Leandro Jorge Fernández Vega
m = E-8298
n = 98

HOMEWORK NUMBER 2

Exercise 1.

Let r is the remainder of the division of n by 5.

a) Check if the following matrix A:

$$\begin{matrix} 1 & r & 1 \\ r & 0 & 1 \\ 0 & 1 & r \end{matrix}$$

is invertible in Z_6 .

b) *By* a sequential use of the three elementary operations on rows in Z_5, determine the inverse B^{-1} the following matrix B:

$$\begin{matrix} 1 & r & 1 \\ 0 & 0 & 1 \\ 0 & 1 & r \end{matrix}$$

Describe all the sequential steps.

$r = 98 \mod 5 = 3$

A) $A = \begin{pmatrix} 1 & 3 & 1 \\ 3 & 0 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ $|A| = 3 - 1 - 27 \mod 6 = -25 \mod 6 = 5.$
$\gcd(5,6) = 1 \Rightarrow \exists\, 5^{-1} \in \mathbb{Z}_6 \Rightarrow A$ invertible.

B) As $\mathbb{Z}_5$ is a field, we know every element is invertible.

$B = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ $|B| = -1 \mod 5 = 4 \neq 0$

$-3 \mod 5 = 2$
$-3^{-1} \mod 5 = -2 \mod 5 = 3$
$-2 \cdot 3^{-1} \mod 5 = -2 \cdot 2 \mod 5 = 1$
$-2 \mod 5 = 3$

$$(B|I) = \left(\begin{array}{ccc|ccc} 1 & 3 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & 0 & 1 \end{array}\right) \overset{R2 \leftrightarrow R3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 3 & 1 & 1 & 0 & 0 \\ 0 & 1 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \overset{2R2+R1}{\sim}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 2 \\ 0 & 1 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \overset{2R3+R2}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \overset{3R3+R1}{\sim}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 3 & 2 \\ 0 & 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \Rightarrow B^{-1} = \begin{pmatrix} 1 & 3 & 2 \\ 0 & 2 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

~~Leandro~~ FV.

Leandro Jorge Fernández Vega
$m = F-8298$
$n = 98$

Exercise 2 .

a) Check if the following code over Z_n:

C = {0 0 0 0 0, 1 1 1 1 1, … , *n*-1 *n*-1 *n*-1 *n*-1 *n*-1}

is linear.

b) Determine the minimum Hamming distance of *C* and then evaluate how many errors can be detected and how many errors can be corrected by this code

A)

1) $\forall (a,a,a,a,a),(b,b,b,b,b) \in C, \quad (a,a,a,a,a)+(b,b,b,b,b) =$
$(a+b \bmod n, a+b \bmod n, a+b \bmod n, a+b \bmod n) \in C$

2) $\forall (a,a,a,a,a) \in C, \lambda \in \mathbb{R}, \quad \lambda(a,a,a,a,a) = (\lambda a \bmod n, \lambda a \bmod n, \lambda a \bmod n, \lambda a \bmod n) \in C$

B) $d = \min \{ d(v,w) \mid v,w \in C, v \neq w \} = d(u,v) = 4 \quad \forall u,v \in C \overset{\text{theorem 3}}{\Longrightarrow}$
C can detect $t = 3 < d$ errors and correct $t = 1 < 2 = \frac{d}{2}$ errors

Exercise 3 .

The generating matrix *G* for the Hamming (7,4)-code is of form:

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

It encodes every binary 4-word as a binary 7-word which is ready to be transmitted.

Your two 4-words are: w_j, $j=n \bmod 8$. They are taken from the following sixteen 4-words:

w_0=0000, w_1=0001, w_2=0010, w_3=0011 ,w_4=0100, w_5=0101, w_6=0110, w_7=0111,

w_8=1000, w_9=1001, w_{10}=1010, w_{11}= 1011, w_{12} =1100, w_{13}=1101, w_{14}=1110, w_{15}=1111,

Evaluate the Hamming distance of these two 4-words. Encode them, by matrix *G*, as two 7-words ready to be transmitted. Evaluate the Hamming distance of the encoded 7-words. Describe the process you apply.

$98 \bmod 8 = 2 \bmod 8 = 10 \bmod 8 \Longrightarrow j_1 = 2, \ j_2 = 10$

$w_2 = 0010, w_{10} = 1010 \Longrightarrow d(w_2, w_{10}) = |\{ i \in \mathbb{N} \mid w_2^i \neq w_{10}^i \}| = 1$

$w_2 G = 0010101, w_{10} G = 1010212 = 1010010 \Longrightarrow d(w_2 G, w_{10} G) = 4$

~~Leandro~~ FV.