Corrigé

Exercice 1:

1.a : $P(X = k) = C_5^k p^k (1-p)^{5-k}, k = 0,1,2,3,4,5$

1.b : L'erreur est détectée lorsque le nombre de bits erronés est 1, 2, 3,ou 4 c-à-d

P(X=1)+P(X=2)+P(X=3)+P(X=4) = 1 –(P(X=0)+P(X=5)) = $1 - (p^5 + (1-p)^5)$

1.c : L'erreur n'est pas détectée lorsque tous les bits sont erronés càd P(X=5) = p^5

2 : 00000 11111 11111 11111 00000

3 : 0 1 0 1

4 : 1/5

5: 1/9

6 : $P(X = 5) = C_9^5 p^5 (1-p)^4$

7 : $\frac{P(X=5)}{P(X=6)} = \frac{C_9^5 p^5 (1-p)^4}{C_9^6 p^6 (1-p)^3} = \frac{C_9^5 (1-p)}{C_9^6 p} = \frac{1}{24}\frac{(1-p)}{p} \approx \frac{1}{24}\frac{1}{10^{-3}} = 41{,}666$

8 : $P(X = 9) = p^9 = 10^{-27}$ *contre* 10^{-15} *pour un code* à *répétitions sur* 5 *bits*

Exercice 2:

1 : Pour n=8 ; $G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

3 : d= n/2 => on peut détecter jusqu'à q= (n/2)-1 bits erronés et en corriger $t = \left\lfloor \frac{(n/2)-1}{2} \right\rfloor$

4 : pour le second code, d=2 (puisque le code de (1 1) est (1 1 0 0 0… 0) => q=1 et t=0. Le premier code est donc bien meilleur.

5 : Pour n=6, le code précédent a une distance de 3 et permet de détecter jusqu'à 2 bits erronés.

Le code ci-dessous a une distance de 4 et permet jusqu'à 3 bits erronés : $G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$

Exercice 3:

a: $Gpaire = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$. Le code par parité impaire n'est pas linéaire puisque Code (00) = 001 qui n'est pas le vecteur nul.

b: Le code par parité paire est linéaire, sa capacité de détection est de 1 bit , pour tout n. Le code par parité impaire n'est pas linéaire, sa capacité de détection est de 1 bit , pour tout n.

Exercice 4:

a: toute erreur sur un nombre impair de bit. Pas de correction possible (d=2 => t=0)

b :

- 1101011001 => 11010110011**1**
- 100 => 100**1**
- 11111000111001111 =>111110001110011110

c: de façon générale k/k+1

Exercice 5:

a: Les bits d'information se retrouvent à l'identique dans le code. Les bits supllémentaires sont obtenus à l'aide d'applications linéaires. Il s'agit donc d'un code linéaire systématique.

b: Pour K=L=2, $G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$

Exercice 6:

a: n=6,k=3

b: $H(m1) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} => m1 \notin code$, $M(m2) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} => m2 \in code$

c: Il s'agit d'un code systématique. $G = \begin{pmatrix} 1\ 0\ 0 \\ 0\ 1\ 0 \\ 0\ 0\ 1 \\ 1\ 0\ 1 \\ 1\ 1\ 0 \\ 0\ 1\ 0 \end{pmatrix}$

000	000000
001	001100
010	010011
011	011111
100	100110
101	101010
110	110101
111	111001

Exercice 7:

Soit le code linéaire $C_{7,4}$ qui au vecteur d'information $i = (i_1,i_2,i_3,i_4)$ associe le mot de code $c= (i_1,i_2,i_3,i_4,c_5,c_6,c_7)$ avec $c_5 = i_1+i_3+i_4$, $c_6 = i_1+i_2+i_3$, et $c_7 = i_2+i_3+i_4$.

a. Donner la matrice génératrice et la matrice de contrôle de ce code
b. Soit i = (1 0 1 0), quel est le mot de code associé ?
c. Soit le message m = (1 1 1 1 0 0 1). Est-il un mot du code ?

a: $G = \begin{pmatrix} 1\ 0\ 0\ 0 \\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1 \\ 1\ 0\ 1\ 1 \\ 1\ 1\ 1\ 0 \\ 0\ 1\ 1\ 1 \end{pmatrix}, H = \begin{pmatrix} 1\ 0\ 1\ 1\ 1\ 0\ 0 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \end{pmatrix}$

b: c= (1 0 1 0 **0 0 1**)

c: $H(m) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} => m \notin code$

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

Exercice 8:

1.

