding theory

Outline of the lecture

- Dual code.
- Examples of linear block codes
  - Repetition code
  - Single parity check code
  - Hamming code

Dual code

- Two n-tuples $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if their inner product $(\mathbf{u}, \mathbf{v})$ is zero, i.e.,

$$(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{n} (u_i \cdot v_i) = 0$$

Dual code

- Two n-tuples $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if their inner product $(\mathbf{u}, \mathbf{v})$ is zero, i.e.,

$$(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{n} (u_i \cdot v_i) = 0$$

- For a binary linear (n, k) block code C, the $(n, n-k)$ dual code, C_d is defined as set of all codewords, $\mathbf{v}$ that are orthogonal to all the codewords $\mathbf{u} \in C$.

Dual code

- Two n-tuples $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if their inner product $(\mathbf{u}, \mathbf{v})$ is zero, i.e.,

$$(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{n} (u_i \cdot v_i) = 0$$

- For a binary linear (n, k) block code C, the $(n, n-k)$ dual code, C_d is defined as set of all codewords, $\mathbf{v}$ that are orthogonal to all the codewords $\mathbf{u} \in C$.
- $(n, n-k)$ dual code, C_d is also a linear code.

Dual code

- Two n-tuples $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if their inner product $(\mathbf{u}, \mathbf{v})$ is zero, i.e.,

$$(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{n} (u_i \cdot v_i) = 0$$

- For a binary linear (n, k) block code C, the $(n, n-k)$ dual code, C_d is defined as set of all codewords, $\mathbf{v}$ that are orthogonal to all the codewords $\mathbf{u} \in C$.
- $(n, n-k)$ dual code, C_d is also a linear code.
- Proof: Let $\mathbf{x}, \mathbf{y} \in C_d$, then $\mathbf{x} \cdot \mathbf{u} = \mathbf{y} \cdot \mathbf{u} = 0$ for every $\mathbf{u} \in C$

Dual code

- Two n-tuples $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if their inner product $(\mathbf{u}, \mathbf{v})$ is zero, i.e.,

$$(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{n} (u_i \cdot v_i) = 0$$

- For a binary linear (n, k) block code C, the $(n, n-k)$ dual code, C_d is defined as set of all codewords, $\mathbf{v}$ that are orthogonal to all the codewords $\mathbf{u} \in C$.
- $(n, n-k)$ dual code, C_d is also a linear code.
- Proof: Let $\mathbf{x}, \mathbf{y} \in C_d$, then $\mathbf{x} \cdot \mathbf{u} = \mathbf{y} \cdot \mathbf{u} = 0$ for every $\mathbf{u} \in C$
- Thus,

$$(\lambda \mathbf{x} + \mu \mathbf{y}) \cdot \mathbf{u} = \lambda(\mathbf{x} \cdot \mathbf{u}) + \mu(\mathbf{y} \cdot \mathbf{u}) = 0$$

for every $\mathbf{u} \in C$

Dual code

- Two n-tuples $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if their inner product $(\mathbf{u}, \mathbf{v})$ is zero, i.e.,

$$(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{n} (u_i \cdot v_i) = 0$$

- For a binary linear (n, k) block code C, the $(n, n-k)$ dual code, C_d is defined as set of all codewords, $\mathbf{v}$ that are orthogonal to all the codewords $\mathbf{u} \in C$.
- $(n, n-k)$ dual code, C_d is also a linear code.
- Proof: Let $\mathbf{x}, \mathbf{y} \in C_d$, then $\mathbf{x} \cdot \mathbf{u} = \mathbf{y} \cdot \mathbf{u} = 0$ for every $\mathbf{u} \in C$
- Thus,

$$(\lambda \mathbf{x} + \mu \mathbf{y}) \cdot \mathbf{u} = \lambda(\mathbf{x} \cdot \mathbf{u}) + \mu(\mathbf{y} \cdot \mathbf{u}) = 0$$

  for every $\mathbf{u} \in C$
- This implies $\lambda \mathbf{x} + \mu \mathbf{y} \in C_d$

Dual code

- Let C be a linear code with generator matrix $\mathbf{G}$. Then $\mathbf{x} \in C_d$ if and only if $\mathbf{x}\mathbf{G}^T = 0$

Dual code

- Let C be a linear code with generator matrix $\mathbf{G}$. Then $\mathbf{x} \in C_d$ if and only if $\mathbf{x}\mathbf{G}^T = 0$
- Let $\mathbf{G}$ be given by

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \cdots \\ \mathbf{g}_{k-1} \end{bmatrix}$$

where $\{\mathbf{g}_0\}$ is some basis of $\mathbf{G}$.

