Problems for the Midterm test

Coding Technology

Illés Horváth

2025/11/05

Problem A1

A. Any C(n, k) binary code has 2^k codewords.

   True. There are 2^k possible message vectors, and one codeword for each.

B. For any C(n, k) binary Hamming code, $n = 2^k - 1$.

   False, for a binary Hamming code, $n = 2^{n-k} - 1$ instead.

C. If two error correction codes are equivalent, they have the same error correction capabilities.

   True. For equivalent codes, we can permute the codeword bits, and we can permute how the codewords are assigned to the messages, but neither of those operation changes the minimal distance between codewords, which determines the error correction capability.

Problem A1

D. In a Galois field, every nonzero element has a multiplicative inverse.

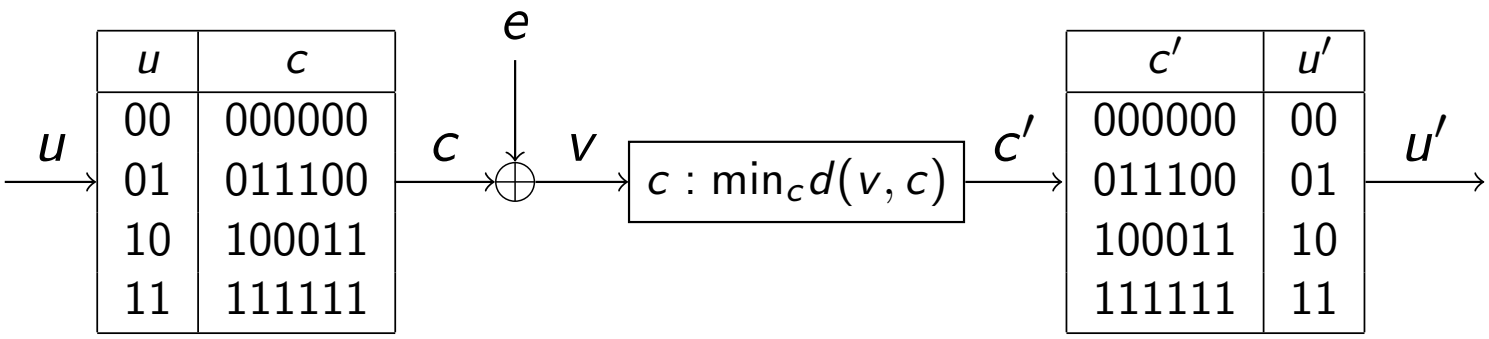
   True, this is one of the field axioms, so it is true by definition.

E. $g(x) = y^5x + y^2x + x^2$ generates a BCH code over GF(8).

   False, BCH codes are generated by binary polynomials (so only 0 or 1 coefficients).

Problem A2

Consider the following coding scheme.

