

Sécurité des réseaux :
codage

TRAVAUX DIRIGES

Auteurs

Line Perret & Jean-Yves ANTOINE

Introduction

QUESTIONS DE COURS

Exercice 1 — Etude d'un code

On considère l'application e définie de $\{0,1\}^3$ vers $\{0,1\}^8$ donnée par le tableau suivant:

b	e(b)
000	00000000
001	10111000
010	00101101
011	10010101
100	10100100
101	10001001
110	00011100
111	00110001

1- Etude du code

- a) S'agit-il d'un code?
- b) Quelle est sa distance minimale ?
- c) Que peut-on affirmer sur le nombre d'erreurs détectées?
- d) Que peut-on affirmer sur le nombre d'erreurs corrigées?

2- Comment décoder le mot reçu (11100101) par maximum de vraisemblance?

3 – Ce code est-il un code parfait ?

Exercice 2 — Code par répétition

On s'intéresse dans cet exercice au codage par répétition. Il s'agit d'un codage $(m,3m)$ dans lequel chaque mot $b=b_1b_2\dots b_m$ est codé $e(b)=b_1b_2\dots b_mb_1b_2\dots b_mb_1b_2\dots b_m$. On se place dans le cas où $m=1$. On note p la probabilité qu'un bit soit mal transmis.

- 1- Quelle est la probabilité qu'un mot de code $e(b)$ soit mal transmis?
- 2- Quelle est la probabilité que le receveur ne détecte pas qu'un message est faux?
- 3- Parmi les messages mal transmis, quelle est la proportion de messages non détectés?
- 4- Application numérique : $p=0.1$ et $p=0.05$.
- 5- Comparer ces résultats numériques à un envoi simple sans codage préalable. L'augmentation du nombre de bits à introduire par le codage introduit-il finalement un risque plus grand d'avoir une transmission erronée de l'information désirée ?
- 6- On revient au code par répétition. On suppose que le receveur effectue sur chaque message reçu une correction par maximum de vraisemblance lorsque celui-ci n'est pas un mot de code et qu'il l'accepte sinon. Quelle est la probabilité que le message soit faux après correction?

Exercice 3 — Etude d'un code

Dans le cadre de la transmission d'informations binaires, on considère un codage $e: B^m \rightarrow B^n$ où $B = \{0,1\}$.

b	e(b)
000	00000000
001	10101010
010	11110000
011	01010101
100	00001111
101	00110011
110	11001100
111	11000001

- 1- Est-ce un code ? Comment décode-t-on les mots (10000001) et (10001000) par maximum de vraisemblance. Conclusion sur la capacité de correction du code ?
- 2- Quel est la distance du code ?
- 3- Quelle est sa capacité de détection et de correction ? Ce résultat était-il attendu ?

EXERCICES THÉORIQUES

Exercice 4 — Inégalité de Hamming

L'inégalité de Hamming n'est pas qu'un résultat théorique sans intérêt. Elle permet au contraire de définir les caractéristiques grossières (distance optimale ou nombre de bits de contrôle minimal) d'un codage pour répondre à un besoin donné. On s'intéresse ici à des codes quelconques de $\{0,1\}^m$ dans $\{0,1\}^n$. On note t le nombre d'erreurs corrigés (nombre de bits erronés qu'un code est capable de corriger).

- 1- Rappeler l'inégalité de Hamming permettant de lier m, n et t .
- 2- *Utilisation de l'inégalité*
 - a) On suppose ici $n=6$ et $m=3$. Quel est le nombre max d'erreurs corrigées donné par l'inégalité de Hamming? Existe-t-il un code satisfaisant ces conditions?
 - b) On s'intéresse ici à une transmission sur deux octets ($m=16$) pour laquelle on aimerait pouvoir corriger deux bits ($t=2$). Quel est le nombre minimal de bits de contrôle nécessaire pour espérer satisfaire ces conditions.
 - c) On se propose enfin de chercher la plus petite longueur possible d'un code (binaire) corrigeant deux erreurs et contenant 4 bits d'information. Quelle est la distance minimale d'un tel code? Trouver la plus petite longueur de code convenant à cette expression des besoins.

Codes linéaires

QUESTIONS DE COURS

Exercice 1

On considère le code suivant:

b	e(b)
000	0000000
001	0010110
010	0101000
011	0111110
100	1000101
101	1010011
110	1101101
111	1111011

Vérifier qu'il s'agit d'un code linéaire. On précisera sa matrice génératrice.

