Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 14
March 7, 2023

Hamming codes

For any positive integer $m \geq 3$ there exists a Hamming code with the following parameters:

Code length: $n = 2^m - 1$

Number of information bits: $k = 2^m - m - 1$

Number of parity-check bits: $n - k = m$

Error-correcting capability: $t = 1, d_{\min} = 3$

Hamming codes

For any positive integer $m \geq 3$ there exists a Hamming code with the following parameters:

Code length: $n = 2^m - 1$

Number of information bits: $k = 2^m - m - 1$

Number of parity-check bits: $n - k = m$

Error-correcting capability: $t = 1, d_{\min} = 3$

The parity-check matrix in the systematic form is:

$$\mathbf{H} = \begin{bmatrix} I_m & Q \end{bmatrix}$$

where Q consists of $2^m - m - 1$ columns that are the m-tuples of weight 2 or more

Hamming code

For example, setting $m = 3$ we have

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

Hamming code

For example, setting $m = 3$ we have

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

Thus the generator matrix is

$$\mathbf{G} = \begin{bmatrix} Q^T & I_{2^m - m - 1} \end{bmatrix}$$

Hamming code

For example, setting $m = 3$ we have

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

Thus the generator matrix is

$$\mathbf{G} = \begin{bmatrix} Q^T & I_{2^m - m - 1} \end{bmatrix}$$

Question Show that $d_{\min} = 3$

Hamming code

Observation

→ The standard array of the Hamming code of length $n = 2^m - 1$ the coset leaders are $(2^m - 1)$ tuples of weight 1

Hamming code

Observation

- $\rightarrow$ The standard array of the Hamming code of length $n = 2^m - 1$ the coset leaders are $(2^m - 1)$ tuples of weight 1
- $\rightarrow$ The code has 2^m cosets

Hamming code

Observation

- → The standard array of the Hamming code of length $n = 2^m - 1$ the coset leaders are $(2^m - 1)$ tuples of weight 1
- → The code has 2^m cosets
- → Hamming code corrects only error patterns of single error and no others

Hamming code

Observation

- $\rightarrow$ The standard array of the Hamming code of length $n = 2^m - 1$ the coset leaders are $(2^m - 1)$ tuples of weight 1
- $\rightarrow$ The code has 2^m cosets
- $\rightarrow$ Hamming code corrects only error patterns of single error and no others

Perfect code For an (n, k) code, $2^{nk} \geq n + 1$. If this bound is achieved with equality, i.e. $n = 2^{n-k} - 1$, then the code is a perfect code

Hamming code

Observation

- → The standard array of the Hamming code of length $n = 2^m - 1$ the coset leaders are $(2^m - 1)$ tuples of weight 1
- → The code has 2^m cosets
- → Hamming code corrects only error patterns of single error and no others

Perfect code For an (n, k) code, $2^{nk} \geq n + 1$. If this bound is achieved with equality, i.e. $n = 2^{n-k} - 1$, then the code is a perfect code

Question Hamming code is a perfect code!!

Golay codes

This is a perfect code constructed by M. J. E. Golay in 1949.

$n = 23,\ k = 12$

Golay codes

This is a perfect code constructed by M. J. E. Golay in 1949.

$n = 23, \ k = 12$

$d_{\min} = 7$

Golay codes

This is a perfect code constructed by M. J. E. Golay in 1949.

$n = 23$, $k = 12$

$d_{\min} = 7$

capable of correcting any combination of three or fewer random errors

Golay codes

This is a perfect code constructed by M. J. E. Golay in 1949.

$n = 23$, $k = 12$

$d_{\min} = 7$

capable of correcting any combination of three or fewer random errors

It is also known as $(23, 12)$ Golay code. It can be extended to a $(24, 12)$ code by adding an overall parity-check bit to each codeword, and the minimum distance of this code is 8. This extended code is capable of correcting 3 of fewer errors and detecting all error patterns of 4 errors. It is not a perfect code, but widely used for error control such as in the US space program. It served as the primary Voyager error-control system, providing clear color pictures of Jupiter and Saturn between 1979 and 1981.