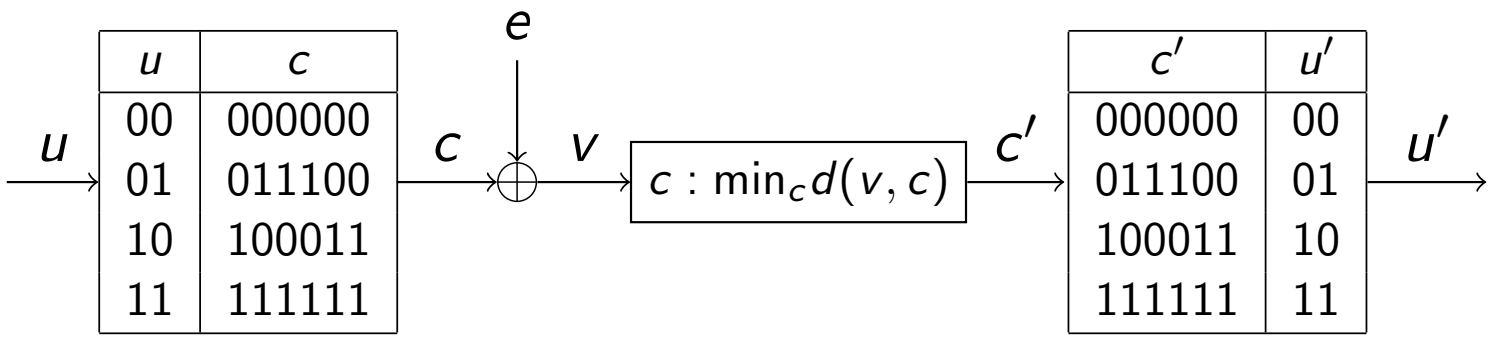


(a) What are the n and k parameters of the code? (2 pts)

(b) How many errors can this code correct? (2 pts)

(c) Execute the entire coding scheme for $u = (0\,1)$ and $e = (0\,0\,0\,0\,1\,0)$, that is, calculate c, v, c', u'. Is the decoding correct? (6 pts)

Problem A2



(a) What are the n and k parameters of the code? (2 pts)

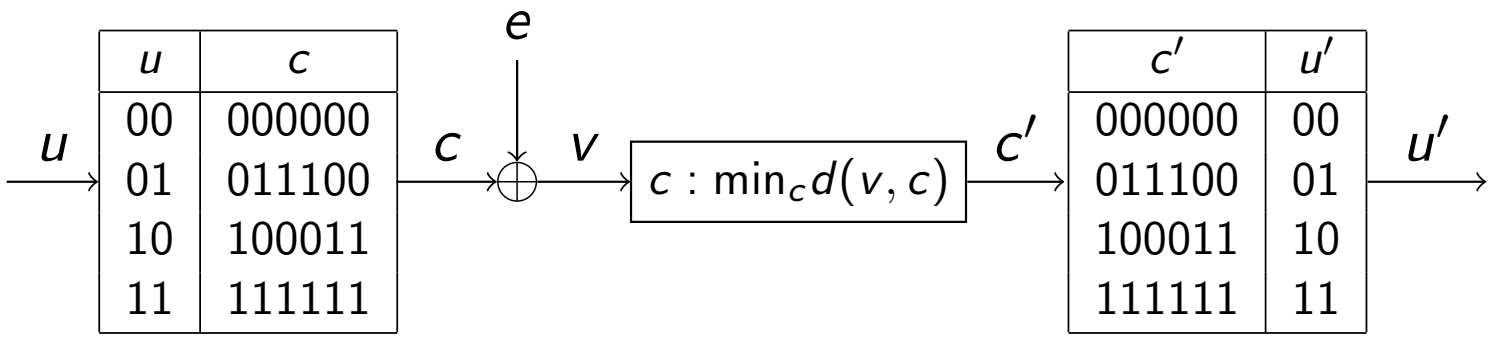
$n = 6$ (the length of the codewords), $k = 2$ (there are $4 = 2^k$ messages).

(b) How many errors can this code correct? (2 pts)

By pairwise comparison, the minimal codeword distance is $d_{\text{min}} = 3$.

Alternatively, due to (011100)+(100011)=(111111), this is a linear code, so $d_{\text{min}} = \min_{c \neq 0} w(c) = 3$.

Problem A2



(c) Execute the entire coding scheme for $u = (0\,1)$ and $e = (0\,0\,0\,0\,1\,0)$, that is, calculate c, v, c', u'. Is the decoding correct? (6 pts)

$$u = (01) \quad \rightarrow \quad c = (011100)$$
$$v = c + e = (011110)$$
$$d((011110), (011100)) = 1 \text{ is minimal } \rightarrow c' = (011100)$$
$$u' = (01)$$

The decoding is correct.

Problem A3

The C(16,11) extended Hamming code can distinguish between 0, 1 or 2 errors (assuming ≤ 2 errors occurred), and for 0 or 1 errors, it can decode correctly. For a channel with bit error probability $p_b = 0.01$, calculate the probability of each of the following outcomes for a single block:

(a) 0 or 1 errors detected, correct decoding (4 pts);

(b) 2 errors detected, no decoding (3 pts);

(c) erroneous decoding (3 pts).

