DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

EEE416(18/19) Coding and Cryptography

Lab 1 - Source coding and channel capacity

EEE416

Lab Report

Student Name	:	Enge Xu
Student ID	:	1821635
Date	:	2019/5/12
Professor	:	Liming Yu

ABSTRACT

This assessment aims at evaluating students' understanding and problem solving skills involved in channel coding and cryptography, which are accumulated during lectures, tutorials and after-class study.

TASK

Question 1: Entropy, Joint Entropy and Mutual Information (25 points)

Consider the systematic (7, 4) Hamming code. The parity-bit generator matrix P is shown below.

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

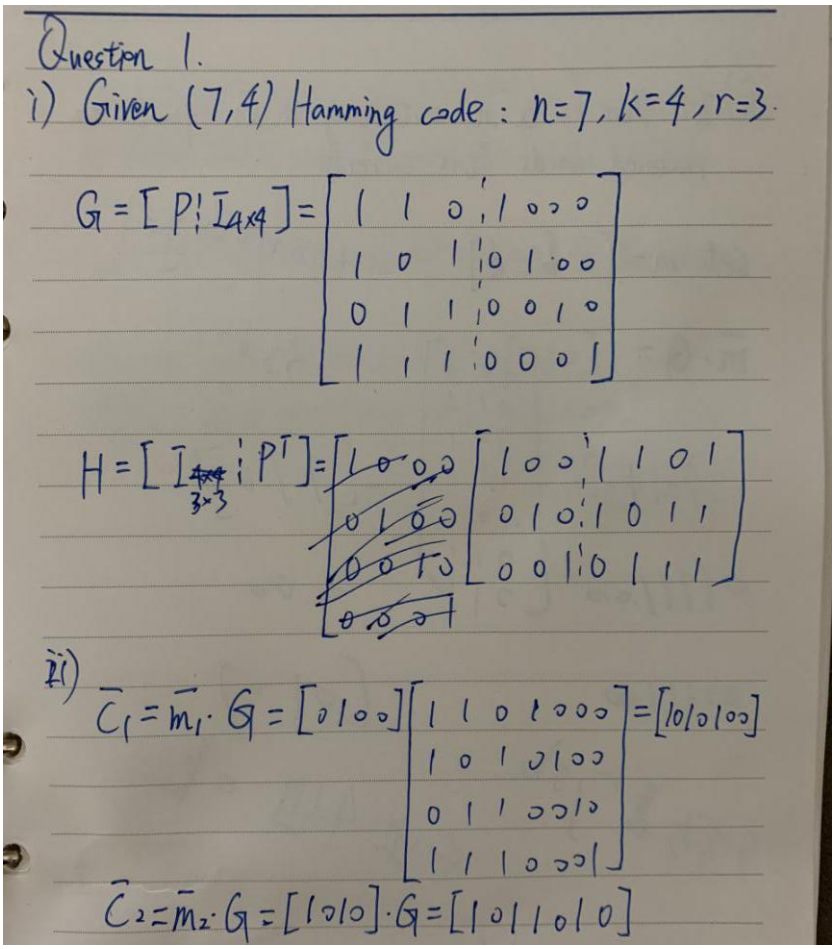
i) Give the corresponding generator matrix G and the parity check matrix H. (4 points)

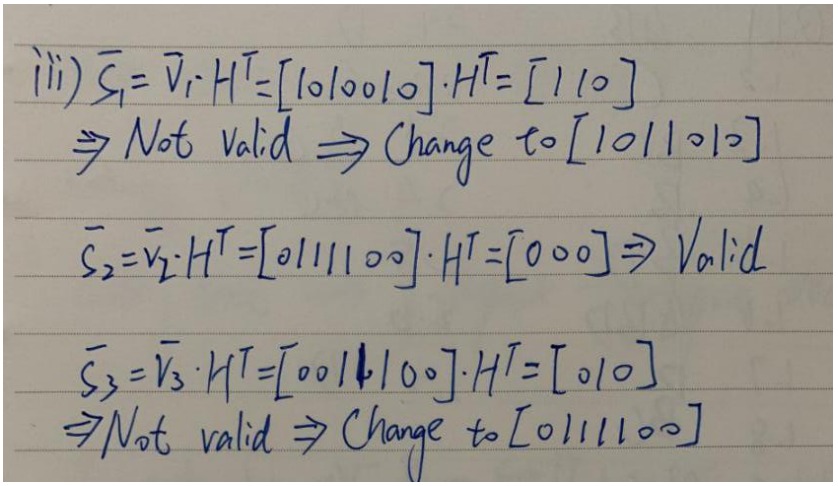
ii) Generate the code words for the following messages: 0100, 1010. (8 points)