Golay code

$(24, 12)$ Golay code A generator matrix in the systematic form for this code is

$$\mathbf{G} = \begin{bmatrix} P & I_{12} \end{bmatrix},$$

where P has the following properties

- $P^T = P$
- $P \cdot P^T = I_{12}$
- The submatrix obtained by deleting the last row and last column is formed by cyclically shifting the first row to the left 11 times or cyclically shifting the first column upward 11 times

Golay code

$$P = \begin{bmatrix} 1&0&0&0&1&1&1&0&1&1&0&1 \\ 0&0&0&1&1&1&0&1&1&0&1&1 \\ 0&0&1&1&1&0&1&1&0&1&0&1 \\ 0&1&1&1&0&1&1&0&1&0&0&1 \\ 1&1&1&0&1&1&0&1&0&0&0&1 \\ 1&1&0&1&1&0&1&0&0&0&1&1 \\ 1&0&1&1&0&1&0&0&0&1&1&1 \\ 0&1&1&0&1&0&0&0&1&1&1&1 \\ 1&1&0&1&0&0&0&1&1&1&0&1 \\ 1&0&1&0&0&0&1&1&1&0&1&1 \\ 0&1&0&0&0&1&1&1&0&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{bmatrix}$$

Golay code

The parity-check matrix in systematic form for the $(24, 12)$ extended Golay code is

$$\mathbf{H} = \begin{bmatrix} I_{12} & P \end{bmatrix}$$

Golay code

The parity-check matrix in systematic form for the $(24, 12)$ extended Golay code is

$$\mathbf{H} = \begin{bmatrix} I_{12} & P \end{bmatrix}$$

Question Show that it is self-dual code

Golay code

The parity-check matrix in systematic form for the $(24, 12)$ extended Golay code is

$$\mathbf{H} = \begin{bmatrix} I_{12} & P \end{bmatrix}$$

Question Show that it is self-dual code 0.1cm
Observation

1. For $0 \leq i \leq 11$, let p_i denote the i-th row of P and $u^{(i)}$ the 12-tuple in which only the i-th entry is nonzero. For example, $u^{(5)} = (000010000000)$. Then

$$p_i = u^{(i)} \cdot P$$

Golay code

2. Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be a received 24-tuple for a transmitted tuple $\mathbf{v}$, and the error vector $\mathbf{e} = (\mathbf{x}, \mathbf{y})$ Then

$$s = r \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T = (\mathbf{x}, \mathbf{y}) \begin{bmatrix} I_{12} \\ P \end{bmatrix} = \mathbf{x} + \mathbf{y}P$$

Golay code

2. Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be a received 24-tuple for a transmitted tuple $\mathbf{v}$, and the error vector $\mathbf{e} = (\mathbf{x}, \mathbf{y})$ Then

$$s = r \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T = (\mathbf{x}, \mathbf{y}) \begin{bmatrix} I_{12} \\ P \end{bmatrix} = \mathbf{x} + \mathbf{y}P$$

3. Then $\mathbf{y} = (\mathbf{s} + \mathbf{x}) \cdot P$ since $PP^T = I_{12}$

Golay code

2. Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be a received 24-tuple for a transmitted tuple $\mathbf{v}$, and the error vector $\mathbf{e} = (\mathbf{x}, \mathbf{y})$ Then

$$s = r \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T = (\mathbf{x}, \mathbf{y}) \begin{bmatrix} I_{12} \\ P \end{bmatrix} = \mathbf{x} + \mathbf{y}P$$

3. Then $\mathbf{y} = (\mathbf{s} + \mathbf{x}) \cdot P$ since $PP^T = I_{12}$

Correctable error pattern For any correctable error pattern $t = \lfloor (d_{\min} - 1)/2 \rfloor = 3$, we have the following cases