Solution.

(a)

$$\binom{16}{0}(1-0.01)^{16} + \binom{16}{1}0.01^1(1-0.01)^{15} = 0.9891$$

(b)

$$\binom{16}{2}0.01^2(1-0.01)^{14} = 0.0104$$

(c)

$$1 - 0.9891 - 0.0104 = 0.0005$$

Problem A4

An LDPC code has parity check matrix

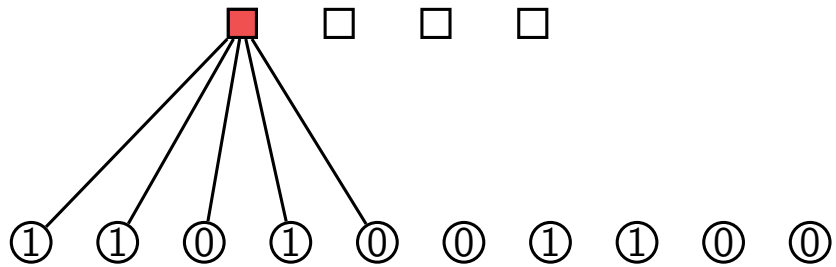
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Execute the bit-flipping algorithm for the received vector $v = (1101001100)$ to obtain the detected codeword c'. (10 pts)

Problem A4

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

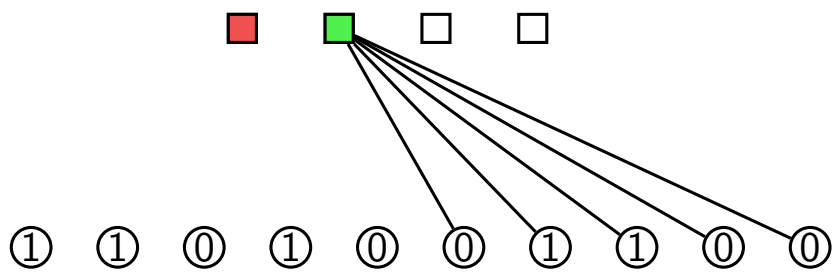
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

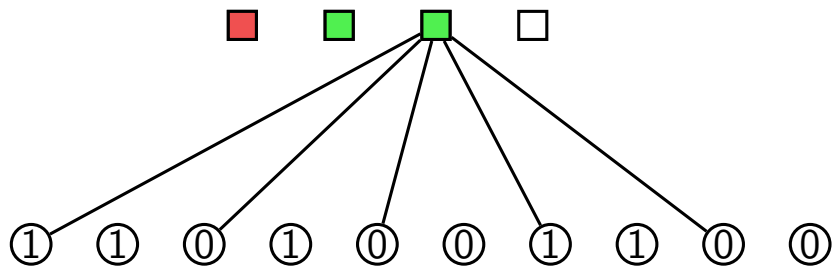
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

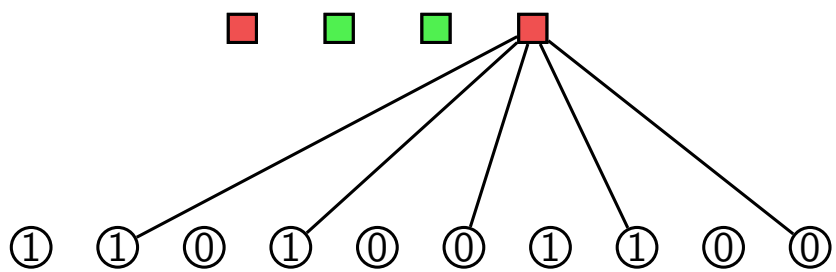
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

