TP 2 – Codes correcteurs – Correction

Exercice 1. Le mot 01101011 a 5 bits valant 1 donc il se code en 011010111. Le mot 00110101 a 4 bits valant 1 donc il se code en 001101010. Si un bit est modifié alors le nombre de bits valant 1 est impair et l'erreur est détectée mais on ne peut pas dire quel bit est altéré. Si deux bits changent d'état alors le nombre de bits valant 1 reste pair et aucune erreur n'est détectées.

Exercice 2.

a. Sa dimentions k est 0, sa longueur n est 3. Il est donc de paramètre $(1, 3)$. Son image est $C = \{\phi(0), \phi(1)\} = \{000, 111\}$.

b. On obtient
- après 0 erreur : $000 \to \{000\}$ et $111 \to \{111\}$
- après 1 erreur : $000 \to \{001, 010, 100\}$ et $111 \to \{110, 101, 011\}$
- après 2 erreurs : $000 \to \{011, 101, 110\}$ et $111 \to \{100, 010, 001\}$
- après 3 erreurs : $000 \to \{111\}$ et $111 \to \{000\}$

c. Le code peur détecter deux erreurs mais en corriger une seule.

Exercice 3. Soient $m = b_1b_2...b_k$ et $m' = b'_1b'_2...b'_k$ des mots de $\mathbb{F}_2^k$. La distance de Hamming $d(m, m')$ est le nombre de lettres distinctes entre m et m'. On a donc $d(m, m') = \text{card}\{i \in \{1, ..., k\} \,|\, b_i \neq b'_i\}$. Comme $0 + 0 = 0$, $1 + 1 = 0$, $0 + 1 = 1$ et $1 + 0 = 1$ on remarque que deux bits sont différents si et seulement si leur somme vaut 1. On a donc

$$d(m, m') = (b_1 + b'_1) + (b_2 + b'_2) + ... + (b_k + b'_k) = w((b_1 + b'_1)(b_2 + b'_2)...(b_k + b'_k)) = w(m + m').$$

Pour $c \in \mathbb{F}_2^k$, on a

$$d(m + c, m' + c) = w(m + c + m' + c) = w(m + m' + 2c) = w(m + m') = d(m, m').$$

Exercice 4.

a. Les mots $m = 000000000$ et $m' = 100000001$ sont deux mots de C. Comme $d(m, m') = 2$ on a $d_\phi \leqslant 2$. Montrons que d_ϕ n'est pas 1. Supposons par l'absurde qu'il existe deux mots m et m' de C tels que $d(m, m') = 1$. Posons $m = b_1...b_9$, $m' = b'_1...b'_9$. Comme m et m' sont dans C, on a $b_1 + ... + b_9 = 0$ et $b'_1 + ... + b'_9 = 0$. Comme $d(m, m') = 1$ il existe $i \in \{1, ..., 9\}$ tel que $b_i \neq b'_i$ et $b_j = b'_j$ pour tout $j \neq i$. On a déjà vue que le relation $b_i \neq b'_i$ est équivalente à $b_i + b'_i = 1$. On a donc $b'_i = b_i + 1$. Ce qui donne

$$0 = b'_1 + ... + b'i + ...b_k = b_1 + ... + b_i + 1 + ... + b_k = 1 + b_1 + ... + b_k = 1 + 0 = 1$$

On a donc nécessairement $d_\phi = 2$. D'où $e_d = 1$ et $e_c = \lfloor \frac{1}{2} \rfloor = 0$.

b. On a $C = \{000, 111\}$ et donc $d_\phi = d(000, 111) = 3$. D'où $e_d = 2$ et $e_c = \lfloor \frac{2}{2} \rfloor = 1$.

Exercice 5.

a. Le rang de G soit être égale à k pour que ϕ soit injective.

b. Pour le code de répétition pure $(1, 3)$, on a $\phi(b_1) = b_1b_1b_1$. Pour

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \text{on a} \quad G\begin{bmatrix} b_1 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_1 \\ b_1 \end{bmatrix}$$

ce que l'on veux.

Pour le code bit de parité $(8,9)$ on a $\phi(b_1...b_8) = b_1...b_8b_9$ avec $b_9 = b_1 + ... + b_8$. Pour

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{on a} \quad G \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7 + b_8 \end{bmatrix}$$

qui est ce qu'on veux.

c. Ce code est de dimension 2 et de longueur 4. On a

$$G \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; G \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \; G \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \text{ et } G \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

On a donc $C = \{0000, 1011, 0101, 1110\}$. De

$$d(0000, 1011) = 3, d(0000, 0101) = 2, d(0000, 1110) = 3,$$
$$d(1011, 0101) = 3, d(1011, 1110) = 2 \text{ et } d(0101, 1110) = 3,$$

on obtient $d_\phi = 2$ et donc $e_d = 1$ et $e_c = 0$.