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

$$En\ ajoutant\ \ la\ 2nde\ colonne\ à\ la\ 1ère\ on\ a : G1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

$$En\ ajoutant\ \ la\ 1ere\ et\ la\ 3ème\ colonne\ à\ la\ 2nde\ on\ a : G2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

$$En\ ajoutant\ \ la\ 1ere\ colonne\ à\ la\ 3ème\ on\ a : G3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

qui est la matrice d'un code sous forme systématique.

b:

000	000000
001	001110
010	010010
011	011100
100	100110
101	101001
110	110101
111	111011

c: dmin=min(w(c))=2 => e=1

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

Exercice 9:

On cherche une base de $C^{\perp}$, qui est de dimension 2.

Soit V = (v1 v2 v3 v4 v5)$^t \in C^{\perp}$, on a : G^t (v1 v2 v3 v4 v5 v6)^t = (0 0 0)^t. Ce qui donne les trois relations : v1+v2+v5 = 0 ; v2+v3+v5=0 , v3+v4 = 0

Une base possible de $C^{\perp}$ est {V1,V2} avec $V1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, V2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$.

D'où $H^t = \begin{pmatrix} 0\ 1 \\ 1\ 1 \\ 0\ 1 \\ 0\ 1 \\ 1\ 0 \end{pmatrix}$.

b: $C^{\perp}$, : $\{0,1\}^2$ -> $\{0,1\}^5$ et tel que :

00	00000
01	11110
10	01001
11	10111

Exercice 10:

a:

Syndrome	Message reçu			
0	000	010	101	111
1	**001**	011	*100*	111

b:

Message reçu	000	001	010	011	100	101	110	111
Transformé	000	000	010	010	101	101	111	111

c: Non, puisque dans ce cas il y a deux représentants de syndrome =1 de poids minimal. On aurait pu également faire une correction en ajoutant le vecteur en italique.

Exercice 11:

Soit le code linéaire $C_{n,r}$ de matrice de contrôle $H=\begin{pmatrix}1&1&0&0&1&0&1\\0&0&1&1&1&0&1\\1&0&1&0&0&1&1\end{pmatrix}$

a: k=4, n =7

b: $Si\ m=\begin{pmatrix}1\\1\\1\\1\\1\\1\\1\end{pmatrix}, H(m)=\begin{pmatrix}0\\0\\0\end{pmatrix} => m \in Code$

c: Il s'agit d'un code de Hamming puisque les colonnes de H décrivent toutes les possibilités sauf la colonne nulle. Si e=1, alors les messages sont correctement corrigés. Si e > 1, alors les messages sont incorrectement corrigés.

$$P=\frac{P(message\ erroné\ mal\ corrigé)}{P(message\ erroné)}=\frac{\sum_{i=2}^{7}C_7^i p^i(1-p)^{7-i}}{1-(1-p)^7}$$

$$=\frac{1-((1-p)^7+C_7^1p^1(1-p)^6)}{1-(1-p)^7}\approx 0{,}29$$

Exercice 12:

- 0101000 => **1**101000
- 1110010 => **0**110010
- 1100011 =>110**1**011
- 1011011 => 1011010
- 1101011 => **0**101011
- 1000011 => 1000011

Exercice 13

a. Codage de 0101 1001 0111 => 0101101 1001100 0111000
b. Décodage de: 0100011 1001010 1101001 => 01**1**0011 **0**001010 1101000

Exercice 14

On considère le code linéaire en blocs défini par une matrice de contrôle

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

obtenue en rajoutant à la matrice de parité du code de Hamming (7,4,3) une colonne de zéros puis une ligne de uns.

a. *n=8, k =4*
b. A rajouter un bit qui est la parité de tous les bits
c. En ajoutant la 8ème colonne aux 5ème, 6ème et 7ème on obtient : $H = \begin{pmatrix} 1&0&1&1&1&0&0&0 \\ 0&1&1&1&0&1&0&0 \\ 1&1&0&1&0&0&1&0 \\ 1&1&1&1&0&0&0&1 \end{pmatrix}$
d. $G = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&1&1 \\ 0&1&1&1 \\ 1&1&0&1 \\ 1&1&1&1 \end{pmatrix}$.
e. d=3. Donc il permet de détecter 2 erreurs et d'en corriger 1.

