Département Informatique
IUT Bordeaux 1

Année 2005-2006
Semestre 2

TD ASR4 - Téléinformatique
Codes

1 Généralités sur les codes

Un *code* C de longueur N est un ensemble de *mots* (séquences) de N bits.[1] Un mot de N bits qui n'appartient pas à C est *invalide*.

Question 1. $N = 3$, $C = \{110, 101, 011\}$.
- Combien y a-t-il de messages de longueur N ?
- On reçoit 111, que fait-on ?
- Et pour 101 ?

La *distance de Hamming* d_h entre deux mots de même longueur est le nombre de positions qui correspondent à des valeurs distinctes.

Question 2. Calculez
- $d_h(110011, 101010) =$
- $d_h(11011111, 10101100) =$
- $d_h(0111110111, 0101110101) =$

La distance de Hamming $D_H(C)$ d'un code C est le minimum des distances entre 2 mots de ce code.

Question 3. Quelle est la distance du code $C = \{0011, 0101, 1001, 0110, 1010, 1100\}$?

La distance de Hamming d'un code permet d'évaluer son *pouvoir détecteur* d'erreur ainsi que son *pouvoir correcteur*. On parle d'*erreur d'ordre n* lorsqu'un mot émis m diffère par n bits du mot reçu m', autrement dit si $d_h(m, m') = n$.

Question 4.
- Quel est le pouvoir détecteur, vis à vis des erreurs d'ordre $n = 1, 2, \ldots$ d'un code C tel que $D_H(C) = 2$?
- A partir de quelle valeur $D_H(C)$ y-a-t-il un pouvoir détecteur ?
- Quelles erreurs sont détectées / corrigées pour $D_H(C) = 6$?

[1] En pratique, N dépasse 1000 et le nombre d'éléments est de l'ordre de $2^{99N/100}$

2 Contrôles de parité

2.1 Parité transversale (ou verticale)

L'information à transmettre est découpée en blocs de m bits[2] auxquels on adjoint un *bit de parité* de sorte que la somme des $m + 1$ bits modulo 2 soit nulle (parité paire) ou 1 (parité impaire).

Question 5. On souhaite envoyer la séquence suivante de "caractères" de 3 bits :

000 111 000 110 101 011 010

- Quelle sera la séquence effectivement transmise (en parité paire) ?
- Montrez qu'on utilise un code de longueur 4.
- Quelle est la distance de Hamming de ce code ? Son pouvoir détecteur-correcteur ?

2.2 Parité longitudinale (ou horizontale)

L'information à transmettre est formée de blocs de m bits. On ajoute, à la fin, un bloc supplémentaire de m bits. Le premier de ces bits est établi de façon à respecter la parité des bits de première position, etc.

Question 6. Quelle est la séquence transmise pour le message

000 111 000 110 101 011 010

avec $m = 3$, en parité impaire ?

Question 7. Donnez *in extenso* le code C qui correspond à des transmissions de 2 "caractères" de 2 bits.

2.3 Parité horizontale et verticale

On combine les deux procédés précédents : on ajoute a chaque caractère un bit de parité (verticale), puis on ajoute un caractère supplémentaire pour la parité horizontale.

Question 8.
- Quelle est la séquence transmise pour le message

  000 111 000 110 101 011 010

  avec $m = 3$, en parité paire verticale et horizontale ?
- Donnez *in extenso* le code C qui correspond à des transmissions de 2 "caractères" de 2 bits.
- Quelle est sa distance de Hamming ? Sa capacité de détection-correction d'erreur ?

[2] Le plus souvent, on transmet des caractères de taille fixe qui se prêtent bien à ce découpage

3 Codes polynomiaux

3.1 Polynômes, opérations

A toute séquence de n bits on peut associer un polynôme dont les coefficients binaires sont les éléments de la séquence. Exemple :

$$\begin{aligned} 011001 &= 0.X^5 + 1.X^4 + 1.X^3 + 0.X^2 + 0.X^1 + 1.X^0 \\ &= X^4 + X^3 + 1 \end{aligned}$$

Sur ces polynômes, on peut effectuer des opérations d'addition et de multiplication (qui correspondent à des opérations modulo 2 sur les coefficients[3]).

Question 9. Calculez
- $(X^7 + X + 1) + (X^3 + X + 1) =$
- $(X^7 + X + 1) \times (X^3 + X + 1) =$

La *division euclidienne* de $A(X)$ par $B(X)$ se déduit des opérations + et $\times$ sur les polynômes : on cherche $Q(X)$ et $R(X)$ tels que

$$A(X) = B(X) \times Q(X) + R(X) \text{ avec } deg(R) < deg(Q).$$

Question 10. Divisez $(X^7 + X + 1)$ par
- $(X + 1)$
- $(X^2 + 1)$

3.2 Codes

Soit $G(X)$ un polynôme (appelé générateur) de degré r. Le code polynomial $C_{G,n}$ est l'ensemble des mots de longueur n, dont le polynôme associé est un multiple de $G(X)$.

Question 11. Donnez les mots du code $C_{G,4}$, avec $G(X) = X^2 + 1$.

3.3 Détection d'erreur

Soit à envoyer un message utile M de m bits. L'émetteur et le récepteur utilisent le même polynôme générateur $G(X)$ de degré r.

Le message M' effectivement transmis est formé des m bits de données de M, suivis par r bits supplémentaires choisis de sorte que le polynôme correspondant aux $m+r$ bits soit un multiple de $G(X)$. On utilise donc le code $C_{G,m+r}$.

L'émetteur calcule les bits supplémentaires, qui sont fournis par le reste $R(X)$ de la division de $M(X) \times X^r$ par $G(X)$. En effet, si $M(X) \times X^r = G(X) \times Q(X) + R(X)$, alors $M(X) \times X^r + R(X) = G(X) \times Q(X)$, qui est un multiple de $G(X)$.

[3] L'addition modulo 2 equivaut à un ou-exclusif (et la soustraction aussi), la multiplication à un "et" logique

Question 12. Soit le message utile $M = 01011011$. Quel est le message transmis pour les polynômes générateurs suivants :
- $G_1(X) = X + 1$
- $G_2(X) = X^2 + 1$

Le récepteur contrôle le message reçu en divisant le polynôme associé par $G(X)$. Un reste non nul indique qu'une erreur a été détectée. Si le reste est nul, on récupère l'information utile (présumée correcte) en supprimant les r derniers bits.

Question 13. On reçoit 0110 1110 010, avec $G(X) = X^3 + 1$. Qu'en penser ?

Note. Les polynômes générateurs utilisés en pratique sont normalisés :
- CRC-12 : $X^{12} + X^{11} + X^3 + X^2 + X + 1$
- CRC-16 : $X^{16} + X^{15} + X^2 + 1$
- CRC-CCITT : $X^{16} + X^{12} + X^5 + 1$