TD Téléinformatique
Codes

Généralités sur les codes.

Un code de longueur N est un ensemble C de séquences de N bits. Une séquence de N bits n'appartenant pas à C sera dite invalide.

Question 1: *N=3, C={110, 101, 011}. Combien de message peut-on avoir ? Quelles sont les séquences non valides ? On reçoit 111, que fait-on ? Même question avec 101 ?*

Dans la pratique, N dépasse 1000 et le nombre d'éléments de C est de l'ordre de $2^{N-N/100}$.

La distance de Hamming d_h entre 2 séquences u et v du code C est le nombre de positions binaires des séquences u et v qui correspondent à des valeurs distinctes.

Question 2: *Calculer d_h(110011,101010), d_h(10111111,101011), d_h(01111011,101110).*

La distance de Hamming d'un code C est le minimum des distances entre 2 séquences quelconques du code C : nous la noterons $D_H(C)$.

Question 3: *Soient N=4 et C={0011,0101,1001,0110,1010,1100}. Quelle est la distance de Hamming de ce code.*

La distance de Hamming d'un code permet d'évaluer son pouvoir détecteur d'erreur ainsi que son pouvoir correcteur.

Question 4: *Que dire d'un code dont la distance de Hamming est 2 ? Même question pour 6 ? Illustrer vos réponses par un schéma.*

Exemples de code

1.1 Parité transversale (ou verticale)

L'information est sectionnée en blocs de *m* bits qui sont généralement des caractères, et on ajoute à chaque bloc un bit de parité (*r*=1) de telle sorte que la somme des *m*+1 bits modulo 2 soit nulle (parité paire) ou égale à 1 (parité impaire).

Question 5: *on souhaite envoyer la séquence suivantes de caractères de longueur 3 (m=3) : 000 111 000 111 110 101 011 010. Quelle est la séquence émise avec ce code ? Quelle est la distance de Hamming de ce code ? Donner le pouvoir détecteur/correcteur de ce code.*

1.2 Parité longitudinale (ou horizontale)

On applique la même méthode aux bits de poids identique sur la totalité d'un message découpé en 'caractères'. On combine généralement la parité transversale et parité longitudinale de la façon suivante : *l* caractères munis de leur bit de parité transversale sont regroupés en blocs, et on ajoute à la fin de chaque bloc un caractère supplémentaire pour la parité longitudinale.

Question 6: *Reprendre les mêmes questions précédentes avec l=4.*

1.3 Codes polynomiaux

Toute séquence de *i* bits peut être représentée par un polynôme à coefficients binaires dont le degré est le rang du bit non nul le plus à gauche. Par exemple, la séquence "001101" peut être représentée par le polynôme x^3+x^2+1. Sur ces polynômes, nous utiliserons les opérations d'addition et de multiplication modulo 2, ainsi que la soustraction.

Question 7: *Donner les tables de ces opérations sur {0,1}. 'Faire' les opérations suivantes :$(X^7 + X - 1) - (X^3 - X + 1)$,*
$(X^7 + X - 1) + (X^3 - X + 1)$, $(X^7 - X^2 + X) * (X^3 - X + 1)$.

La division euclidienne se déduit facilement des opération * et + sur les polynômes.

Question 8: *Donner la définition de la division euclidienne du polynôme P(X) par le polynôme Q(X). 'Faire' la division euclidienne : $(X^7 + X^6 + X^5 + X^3 + X^2)/(X^3 + 1)$*

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

Question 9: *Soient n=4 et $G(X)=X^2+1$. Donner les séquences valides du codes : $C_{G,4}$*

Application à la détection d'erreur :
Le polynôme générateur G(X) de degré *r* est connu de l'émetteur et du récepteur ainsi que la taille *m* des informations utiles. On utilise alors le code $C_{G,m+r}$

Emetteur

1. Soit " $b_{m-1}\ b_{m-2}$ ... $b_2\ b_1\ b_0$ " l'information utile (que l'on désire transférer) de longueur m, et M(X) le polynôme associé à l'information utile. On va travailler avec le code $C_{G,m+r}$.
2. On divise le polynôme $M(X).X^r$ par G(X) et on obtient alors un reste R(X) de degré r-1 : $M(X).X^r = G(X).Q(X) + R(X)$ (division est réalisée par un circuit électronique appelé diviseur et bâti autour d'un registre à décalage)
3. On envoie la séquence de bits de longueur n=m+r associée au polynôme : $N(X)=M(X).X^r + R(X)$. A noter que la séquence envoyée est construite en rajoutant à l'information utile, la suite binaire associée au polynôme R(X). Ce polynôme N(X) est divisible par G(X). En effet : $M(X).X^r + R(X) = G(X).Q(X) + R(X) + R(X) = G(X).Q(X)$.

Récepteur

4. Le récepteur reçoit une séquence binaire. La détection d'erreur consiste à vérifier que le mot reçu est bien un mot du code $C_{G,m+r}$, c'est-à-dire que N'(X), le polynôme associé à la séquence binaire reçue, est divisible par G(X).
   - si le polynôme est divisible par G(X) alors la transmission est supposée correcte (il n'y a pas d'erreur détectable par ce code). Il suffit alors d'extraire l'information utile en supprimant les r derniers bits de la séquence reçue.
   - si le polynôme n'est pas divisible par G(X) alors une erreur a eu lieu pendant la transmission et le récepteur demandera une retransmission du message.

Question 10: *soient $G(X)=X^2+1$ et m=5. On veut transférer l'information " 0 0 1 0 1 ". Quelle séquence est envoyée ?*
On reçoit "0 1 1 0 1 1 0" : sommes-nous en présence d'une erreur de transmission ? Donner un exemple d'une situation inverse.

Dans la pratique, on utilise des polynômes générateurs normalisés :

- CRC-12 = $X^{12}+X^{11}+X^3+X^2+X^1+1$,
- CRC-16 = $X^{16}+X^{15}+X^2+1$,
- CRC-CCITT = $X^{16}+X^{12}+X^5+1$.

Leur efficacité se passe de commentaires puisqu'il permet de détecter :

- 100% des erreurs simples, doubles,
- 100% des paquets d'erreurs de longueur <17,
- 99,997% des paquets d'erreurs de longueur 17...

et tout cela, en rajoutant seulement 16 bits de redondance sur un message dont la taille courante est de l'ordre de 1000 bits.

1.4 Codes ‘i parmi n’

Dans ce code de longueur *n*, *i* bits doivent être égaux à 1.

Question 11: *Donner le nombre de combinaisons valides. Prendre un exemple de ce code et l'étudier…*