Exercice 2

On considère un code linéaire dont la matrice génératrice est donnée ci-dessous:

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

- 1- Comment code-t-on (101) ?
- 2- Déterminer les mots de code.
- 3- Déterminer la distance minimale du code.
- 4- Vérifiez la proposition de Hamming pour ce code.

EXERCICES THÉORIQUES

Exercice 3 — Distance minimale d'un codage linéaire

On considère un code linéaire.

- 1- Montrer que la distance la plus courte qui sépare un mot de code a de tous les autres mots de code est la même quelque soit a (on pourra utiliser le résultat du cours : l'équation $a+x=b$ admet comme unique solution $x=b+a$.)
- 2- En déduire que la distance minimale d'un code linéaire est égale à la plus courte distance séparant 0 de tout autre mot de code.

Exercice 4

Démontrer que dans un code linéaire, ou bien tous les mots de codes ont un poids pair, ou bien la moitié ont un poids pair et la moitié ont un poids impair.

Codes linéaires systématiques

Exercice 1 — Décodage par le tableau standard et par les syndromes

On considère un code linéaire dont la matrice génératrice est donnée ci-dessous:

$$G = \begin{pmatrix} & & & 0 & 1 \\ \text{Id}_3 & & 1 & 0 \\ & & & 1 & 1 \end{pmatrix}$$

- 1- Donnez la longueur, la dimension et la distance de ce code.
- 2- Construisez le tableau standard correspondant à ce code
- 3- Décodez (11010) par la méthode du tableau standard
- 4- Donnez la matrice de contrôle correspondant à ce code systématique.
- 5- Calculez alors les syndrome de ce code
- 6- Décodez maintenant (11010) par la méthode des syndromes.

Exercice 2 — Syndromes

On s'intéresse à un code linéaire systématique dont la matrice génératrice est $G = \begin{bmatrix} 1000011 \\ 0101001 \\ 0010101 \end{bmatrix}$

- 1- Quels sont les mots de code ? Quelle est la distance minimale d'un tel code ?
- 2- Quelle est la matrice de contrôle d'un tel code?
- 3- Quels sont tous les messages dont le syndrome est (0110) ?

Exercice 3

Pour chacun des codes suivants définis par leur matrice génératrice G_i , donner la matrice de contrôle et la liste des syndromes.

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Exercice 4 — Code défini par sa matrice de contrôle

Il arrive que les code linéaires systématiques soient définis non pas par leur matrice génératrice mais par leur matrice de contrôle. C'est en particulier le cas de la classe très connue des codes de Hamming. Soit un code linéaire systématique dont la matrice de contrôle

est la matrice H donnée ci-dessous

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- 1- Quelle est la longueur des mots à transmettre?
- 2- Quelle est la longueur des mots de code?
- 3- Coder les mots (1101) et (0110).
- 4- Corriger les mots reçus (0110101) et (1110011) par maximum de vraisemblance.

Exercice 5

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

On considère un code linéaire donnée par sa matrice génératrice G=

- 1- Déterminer tous les mots de codes. Quelle est la distance minimale du code? Donner le nombre d'erreurs corrigées.
- 2- On reçoit les messages suivants (1111101), (1100111), (0100000), (1111100), (0111000), (1110101). Comment sont-ils corrigés?

Exercice 6 — Codage de Hamming (examen 2004-2005)

On s'intéresse à un codage linéaire systématique de matrice de contrôle H tq :

$$H = \begin{bmatrix} 1101 \\ 1001 \\ 1110 \\ 1111 \\ 0111 \\ 1010 \\ 0101 \\ 1011 \\ 1100 \\ 0110 \\ 0011 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$$

- 1) Ce code est-il un code de Hamming ? Quelle est la longueur des mots à transmettre (dimension du code) ? Quelle est la longueur des mots de codes ? Le nombre de bits de contrôle ? Combien y-a-t-il de mots de codes ? Justifiez vos réponses.
- 2) Donnez la matrice génératrice du code.
- 3) On souhaite transmettre le mot (11101001001). Quel est le mot de code correspondant ?

- 4) On reçoit le mot (000100011011010). Montrez que ce n'est pas un mot de code. Comment est-il corrigé par maximum de vraisemblance ?
- 5) Retrouvez cette correction par la méthode du syndrome.

EXERCICES THÉORIQUES

Exercice 7

On s'intéresse à des codages de B^m dans B^n .

