**EXERCICES SUR LE CODAGE LINEAIRE**

**Rappels de cours**

* **F** est le corps fini.
* **F**2 est le plus petit corps fini composé uniquement de deux éléments 0 et 1.
* (F2)n est une fonction de n éléments dans corps **F**2
* Un code de longueur n est une partie de Fnq. Un code linéaire C de longueur n sur le corps finiFq est un sous-espace vectoriel de Fnq. Par défaut, un code sera supposé linéaire.
* un **sous-espace vectoriel** d'un espace vectoriel Fnq*,* est une partie non vide *C*, de Fnq, stable par combinaisons linéaires. Cette stabilité s'exprime par :
* ***la somme de deux vecteurs de C appartient à C ;***
* ***le produit d'un vecteur de C par un scalaire appartient à C.***
* La distance de Hamming entre deux vecteurs de Fnq est le nombre de coordonnées où les deux vecteurs diffèrent. La distance minimale du code C est la plus petite distance non nulle entre deux mots ducode C. C'est aussi le plus petit poids (nombre de coordonnées non nulles) d'un mot non nul de C.
* Les paramètres [n, k, d] d'un code C sont sa longueur, sa dimension (en tant que Fq-espace vectoriel), sa distance minimale. Le code C contient qk mots de code. Si t < d/2, les boules de Hamming centrées sur les mots de co de sont disjointes. Toute configuration de t erreurs peut être corrigée en cherchant le mot de code le plus proche (pour la distance de Hamming).
* Une matrice génératrice d'un code C est une matrice k×n à éléments dans Fq, dont les lignes constituent une base de C.
* Le code dual C⊥ de C est l'ensemble des vecteurs y= (y1. . . yn) de Fnq tels que, pour tout x= (x1. . . xn)∈C

x.y=x1y1+x2y2+···+xnyn=0 dans Fq.

Le code dual C⊥ a pour dimension dim C⊥=n=dim C.

* Une matrice de contrôle ou de parité de C est une matrice génératrice du code dual C⊥.
* Une matrice génératrice G est dite sous forme systématique si elle s'écrit:

G= [Ik|P].

* Dans ce cas on constate que la matrice H= [Pt|In−k] est une matrice de contrôle de C.
* Le syndrome de y’∈ Fnq est le vecteur (colonne)

s(Y) =HtY’.

Ou bien s(Y’) =∑y’ihi

Où Y’= (y’1,…y’n) et

h1…hn sont les colonnes de la matrice H.

* Si Y est un mot du code C (code original)de matrice de parité H si et seulement si s(Y) = 0
* Décodage par syndrome. Pour trouver le plus proche mot de code de Y, calculer s(Y), puis chercher le plus petit ensemble I⊂{1,2,…,n} tel qu'il existe des λi∈Fq non nuls, i∈I, et

∑λihi=s.

Exercice 1 :

Supposons un canal binaire avec des erreurs indépendantes et Pe = 0,05. Supposons que les symboles à k chiffres de l'alphabet source sont codés à l'aide d'un code de bloc (n, k) qui peut corriger tous les modèles de trois erreurs ou moins. Supposons que n = 20.
(a) Quel est le nombre moyen d'erreurs dans un bloc?
(b) En supposant une transmission binaire à 20000 chiffres binaires par seconde, en déduire le taux d'erreur de symbole à la sortie du décodeur.

Exercice 2 :

Un signal binaire est transmis par un canal qui ajoute un bruit centré, blanc et gaussien. La probabilité d'erreur sur les bits est de 0,001.

1. Quelle est la probabilité d'erreur dans un bloc de quatre bits de données? Si la bande passante est étendue pour accueillir un code de bloc (7,4),
2. quelle serait la probabilité d'une erreur dans un bloc de quatre bits de données?

Exercice 3 :

Supposons un code de bloc systématique (n, k) où n = 4, k = 2 et les quatre mots de code sont 0000, 0101, 1011, 1110.

1. Construire une table de décodage du maximum de vraisemblance pour ce code.
(b) Combien d'erreurs le code corrigera-t-il?
2. Y a-t-il des erreurs détectables mais non corrigibles?
3. Supposons que ce code est utilisé sur un canal avec Pe = 0,01. Quelle est la probabilité d'avoir une séquence d'erreur détectable?
4. Quelle est la probabilité d'avoir une séquence d'erreur indétectable?

Exercice 4 : Codes binaires

Parmi ces codes binaires, lesquels sont linéaires et quel est le nombre d’erreurs que chacun peut détecter ?