Exercice 15

L'objet de cet exercice est de comparer les taux de transmission et la fiabilité d'un code par répétition et un code de Hamming. Le but est de démontrer que dans le cas d'un canal bruité, émettre des paquets longs est plus efficace qu'émettre des paquets courts. On désire transmettre un message de 10000 bits à travers un canal bruité. On considère une probabilité d'erreur p = 0,01.

Codage par répétition : Chaque bit est émis trois fois. Le décodage se fait par un vote à la majorité.

a. 1/3
b. Le décodage est incorrect lorsque 2 ou 3 bits sont erronés càd P(X=2)+P(X=3) = $3p^2(1-p)+p^3 = 3.10^{-4}$
c. $3.10^{-4} * 10^4 = 3$

Paquets de 9 bits : On considère un code Hamming(9,3). Le message est envoyé sous forme de paquets de 9 bits, de la forme (s1, s2, s3, t1, t2, t3, t4, t5, t6). Les trois premiers bits s1, s2, s3 constituent le message original, les six suivants t1, ... , t6 sont les bits de contrôle.

d. 1/3
e. $1 + 9 + 36$
f. $8.10^{-5} = 10^{-6}$
g. $8.10^{-5} . (3*10^4 / 9) . 1/3 = 10^{-1}$

Exercice 16

Soit le code linéaire $c_{3,2}$ de matrice génératrice $G = \begin{pmatrix} 1&1 \\ 0&1 \\ 1&0 \end{pmatrix}$

Information	Poly. correspondant	Code	Poly. Correspondant	Nom
0 0	0	0 0 0	0	a
0 1	1	1 1 0	x^2+x	b
1 0	x	1 0 1	x^2+1	c
1 1	x+1	0 1 1	x+1	d

a. Tous les codes sont des multiples de d = x+1, c'est son poly. générateur.

   a = 0 * d ; b = x* d; c =(x+1) *d

b. Matrice caractéristique $G=\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$. Matrice normalisée = $G=\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$.

c. Les codes polynomiaux $C_{3,2}$ sont engendrés par des poly de degré 1. Il n'y a que 2 poly de degré 1 : P1(x) = x et P2(x)=x+1.

   Pour P1(x), le code consiste à rajouter 0 aux bits d'information.

   Pour P2(x) cela correspond au code ci-dessus

Exercice 17

Soit C un code polynomial obtenu par codage systématique, de générateur :

$g(x) = x^3+x^2+x+1$

a. 3 bits

b. Matrice caractéristique: $G_{5,2} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$, Matrice carac. normalisée: $G_{5,2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$,

c. $G_{6,3} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $G_{7,4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Exercice 18

i	i(x)	i(x). x^2	reste modulo x^2+1	code
000	0	0	0	00000
001	1	x^2	1	00101
010	x	x^3	x	01010
011	x+1	x^3+x^2	x+1	01111
100	x^2	x^4	1	10001
101	x^2+1	x^4+x^2	0	10100
110	x^2+x	x^4+x^3	x+1	11011
111	x^2+x+1	$x^4+x^3+x^2$	x	11110

Exercice 19

a.

i	i(x)	i(x). x^2	reste modulo x^2	code
000	0	0	0	00000
001	1	x^2	0	00100
010	x	x^3	0	01000
011	x+1	x^3+x^2	0	01100
100	x^2	x^4	0	10000
101	x^2+1	x^4+x^2	0	10100
110	x^2+x	x^4+x^3	0	11000
111	x^2+x+1	$x^4+x^3+x^2$	0	11100

L'effet d'un codage systématique par un poly. de la forme x^n est l'ajout de 0 à la fin.

b. Les erreurs sur c4 et c5 peuvent être détectées puisque en ce cas ils valent 1.
   Les erreurs sur c1, c2, c3 ne peuvent être détectées puisque on a l'ensemble des 8 valeurs sur ces 3 bits.
c. Les erreurs de poids 2 détectables sont celles qui font intervenir au moins un des bits c4 et c5

Exercice 20

Soit $g(x) = x^3+x+1$ le polynôme générateur d'un code polynomial de longueur 6.

a. 3
b. Erreurs de poids 1 détectées (2 termes dans g(x), il ne divise pas de poly de la forme x^k)

   Les erreurs de poids 2 sont de la forme $x^j+x^k = x^k(x^{j-k}+1)$ avec j>k. On a vu que g(x) ne divise aucun monôme x^k.

