Homework 2 - Naiara Alonso Montes

Problem 1

Formulate the information set decoding rule

1. For each information set I, calculate syndrome $s = y - H_1 x_1$, where y is the received word, H_1 is the parity-check matrix corresponding to the information set I, and x_1 is the information bits corresponding to the information set I.
2. If the syndrome s is zero, then the decoded codeword is $x = [x_1], H_I^{-1} s]$.
3. Otherwise, continue to the next information set.
4. If no information set results in a zero syndrome, then a decoding error has ocurred.

Estimate the probability that a 8×8 submatrix of a generator matrix of the $[16, 8]$ random linear code is non-degenerated.

- A square matrix is non-degenerate if its determinant is non-zero.
- Probability of a non-zero product is $(q-1)/q$, where q is the field size.
- Calculate the probability of the 8×8 matrix determinant to be non-zero.

Probability of at least one non-zero product

$$1 - (\frac{q-1}{q})^n, \text{ where n is the number of product terms}$$

Number of product terms

$$n = 8!$$

Final approach

$$1 - (\frac{q-1}{q})^{8!}$$

By using Striling approximation $n! = \sqrt{2\pi n}(\frac{n}{e})^n$ show that asymptotically $\binom{n}{\rho} \approx n^{nh\frac{\rho}{n}}$, where $h(x)$ is the binary entropy function.

$$\binom{n}{p} \approx \frac{\sqrt{2\pi n}(\frac{n}{e})^n}{\sqrt{2\pi(n-\rho)}(\frac{n-\rho}{e})^(n-\rho) * \sqrt{2\pi\rho}(\frac{\rho}{e})^\rho}$$

$$\binom{n}{\ } \approx \quad n^n \quad * \sqrt{\quad 1}$$

$$\binom{n}{\rho} \sim \frac{}{\sqrt{2\pi n} * (n-\rho)^(n-\rho) * \rho^\rho} * \sqrt{\frac{}{2\pi(n-\rho)\rho}}$$

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$$

$$\binom{n}{\rho} \approx \frac{n^n}{\sqrt{2\pi n} * 2^(n * h(\rho/n))} * \sqrt{\frac{1}{2\pi(n-\rho)\rho}}$$

$$\binom{n}{\rho} \approx n^n * 2^{-n*h(\rho/n)}$$

$$\binom{n}{\rho} \approx n^n * e^{-n*h(\rho/n)*\log_e(2)}$$

$$\binom{n}{\rho} \approx n^{n-n*h(\rho/n)}$$

$$\binom{n}{\rho} \approx n^{nh(\rho/n)}$$

How many information set has the binary linear $[9,4]$ code with generator matrix?

$$\binom{9}{4} = \frac{9!}{4! \cdot 5!} = 126$$

Problem 2

Find the primitive element of GF(13)

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$2^1=2,\ 2^2=4,\ 2^3=8,\ 2^4=3,\ 2^5=6,\ 2^6=12,\ 2^7=11,\ 2^8=9,\ 2^{10}=10,\ 2^{11}=7,\ 2^{12}=1$ 12^{p-1}

$3^1=3,\ 3^2=9,\ 3^3=1$ 3

$4^1=4,\ 4^2=3,\ 4^3=12,\ 4^4=9,\ 4^5=10,\ 4^6=1$ 6

$5^1=5,\ 5^2=12,\ 5^3=8,\ 5^4=1$ 4

$6^1=6,\ 6^2=10,\ 6^3=8,\ 6^4=9,\ 6^5=2,\ 6^6=12,\ 6^7=7,\ 6^8=3,\ 6^9=5,\ 6^{10}=4,\ 6^{11}=11,\ 6^{12}=1$ 12^{p-1}

$7^1=7,\ 7^2=10,\ 7^3=5,\ 7^4=9,\ 7^6=11,\ 7^6=12,\ 7^7=6,\ 7^8=3,\ 7^9=8,\ 7^{10}=4,\ 7^{11}=2,\ 7^{12}=1$ 12^{p-1}

$8^1=8,\ 8^2=12,\ 8^3=5,\ 8^4=1$ 4

$9^1=9,\ 9^2=3,\ 9^3=1$ 3

$10^1=10,\ 10^2=9,\ 10^3=12,\ 10^4=3,\ 10^5=4,\ 10^6=1$ 6

$11^1=11,\ 11^2=4,\ 11^3=5,\ 11^4=3,\ 11^5=7,\ 11^6=12,\ 11^7=2,\ 11^8=9,\ 11^9=8,\ 11^{10}=10,\ 11^{11}=6,\ 11^{12}=1$ 12^{p-1}

$12^1 = 12, 12^2 = 1$ (2)

Primitive elements of GF(13) are 2, 6, 7 and 11.