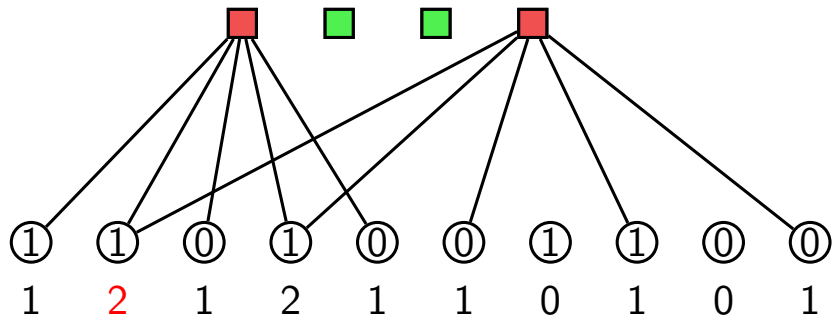
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

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



Problem A4

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

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

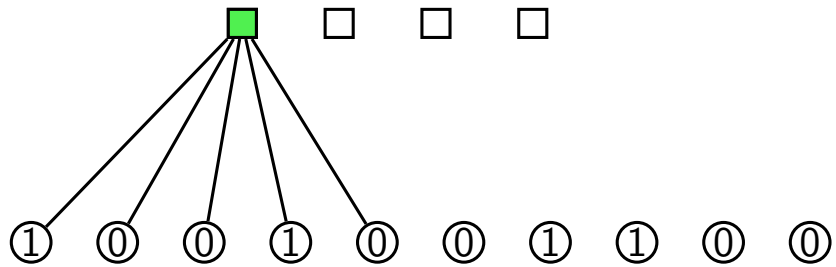
□ □ □ □

① 0 ⓪ ① ⓪ ⓪ ① ① ⓪ ⓪

Problem A4

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

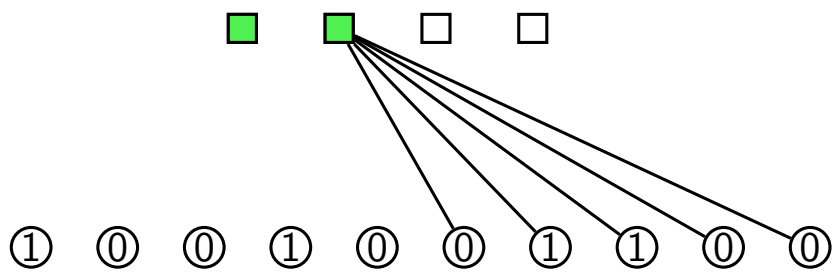
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

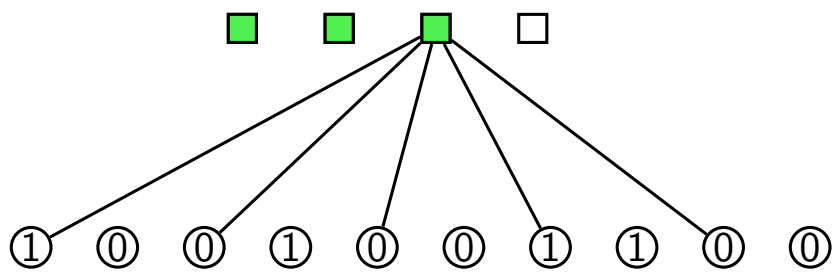
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

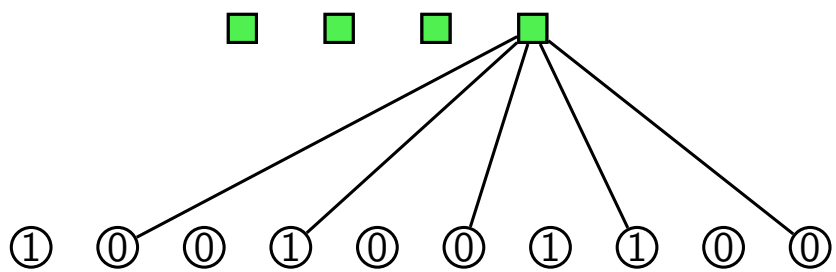
$$v = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$



Problem A4

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

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



Problem A4

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

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

$$\textcircled{1} \quad \textcircled{0} \quad \textcircled{0} \quad \textcircled{1} \quad \textcircled{0} \quad \textcircled{0} \quad \textcircled{1} \quad \textcircled{1} \quad \textcircled{0} \quad \textcircled{0}$$

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

Problem A5

Design a code over GF(5) that can correct 1 error by generator matrix. (Primitive elements over GF(5) are 2 and 3.)