Dual code

- Let C be a linear code with generator matrix $\mathbf{G}$. Then $\mathbf{x} \in C_d$ if and only if $\mathbf{x}\mathbf{G}^T = 0$
- Let $\mathbf{G}$ be given by

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \cdots \\ \mathbf{g}_{k-1} \end{bmatrix}$$

where $\{\mathbf{g}_0\}$ is some basis of $\mathbf{G}$.

- Also, $\mathbf{x}\mathbf{G}^T = (\mathbf{x} \cdot \mathbf{g}_0, \cdots, \mathbf{x} \cdot \mathbf{g}_{k-1})$.

Dual code

- Let C be a linear code with generator matrix $\mathbf{G}$. Then $\mathbf{x} \in C_d$ if and only if $\mathbf{x}\mathbf{G}^T = 0$
- Let $\mathbf{G}$ be given by

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \cdots \\ \mathbf{g}_{k-1} \end{bmatrix}$$

  where $\{\mathbf{g}_0\}$ is some basis of $\mathbf{G}$.
- Also, $\mathbf{x}\mathbf{G}^T = (\mathbf{x} \cdot \mathbf{g}_0, \cdots, \mathbf{x} \cdot \mathbf{g}_{k-1})$.
- If $\mathbf{x} \in C_d$, then $\mathbf{x} \cdot \mathbf{g}_i = 0$ for every i, so $\mathbf{x}\mathbf{G}^T = 0$.

Dual code

- If $\mathbf{x}\mathbf{G}^T = 0$, then $\mathbf{x} \cdot \mathbf{g}_i = 0$ for every i. If $\mathbf{c} \in C$, then $\mathbf{c} = \sum_i \lambda_i \mathbf{g}_i$ for some binary λ_i, so

$$\mathbf{x} \cdot \mathbf{c} = \mathbf{x} \cdot \left(\sum_i \lambda_i \mathbf{g}_i \right) = \sum_i \lambda_i (\mathbf{x}_i \cdot \mathbf{g}_i) = 0$$

  and thus $\mathbf{x} \in C_d$

Dual code

- If $\mathbf{x}\mathbf{G}^T = 0$, then $\mathbf{x} \cdot \mathbf{g}_i = 0$ for every i. If $\mathbf{c} \in C$, then $\mathbf{c} = \sum_i \lambda_i \mathbf{g}_i$ for some binary λ_i, so

$$\mathbf{x} \cdot \mathbf{c} = \mathbf{x} \cdot \left(\sum_i \lambda_i \mathbf{g}_i \right) = \sum_i \lambda_i (\mathbf{x}_i \cdot \mathbf{g}_i) = 0$$

  and thus $\mathbf{x} \in C_d$
- Thus the generator matrix $\mathbf{G}$ of a linear (n, k) block code, is the parity check matrix $\mathbf{H}$ of its dual code and vice-versa.

Self-Dual code

- A linear block code C that is equal to its dual code C_d is called *self-dual code*.

Self-Dual code

- A linear block code C that is equal to its dual code C_d is called *self-dual code*.
- The code rate of self-dual code, $R = 1/2$.

Self-Dual code

- A linear block code C that is equal to its dual code C_d is called *self-dual code*.
- The code rate of self-dual code, $R = 1/2$.
- Code length of self-dual code n is even, and dimension k of the code is $n/2$.

Self-Dual code

- A linear block code C that is equal to its dual code C_d is called *self-dual code*.
- The code rate of self-dual code, $R = 1/2$.
- Code length of self-dual code n is even, and dimension k of the code is $n/2$.
- $(24, 12)$ Golay code is a self-dual code.