Find the multiplicative orders of all elements in GF(13)

Element	2	3	4	5	6	7	8	9	10	11	12
Multiplication order	12	3	6	4	12	12	4	3	6	12	2

Find the order of the multiplicative group of GF(13)

Since GF(13) group has 13 elements and 0 is not included in the multiplicative group, the multiplicative group if GF(13) is 12. Therefore the **order of the multiplicative group is 12**.

Find the inverse for element 3 in GF(13)

Based on the results of the first exercise, $3^3 = 27$, in modulo 13, $3^3 = 1 = 3^1 \cdot 3^2$, so the inverse of 3 in this group field is $3^2 = 9$.

Compute expression $4 \cdot 5 + \frac{3}{7}$

Divide expression in parts:

- $4 \cdot 5 = 20$, in modulo 13, 7
- $\frac{3}{7} = 3 \cdot 7^{-1}$, what is the inverse of 7? Acording to the previous exercise, $7^{12} = 1$. so $7^1 \cdot 7^{11} = 1$ in modulo 13, 11 is the inverse of 7. $3 \cdot 11 = 33$, in modulo 13, 7.

Puting all together:

- $7 + 7 = 14$, 14 in modulo 13 equals 1.

Problem 3

Construct extension fiedl GF(2^5) by using polynomial $x^5 + x^2 + 1$

By using the Matlab code, it return the integers of the binary representation of polynomials. Now I transform those integers into binary representation.

Powers of alpha	Polynomial
$\alpha^{-\infty}$	00000
$\alpha^0 = 1$	00001

α^1	00010
α^2	00100
α^3	01000
α^4	10000
$\alpha^5 = \alpha^2 + 1$	00101
$\alpha^6 = \alpha^3 + \alpha$	01010
$\alpha^7 = \alpha^4 + \alpha^2$	10100
$\alpha^8 = \alpha^3 + \alpha^2 + 1$	01101
$\alpha^9 = \alpha^4 + \alpha^3 + \alpha$	11010
$\alpha^{10} = \alpha^4 + 1$	10001
$\alpha^{11} = \alpha^2 + \alpha + 1$	00111
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha$	01110
$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2$	11100
$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha^2 + 1$	11101
$\alpha^{15} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	11111
$\alpha^{16} = \alpha^4 + \alpha^3 + \alpha + 1$	11011
$\alpha^{17} = \alpha^4 + \alpha + 1$	10011
$\alpha^{18} = \alpha + 1$	00011
$\alpha^{19} = \alpha^2 + \alpha$	00110
$\alpha^{20} = \alpha^3 + \alpha^2$	01100
$\alpha^{21} = \alpha^4 + \alpha^3$	11000
$\alpha^{22} = \alpha^4 + \alpha^2 + 1$	10101
$\alpha^{23} = \alpha^3 + \alpha^2 + \alpha + 1$	01111
$\alpha^{24} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	11110
$\alpha^{25} = \alpha^4 + \alpha^3 + 1$	11001
$\alpha^{26} = \alpha^4 +$	

$\alpha = \alpha + \alpha^3 + \alpha^2 + \alpha$	10111
$\alpha^{27} = \alpha^3 + \alpha + 1$	01011
$\alpha^{28} = \alpha^4 + \alpha^2 + \alpha$	10110
$\alpha^{29} = \alpha^3 + 1$	01001
$\alpha^{30} = \alpha^4 + \alpha$	10010
$\alpha^{31} = 1$	00001 **it repeats**

Find the inverse of α^{19}

$$\alpha^{19} \cdot \alpha^{x} = 1$$
$$00110 \cdot XXXXX = 00001$$
$$XXXXX = 00111 = \alpha^{11}$$