- 1- Dans le cas où $m=2$ et $n=3$, faire la liste de tous les codages systématiques possibles. Combien sont linéaires?
- 2- Plus généralement pour m et $n>m$ fixés, combien existe-t-il de codages systématiques? Combien sont linéaires?

Exercice 8

Que peut-on dire d'un codage linéaire systématique dont la matrice de contrôle contient deux lignes identiques?

Exercice 9 — Codes de Hamming : démonstrations du cours

Soit r un entier supérieur ou égal à 2. On parle de code de Hamming pour tout codage linéaire systématique $e: \{0,1\}^m \rightarrow \{0,1\}^n$ tel que $m=2^{r-1}-r$ et $n=2^r-1$ pour lequel les lignes de la matrice de contrôle sont tous les mots non nuls de r bits. (On pourra remarquer que r correspond au nombre de bits de contrôle de ce code)

- 1- Donner les matrices de contrôles pour les codes de Hamming correspondant aux valeurs $r=3$ et $r=4$. Quelle est la distance minimale de ces codes?
- 2- Justifier que pour tout code de Hamming, la distance minimale est toujours égale à 3.
- 3- "*Code de Hamming et code parfait*"
 - a) Ecrire l'inégalité de Hamming.
 - b) On revient au cas où $r=3$. Donner tous les mots de codes. Etant donné un mot de code quelconque noté M , combien y-a-t-il de mots de $\{0,1\}^7$ à une distance 1 de M ? En déduire que l'inégalité de Hamming est une égalité pour ce code.
 - b) Montrer que pour tout code de Hamming, l'inégalité de Hamming est une égalité. (De tels codes sont dits parfaits)
- 4- Expliquer pourquoi les lignes de la matrice de contrôle d'un code de Hamming sont distinctes et non nulles.
- 5- Etant donné un code quelconque $e: \{0,1\}^m \rightarrow \{0,1\}^n$, on appelle rendement d'un tel code le rapport $\rho=m/n$, qui correspond à la proportion de bits porteurs d'informations. Montrer que pour r fixé (nombre de bits de contrôle), un code de Hamming est un codage linéaire systématique satisfaisant ρ maximum.

Codes polynomiaux

QUESTIONS DE COURS

Exercice 1

On s'intéresse dans cet exercice à des code polynomiaux de polynôme générateur $G(x)$.

- 1- On considère $G(x)=x^3+1$. Le message à envoyer est $M=(10011011)$, quel est le message transmis?
- 2- Même question pour $G(x)=x^4+x+1$, le message à envoyer étant (1101011011) .

Exercice 2

On s'intéresse dans cet exercice à un code polynomial de polynôme générateur $G(x)=x^6+x^4+x+1$.

- 1- On reçoit le message (101011000110) . Le message reçu est-il correct? Si oui, quel est le message initialement transmis? Quel est son syndrome ?
- 2- Mêmes questions pour le message (110111111000) .


Exercice 3

On considère un code polynomial de $\{0,1\}^4 \rightarrow \{0,1\}^7$ dont le polynôme générateur est $G(X)=X^3+X+1$.

- 1- Déterminer la matrice génératrice de ce code et tous les mots de code. Donner la matrice de contrôle. Déterminer la distance minimale du code. Donner le nombre d'erreurs détectées et le nombre d'erreurs corrigées. Le code proposé est-il un code parfait ?
- 2- Le mot reçu est (1010111) . S'agit-il d'un mot de code ? Calculer son syndrome de 2 façons différentes (en utilisant la matrice de contrôle, et en se servant du polynôme générateur). Comment est-il corrigé ?
- 4- On considère le mot à transmettre (0000) . On suppose qu'à la transmission se produit une salve d'erreurs de longueur 3. Quels sont les différents mots susceptibles d'être reçus ? Retrouver qu'une telle erreur est nécessairement détectée. Faire de même pour (1111) .

Exercice 4 (Examen 2004-2005)

On s'intéresse à un code polynomial de $B^m \rightarrow B^n$ et de polynôme générateur $P(X) = 1 + X^2 + X^4 + X^5$.

- a) On souhaite transmettre des mots binaires de longueur 4 avant codage (dimension $m = 4$). Quelle est la longueur du code correspondant ?
- b) On considère le mot à transmettre $M = (1 0 1 1)$. Quel est le mot de code correspondant à M ?
- c) Montrez que ce code polynomial est bien un code linéaire 

- d) Construisez alors la matrice génératrice correspondant au code. Est-on en présence d'un code systématique ? Justifiez votre réponse.