Repetition code

- A repetition code of length n is a linear $(n, 1)$ block code.

Repetition code

- A repetition code of length n is a linear $(n, 1)$ block code.
- It consists of two codewords, all zero codeword $\mathbf{0} = (0, 0, \cdots, 0)$ and all one codeword $\mathbf{1} = (1, 1, \cdots, 1)$.

Repetition code

- A repetition code of length n is a linear $(n, 1)$ block code.
- It consists of two codewords, all zero codeword $\mathbf{0} = (0, 0, \cdots, 0)$ and all one codeword $\mathbf{1} = (1, 1, \cdots, 1)$.
- Codeword is obtained by repeating the information bit n times.

Repetition code

- A repetition code of length n is a linear $(n, 1)$ block code.
- It consists of two codewords, all zero codeword $\mathbf{0} = (0, 0, \cdots, 0)$ and all one codeword $\mathbf{1} = (1, 1, \cdots, 1)$.
- Codeword is obtained by repeating the information bit n times.
- Generator matrix is given by

$$\mathbf{G} = [1\ 1\ \cdots 1]$$

Repetition code

- A repetition code of length n is a linear $(n, 1)$ block code.
- It consists of two codewords, all zero codeword $\mathbf{0} = (0, 0, \cdots, 0)$ and all one codeword $\mathbf{1} = (1, 1, \cdots, 1)$.
- Codeword is obtained by repeating the information bit n times.
- Generator matrix is given by

$$\mathbf{G} = [1\ 1\ \cdots 1]$$

- Decoding is based on majority decision of n coded bits.

Repetition code

- A repetition code of length n is a linear $(n, 1)$ block code.
- It consists of two codewords, all zero codeword $\mathbf{0} = (0, 0, \cdots, 0)$ and all one codeword $\mathbf{1} = (1, 1, \cdots, 1)$.
- Codeword is obtained by repeating the information bit n times.
- Generator matrix is given by

$$\mathbf{G} = [1\ 1\ \cdots 1]$$

- Decoding is based on majority decision of n coded bits.
- Minimum distance of the code is n.

Single parity check code

- It is a linear $(k + 1, k)$ block code with single parity bit.

Single parity check code

- It is a linear $(k+1, k)$ block code with single parity bit.
- If $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$, then the parity check bit is given by

$$p = u_0 + u_1 + \cdots + u_{k-1}$$

Single parity check code

- It is a linear $(k+1, k)$ block code with single parity bit.
- If $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$, then the parity check bit is given by

$$p = u_0 + u_1 + \cdots + u_{k-1}$$

- Each codeword is of the form

$$\mathbf{v} = (p, u_0, u_1, \cdots, u_{k-1})$$

Single parity check code

- It is a linear $(k+1, k)$ block code with single parity bit.
- If $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$, then the parity check bit is given by

$$p = u_0 + u_1 + \cdots + u_{k-1}$$

- Each codeword is of the form

$$\mathbf{v} = (p, u_0, u_1, \cdots, u_{k-1})$$

- The generator matrix for the single parity check code in systematic form is given by

$$\mathbf{G} = \left[\begin{array}{c|ccccc} 1 & 1 & 0 & 0 & 0 & \cdots 0 \\ 1 & 0 & 1 & 0 & 0 & \cdots 0 \\ 1 & 0 & 0 & 1 & 0 & \cdots 0 \\ \vdots & & & \vdots & & \\ 1 & 0 & 0 & 0 & 0 & \cdots 1 \end{array}\right]$$

Single parity check code

- The parity check matrix for the single parity check code in systematic form is given by

$$\mathbf{H} = [1\ 1\ \cdots 1]$$

Single parity check code

- The parity check matrix for the single parity check code in systematic form is given by

$$\mathbf{H} = [1\ 1\ \cdots 1]$$

- All codewords of the single parity check (SPC) codes are even weight.

Single parity check code

- The parity check matrix for the single parity check code in systematic form is given by

$$\mathbf{H} = [1\ 1\ \cdots 1]$$

- All codewords of the single parity check (SPC) codes are even weight.
- Minimum distance of SPC code is 2.