Compute $\alpha^{12} \cdot \alpha^{25} + \frac{\alpha 10}{\alpha^{19}}$

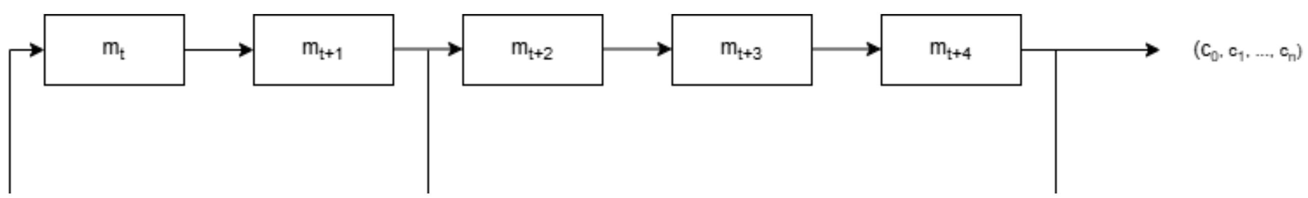
- $\alpha^{12} \cdot \alpha^{25} + \alpha 10 \cdot \alpha^{11}$
- $\alpha^{37} + \alpha^{21}$ in mod 32
- $\alpha^{5} + \alpha^{21} = \alpha^2 + 1 + \alpha^4 + \alpha^3 = \alpha^4 + \alpha^3 + \alpha^2 + 1 = \alpha^{14} = 11101$

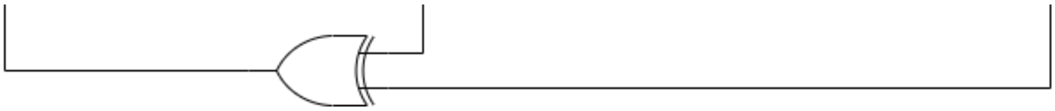
Find the minimal polynom for α^5

$$m^5(x) = (x - \alpha^{5\cdot 1})(x - \alpha^{5\cdot 2})(x - \alpha^{5\cdot 4})(x - \alpha^{5\cdot 8})(x - \alpha^{5\cdot 16})$$
$$(x - \alpha^{5})(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^{9})(x - \alpha^{18})$$

Problem 4

Draw scheme generating the maximal length sequence of $x^5 + x^2 + 1$ or equivalent scheme of encoder of [31, 5]-code.





Starting with the initial state 00101, show that 31 sequential states of the generator (encoder) are diferent

Step	State	Output
0	00101	1
1	10010	0
2	01001	1
3	00100	0
4	00010	0
5	00001	1
6	10000	0
7	01000	0
8	10100	0
9	01010	0
10	10101	1
11	11010	0
12	11101	1
13	01110	0
14	10111	1
15	11011	1
16	01101	1
17	00110	0
18	00011	1
19	10001	1
20	11000	0
21	11100	0
22	11110	0
23	11111	1
24	01111	1
25	00111	1
26	10011	1
27	11001	1
28	01100	0
29	10110	0
30	01011	1

Problem 5

Construct cyclic codes of lengths $n = 3..7$. Compute code rate and minimum distance of the constructed codes and their duals

$$c(x) = m(x) \cdot g(x)$$

Case $n = 3$

$$(x^3 - 1) = (a^3 - b^3) = (a - b)(a^2 + ab + a^2) = (x - 1)(x^2 + +1)$$
$$\text{Take } g(x) = (x - 1) \text{ as generator polynom}$$
$$\text{Degree of } g(x) \text{ is } 1,\ k = 3 - 1 = 2$$
$$c(x) = (m_0, m_0) \cdot g(x) = (0, 0) \cdot (x - 1) = 0 \equiv 000$$
$$c(x) = (m_0, m_1) \cdot g(x) = (0, 1) \cdot (x - 1) = x - 1 \equiv 011$$
$$c(x) = (m_1, m_0) \cdot g(x) = (1, 0) \cdot (x - 1) = x^2 - x \equiv 110$$
$$c(x) = (m_1, m_1) \cdot g(x) = (x + 1) \cdot (x - 1) = x^2 - 1 \equiv 101$$

