

TD n° 1 (suite) – Méthodes pour garantir l'intégrité de l'information

F. Butelle & L. Finta

02/2016

Objectifs : comprendre les principes des méthodes de détection et de correction d'erreur.

EXERCICE 1 - Détection d'erreur

1.1 Bit de parité

Pour protéger l'information utile on peut utiliser dans une communication la parité paire. On considère ici que l'information utile échangée est de type texte ASCII 7 bits.

Question 1 : Donnez la suite de bits à émettre pour le mot "BAC"

Le destinataire reçoit à un instant donné la suite de bits suivante : 0x 46 41 42 45.

Question 2 : Que peut-il conclure sur l'intégrité de l'information reçue ? Quel est le contenu du message ?

Question 3 : Quelles sont les limites de l'utilisation du bit de parité ? Et ses avantages ?

1.2 VRC+LRC

Une technique un peu plus robuste basée sur la parité est le VRC+LRC.

On considère le message «CONNECT» (codes ASCII : 0x 43 4F 4E 4E 45 43 54), transmis avec VRC (parité impaire) et LRC (idem) (ASCII 7bits).

Question 4 : Quelle est la suite de bits transmise ?

Question 5 : Quelle est la plus simple altération des bits non détectable par le VRC+LRC ? Indication : il faut changer 4 bits.

Question 6 : Quelles sont les limites de l'utilisation du VRC+LRC ? Et ses avantages ?

1.3 Checksum

C'est un autre moyen de détection des erreurs un peu plus efficace que les techniques basées sur la parité.

Il est employé par exemple dans les archives de type zip et dans l'entête du paquet IP.

Question 7 : On veut protéger par Checksum le texte ASCII 8bits suivant : hello (le code ASCII de "a" est : 0x61). Quelle est la suite d'octets transmise ?

Question 8 : Donnez une altération des bits non détectable par le Checksum. Indication : au min. il faut changer 2 bits.

Question 9 : On ajoute un compteur sur un octet à la fin du message précédent. Calculez le nouveau checksum si ce compteur vaut 1 ou 0.

Question 10 : Quelles sont les limites de l'utilisation du Checksum ? Et ses avantages ?

1.4 CRC

C'est une méthode plus élaborée de détection des erreurs. On considère la suite de bits utile suivante : 10 1111 1101 et le polynôme générateur $G(X) = X^4 \oplus X^3 \oplus X^2 \oplus 1$.

Question 11 : Quelle est la suite de bits transmise ?

Question 12 : Le destinataire reçoit la suite suivante : 1 1111 0000. La suite est elle intègre ? Si oui quel est le message utile reçu ?

Question 13 : Quelles sont les limites de l'utilisation du CRC ? Et ses avantages ?

EXERCICE 2 - Détection et correction d'erreur

2.1 Code de Hamming

Soit le jeu de 4 caractères avec le codage de Hamming suivant : A=0000 0000, B=0110 1101, C=1011 0110 et D=1101 1011.

Question 1 : Quelle est la quantité d'information portée par chaque caractère transmis ?

Question 2 : Quelle est la distance de Hamming de ce jeu de caractères ?

Question 3 : Calculez les distances de Hamming entre chaque caractère du jeu et la suite de bits reçue : $x=1100\ 1010$. Peut-on distinguer à quel caractère réellement émis correspond x ?

Question 4 : Même question que 3 mais pour la suite reçue $y=1000\ 1010$.

Question 5 : Quelles sont les limites de l'utilisation du code de Hamming ? Et ses avantages ?