Problems 2 - Hamming, Hadamard, binary Golay, CRC, LDPC codes

Coding Technology

Illés Horváth

2025/10/03

A linear binary block code has syndrome vectors of length 7 bits, and each error group contains 32 error vectors. What are the parameters of the code?

Solution. Syndrome vectors are n-k bits long, so n-k=7. Each error group contains 2^k error vectors (same as the number of codewords), so $2^k=32$ and k=5. Finally, n=12, so this is a C(12,5) code.

vector	length
message vector	k
codeword vector	n
error vector	n
received vector	n
syndrome vector	n-k
detected error	n
detected codeword	n
detected message	k

For a binary linear systematic code, we know the error group corresponding to one of the syndromes:

$$(111) \quad \to \quad \{(11111), (10000), (01001), (00110)\}.$$

- (a) Which is the group leader?
- (b) What are the parameters of the code?
- (c) List the codewords.
- (d) Compute the generator matrix and parity check matrix.
- (e) How many errors can the code detect? How many errors can the code correct?

Solution.

- (a) Which is the group leader?
 - The vector with minimal weight, so (10000).
- (b) What are the parameters of the code?
 - Error vectors are n bits long, so n = 5. Each error group contains 2^k error vectors, so $2^k = 4$ and k = 2. This is a C(5,2) code.
- (c) List the codewords.

The codewords can be obtained by subtracting (or adding) one of the error vectors from all other error vectors in the error group:

$$(11111) - (11111) = (00000)$$
 $(11111) - (10000) = (01111)$ $(11111) - (01001) = (10110)$ $(11111) - (00110) = (11001)$

(d) Compute the generator matrix and parity check matrix.

The codewords are (00000), (01111), (10110), (11001). The code is systematic, so

$$(01) \to (01111), \quad (10) \to (10110).$$

The generator matrix can be built from the codewords corresponding to the unit vectors, so

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

and then

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

(e) How many errors can the code detect? How many errors can the code correct?

The code is linear, so

$$d_{\min} = \min_{c \neq 0} w(c) = 3,$$

so the code can detect

$$d_{\min} - 1 = 2$$

errors, and correct

$$\left\lfloor \frac{d_{\mathsf{min}} - 1}{2} \right\rfloor = 1$$

error.

Hamming codes

Hamming codes can correct t = 1 error.

Hamming codes are perfect codes:

$$n = 2^{n-k} - 1$$
 \iff $\sum_{i=0}^{1} {n \choose i} = 2^{n-k}$

Construction of C(n, k) Hamming code:

▶ the column vectors of the parity check matrix H run through all different nonzero binary vectors of length n - k.

A binary linear code has generator matrix

$$G = \left[\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array} \right].$$

Is this a Hamming code?

Solution. n = 5, k = 3, so this is a C(5,3) code. But

$$n = 5 \neq 2^{n-k} - 1 = 3,$$

so this is not a Hamming code.

(Possible Hamming code parameters are (3,1), (7,4), (15,11), (31,26), (63,57) etc. - but no Hamming code in-between!)

A linear binary code has parity check matrix

$$H = \left[\begin{array}{cccccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right].$$

Is this a Hamming code?

Solution. n = 7, k = 4, so $n = 2^{n-k} - 1$ holds, but columns 1 and 4 are the same, so this is not a Hamming code.

We have a 12-bit message to transmit through a channel with bit error probability $p_b = 0.03$.

- (a) We transmit the message without coding. What is the probability that the receiver gets the message wrong?
- (b) We cut the message into 3 sections of 4 bits each, then transmit each section using a C(7,4) Hamming code. When can the receiver decode correctly? Compute the probability of a decoding error for the entire 12-bit message. What is the rate of this code?
- (c) Compute the probability of a decoding error if we use a C(23,12) Golay code for the entire message instead. What is the code rate?
- (d) What is the Shannon-limit for the code rate for this channel?

We have a 12-bit message to transmit through a channel with bit error probability $p_b = 0.03$.

- (a) We transmit the message without coding. What is the probability that the receiver gets the message wrong? Solution. $1 (1 p_b)^{12} \approx 0.306$.
- (b) We cut it into 3 sections of 4 bits each, then transmit each section using a C(7,4) Hamming code. When can the receiver decode correctly? Compute the probability of a decoding error for the entire 12-bit message. What is the rate of this code?
 - Solution. The receiver can decode correctly if all 3 blocks are decoded correctly. The Hamming code can correct 1 error, so each block is decoded correctly if there are either 0 or 1 errors in each block.