(a) $w(\mathbf{x}) \leq 3$ and $w(\mathbf{y}) = 0$

Golay code

2. Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be a received 24-tuple for a transmitted tuple $\mathbf{v}$, and the error vector $\mathbf{e} = (\mathbf{x}, \mathbf{y})$ Then

$$s = r \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T = (\mathbf{x}, \mathbf{y}) \begin{bmatrix} I_{12} \\ P \end{bmatrix} = \mathbf{x} + \mathbf{y}P$$

3. Then $\mathbf{y} = (\mathbf{s} + \mathbf{x}) \cdot P$ since $PP^T = I_{12}$

Correctable error pattern For any correctable error pattern $t = \lfloor (d_{\min} - 1)/2 \rfloor = 3$, we have the following cases

(a) $w(\mathbf{x}) \leq 3$ and $w(\mathbf{y}) = 0$

(b) $w(\mathbf{x}) \leq 2$ and $w(\mathbf{y}) = 1$

Golay code

2. Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be a received 24-tuple for a transmitted tuple $\mathbf{v}$, and the error vector $\mathbf{e} = (\mathbf{x}, \mathbf{y})$ Then

$$s = r \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T = (\mathbf{x}, \mathbf{y}) \begin{bmatrix} I_{12} \\ P \end{bmatrix} = \mathbf{x} + \mathbf{y}P$$

3. Then $\mathbf{y} = (\mathbf{s} + \mathbf{x}) \cdot P$ since $PP^T = I_{12}$

Correctable error pattern For any correctable error pattern $t = \lfloor (d_{\min} - 1)/2 \rfloor = 3$, we have the following cases

(a) $w(\mathbf{x}) \leq 3$ and $w(\mathbf{y}) = 0$

(b) $w(\mathbf{x}) \leq 2$ and $w(\mathbf{y}) = 1$

(c) $w(\mathbf{x}) \leq 1$ and $w(\mathbf{y}) = 2$

Golay code

2. Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be a received 24-tuple for a transmitted tuple $\mathbf{v}$, and the error vector $\mathbf{e} = (\mathbf{x}, \mathbf{y})$ Then

$$s = r \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T = (\mathbf{x}, \mathbf{y}) \begin{bmatrix} I_{12} \\ P \end{bmatrix} = \mathbf{x} + \mathbf{y}P$$

3. Then $\mathbf{y} = (\mathbf{s} + \mathbf{x}) \cdot P$ since $PP^T = I_{12}$

Correctable error pattern For any correctable error pattern $t = \lfloor (d_{\min} - 1)/2 \rfloor = 3$, we have the following cases

(a) $w(\mathbf{x}) \leq 3$ and $w(\mathbf{y}) = 0$

(b) $w(\mathbf{x}) \leq 2$ and $w(\mathbf{y}) = 1$

(c) $w(\mathbf{x}) \leq 1$ and $w(\mathbf{y}) = 2$

(d) $w(\mathbf{x}) \leq 0$ and $w(\mathbf{y}) = 3$

Golay code

Thus for $0 \leq j \leq 3$, set $e^{(j)} = (\mathbf{x}, \mathbf{y})$ such that $w(\mathbf{y}) = j$ and $w(\mathbf{x}) \leq 3 - j$.

Golay code

Thus for $0 \leq j \leq 3$, set $e^{(j)} = (\mathbf{x}, \mathbf{y})$ such that $w(\mathbf{y}) = j$ and $w(\mathbf{x}) \leq 3 - j$.

For $j = 0$, $\mathbf{e}^{(0)} = (\mathbf{x}, \mathbf{0}) = (\mathbf{s}, \mathbf{0})$ where $\mathbf{0}$ is all-zero 12-tuple, since $\mathbf{s} = \mathbf{x} + \mathbf{y}P$

Golay code

Thus for $0 \leq j \leq 3$, set $e^{(j)} = (\mathbf{x}, \mathbf{y})$ such that $w(\mathbf{y}) = j$ and $w(\mathbf{x}) \leq 3 - j$.