Code rate: $\frac{k}{n} = \frac{2}{3}$

Minimum distance: 1

Case $n = 4$

$$(x^4 - 1) = (a^4 - b^4) = (a^2 - b)(a^2 + ab + a^2) = (x^2 - 1)(x^2 + +1)$$
$$\text{Take } g(x) = (x^2 - 1) \text{ as generator polynom}$$
$$\text{Degree of } g(x) = (x^2 - 1) \text{ is } 2,\ k = 4 - 2 = 2$$
$$c(x) = (m_0, m_0) \cdot g(x) = (0, 0) \cdot (x^2 - 1) = 0 \equiv 0000$$
$$c(x) = (m_0, m_1) \cdot g(x) = (0, 1) \cdot (x^2 - 1) = x - 1 \equiv 0101$$
$$c(x) = (m_1, m_0) \cdot g(x) = (1, 0) \cdot (x^2 - 1) = x^2 - x \equiv 1010$$
$$c(x) = (m_1, m_1) \cdot g(x) = (1, 1) \cdot (x^2 - 1) = x^2 - 1 \equiv 1111$$

Code rate: $\frac{k}{n} = \frac{2}{4}$

Minimum distance: 2

Case $n = 5$

$$(x^5 - 1) = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$
$$\text{Take } g(x) = (x - 1) \text{ as generator polynom}$$
$$\text{Degree of } g(x) = (x - 1) \text{ is } 1,\ k = 5 - 1 = 4$$
$$c(x) = (m_0, m_0, m_0, m_0) \cdot g(x) = (0, 0, 0, 0) \cdot (x - 1) = 0 \equiv 00000$$
$$c(x) = (m_0, m_0, m_0, m_1) \cdot g(x) = (0, 0, 0, 1) \cdot (x - 1) = x - 1 \equiv 00011$$
$$c(x) = (m_0, m_0, m_1, m_0) \cdot g(x) = (0, 0, 1, 0) \cdot (x - 1) = x^2 - x \equiv 00110$$
$$c(x) = (m_0, m_0, m_1, m_1) \cdot g(x) = (0, 0, 1, 1) \cdot (x - 1) = x^2 - 1 \equiv 00101$$
$$c(x) = (m_0, m_1, m_0, m_0) \cdot g(x) = (0, 1, 0, 0) \cdot (x - 1) = 0 \equiv 01100$$
$$c(x) = (m_0, m_1, m_0, m_1) \cdot g(x) = (0, 1, 0, 1) \cdot (x - 1) = 0 \equiv 01111$$
$$c(x) = (m_0, m_1, m_1, m_0) \cdot g(x) = (0, 1, 1, 0) \cdot (x - 1) = 0 \equiv 01010$$
$$c(x) = (m_0, m_1, m_1, m_1) \cdot g(x) = (0, 1, 1, 1) \cdot (x - 1) = 0 \equiv 01100$$
$$c(x) = (m_1, m_0, m_0, m_0) \cdot g(x) = (1, 0, 0, 0) \cdot (x - 1) = 0 \equiv 11000$$

$$c(x) = (m_1, m_0, m_0, m_1) \cdot g(x) = (1, 0, 0, 1) \cdot (x - 1) = 0 \equiv 11011$$
$$c(x) = (m_1, m_0, m_1, m_0) \cdot g(x) = (1, 0, 1, 0) \cdot (x - 1) = 0 \equiv 11110$$
$$c(x) = (m_1, m_0, m_1, m_1) \cdot g(x) = (1, 0, 1, 1) \cdot (x - 1) = 0 \equiv 11101$$
$$c(x) = (m_1, m_1, m_0, m_0) \cdot g(x) = (1, 1, 0, 0) \cdot (x - 1) = 0 \equiv 10100$$
$$c(x) = (m_1, m_1, m_0, m_1) \cdot g(x) = (1, 1, 0, 1) \cdot (x - 1) = 0 \equiv 10111$$
$$c(x) = (m_1, m_1, m_1, m_0) \cdot g(x) = (1, 1, 1, 0) \cdot (x - 1) = 0 \equiv 10001$$
$$c(x) = (m_1, m_1, m_1, m_1) \cdot g(x) = (1, 1, 1, 1) \cdot (x - 1) = 0 \equiv 10010$$

