Durée : 2h — Documents autorisés

Code détecteur et correcteur d'erreurs — 8 points

1 – Soient les 6 séquences binaires sur 6 bits suivantes :
4pts

A. `000000`	C. `001110`	E. `011011`
B. `010000`	D. `010101`	F. `000001`

a. Est-ce que ces séquences binaires peuvent être utilisées pour permettre la transmission de données :

◇ pour des données de quelle taille en nombre de bits ?
Il y a 6 séquences binaires et la plus grande puissance de 2 inférieure à 6 est $2^2 = 4$: on peut donc au maximum associer des séquence de données sur 2 bits.
Pour sélectionner les 4 séquences à utiliser, on va calculer les distances de Hamming et enlever les séquences qui donne une distance trop petite :
⋆ *on peut supprimer la séquence B* `010000`*, qui donne une distance de 1 avec la séquence A ;*
⋆ *on peut supprimer la séquence F* `000001`*, qui donne une distance de 1 avec la séquence A ;*
Il nous reste alors 4 séquences : A `000000`*, C* `001110`*, D* `010101` *et E* `011011` *et on peut choisir de les associer de la manière suivante :*

séquence	*donnée utilisateur*
A	*00*
C	*01*
D	*10*
E	*11*

Après avoir calculer les différentes distance de Hamming entre tous les mots de code, on détermine aue la distance de Hamming du code est 3.

◇ avec détection d'erreur ?
$d = p + 1, 3 = p + 1, p = 2 \Longrightarrow$ *on peut détecter deux erreurs simples*

◇ avec correction d'erreur ? $d = 2p + 1, 2 = p + 1, p = 1 \Longrightarrow$ *on peut corriger une erreur simple*

b. Sur le récepteur, la séquence `010101` est reçue :

◇ Est-elle correcte ? *oui, elle correspond à la séquence D*

◇ Si non, comment retrouver la séquence émise initialement ? *En s'assurant qu'une seule erreur simple a pu se produire et en calculant la distance de Hamming de cette séquence reçue avec les tous les mots de code et en remplaçant la séquence reçue par le mot de code dont la distance calculée est la plus petite.*

2 – Soit la séquence à transmettre `1010010111`.
4pts a. On veut utiliser la méthode de Hamming.

◇ Combien de bits de contrôle sont nécessaires ? *il faut 4 bits de contrôle d'après la formule de calcul* $m + k + 1 \leq 2^k$

◇ Quelle séquence sera transmise ? *La séquence* `[0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1]`.

b. On veut utiliser maintenant la méthode du CRC, « *Cyclic Redundancy Check* », avec le polynôme générateur $x^4 + x^2 + x + 1$

◇ Quelle séquence sera transmise ?

1 0 1 0 0 1 0 1 1 1 **0 0 0 0**	1 0 1 1 1
1 0 1 1 1	100 110 0100
0 0 0 1 1 1 0 1	ce quotient est sans intérêt
1 0 1 1 1	
0 1 0 1 0 1	
1 0 1 1 1	
0 0 0 1 0 1 **0 0**	
1 0 1 **1 1**	
0 0 0 **1 1 0 0**	

La séquence transmise est 10100101111100

c. On veut utiliser une méthode « hybride » : la séquence obtenue par la méthode de Hamming est ensuite utilisée avec la méthode du CRC :

◇ Quelle sera la taille de la séquence transmise ?

⋆ *la taille de la séquence transmise par la méthode du CRC est de 14 bits ;*

⋆ *on ajoute 5 bits de contrôle par la méthode de Hamming car on a :*
$m + k + 1 \leq 2^k \longrightarrow 14 + 5 + 1 \leq 2^5$

◇ Est-ce une méthode intéressante ?

L'avantage de la méthode de Hamming est de pouvoir corriger une erreur simple, alors que l'avantage de la méthode de la méthode du CRC est de pouvoir détecter des erreurs en rafales :

⋆ *Si le support de transmission ne subit qu'une erreur simple alors la méthode de Hamming est suffisante*

⋆ *Si le support de transmission subit des erreurs en rafales la méthode de Hamming ne sert à rien et son utilisation en plus de celle du CRC empèche d'utiliser la méthode du CRC.*

Cette méthode est donc inintéressante voir néfaste.