C1 = {00, 01, 11} ⊂ (F2)2 (1)

C1 = {000, 100, 101, 101, 011, 111} ⊂ (F2)3 (2)

 C1 = {0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111} ⊂ (F2)4 (3)

C2 = {10000, 01010, 00001} ⊂ (F2)5 (4)

C3 = {000000, 101010, 010101} ⊂ (F2)6 . (5)

Exercice 5

Pour un code de bloc linéaire systématique (6,3), les trois chiffres du contrôle de parité sont:

P1 = 1 × I1⊕1 × I2⊕1 × I3

P2 = 1 × I1⊕1 × I2⊕0 × I3

P3 = 0 × I1⊕1 × I2⊕1 × I3

Où ⊕ représente un addition modulo (binaire)

* 1. Construisez la matrice génératrice G pour ce code.
	2. Construisez tous les mots de code possibles générés par cette matrice.
	3. Déterminez les capacités de correction d'erreur pour ce code.
	4. Préparer une table de décodage appropriée.
	5. Décoder les mots reçus 101100, 000110 et 101010.

Exercice 6 :

Étant donné un code avec la matrice de contrôle de parité:



(a) E déduire la matrice génératrice en montrant clairement comment l’obtenir à partir de la matrice H.
(b) En déduire le de ce code et trouver sa distance minimale de Hamming. Combien d'erreurs ce code peut-il corriger? Combien d'erreurs ce code peut-il détecter? Peut-il être utilisé simultanément en modes correction et détection?
(c) Notez le tableau des syndromes pour ce code montrant comment le tableau peut être obtenu en tenant compte du mot de code tout-zéros. Également commenter l'absence d'une colonne tout-zéros de la matrice.
(d) Décoder la séquence reçue 1001110, indiquer le motif d'erreur le plus probable associé à cette séquence et donner le mot de code correct. Expliquez l'énoncé «modèle d'erreur le plus probable».

**Exercice7 :**

Construire un code binaire de 4 mots de longueur 3 et de distance minimum 2. 2. Montrer qu'un code binaire C de longueur 3 et de distance minimum 2 possède au plus 4 mots.

Soit C le code linéaire sur F3 de matrice génératrice :



1. Montrer que C est systématique et en donner une matrice génératrice normalisée G0 .

2. Encoder le message (12) avec G, puis avec G’ .

3. Construire une matrice de contrôle de C et calculer sa distance minimale. Le code est-il MDS (Maximum Distance Separable) ?

4. On reçoit le message 11102 codé par G. Quel est le message d'origine ? Le mot 12121 est-il un mot de code ? Le décoder sachant qu'il a été encodé par G.

Exercice 8

Soit C le code linéaire sur F5 de matrice génératrice :



1. Donner le nombre de mots de C.

2. Le code est-il systématique ?

3. Déterminer une matrice de contrôle de C.

4. Calculer la capacité de correction t de C. Le code est-il MDS ?

5. Donner la table de contrôle contenant tous les vecteurs erreurs possibles de poids ≤ t.

6. Décoder quand c'est possible les mots 3001, 1101 et 2311.

Exercice 9

Soit C le code sur F5 de matrice génératrice G avec



1. Montrer que G0 est une matrice normalisée génératrice du même code C.

2. En déduire une matrice de contrôle.

3. Quelle est la capacité de correction de C ?

4. Décoder les mots 432100 et 411141.

Exercice 10

Soit le code linéaire C3,2 de matrice génératrice 

1. Montrer qu'il s'agit d'un code polynomial
2. Donner les matrices génératrices caractéristique et normalisée (forme systématique) du code.
3. Décrire tous les codes polynomiaux C3,2

Exercice 11

Soit Cun code polynomial obtenu par codage systématique, de générateur :

g(x) = x3+x2+x+1

1. Donner la longueur de la clé de contrôle des mots du code
2. Donner la matrice génératrice normalisée G5,2 du code C5,2 de générateur g(x).
3. Donner les matrices génératrices des codes C6,3 et C7,4 ayant le même générateur g(x).

Exercice 12

Soit C5,3 le code polynomial engendré par le polynôme g(x) = x2+1.

1. Construire le code par codage systématique

Exercice 13

Soit C5,3 le code polynomial engendré par le polynôme g(x) = x2.

1. Construire le code par codage systématique.
2. Tout polynôme de code s'écrivant : $c\left(x\right)=c1x^{4}+c2x^{3}+c3x^{2}+c4x+c5$ montrer que les erreurs de poids 1 situées sur les bits c4 et c5 sont détectées et que les autres erreurs de poids 1 ne peuvent l'être.
3. Quelles erreurs de poids 2 peut-on détecter ?