iii) Determine whether the received words 1010010, 0111100, 0011100 are valid code words using the syndrome decoding and correct if necessary. Decode the codewords to recover the original messages. (13 points)

Solution

The answer is shown as below;





Question 2: Cyclic Codes (24 points)

Consider a (*n*, *k*) cyclic redundancy check (CRC) code. Verify if the following generator polynomials are able to catch certain types of errors.

i) Single-bit of error with error polynomial of $e(x) = x^i$:

$g(x) = x + 1$; *(6 points)*

$g(x) = x^5$; *(6 points)*

ii) Two isolated single-bit errors with error polynomial of $e(x) = x^j + x^i$:

$g(x) = x^2 + 1$; *(6 points)*

$g(x) = x^{14} + x^{13} + 1$. *(6 points)*

Solution

i)

From the reference book, it can be seen that if G(x) has 2 or more polynomial, E(x)/G(x) can not be 0, so the error can be caught.
G(x) = x + 1 has 2 polynomial, CRC can catch the error.

G(x) = x^5 has 1 polynomial, CRC can not catch the error.

ii)

If we assume that G(x) is not divisible by x, then the sufficient condition that we can detect all two errors is that G(x) is not divisible for all values that are not greater than i minus j.

For G(x) = $x^2 + 1$, if i-j > 2, it can catch two isolated single-bit error.

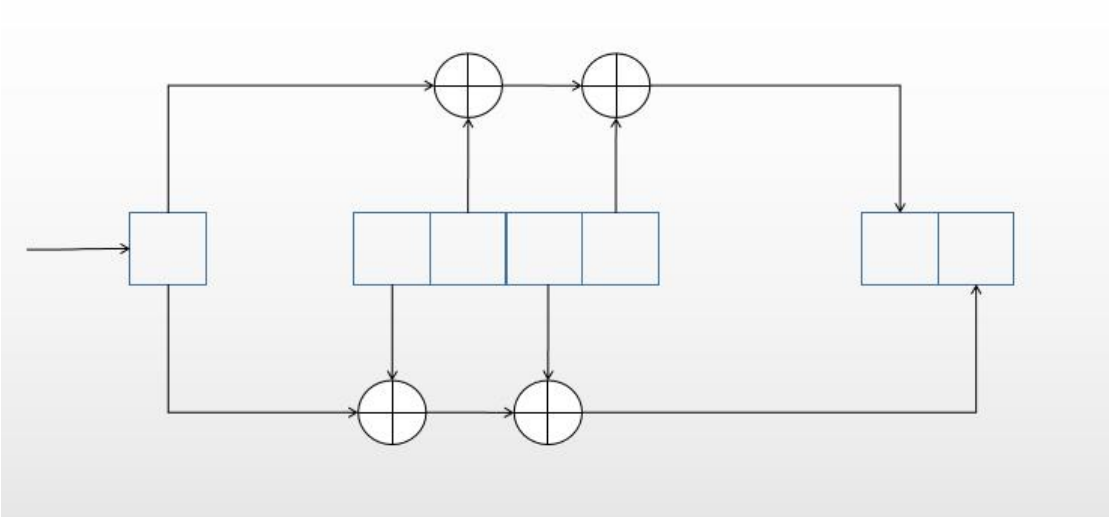
For G(x) = $x^{14} + x^{13} + 1$, if i-j> 14, it can catch two isolated single-bit error.