(a) What are the code parameters? (2 pts)

(b) Calculate the code rate. (2 pts)

(c) Determine the generator matrix of the code. (3 pts)

(d) Calculate the codeword corresponding to the message vector whose digits are all 3's. (3 pts)

We make a Reed–Solomon code over GF(5).

(a) $n = 5 - 1 = 4$. RS codes can correct $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors, and from $\left\lfloor \frac{n-k}{2} \right\rfloor = 1$, we have $k = 2$ (or $k = 1$, but $k = 2$ is better).

(b) For a C(4,2) code, the code rate is $2/4 = 0.5$.

Problem A5

(c) Determine the generator matrix of the code. (3 pts)

We need to pick a primitive element α. For $\alpha = 2$ or 3 respectively, the generator matrix is

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{bmatrix} \qquad G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

(d) Calculate the codeword corresponding to the message vector whose digits are all 3's. (3 pts)

$$(3\,3) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{bmatrix} = (1\,4\,0\,2)$$

$$(3\,3) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \end{bmatrix} = (1\,2\,0\,4)$$

Problem B1

A. Any $C(n, k)$ binary code has 2^n codewords.

False. There are 2^k codewords.

B. Perfect $C(n, k)$ codes have minimal code distance $d_{\min} = n - k + 1$.

False. For perfect codes, the Hamming-bound holds with equality, not the Singleton bound.

C. The code rate of a $C(n, k)$ code is k/n.

True.

D. For a systematic linear binary code, the rightmost $(n - k) \times (n - k)$ block of H is the identity matrix.

True. The size of H is $(n - k) \times n$, so the rightmost square block is $(n - k) \times (n - k)$.

E. Reed-Solomon codes are MDS codes.

True.

Problem B2

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

$$(100) \quad \rightarrow \quad \{(10011), (01010), (00100), (11101)\}.$$

(a) Which is the group leader? (2 pts)

(b) What are the parameters of the code? (2 pts)

(c) List the codewords. (2 pts)

(d) Compute the generator matrix and parity check matrix. (2 pts)

(e) How many errors can the code detect? How many errors can the code correct? (2 pts)

Problem B2

(a) Which is the group leader? (2 pts)

The group leader from the error group is the vector with minimal weight, so (00100).

(b) What are the parameters of the code? (2 pts)

Each error group contains $2^k = 4$ received vectors $\rightarrow k = 2$. The length of each received vector is $n = 5$. This is a C(5,2) code.

(c) List the codewords. (2 pts)

The codewords are obtained by adding of the group members to all of the vectors in the error group, so

$$c^{(1)} = (10011) + (10011) = (00000)$$
$$c^{(2)} = (01010) + (10011) = (11001)$$
$$c^{(3)} = (00100) + (10011) = (10111)$$
$$c^{(4)} = (11101) + (10011) = (01110)$$

Problem B2

(d) Compute the generator matrix and parity check matrix. (2 pts)

G can be put together from the codewords assigned to the messages (10) and (01). The code is systematic, so $(10) \to (10111), (01) \to (01110)$, and

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

$H = [B^T|I]$ is obtained from $G = [I|B]$:

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

Problem B2

(e) How many errors can the code detect? How many errors can the code correct? (2 pts)

The codewords from part (c) are
$(00000), (11001), (10111), (01110)$.