EXERCICES THÉORIQUES

Exercice 5

On considère un code polynomial de $B^m \rightarrow B^n$ de polynôme générateur G de degré $r=n-m$.

- 1- On suppose qu'à la transmission une salve d'erreur de longueur $r+1$ s'est produite. Déterminer - en fonction de r - la probabilité qu'elle soit détectée.
- 2- Application numérique pour les polynômes CRC-12, CRC-16 et CRC-CCITT

Exercice 6

A chaque lettre de l'alphabet, on fait correspondre un mot binaire de 5 lettres selon le principe suivant A codé en 00000, B codé en 00001, C codé en 00010, D codé en 00011 etc. l'espace est codé en 11010, le point en 11011, la virgule en 11100, le point d'interrogation en 11101 et le point d'exclamation en 11110, l'apostrophe en 11111.

- 1- Faire un tableau complet représentant les différents codes binaires et les polynômes correspondants de chacun des caractères décrit ci dessus.
- 2- On s'intéresse à un code polynomial de polynôme générateur $G(x)=x^3+1$. Quelle est la longueur des mots transmis?
- 3- Ecrire un message et le coder. (message de 7 caractères au plus...)
- 4- Prendre le message codé de son voisin, vérifier qu'il n'y a pas d'erreur et le décoder

Codes cycliques

QUESTION DE COURS

Exercice 1

On considère un code polynomial de $\{0,1\}^4 \rightarrow \{0,1\}^7$ dont le polynôme générateur est $G(X)=X^3+X+1$.

- 1- G est-il un polynôme primitif? Le code considéré est-il un code cyclique ?
- 2- Déterminer la matrice génératrice de ce code et tous les mots de code. Donner la matrice de contrôle.
- 3 - A l'aide de la question précédente, déterminer la distance minimale du code. Donner le nombre d'erreurs détectées et le nombre d'erreurs corrigées. Ce résultat est-il cohérent avec les résultats du cours sur les codes cycliques primitifs ?
- 4 - Le mot reçu est 1010111. S'agit-il d'un mot de code ? Calculer son syndrome de 2 façons différentes (en utilisant la matrice de contrôle, et en se servant du polynôme générateur). Comment est-il corrigé ?
- 5 - Le code proposé est-il un code parfait ? S'agit-il d'un code de Hamming ?
- 6 - On considère le mot à transmettre 0000. On suppose qu'à la transmission se produit une salve d'erreur de longueur 3. Quels sont les différents mots susceptibles d'être reçus ? Retrouver alors qu'une telle erreur est nécessairement détectée. Faire de même pour le mot 1111.

REGISTRES LINEAIRES

Exercice 2

On considère un code polynomial de $\{0,1\}^2 \rightarrow \{0,1\}^4$ dont le polynôme générateur est $G(X)=X^2+1$.

- 1 - G est-il un code cyclique ?
- 2 – En utilisant un registre linéaire correspondant à $G(X)$, calculez tous les mots du code. Quelles propriétés des codes cycliques vérifiez-vous ?
- 3- On veut transmettre le mot (11). Codez ce mot tout d'abord par calcul polynomial et ensuite à l'aide d'un registre linéaire.

Codes correcteurs de paquets d'erreurs

CODE ENTRELACÉ

Exercice 1 – Décodage de paquets d'erreurs et codes entrelacés

On considère le code polynomial de $\{0,1\}^2 \rightarrow \{0,1\}^6$ dont le polynôme générateur est $G(X)=X^4+X^2+1$.

- 1 – Calculez l'ensemble des mots de code de G par la méthode de votre choix.
- 2 – Quelle est la distance de ce code ? Déduisez-en les capacités de détection du code.
- 3 – Etablissez le tableau standard du code dans l'hypothèse du décodage de paquets d'erreurs non aléatoires. Pouvez-vous en déduire les capacités du code en matière en terme d'étendue maximale des paquets d'erreurs détectables ?.
- 4 – On utilise ce code avec un entrelacement de profondeur 3. Donnez la suite de mots correspondant alors au codage du message (11) (10) (01).
- 5 – Quelles sont les capacités de détection de paquets d'erreur de ce nouveau code ? Vérifiez expérimentalement cette capacité sur un exemple bien choisi par vos soins.
- 6 – Mêmes questions avec un entrelacement à retard de 1.