Exercice 6.

a. Démontrons la proposition 7. On a $C = \mathrm{Im}(\phi) = \{G \cdot m \,|\, m \in \mathbb{F}_2^k\}$ qui est sous-espace vectoriel. de $\mathbb{F}_2^n$.
Démontrons la proposition 8. Posons $p = \min\{w(m) \,|\, m \in C \setminus \{0\}\}$. Soit $m \in C \setminus \{0\}$, on a $d_\phi \leqslant d(0, m) = w(m)$ et donc $d_\phi \leqslant p$. Soit m et m' dans C distincts tels que $d_\phi = d(m, m')$. On a alors $d_\phi = d(m+m, m+m') = d(0, m+m') = w(m+m')$. De $m \neq m'$ on obtient $m + m' \neq 0$. Comme C est un espace vectoriel $m + m' \in C$. On obtient donc $p \leqslant d_\phi$. D'où $d_\phi = p$.
Démontrons la proposition 9. Pour avoir $d_\phi \leqslant n - k + 1$ il est suffisant de montrer qu'il existe un mot m dans C avec au moins $k - 1$ bits nuls. Notons D l'espace vectoriel des mots de C ayant leurs $k - 1$ composantes nulles. On a alors $\dim(D) = n - (k - 1) = n - k + 1$. De $\dim(D \cup C) = \dim(D) + \dim(C) - \dim(D \cap C)$ on obtient

$$\dim(D \cap C) = \dim(D) + \dim(C) - \dim(D \cup C) \geqslant k + (n - k + 1) - n = 1.$$

Il existe un donc un mot de code m non nul avec ses $k - 1$ composantes nulles. On a donc $d_\phi \leqslant w(m) \leqslant n - k + 1$.

b. Le code bit de parité est MDS car $d_\phi = 2 = 9 - 8 + 1 = n - k + 1$. Le code répétition pure est MDS car $d_\phi = 3 = 3 - 1 + 1 = n - k + 1$. Le code donnée par matrice génératrice n'est pas MDS car $d_\phi = 2 < 3 = 4 - 2 + 1 = n - k + 1$.

Exercice 7.

a. Montrons d'abord que pour tout mode de code c de $\mathbb{F}_2^n$ on a $Hc = 0$, ce qui revient à montrer que $\mathrm{Im}(G)$ est inclus dans $\ker(H)$. Si c est un mot de code alors il existe $m \in \mathbb{F}_2^k$ tel que $c = Gm$. D'où

$$Hc = HGm = \begin{bmatrix} G' & I_{n-k} \end{bmatrix} \begin{bmatrix} I_k \\ G' \end{bmatrix} m = \begin{bmatrix} G'I_k + G'I_{n-k} \end{bmatrix} m = \begin{bmatrix} 2G' \end{bmatrix} m = \begin{bmatrix} 0 \end{bmatrix} m = 0$$

On a donc montrer $\mathrm{Im}(G) \subseteq \ker(H)$. Pour avoir égalité il suffit de montrer l'égalité des dimensions. Par construction de G, on a $C = \mathrm{Im}(G)$ et donc $\dim(C) = \dim(\mathrm{Im}(G)) = \mathrm{rang}(G) = k$. De $H = \begin{bmatrix} G' & I_{n-k} \end{bmatrix}$, on obtient $\dim(\mathrm{Im}(H)) = \mathrm{rang}(H) = n - k$. Par le théorème du rang, on a $\dim \mathbb{F}_2^n = \mathrm{rang}(H) + \dim(\ker(H))$. On a donc $\dim(\ker(H)) = n - (n - k) = k$. On a donc bien $\ker(H) = \mathrm{Im}(G)$ et H est une matrice de contrôle de ϕ.

b. La matrice génératrice du code $(8,9)$ est

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

une de ses matrices de controle est donc

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

La matrice génératrice du code $(1,3)$ est

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

une de ses matrices de controle est donc

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

Une des matrice de controles du code dont la matrice génératrice est

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

est la matrice

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

Exercice 8. Pour le code bit de parité $(8,9)$, on a $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$. L'ensemble des syndromes est $\mathbb{F}_2^{n-k} = \mathbb{F}_2 = \{0,1\}$. On liste les mots z de $\mathbb{F}_2^n = \mathbb{F}_2^9$ par poid croissant:

$z \in \mathbb{F}_2^9$	$s = Hz$
000000000	0
000000001	1

On obtient alors la table de décodage

syndrome	erreur
0	000000000
1	000000001

Si on recoit le mot $z = 101010100$. On calcule

$$s = H \times z = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 0,$$

on retourne alors le préfixe de longueur 8 de z à savoit 10101010.