Question 3: Convolutional Codes (26 points)

Design a rate 1/2 convolutional encoder with a constraint length v = 4 and d* = 6.
i) Construct the State Diagram of this encoder. (6 points)
ii) Construct the Trellis Diagram of this encoder. (6 points)
iii) What is the dfree of this code. (4 points)
iv) Determine the Generator Matrix G. (6 points)
v) Is this code Non-Catastrophic? Why? (4 points)

Solution

Because the rate is 1/2, v = 4 and d* = 6, the input output and the model can be ensured.
The model can be shown as below;

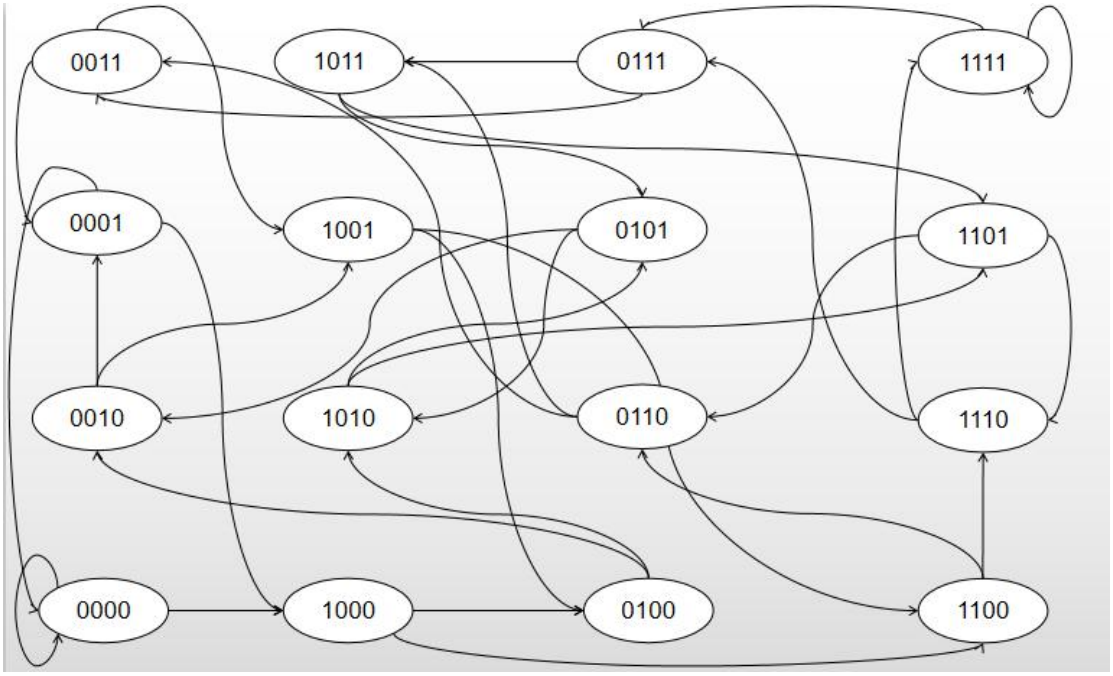


So the input bit, state of encoder and output bit can be listed;