Exercice 14

Soit g(x) = x3+x+1 le polynôme générateur d'un code polynomial de longueur 6.

1. Quelle est la longueur des mots d'information ?
2. Evaluer le pourcentage de messages erronés reconnus comme tels parmi tous les messages erronés pour des erreurs par bit de probabilité p = 0,1.

Exercice 15

Soit un code polynomial de longueur 5 de polynôme générateur g(x) = x3+x2+x+1.

1. Montrer que le message m(x)= x4+x3+x2+x est un polynôme de code. Avec quelle probabilité a-t'il été correctement transmis ?
2. si il est accepté comme correct, bien qu'il soit erroné, que peut-on dire du poids de son erreur ?
3. Donner l'ensemble des mots du code, préciser leur poids et retrouver les résultats de la question précédente
4. De quel mot de code émis, le message (01111), s'il est erroné, peut 'il provenir et avec quelle probabilité ?

Exercice 16

Soit le code C20,12 polynomial de polynôme générateur x8 + x2 + x + 1.

Quelles sont les erreurs détectables ?

Exercice 17: Code de Reed-Muller

Soit le code de Reed-Muller RM(1,4)

a/ Quelle est le nombre de bits des mots d'informations

b/ Quelle est sa distance et sa capacité de correction

c/ Soit le mot reçu m = (0 1 0 1 0 0 1 0 0 0 1 0 1 1 0 1 ). Quel est le mot d'information envoyé?

d/ Quels sont (si il y en a) les bits mal transmis.

**A propos du Code de Reed-Muller**

Les codes de Reed-Muller. Il s'agit d'un algorithme permettant de fabriquer facilement des codes, en particulier des codes linéaires, ayant des caractéristiques intéressantes en termes de rapport dimension/longueur et de pouvoir de correction. Ils ont été introduits par Reed et Muller vers 1954. L'un d'entre eux a été utilisé par la NASA pour les missions spatiales de 1969 à 1976.

Soient C1 un code [n, k1, d1] (n taille des mots de code, k1 taille du message d’information et d1 la distance minimale) et C2un code [n, k2, d2] deux codes linéaires de même longueur. On fabrique un nouveau code C3= C1\* C2 de longueur 2n et de dimension k1+ k2 de la façon suivante : les mots de C3 sont les mots w= (u, u+ v) où u et v sont tous les mots de C1 et de C2 respectivement. La longueur de C3 vaut bien 2n et sa dimension k1+ k2. Pour ce qui est du poids minimum d'un tel mot w, si v≠0, son poids est au moins celui de v. Sinon, son poids est deux fois celui de u. En d'autres termes, C3= C1\* C2 est un code [2n, k1+ k2, min(2d1, d2)].

Exemples: Partons de {00, 01, 10, 11}, code [2, 2, 1] et de {00, 11}, code [2, 1, 2]. On fabrique un code [4, 3, 2] constitué de{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100}. Combinant celui-ci avec {0000, 1111} qui est un code [4,1,4], on fabrique Ĥ, code [8, 4, 4]. Combinant de dernier avec un code [8, 1, 8], on fabrique un code [16, 5, 8]. Celui-ci, à son tour combiné avec un code à répétition [16, 1, 16] fournit un code [32, 6, 16] qui a été le code utilisé par la NASA, code où 6 bits sont codés sur 4 octets avec une capacité de corriger 7 erreurs (et d'en détecter 8, mais sans pouvoir les corriger). On peut aussi mentionner les codes [32, 16, 8], proche des caractéristiques du code de Golay, et un [128, 64,16].Tous ces codes sont appelés codes de Reed-Muller.

Exercice 18:

Lors de la génération d'un code de bloc (7,4) cyclique à l'aide du polynôme x3 + x2 + 1:
(a) Quels seraient les mots de code générés pour les séquences de données 1000 et 1010?

(b) Vérifier que ces mots de code produiraient un syndrome zéro s'ils étaient reçus sans erreur. (c) Dessiner un circuit pour générer ce code et montrer comment il génère les bits de parité 110 et 001 respectivement pour les deux séquences de données dans la partie (a).
(d) Si le mot de code 1000110 est corrompu en 1001110, c'est-à-dire qu'une erreur se produit dans le quatrième bit, quel est le syndrome au niveau du récepteur? Vérifiez qu'il s'agit du même syndrome que pour le mot de code 1010001 corrompu en 1011001.

