Fundamentals Of Information Science **2022 Spring**

Homework5

学生: 华园（202000120027）） *时间: 2022.3.23*

Problem 1.

Consider the discrete memoryless channel $Y_i = Z_i X_i$ with input alphabet $X_i \in \{-1, 1\}$.
(a) What is the capacity of this channel when $\{Z_i\}$ is i.i.d. with

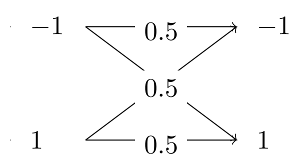
$$Z_i = \begin{cases} 1 & \text{p} = 0.5 \\ -1 & \text{p} = 0.5 \end{cases}$$

(b) Now consider the channel with memory. Before transmission begins, Z is randomly chosen and fixed for all time. Thus, $Y_i = Z X_i$. What is the capacity if

$$Z = \begin{cases} 1 & \text{p} = 0.5 \\ -1 & \text{p} = 0.5 \end{cases}$$

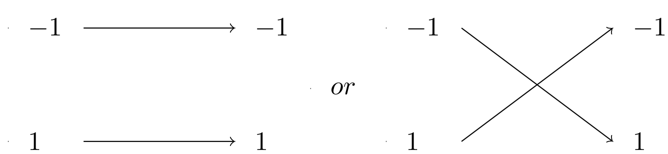
Solution.

(a)



$$C = max(I(X;Y)) = max[H(Y) - H(Y|X)] = 1 - 1 = 0$$

(b)



$$C = 0.5max(I_1(X;Y)) + 0.5max(I_2(X;Y)) = 0.5 + 0.5 = 1$$

Problem 2.

Neo receives a 7-bit string, $D_1 D_2 D_3 D_4 P_1 P_2 P_3$ from Morpheus, sent using a code, $\mathcal{C}$, with parity equations

$$P_1 = D_1 + D_2 + D_3$$
$$P_2 = D_1 + D_2 + D_4$$
$$P_3 = D_1 + D_3 + D_4$$

(a)Write down the generator matrix, G, for $\mathcal{C}$. (b)Write down the parity check matrix, H, for $\mathcal{C}$. (c)If Neo receives 1000010 and does maximum-likelihood decoding on it, what would his estimate of the data transmission $D_1D_2D_3D_4$ from Morpheus be? For your convenience, the syndrome s_i corresponding to data bit D_i being wrong are given below, for $i = 1, 2, 3, 4$:

$$s_1 = (111)^T, s_2 = (110)^T, s_3 = (101)^T, s_4 = (011)^T.$$

(d)If Neo uses syndrome decoding for error correction, how many syndromes does he need to compute and store for this code, including the syndrome with no errors?

Solution.

(a)because $P_1 = D_1 + D_2 + D_3, P_2 = D_1 + D_2 + D_4, P_3 = D_1 + D_3 + D_4$,we can get:

$$[D_1, D_2, D_3, D_4] \cdot G = [D_1, D_2, D_3, D_4, P_1, P_2, P_3]$$

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

(b)According to G,we can also get:

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

(c)

$$S = H \cdot r^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}^T$$

Therefore, we believe that D_3 occurred an error in the transmission process

$$D_1D_2D_3D_4 = 1010$$

(d) If there is only one error in 7-bit coding, there are 7 cases in total. Plus the case that there is no error, a total of 8 syndromes are required

Problem 3.

For any linear block code over $\mathbb{F}_2$ with minimum Hamming distance at least $2\mathrm{t}+1$ between codewords, show that:

$$2^{n-k} \geq 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t}.$$

Hint: How many errors can such a code always correct?
For each (n, k, d) combination below, state whether a linear block code with those parameters exists or not. Please provide a brief explanation for each case: if such a code exists, give an example; if not, you may rely on a suitable necessary condition.
(a) $(31, 26, 3)$: Yes / No
(b) $(32, 27, 3)$: Yes / No
(c) $(43, 42, 2)$: Yes / No
(d) $(27, 18, 3)$: Yes / No
(e) $(11, 5, 5)$: Yes / No

Solution.

最小汉明顿距离为2t+1的线性分组码可以纠正至多t个错误，码字长度为n，当发生a个错误时，有C_n^a种情况，所以全部可纠正错误的个数为：

$$\binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t}.$$

sysndromes 可以代表的错误个数为：

$$2^{n-k} - 1$$

减一代表减去全部传输正确的情况，即S=0的情况。
为了在解码过程中能够根据sysndromes纠正错误，所以sysndromes所能代表的错误个数必须要大于或者等于可以纠正的错误的个数，因此满足以下不等式：

$$2^{n-k} - 1 \geq \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{th}.$$

从而可以获得：

$$2^{n-k} \geq 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t}.$$

(a)YES, $\frac{d-1}{2} = 1$ and $2^{n-k} - 1 = 31 = n$,this code exists and the example is Hamming code.
(b)NO, $\frac{d-1}{2} = 1$ and $2^{n-k} - 1 = 31 < n$,this code doesn't exist.
(c)NO, $\frac{d-1}{2} = 0.5$,thus this code can not correct the error,this code doesn't exist
(d)YES, $\frac{d-1}{2} = 1$ and $2^{n-k} - 1 = 511 > n$,this code exists
(e))NO, $\frac{d-1}{2} = 2$ and $2^{n-k} - 1 = 63 < n + n(n-1)/2 = 66$,this code doesn't exist.

Problem 4.

(a) List the elements in Galois field $GF\left(2^3\right)$ of primitive $x^3 + x + 1$ as successive powers of the primitive element x.
(b) Construct a Reed-Solomon Code with $n = 5$ and $k = 3$, and use this code to encode a sequence 001010011 (first converting 001,010,011 to elements in $GF\left(2^3\right)$). Please show how the codeword is generated.

Solution.

(a)

$$
\begin{aligned}
\alpha^0 &= \qquad\quad 1\\
\alpha^1 &= \qquad x\\
\alpha^2 &= x^2\\
\alpha^3 &= \qquad x+1\\
\alpha^4 &= x^2+x\\
\alpha^5 &= x^2+x+1\\
\alpha^6 &= x^2 \quad + \quad 1\\
\alpha^7 &= \qquad\quad 1
\end{aligned}
$$

(b)

$$\beta_1 = 0 \qquad \beta_2 = 1 \qquad \beta_3 = x \qquad \beta_4 = x^2$$
$$\beta_5 = x+1 \qquad \beta_6 = x^2+x \qquad \beta_7 = x^2+x+1 \qquad \beta_8 = x^2+1$$

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \beta_4^2 & \beta_5^2 \end{bmatrix}$$

$$(001, 010, 011) \rightarrow (1, x, x+1)$$

$$M = \begin{bmatrix} 1 & \text{x} & x+1 \end{bmatrix}$$

Accoring to C=M • A, we can get:

$$
\begin{aligned}
C_1 &= m_0 + m_1\beta_1 + m_2\beta_1^2 = 1\\
C_2 &= m_0 + m_1\beta_2 + m_2\beta_2^2 = 0\\
C_3 &= m_0 + m_1\beta_3 + m_2\beta_3^2 = x\\
C_4 &= m_0 + m_1\beta_4 + m_2\beta_4^2 = x+1\\
C_5 &= m_0 + m_1\beta_5 + m_2\beta_5^2 = x+1
\end{aligned}
$$

so the code is (1,0,x,x+1,x+1)