The minimal weight among nonzero codewords is $d_{\text{min}} = 3$, so the code can

- detect $d_{\text{min}} - 1 = 2$ errors, and
- correct $\left\lfloor \frac{d_{\text{min}}-1}{2} \right\rfloor = 1$ error.

Problem B3

A binary linear code has parity check matrix

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

(a) What are the code parameters? (2 pts)

(b) Is this a Hamming code? (2 pts)

(c) Decode the received vector $v = (0\,1\,0\,1\,1\,0\,0)$. Describe how the error vector is detected based on the syndrome, then decode the message. (6 pts)

(a) What are the code parameters? (2 pts)

H has size $(n-k) \times n$, so $n-k=3, n=7$, then $k=4$, and this is a C(7,4) code.

Problem B3

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

(b) Is this a Hamming code? (2 pts)

Yes, it is! The columns of H are all nonzero binary vectors of length $n - k = 3$. (Also, the rightmost block of H is the identity matrix, so the code is systematic.)

(c) Decode the received vector $v = (0\,1\,0\,1\,1\,0\,0)$. Describe how the error vector is detected based on the syndrome, then decode the message. (6 pts)

Problem B3

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

(c) To decode, we first compute the syndrome vector

$$s = vH^T = (1\,0\,1).$$

For Hamming codes, we find the column of H corresponding to s. It is column $1 \rightarrow$

$$e' = (1000000)$$
$$c' = v + e' = (0101100) + (1000000) = (1101100)$$
$$u' = (1101)$$

because the code is systematic.

Problem B4

A binary CRC code adds 3 bits to each message, with parameter vector $d = (011)$.

(a) What is the codeword corresponding to the message $u = (1011101)$? (5 pts)

(b) Does the code detect the error for $e = (0001001000)$? (5 pts)

First we extend both u and d:

$$\begin{aligned} u = (1011101) &\quad \rightarrow \quad (1011101000) \\ d = (011) &\quad \rightarrow \quad (1011) \end{aligned}$$

Problem B4

(a) Coding:

1	0	1	1	1	0	1	0	0	0
1	0	1	1						
0	0	0	0	1	0	1	0	0	0
$\rightarrow$				1	0	1	1		
0	0	0	0	0	0	0	1	0	0

The codeword is the last 3 bits appended to the original message, so

$$c = (1\,0\,1\,1\,1\,0\,1\,1\,0\,0)$$

Problem B4

(b) Error detection:

0	0	0	1	0	0	1	0	0	0
			1	0	1	1			
0	0	0	0	0	1	0	0	0	0
$\rightarrow$					1	0	1	1	
0	0	0	0	0	0	0	1	1	0

Last 3 bits are nonzero $\rightarrow$ error detected.

Problem B5

Consider GF(8) with reducing polynomial $p(y) = y^3 + y + 1$. Design a code over GF(8) that can correct 1 error by generator polynomial.

(a) Determine the generator polynomial of the code. (2 pts)

(b) Calculate the code rate. (2 pts)

(c) When using this code to transmit a message over a channel with digit error probability $p = 0.01$, what is the probability of a decoding error? (6 pts)

We can design either a BCH or RS code.

(a) For the RS code, parameters are $n = 7, k = 5$, and the generator polynomial is

$$g(x) = (x - y)(x - y^2).$$

For the BCH code, we need y^1 and y^2 among the roots of $g(x)$, and they belong to the conjugate group $\{y^1, y^2, y^4\}$ with minimal polynomial $x^3 + x + 1$, so

$$g(x) = x^3 + x + 1$$

Problem B5

(b) Calculate the code rate. (2 pts)

The degree of $g(x)$ is $n - k$, so the RS code is a C(7,5) code with code rate $5/7$, and the BCH code is a C(7,4) code with code rate $4/7$.

(c) When using this code to transmit a message over a channel with digit error probability $p = 0.01$, what is the probability of a decoding error? (6 pts)

$$1 - (1 - p)^7 - 7p(1 - p)^6 \approx 0.00203$$