Single parity check code

- The parity check matrix for the single parity check code in systematic form is given by

$$\mathbf{H} = [1\ 1\ \cdots 1]$$

- All codewords of the single parity check (SPC) codes are even weight.
- Minimum distance of SPC code is 2.
- SPC code can detect all error patterns with odd number of error.

Single parity check code

- The parity check matrix for the single parity check code in systematic form is given by

$$\mathbf{H} = [1\ 1\ \cdots 1]$$

- All codewords of the single parity check (SPC) codes are even weight.
- Minimum distance of SPC code is 2.
- SPC code can detect all error patterns with odd number of error.
- The $(n, n-1)$ SPC code and $(n, 1)$ repetition code are dual to each other.

Hamming code

- Hamming codes are single error correcting codes.

Hamming code

- Hamming codes are single error correcting codes.
- For any $m \geq 3$, there exist a Hamming code with following parameters

Code length:	$n = 2^m - 1$
Information bits:	$k = 2^m - m - 1$
Parity bits:	$n - k = m$
Error correcting capability:	$t = 1$
Minimum distance:	$d_{\min} = 3$

Hamming code

- Hamming codes are single error correcting codes.
- For any $m \geq 3$, there exist a Hamming code with following parameters

Code length:	$n = 2^m - 1$
Information bits:	$k = 2^m - m - 1$
Parity bits:	$n - k = m$
Error correcting capability:	$t = 1$
Minimum distance:	$d_{\min} = 3$

- The parity check matrix

$$\mathbf{H} = \left[\mathbf{I}_m : \mathbf{P}^{\mathbf{T}}\right],$$

where the $2^m - m - 1$ columns of $\mathbf{P}^{\mathbf{T}}$ consists of all m-tuples of weight 2 or more.

Hamming code

- For $m = 3$, the Hamming code is of length $n = 2^3 - 1 = 7$, $k = 2^3 - 3 - 1 = 4$, that has parity check matrix $\mathbf{H}$,

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

and generator matrix $\mathbf{G}$,

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Hamming code

- We can rearrange the columns of the parity check matrix of Hamming code such that column in position i represents the integer i.

Hamming code

- We can rearrange the columns of the parity check matrix of Hamming code such that column in position i represents the integer i.
- For example for $m = 3$, the Hamming code is of length $n = 2^3 - 1 = 7, k = 2^3 - 3 - 1 = 4$, that has parity check matrix $\mathbf{H}$,

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Hamming code

- We can rearrange the columns of the parity check matrix of Hamming code such that column in position i represents the integer i.
- For example for $m = 3$, the Hamming code is of length $n = 2^3 - 1 = 7, k = 2^3 - 3 - 1 = 4$, that has parity check matrix $\mathbf{H}$,

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- Here the column $(x, y, z)^T$ represents the number $x(2^0) + y(2^1) + z(2^2)$.

Hamming code

- Let $\mathbf{r}$ be the received vector. For decoding we compute the syndrome $\mathbf{r}\mathbf{H}^T$.

Hamming code

- Let $\mathbf{r}$ be the received vector. For decoding we compute the syndrome $\mathbf{r}\mathbf{H}^T$.
- If at most one error has occurred, the syndrome would be either the zero vector or a column of $\mathbf{H}$.

Hamming code

- Let $\mathbf{r}$ be the received vector. For decoding we compute the syndrome $\mathbf{r}\mathbf{H}^T$.
- If at most one error has occurred, the syndrome would be either the zero vector or a column of $\mathbf{H}$.
- When one error has happened, the number represented by the column of the calculated syndrome is the position in codeword which is in error, and since we considered binary code, it can be corrected.

Hamming code

- Let 0 1 0 1 0 1 0 be a codeword in [7, 4] Hamming code. Suppose we received the vector 0 0 0 1 0 1 0.

Hamming code

- Let 0 1 0 1 0 1 0 be a codeword in [7, 4] Hamming code. Suppose we received the vector 0 0 0 1 0 1 0.
- Syndrome is given by

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = (0\,1\,0)$$

Hamming code

- Let 0 1 0 1 0 1 0 be a codeword in [7, 4] Hamming code. Suppose we received the vector 0 0 0 1 0 1 0.
- Syndrome is given by

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = (0\,1\,0)$$

- The number represented by syndrome is 2, hence the error is in second bit position. Hence estimated codeword is 0 1 0 1 0 1 0.