(b) The probability that 1 out of the 3 blocks is decoded correctly is

$$(1-p_b)^7+6p_b(1-p_b)^6\approx 0.958,$$

the probability that all 3 blocks are correct is

$$((1-p_b)^7+6p_b(1-p_b)^6)^3\approx 0.879,$$

and the probability of a decoding error for the entire 3 block message is

$$1 - ((1 - p_b)^7 + 6p_b(1 - p_b)^6)^3 \approx 0.121.$$

The code rate is $4/7 \approx 0.571$.

(c) Compute the probability of a decoding error if we use a C(23,12) Golay code for the entire message instead. What is the code rate?

Solution. With the C(23,12) Golay code, the entire 12-bit message will be a single block. This code can correct 3 errors, so the block error probability is

$$1 - (1 - p_b)^{23} - {23 \choose 1} (1 - p_b)^{22} p_b - {23 \choose 2} (1 - p_b)^{21} p_b^2$$
$$- {23 \choose 3} (1 - p_b)^{20} p_b^3 \approx 0.00454.$$

The code rate is $12/23 \approx 0.522$.

(d) The Shannon-limit of the channel is

$$1 - (-p_b \log_2 p_b - (1 - p_b) \log_2 (1 - p_b)) \approx 0.806.$$



We transmit a single bit through a channel with bit error probability $p_b = 0.1$ using the C(4,1) extended Hamming code. Due to the SECDED property of the extended Hamming code, the possible outcomes of the decoding are the following:

- no error detected, correct decoding;
- 1 error detected, correct decoding;
- 2 errors detected, no decoding;
- ▶ 3 or more errors but no error detected, decoding error

Compute the probability of each of the above outcomes.

The error groups are:

```
 \begin{array}{lll} (000) \rightarrow \{(0000), (1111)\}, & (001) \rightarrow \{(0001), (1110)\} \\ (010) \rightarrow \{(0010), (1101)\}, & (100) \rightarrow \{(0100), (1011)\} \\ (101) \rightarrow \{(0101), (1010)\}, & (110) \rightarrow \{(1001), (0110)\} \\ (011) \rightarrow \{(0011), (1100)\}, & (111) \rightarrow \{(1000), (0111)\} \\ \end{array}
```



Solution.

no error detected, correct decoding

$$P(0 \text{ errors}) = (1 - p_b)^4 = 0.9^4 = 0.6561$$

▶ 1 error detected, correct decoding

$$P(1 \text{ error}) = {4 \choose 1} (1 - p_b)^3 p_b = 4 \cdot 0.9^3 \cdot 0.1 = 0.2916$$

▶ 2 errors detected, no decoding

$$P(2 \text{ errors}) = {4 \choose 2} 0.9^2 0.1^2 = 0.0486$$

3 or more errors but no error detected, decoding error

$$P(3 \text{ or more errors}) = {4 \choose 3} 0.9^1 0.1^3 + {4 \choose 4} 0.1^4 = 0.0037$$

The C(8,4) extended Hamming code has generator

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

and the C(8,4) augmented Hadamard code has generator

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

Are the two codes equivalent?

Solution. Two linear binary block codes are equivalent if the generators can be transformed into each other by a sequence of the following steps:

- permutation of the rows;
- permutation of the columns;
- adding one row to another row.

The original G is in systematic form; let's try to bring G' to systematic form too.

Targeting a leftmost *I* block. Exchange columns 2 and 5:

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

Add row 2 to row 1:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Add row 3 to row 1:

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Add row 4 to row 3:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

The goal is

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

which can clearly be obtained by a permutation of columns 5-8, so the two codes are equivalent.

A CRC code adds 3 parity bits and has parameter vector (101).

- (a) What is the codeword corresponding to the message (1010011)?
- (b) The codeword from part (a) is transmitted through a channel. The error vector is 0001100000. Execute error detection for the received codeword.

Solution. We first extend the vectors:

(a)

$$(1010011)
ightarrow (1010011|000) \ (101)
ightarrow (1101)$$

(a) Then

Nonzero remainder \rightarrow error detected!

An LDPC code has parity check matrix

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

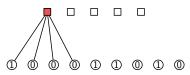
Execute the bit-flipping algorithm for the received vector

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

to obtain the detected codeword c'.

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

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



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

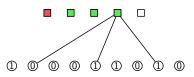
$$v = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

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

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

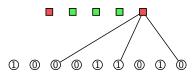
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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



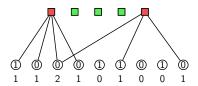
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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



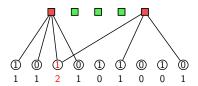
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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



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

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



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

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



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

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

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

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

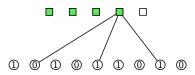
$$0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

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

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

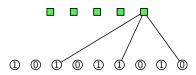
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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



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

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



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

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

$$c' = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$