Pour le code de répétition pure $(1,3)$, on a $H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$. L'ensemble des syndromes est $\mathbb{F}_2^{n-k} = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$. On liste les mots z de $\mathbb{F}_2^n = \mathbb{F}_2^3$ par poid croissant:

$z \in \mathbb{F}_2^3$	$s = Hz$
000	00
001	01
010	10
100	11

Détaillons le calcul du syndrome de la troizième ligne. On a

$$s = Hz = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

La table de décodage est donc

syndrome	erreur
00	000
01	001
10	010
11	100

Si on recoit le mot $z = 101$. On calcule

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

D'après la table de décodage, l'erreur associé à 10 est 010, on retournr le préfixe de longueur 2 de $z + 010 = 101 + 010 = 111$, à savoir 11.

Le code correteur de matrice génératrice

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

à la matrice

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

comme matrice de controle. L'ensemble des syndomes est $\mathbb{F}_2^{n-k} = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$. On liste les mots z de $\mathbb{F}_2^n = \mathbb{F}_2^4$ par poid croissant:

$z \in \mathbb{F}_2^4$	$s = Hz$
0000	00
0001	01
0010	10
0100	01
1000	11

La table de décodage est donc

syndrome	erreur
00	0000
01	0001
10	0100
11	1000

Si on recoit le mot $z = 1100$, on calcule

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

D'apres la table de décodage, l'erreur associée au syndrome 10 est 0100 qui est de poids 1 or ce code ne corrige aucune erreur, on ne peut donc pas finir le décodage.

Exercice 10

On commence par construire le corps $\mathbb{F}_2$:

```
F2=FiniteField(2)
```

a.

```
def image(G):
    (n,k)=G.dimensions()
    U=VectorSpace(F2,k)
    return [G*m for m in U]
```

b. On introduit la fonction suivante retournant le poids de Hamming d'un mot sur $\mathbb{F}2$.

```
def poids_Hamming(x):
    d=0
    for i in range(len(x)):
        if x[i]!=0:
            d=d+1
    return d
```

On obtient alors

```
def distance(G):
    C=image(G)
    d=Infinity
    for x in C:
        if x!=0:
            d=min(d,poids_Hamming(x))
    return d
```

c.

```
def est_mds(G):
    (n,k)=G.dimensions()
    d=distance(G)
    return d==n-k+1
```

d.

```
def est_systematique(G):
    (n,k)=G.dimensions()
    return G.submatrix(0,0,k,k).is_one()
```

e.

```
def matrice_controle(G):
    (n,k)=G.dimensions()
    GG=G.submatrix(k,0,n-k,k)
    H=matrix(F2,n-k,n)
    H.set_block(0,0,GG)
    H.set_block(0,k,identity_matrix(F2,n-k))
    return H
```

f.

```
def table_decodage(G):
    H=matrice_controle(G)
    (n,k)=G.dimensions()
    d=distance(G)
    table=
    E=VectorSpace(F2,n)
    for e in E:
        s=H*e
        s.set_immutable() # Transfome s en vecteur que l'on ne pourra plus modifier
        if s in table: # Une erreur est deja affecte au syndrome
            f=table[s] # On recupere l'erreur affecte
            if poids_Hamming(e)<poids_Hamming(f):
                # Si e a un poid de Hamming inferieur a celle presente dans la table
                # on met à jour l'erreur associée au syndrome e
                table[s]=e
        else:
            table[s]=e
    return table
```

g.

```
def decode(G,m):
    m=vector(F2,m)
    (n,k)=G.dimensions()
    H=matrice_controle(G)
    d=distance(G)
    ec=(d-1)/2
    table=table_decodage(G)
    s=H*m
    s.set_immutable()
    if s==0:
        return m[:k]
    else:
        e=table[s]
        if poids_Hamming(e)<=ec:
            m=m+e
            return m[:k]
        print("Correction impossible")
```