   D'autre part, x^3+x+1 ne divise ni (x+1), ni (x^2+1), ni (x^3+1) (évident). D'autre part il ne divise pas (x^4+1), ni (x^5+1).

Donc au final il ne divise aucun poly de la forme x^j+x^k. Toutes les erreurs de poids 2 sont donc détectées.

x^3+x+1 n'est pas un multiple de x+1. Donc toutes les erreurs de poids impairs (>1) ne sont pas détectées.

P(X=1)+P(X=2) = $C_6^1 p^1(1-p)^5 + C_6^2 p^2(1-p)^4 = 0{,}45$

Perr = $1-(1-p)^6 = 0{,}47$

La probabilité de détection des messages erronés est donc de 0,45/0,47 = 96 %

Exercice 21

Soit un code polynomial de longueur 5 de polynôme générateur $g(x) = x^3+x^2+x+1$.

a. Le polynôme générateur est de degré 3, la longueur des mots d'information est donc de 5-3=2 bits

   $m(x)= x^4+x^3+x^2+x = (x^3+x^2+x+1)\ x$, c'est donc un multiple de g(x).

Il est correctement transmis si le message ne comporte aucune erreur càd avec la probabilité $P(X=0)= 1-(1-p)^5$, où p est la probabilité qu'un bit soit mal transmis.

b. Un message erroné peut avoir 1, 2, 3, 4 ou 5 erreurs. On remarque que :

   - toutes les erreurs de poids impair sont détectées puisque g(x) est un multiple de x+1. En effet $g(x) = x^3+x^2+x+1 = (x+1)\ (x^2+1)$
   - toutes les erreurs de poids 2 ne sont pas détectées puisque g(x) divise le polynôme x^4+1. ($x^4+1= (x+1)\ (x^3+x^2+x+1)$
   - pas de renseignement pour les erreurs de poids 4.

   En résumé, si le message est erroné et semble correct, c'est que le message ne peut pas avoir d'erreur de poids impair.

c. L fonction f : i(x)-> i(x) (x^3+x^2+x+1) construit le code suivant.

i	i(x)	c(x)	c	w(c)
00	0	0	00000	0
01	1	x^3+x^2+x+1	01111	4
10	x	$x^4+x^3+x^2+x$	11110	4
11	x+1	x^4+1	10001	2

Un message erroné est non reconnu comme tel si et seulement si le polynome d'errur n'est pas un mot du code. Aucun mot de code n'est de poids impair, donc :

- les erreurs de poids impair sont toutes détectées
- les erreurs non détectées sont
  - de poids 2, il s'git de l'erreur x^4+1
  - de poids 4, càd les erreurs x^3+x^2+x+1 et $x^4+x^3+x^2+x$

d. le message (01111) correspond à x^3+x^2+x+1 qui est le polynôme générateur. Il est donc considéré comme exact. Si, cependant, il ne l'est pas, il porte une erreur de poids pair.

- si l'erreur est de poids 2, le polynôme d'erreur est $e(x) = x^4+1$ càd (10001). Le message émis était donc (11110).
- si l'erreur est de poids 4, le polynôme d'erreur est, ou bien $e(x) = x^3+x^2+x+1$ càd (01111), ou bien $e(x) = x^4+x^3+x^2+x$ càd (11110) . Le message émis était donc ou bien (00000) ou bien (10001).

- La probabilité que m erroné ne soit pas détectée est : $p^2(1-p)^3 + 2p^4(1-p)$.
- En ce cas , m provient de :
  - $x^4+x^3+x^2+x$ avec la probabilité $\frac{p^2(1-p)^3}{p^2(1-p)^3+2p^4(1-p)}$
  - 0 avec la probabilité $\frac{p^4(1-p)}{p^2(1-p)^3+2p^4(1-p)}$
  - x^4+1 avec la probabilité $\frac{p^4(1-p)}{p^2(1-p)^3+2p^4(1-p)}$