Shortened Hamming code

- If we delete any l columns from the parity check matrix of a Hamming code, we get shortened Hamming code with following parameters

Code length:	$n = 2^m - l - 1$
Information bits:	$k = 2^m - m - l - 1$
Parity bits:	$n - k = m$
Minimum distance:	$d_{\min} \geq 3$

Shortened Hamming code

- If we delete any l columns from the parity check matrix of a Hamming code, we get shortened Hamming code with following parameters

Code length:	$n = 2^m - l - 1$
Information bits:	$k = 2^m - m - l - 1$
Parity bits:	$n - k = m$
Minimum distance:	$d_{\min} \geq 3$

- $\mathbf{H}$ matrix of (7,4) Hamming code given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Shortened Hamming code

- If we delete any l columns from the parity check matrix of a Hamming code, we get shortened Hamming code with following parameters

Code length:	$n = 2^m - l - 1$
Information bits:	$k = 2^m - m - l - 1$
Parity bits:	$n - k = m$
Minimum distance:	$d_{\min} \geq 3$

- $\mathbf{H}$ matrix of (7,4) Hamming code given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- Shortened (6,3) Hamming code has a parity check matrix

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Expurgated Hamming code

- Let C be a (n, k) Hamming code with parity check matrix $\mathbf{H}$. Let us define a new code C_1 with parity check matrix H_1. (all one vector as the last row.)

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{H} \\ \cdots\cdots \\ 1 \cdots 1 \end{pmatrix}$$

Expurgated Hamming code

- Let C be a (n, k) Hamming code with parity check matrix $\mathbf{H}$. Let us define a new code C_1 with parity check matrix H_1. (all one vector as the last row.)

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{H} \\ \cdots\cdots \\ 1 \cdots 1 \end{pmatrix}$$

- Since the parity check matrix of Hamming code doesnt have an all one vector in any of the rows, any linear combination including the last row of $\mathbf{H}_1$ will never yield a zero vector.

Expurgated Hamming code

- Let C be a (n, k) Hamming code with parity check matrix $\mathbf{H}$. Let us define a new code C_1 with parity check matrix H_1. (all one vector as the last row.)

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{H} \\ \cdots\cdots \\ 1 \cdots 1 \end{pmatrix}$$

- Since the parity check matrix of Hamming code doesnt have an all one vector in any of the rows, any linear combination including the last row of $\mathbf{H}_1$ will never yield a zero vector.
- Thus all the rows of $\mathbf{H}_1$ are linearly independent. Hence the row space of $\mathbf{H}_1$ has dimension $(n - k + 1)$.

Expurgated Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n) - (n - k + 1) = k - 1$$

Expurgated Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n) - (n - k + 1) = k - 1$$

- Hence C_1 is an $(n, k-1)$ linear code. This is an expurgated Hamming code.

Expurgated Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n) - (n - k + 1) = k - 1$$

- Hence C_1 is an $(n, k-1)$ linear code. This is an expurgated Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

and so $\mathbf{v}$ can not be a codeword.

Expurgated Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n) - (n - k + 1) = k - 1$$

- Hence C_1 is an $(n, k-1)$ linear code. This is an expurgated Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

and so $\mathbf{v}$ can not be a codeword.
- Thus, this expurgated Hamming code only has even weight codewords (all odd weight codewords are expurgated).

Expurgated Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n) - (n - k + 1) = k - 1$$

- Hence C_1 is an $(n, k-1)$ linear code. This is an expurgated Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

and so $\mathbf{v}$ can not be a codeword.
- Thus, this expurgated Hamming code only has even weight codewords (all odd weight codewords are expurgated).
- The submatrix formed by the original Hamming code insures that all nonzero codewords must have a weight of atleast three.

