Réseaux et protocoles

Maitrise d'informatique ©

REPR
td 4
99-00

La protection contre les erreurs

Introduction

Lors des premiers TD nous avons étudié les différentes techniques permettant d'adapter le signal au support de transmission, ceci afin d'exploiter au mieux les capacités (en débit) du support tout en limitant l'altération du signal, et donc en limitant les erreurs sur le message reçu. Néanmoins, pour parfaire la qualité de la transmission, des procédés supplémentaires sont nécessaires : nous travaillerons dans ce TD sur les procédés de détection et de corrections d'erreurs faisant intervenir un codage redondant des messages à transmettre.

L'idée de base est la suivante (détection d'une erreur): les messages à transmettre (données) sont des éléments de B^k (2^k mots binaires de longueur k). La permutation d'un bit d'un élément de B^k fournit un autre élément de B^k.

Les éléments de B^k vont être codé par des éléments de B^n $(n \succeq k)$. L'image des éléments de B^k dans B^n fournit l'ensemble des codes possibles (ou tout simplement "le code"). "Le code" est en bijection avec B^k un mot du code correspond à une donnée et une seule.

B^n étant "plus grand" que B^k (2^n éléments) on s'arrange pour que les mots de code possibles soient "espacés" les un des autres. Ainsi, une erreur sur un bit d'un mot codé fournit un mot qui ne fait pas partie des codes possibles :on peut détecter l'erreur (et éventuellement la coriger).

Question 1 *On se place du point de vue du récepteur, recevant un message codé.*

a) Qu'est-ce qu'un message éronné?

b) Qu'est-ce qu'un message détecté éronné?

c) Qu'est-ce qu'un message corrigeable?

d) Dans quel cas un message éronné peut-il être jugé correct par le recepteur (i.e. non éronné)? Dans ce cas qu'en est-il des données délivrées par le décodage du message?

1 Codes de parités longitudinales (LRC) et verticales (VRC)

Note : VRC = Vertical Redundancy Check, LRC = Longitudinal Redundancy Check

Question 2 *On considère les lettres O,S,I codées sur 7 bits par 1001111, 1010011 et 1000011.*

a) Donner la suite de bits transmise lorsque l'on effectue un codage de parité paire vertical (VRC).

b) Idem lorsque l'on compète par un LRC.

c) Combien d'erreurs un tel codage permet il de détecter et/ou corriger ?

d) Quel est le rendememt d'un tel code ?

2 Codes Linéaires

Dans un code linéaire, les bits du code s'obtiennent par combinaison linéaire des bits de données. Le procédé de codage peut être définit par une matrice G dite matrice génératrice du code. Le code du message M est M*G.

Question 3 *Rappeler la signification des paramètres n et k d'un code (n,k). Rappeler ce qu'est* la distance de Hamming entre deux mots, ce qu'est la *distance de Hamming d'un code. Soit poids(m) le nombre de bits un dans le mot m, soit + l'addition binaire (i.e. ou exclusif). Exprimer la distance de Hamming entre deux mots à l'aide de poids et de +.*

Question 4 *Donner l'ensemble des mots du code (3,2) dit code par bit de parité paire. Quelle est sa distance ?*

Question 5 *Détection et correction d'une erreur : taille minimale de l'espace de codage. Trouver une relation reliant k (taille des mots à coder), et r (bits supplémentaires du codage) pour que la détection et la correction d'erreurs simples soit possible.*

Question 6 *Quelle distance de Hamming minimale un code doit-il avoir pour être sûr de détecter (resp. corriger) p erreurs ?*

Question 7 *Soit G la matrice génératrice*

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

a) Donner le code de M = 010.

b) Qu'est-ce qu'un matrice de contrôle ? Qu'est-ce que le syndrôme *?*

c) Donner la forme (générale) de G et de H lorsque le code est systématique (cf. cours).

d) Donner la matrice de contrôle de la matrice G ci-dessus.

e) Vérifier, en calculant le syndrôme, *que le code trouvé en a) est reconnu .*

Question 8 *Qu'appelle t-on code de Hamming? Quelles sont ses propriétés?*

Question 9 *Soit M' le code de M=010 par la matrice G précédente. Soit M" un message éronné (erreur sur le bit 3 de M'). Montrer comment le code G permet de détecter cette erreur. Peut-on la corriger?*

3 Codes cycliques et polynomes

Les polynômes fournissent un outil puissant (et élégant) pour représenter les mots binaires et manipuler les codes. Un mot binaire $a_n a_{n-1} ... a_0$ (avec $a_i \in B$) va être représenté par le polynôme $a_n x^n + a_{n-1} x^{n-1} + ... + a_0 x^0$. Noter qu'un mot de longueur L s'exprime par un polynôme de degré $\preceq L-1$ (= L-1 si le bit de poids fort du mot est 1). Exemple : le mot 1001 est représenté par le polynôme $x^3 + 1$.

Un code (polynomial) (n,k) est défini à partir d'un polynôme, dit *polynôme générateur* G(x), de degré r =n-k. est le nombre de bits redondants, qui viennent compléter le mot de longueur k à coder. Soit M(x) le mot à coder. Le codage consiste à calculer le reste $R(x)$ de la division de $x^r * M(x)$ par $G(x)$. $x^r * M(x) = Q(x)G(x) + R(x)$, ou encore : $R(x) = x^r * M(x) \, mod \, G(x)$. R(x) est de degré $\preceq r$. Le code transmis est $T(x) = x^r * M(x) - R(x)$ (qui vaut aussi $x^r * M(x) + R(x)$).

Le décodage d'un mot reçu T'(x) consiste à calculer le reste de T(x) par le même polynôme générateur G(x). T'(x) fait partie du code ssi ce reste est nul.

Question 10 *Vérifier, sur l'exemple déjà traité en question 2, que le procédé de parité longitudinale revient à effectuer un codage à l'aide du polynôme générateur* $x^8 + 1$.

Question 11 *Coder les deux premiers octets de la question 1 selon le polynôme générateur de l'avis V41 du CCITT :* $x^{16} + x^{12} + x^5 + 1$.

Remarque : ce code fait partie des codes "cycliques" ; on appel ainsi les codes linéaires tels que toute permutation circulaire d'un mot du code fournit un autre mot du code.

Question 12 Quelques résultats généraux *Soit T(x) un code transmis, et T'(x) = T(x) + E(x) le code reçu. E(x) représente l'erreur (i.e. la liste des bits inversés).*
a) Montrer que T'(x) appartient au code ssi E(x)/G(x) est nul.
b) Pourquoi les erreurs telles que E(x) est multiple de G(x) ne sont elles pas détectées?
c) Pourquoi les erreurs simples sont elles détectées dès que G(x) contient au moins deux termes?
d) Montrer qu'une erreur double s'exprime sous la forme $E(x) = x^i * (x^{j-i} + 1)$. *Expliquer pourquoi les erreurs doubles sont détectées des que G(x) n'est pas multiple de x ET G(x) n'est pas multiple de* $x^k + 1$ *pour tout* $k \in [1...n]$.
e) Montrer qu'un polynôme divisible par (x+1) comporte nécessairement un nombre pair de termes. Quels types d'erreurs les polynômes générateurs multiples de x+1 permettent ils de détecter?