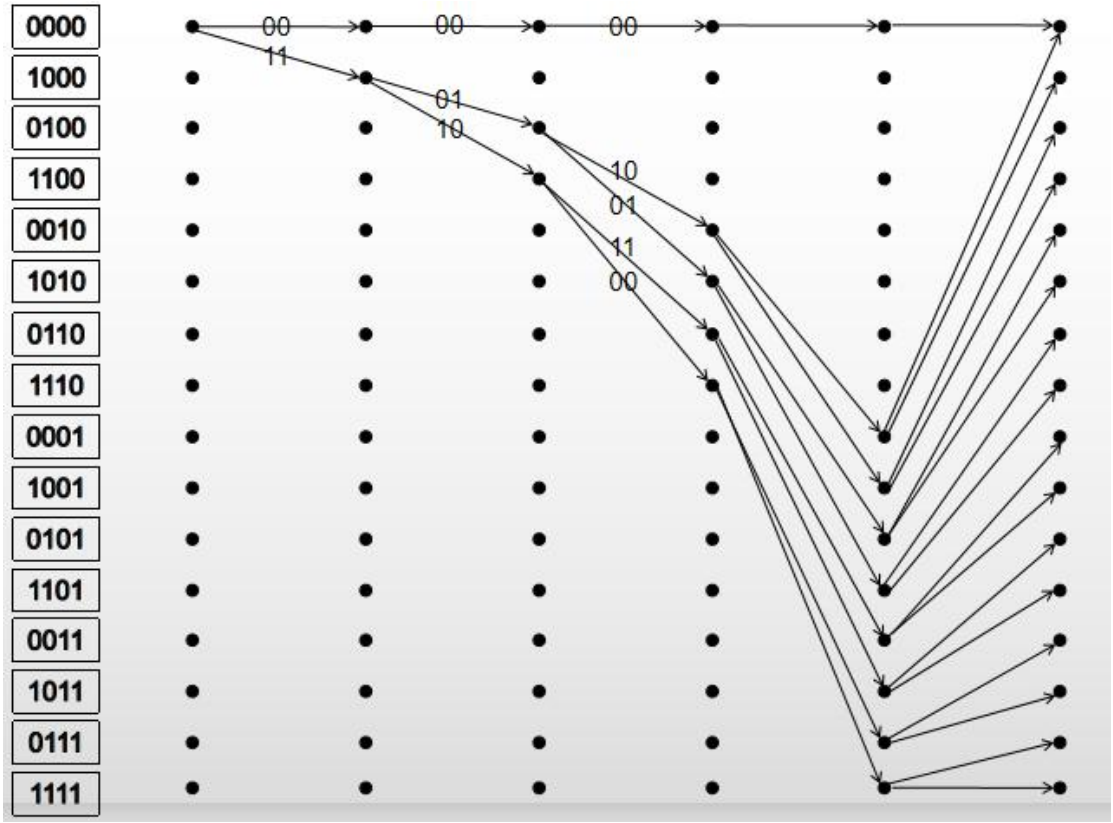
Input bit	The state of encoder	Output bit
0	0000	00
1	0000	11
0	1000	01
1	1000	10
0	0100	10
1	0100	01
0	1100	11
1	1100	00
0	0010	01
1	0010	10
0	1010	00
1	1010	11
0	0110	11
1	0110	00
0	1110	10
1	1110	01
0	0001	10
1	0001	01
0	1001	11
1	1001	00
0	0101	00
1	0101	11
0	1101	01
1	1101	10
0	0011	11
1	0011	00
0	1011	10
1	1011	01
0	0111	01
1	0111	10
0	1111	00
1	1111	11

The answer is shown as below;

i)



ii)



iii) dfree = 6.

iv)

According to the convolutional encoder, it can be achieved that

$n_1 = 1 + D^2 + D^4$

$n_2 = 1 + D + D^3$

Therefore, the Generator Matrix G is

G[D] = $[1 + D^2 + D^4, 1 + D + D^3]$

v)

G[D] = $[1 + D^2 + D^4, 1 + D + D^3]$

GCD = 1

Therefore, the code is Non-Catastrophic.

Question 4: Cryptography (25 points)

Given two prime numbers 29 and 61, calculate

i) Public key for the RSA algorithm. (10 points)
ii) Private key for the RSA algorithm. (15 points)

Solution

i) The two prime numbers are:
p = 29, q = 61, then there are
n = p.q = 29 * 61 = 1769;
x = (p-1) (q-1) = 28 * 60 = 1680.
The public key ‘e’ is relative prime to x.
e = 11.
ii) Given k = 11, the private key d sanctifies
d × e = 1 (mod x)
or the greatest common divisor GCD(x, e) = 1.
d is calculated by calculating the multiplicative inverse of e modulo x.

i	Quotient q	Reminder r	s	t
0		r0 = 1680	1	0
1		R1 = 11	0	1
2	1680/11 = 152	1680-152*11 = 8	1-152*0 = 1	0-152*1 = -152
3	11/8 = 1	11-1*8 = 3	0 - 1*1 = -1	1-1*(-152) = 153

4	8/3 = 2	8 - 2*3 = 2	1- 2*(-1) = 3	-152 - 2*153 = 458
5	3/2 = 1	2- 1*2 = 1	-1 - 1*3 = -4	153 - 1(-458) = 611

GCD(1680,11) = 1 = -4 *1680 +611*11

PRIVATE KEY = {1769,611}