Expurgated Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n) - (n - k + 1) = k - 1$$

- Hence C_1 is an $(n, k-1)$ linear code. This is an expurgated Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

  and so $\mathbf{v}$ can not be a codeword.
- Thus, this expurgated Hamming code only has even weight codewords (all odd weight codewords are expurgated).
- The submatrix formed by the original Hamming code insures that all nonzero codewords must have a weight of atleast three.
- The expurgated parity check matrix defines a code with minimum distance four.

Expurgated Hamming code: Example

- $\mathbf{H}$ matrix of (7,4) Hamming code given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Expurgated Hamming code: Example

- **H** matrix of (7,4) Hamming code given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

- Distance-4 expurgated Hamming code has a parity check matrix $\mathbf{H}_1$ given by

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Extended Hamming code

- Let C be a (n, k) Hamming code with parity check matrix **H**. Let us define a new code C_1 with parity check matrix $\mathbf{H}_1$. (all one vector as the last row.)

$$\mathbf{H}_1 = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \cdots\cdots & \cdots \\ 1 \cdots 1 & 1 \end{array} \right)$$

Extended Hamming code

- Let C be a (n, k) Hamming code with parity check matrix $\mathbf{H}$. Let us define a new code C_1 with parity check matrix $\mathbf{H}_1$. (all one vector as the last row.)

$$\mathbf{H}_1 = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \cdots\cdots & \cdots \\ 1 \cdots 1 & 1 \end{array}\right)$$

- Since the parity check matrix of Hamming code doesnt have an all one vector in any of the rows, any linear combination including the last row of $\mathbf{H}_1$ will never yield a zero vector.

Extended Hamming code

- Let C be a (n, k) Hamming code with parity check matrix $\mathbf{H}$. Let us define a new code C_1 with parity check matrix $\mathbf{H}_1$. (all one vector as the last row.)

$$\mathbf{H}_1 = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \cdots\cdots & \cdots \\ 1 \cdots 1 & 1 \end{array}\right)$$

- Since the parity check matrix of Hamming code doesnt have an all one vector in any of the rows, any linear combination including the last row of $\mathbf{H}_1$ will never yield a zero vector.
- Thus all the rows of $\mathbf{H}_1$ are linearly independent. Hence the row space of $\mathbf{H}_1$ has dimension $(n - k + 1)$.

Extended Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n+1) - (n-k+1) = k$$

Extended Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n+1) - (n-k+1) = k$$

- Hence C_1 is an $(n+1, k)$ linear code. This is an extended Hamming code.

Extended Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n+1) - (n-k+1) = k$$

- Hence C_1 is an $(n+1, k)$ linear code. This is an extended Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

and so $\mathbf{v}$ cannot be a codeword.

Extended Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n+1) - (n-k+1) = k$$

- Hence C_1 is an $(n+1, k)$ linear code. This is an extended Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

and so $\mathbf{v}$ cannot be a codeword.

- Thus, this extended Hamming code only has even weight codewords.

Extended Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n+1) - (n-k+1) = k$$

- Hence C_1 is an $(n+1, k)$ linear code. This is an extended Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

  and so $\mathbf{v}$ cannot be a codeword.
- Thus, this extended Hamming code only has even weight codewords.
- The submatrix formed by the original Hamming code insures that all nonzero codewords must have a weight of atleast three.

Extended Hamming code

- The dimension of its null space C_1 is:

$$dim(C_1) = (n+1) - (n-k+1) = k$$

- Hence C_1 is an $(n+1, k)$ linear code. This is an extended Hamming code.
- Now, since the last row of $\mathbf{H}_1$ is an all-one vector, the inner product of any odd weight vector $\mathbf{v}$ and all-one vector is 1. Hence for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}\mathbf{H}^T \neq 0$$

  and so $\mathbf{v}$ cannot be a codeword.
- Thus, this extended Hamming code only has even weight codewords.
- The submatrix formed by the original Hamming code insures that all nonzero codewords must have a weight of atleast three.
- The extended parity check matrix defines a code with minimum distance four.

Extended Hamming code: Example

- **H** matrix of Hamming code given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Extended Hamming code: Example

- **H** matrix of Hamming code given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

- Distance-4 extended hamming code has a parity check matrix $\mathbf{H}_1$ given by

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$