Code rate: $\frac{k}{n} = \frac{4}{5}$

Minimum distance: 2

Case $n = 6$

$$(x^6 - 1) = (x^4 - 1)(x^2 + 1)$$
$$\text{Take } g(x) = (x^4 - 1) \text{ as generator polynom}$$
$$\text{Degree of } g(x) = (x^4 - 1) \text{ is } 4,\ k = 6 - 4 = 2$$
$$c(x) = (m_0, m_0) \cdot g(x) = (0, 0) \cdot (x^4 - 1) = 0 \equiv 000000$$
$$c(x) = (m_0, m_1) \cdot g(x) = (0, 1) \cdot (x^4 - 1) = x - 1 \equiv 010001$$
$$c(x) = (m_1, m_0) \cdot g(x) = (1, 0) \cdot (x^4 - 1) = x^2 - x \equiv 100010$$
$$c(x) = (m_1, m_1) \cdot g(x) = (1, 1) \cdot (x^4 - 1) = x^2 - 1 \equiv 110011$$

Code rate: $\frac{k}{n} = \frac{4}{5}$

Minimum distance: 2

Case $n = 7$

$$(x^7 - 1) = (x^5 - 1)(x^2 + 1)$$
$$\text{Take } g(x) = (x^4 - 1) \text{ as generator polynom}$$
$$\text{Degree of } g(x) = (x^5 - 1) \text{ is } 5,\ k = 7 - 5 = 2$$
$$c(x) = (m_0, m_0) \cdot g(x) = (0, 0) \cdot (x^5 - 1) = 0 \equiv 0000000$$
$$c(x) = (m_0, m_1) \cdot g(x) = (0, 1) \cdot (x^5 - 1) = x - 1 \equiv 00100001$$
$$c(x) = (m_1, m_0) \cdot g(x) = (1, 0) \cdot (x^5 - 1) = x^2 - x \equiv 10010000$$
$$c(x) = (m_1, m_1) \cdot g(x) = (1, 1) \cdot (x^5 - 1) = x^2 - 1 \equiv 1100011$$

Code rate: $\frac{k}{n} = \frac{5}{7}$

Minimum distance: 2

Let a cyclic code of length $n = 9$ be determined by the generator polynomial $g(x) = 1 + x + x^2$

- Find the corresponding check polynomial $h(x)$

$$g(x) = \frac{x^n - 1}{h(x)}$$
$$h(x) = \frac{x^9 - 1}{x^2 + x + 1} = x^7 - x^6 + x^4 - x^3 + x - 1$$

$$x^2 + x + 1$$

- Write the corresponding code generator matrix

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

- Find the correxponding code parity-check matrix

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

```
import numpy as np

# Define the generator matrix G for n = 9 and g(x) = 1 + x + x^2
G = np.array([
    [1, 1, 1, 0, 0, 0, 0, 0, 0],
    [0, 1, 1, 1, 0, 0, 0, 0, 0],
    [0, 0, 1, 1, 1, 0, 0, 0, 0],
    [0, 0, 0, 1, 1, 1, 0, 0, 0],
    [0, 0, 0, 0, 1, 1, 1, 0, 0],
    [0, 0, 0, 0, 0, 1, 1, 1, 0],
    [0, 0, 0, 0, 0, 0, 1, 1, 1]
])

# Function to calculate Hamming distance between two binary vectors
def hamming_distance(a, b):
    return np.sum(a != b)

def generate_codewords(G):
    k, n = G.shape
    codewords = []
    for msg in range(2**k):
        message = np.array([int(x) for x in f"{msg:0{k}b}"])
        codeword = np.dot(message, G) % 2
        codewords.append(codeword)
    return np.array(codewords)

codewords = generate_codewords(G)

min_distance = float('inf')
for i in range(len(codewords)):
    for j in range(i + 1, len(codewords)):
        dist = hamming_distance(codewords[i], codewords[j])
        if dist < min_distance:
            min_distance = dist

print(f"Minimum distance is {min_distance}")
```

```
Minimum distance is 2
```