Exercice 19:

Un code de bloc (7,4) a la matrice de contrôle de parité suivante:



Ce code peut corriger une seule erreur. (a) Dériver la matrice génératrice pour ce code et encoder les données 1110. (b) Dériver un syndrome de décodage pour le code comme décrit ci-dessus et décoder les données reçues 1101110. (c) Calculer le nombre maximum d'erreurs un bloc (15,11) le code peut être corrigé. [1110010, 1]

Exercice 20:

Étant donné le codeur convolutif défini par :

 P1 (x) = 1 + x + x2 et P2 (x) = 1 + x2,

et en supposant que les données sont introduites dans le registre à décalage 1 bit à la fois, dessinez le codeur:

(a) diagramme d'arbre;

(b) diagramme en treillis;

(c) diagramme de transition d'état.

(d) Indiquez le débit du codeur.

(e) Utiliser l'algorithme de décodage de Viterbi pour décoder le bloc de données reçu, 10001000.

Exercice 21:

Pour un codeur convolutif défini par:
P1 (x) = 1 + x + x2,
P2 (x) = x + x2 et
P3 (x) = 1 + x:
(a) Indiquer la longueur de contrainte du codeur et le taux de codage.
(b) Le codeur est utilisé pour coder deux bits de données suivis de deux ‘’flushing zeros’’. Encoder les séquences de données: (i) 10 (ii) 11.
Supposons que l'encodeur contient initialement tous les zéros dans le registre à décalage et que le bit de gauche est le premier bit à entrer dans l'encodeur.
(c) Prendre les deux séquences de bits codées des parties (b) (i) et (b) (ii) ci-dessus et inverser les deuxième et cinquième bits pour créer des mots de code reçus avec deux erreurs dans chacun. Décoder les séquences modifiées à l'aide d'un diagramme en treillis et montrez si le code peut corriger les erreurs que vous avez introduites.

Exercice 22:

Soit le codeur convolutif ci-dessous :



1. S’agit il d’un codeur RSC ou NRC ?
2. Quel est le rendement de ce codeur ?
3. Déterminez le mot de code de sortie en utilisant la transformée D pour la séquence d'entrée x(n) = (1001).
4. Dessinez le diagramme en treillis de ce codeur.
5. Trouvez la fonction de transfert et la distance minimale de ce codeur.

Exercice 23:

Soit le codeur convolutif ci-dessous :



1. S’agit il d’un codeur RSC ou NRC ?
2. Quel est le rendement de ce codeur ?
3. Trouvez la réponse impulsionnelle.
4. Trouvez la matrice des fonctions de transfert.
5. Utilisez la matrice de fonction de transfert pour déterminer le mot de code associé à la séquence d'entrée x = (11,10,01).

Exercice 24:

Considérons un codeur convolutif LTE (***Long Term Evolution*** est une évolution des normes de téléphonie mobile. En octobre 2010, l'UIT a reconnu la technologie LTE-Advanced , une évolution de LTE, comme une technologie 4G) de débit 1/3 avec une longueur de contrainte K = 7, comme le montre la figure suivante :



1. Trouvez la réponse impulsionnelle.
2. Trouvez la matrice des fonctions de transfert.

Exercice 25:

Considérons un codeur convolutif appelé ‘’tail-biting’’ du standard 802.16e (Réseaux informatiques sans fil WiMax) (figure ci-dessous). A noter que les codes convolutifs ‘’tail-biting’’ (TBCC) trouvent des applications dans de nombreuses normes de communication modernes telles que LTE et IEEE 802.16e.



1. S’agit il d’un codeur RSC ou NRC ?
2. Quel est le rendement de ce codeur ?
3. Trouvez la réponse impulsionnelle.
4. Trouvez la matrice des fonctions de transfert.

Exercice 26: Soit le codeur suivant



* 1. S’agit il d’un codeur RSC ou NRC ?
	2. Trouvez les séquences génératrices de ce codeur convolutif
	3. Tracez la représentation du diagramme d'état de ce codeur

Exercice 27:

Dessinez le codeur RSC équivalent du codeur convolutif avec les séquences génératrices suivantes : g1 = [11111]; g1 = [10001].

Exercice 28: Soit le codeur suivant



* 1. S’agit il d’un codeur RSC ou NRC ?
	2. Trouvez les séquences génératrices de ce codeur convolutif
	3. Tracez la représentation du diagramme d'état de ce codeur

**Exercice 29**

Considérons l'encodeur standard CDMA2000 (Code division multiple access 2000, ou accès multiple par répartition en code 2000 est une technologie de [téléphonie mobile](https://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9phonie_mobile)) illustré à la figure suivante.



**Figure : Turbo code du standrad CDMA2000**

Recherchez le mot de code pour la séquence d'entrée x = {101100} en supposant que le treillis des codeurs est terminé. Laissez l'entrelaceur être {031524}.