For $j = 0$, $\mathbf{e}^{(0)} = (\mathbf{x}, \mathbf{0}) = (\mathbf{s}, \mathbf{0})$ where $\mathbf{0}$ is all-zero 12-tuple, since $\mathbf{s} = \mathbf{x} + \mathbf{y}P$

For $j = 1$, set $\mathbf{y} = u^{(1)}$. Then $\mathbf{s} = \mathbf{x} + u^{(i)}P = \mathbf{x} + p_i$. Hence $\mathbf{x} = \mathbf{s} + p_i$ and $w(\mathbf{s} + p_i) = w(\mathbf{x}) \leq 2$. Thus

$$\mathbf{e}^{(1)} = (\mathbf{s} + p_i, u^{(i)})$$

Golay code

Thus for $0 \leq j \leq 3$, set $e^{(j)} = (\mathbf{x}, \mathbf{y})$ such that $w(\mathbf{y}) = j$ and $w(\mathbf{x}) \leq 3 - j$.

For $j = 0$, $\mathbf{e}^{(0)} = (\mathbf{x}, \mathbf{0}) = (\mathbf{s}, \mathbf{0})$ where $\mathbf{0}$ is all-zero 12-tuple, since $\mathbf{s} = \mathbf{x} + \mathbf{y}P$

For $j = 1$, set $\mathbf{y} = u^{(1)}$. Then $\mathbf{s} = \mathbf{x} + u^{(i)}P = \mathbf{x} + p_i$. Hence $\mathbf{x} = \mathbf{s} + p_i$ and $w(\mathbf{s} + p_i) = w(\mathbf{x}) \leq 2$. Thus

$$\mathbf{e}^{(1)} = (\mathbf{s} + p_i, u^{(i)})$$

For $j = 2$ or 3, and $w(\mathbf{x}) = 0$, we have $\mathbf{y} = \mathbf{s}P$ and $w(\mathbf{s}P) = w(\mathbf{y})$ or 3. Thus

$$\mathbf{e}^{(2/3)} = (\mathbf{0}, \mathbf{s}P)$$

Golay code

Thus for $0 \leq j \leq 3$, set $e^{(j)} = (\mathbf{x}, \mathbf{y})$ such that $w(\mathbf{y}) = j$ and $w(\mathbf{x}) \leq 3 - j$.

For $j = 0$, $\mathbf{e}^{(0)} = (\mathbf{x}, \mathbf{0}) = (\mathbf{s}, \mathbf{0})$ where $\mathbf{0}$ is all-zero 12-tuple, since $\mathbf{s} = \mathbf{x} + \mathbf{y}P$

For $j = 1$, set $\mathbf{y} = u^{(1)}$. Then $\mathbf{s} = \mathbf{x} + u^{(i)}P = \mathbf{x} + p_i$. Hence $\mathbf{x} = \mathbf{s} + p_i$ and $w(\mathbf{s} + p_i) = w(\mathbf{x}) \leq 2$. Thus

$$\mathbf{e}^{(1)} = (\mathbf{s} + p_i, u^{(i)})$$

For $j = 2$ or 3, and $w(\mathbf{x}) = 0$, we have $\mathbf{y} = \mathbf{s}P$ and $w(\mathbf{s}P) = w(\mathbf{y})$ or 3. Thus

$$\mathbf{e}^{(2/3)} = (\mathbf{0}, \mathbf{s}P)$$

For $j = 2$ and $w(\mathbf{x}) = 1$, $\mathbf{x} = u^{(i)}$ and hence $\mathbf{y} = (\mathbf{s} + u^{(i)})P = \mathbf{s}P + u^{(i)}P = \mathbf{s}P + p_i$ and $w(sP + p_i) = w(\mathbf{y}) = 2$. Thus

$$\mathbf{e}^{(2)} = (u^{(i)}, \mathbf{s}P + p_i)$$