Université Côte d'Azur — L3 Info, L3 MI, L3 ST
Cryptographie et calcul symbolique — 2023-24

TD n° 2

Codes correcteurs – Codes linéaires – Codes de Hamming

Exercice 1) Citez des exemples de codes issus de la vie courante qui utilisent la redondance afin de contrôler l'intégrité des messages, voire de corriger des erreurs.

Exercice 2) Bits de parité 2D On reçoit le message suivant en un bloc de 4 caractères ASCII. Chaque caractère est donc composé de 7 bits suivis du bit de parité (*Longitudinal Redundancy Check*). La dernière ligne constitue le *Vertical Redundancy Check* opéré sur le bloc tout entier.

lettre	ASCII	code ASCII en binaire							**LRC**
H	72	1	0	0	1	0	0	0	**0**
M	77	1	0	0	1	1	0	1	**1**
L	76	1	0	0	1	1	0	0	**1**
P	80	1	0	1	0	0	0	0	**0**
!	33	0	1	0	0	0	0	1	**0**
	VRC	**0**	**1**	**1**	**0**	**0**	**0**	**0**	

1. Des erreurs se seraient-elles glissées dans le message lors de la transmission en binaire ?
2. Supposons qu'en cas d'erreur, il y en ait au plus une. La correction devient-elle possible ?
3. Le cas échéant, corrigez ce message en forme d'appel au secours.

Exercice 3) N° de Sécurité Sociale Un numéro n de *Sécurité Sociale* ou numéro NIR est muni d'une clef de contrôle k sur 2 chiffres de telle sorte que $n + k \equiv 0 \mod 97$.

1. Quel est le *rendement* de ce code ?
2. Chloé a oublié la clef de son numéro de sécurité sociale $n = 2.99.11.06.222.007$. Aidez-la à retrouver cette clef.
3. Eric se présente avec le numéro $m = 1.20.02.06.071.003$ assortie de la clef est $k = 68$. Ce numéro est-il valide ? Peut-on détecter s'il y a eu erreur ? En supposant qu'il y ait une erreur au maximum dans le numéro (pas dans la clef !), peut-on la corriger ?
4. Vous pourrez vérifier, en toute confidentialité, que votre propre numéro est valide.

Exercice 4) Code linéaire On considère un code linéaire C de distance minimale $d_{min}(C) = d$. Montrez les trois assertions suivantes :

1. La distance minimale d de C coïncide avec le poids minimal $w_{min}(C)$;
2. Si $d \geq e + 1$ alors C peut détecter au plus e erreurs ;
3. Si $d \geq 2e + 1$ alors C peut corriger au plus e erreurs.

Exercice 5) Petits codes de Hamming

1. Combien y a-t-il *a priori* de codes de Hamming de redondance $r = 2$? Précisez pour chacun sa matrice de contrôle.
2. Considérons celle où les colonnes donnent dans l'ordre les 3 premiers entiers en binaire. Trouvez la matrice génératrice G correspondante.
3. Les autres matrices de contrôle donneraient-elles une matrice génératrice différente ?
4. Combien y a-t-il de mots dans ce code ?
5. Donnez pour chaque mot du code ceux qui sont dans sa boule de Hamming de rayon 1.
6. Pourquoi dit-on d'un tel code qu'il est *parfait* ?

Exercice 6) Codes de Hamming

On considère le code de Hamming entièrement spécifié par la matrice de contrôle H suivante :

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

1. Trouvez la matrice génératrice G de ce même code de Hamming. Quel lien a-t-elle avec la matrice de contrôle H ?
2. Un émetteur veut encoder les deux messages $\mathcal{M}_1 = 0110$ et $\mathcal{M}_2 = 1011$. Calculez les messages codés $\mathcal{C}_1$ et $\mathcal{C}_2$ correspondants en indiquant comment vous faites.
3. Le récepteur reçoit le message $\mathcal{R} = 1101000$. Pour contrôler l'intégrité de $\mathcal{R}$, calculez-en le syndrome S. Vérifiez si le message reçu $\mathcal{R}$ est bien celui qui a été transmis.
4. Le cas échéant, proposez une correction de $\mathcal{R}$ qui corresponde au message codé réellement transmis puis ôtez-lui sa redondance.

Exercice 7) Codes de Hamming

On considère le code de Hamming qui, au message binaire $\mathcal{M} = (m_1\ m_2\ m_3\ m_4)$ associe le mot de code $\mathcal{C} = (m_1\ m_2\ m_3\ c_1\ m_4\ c_2\ c_3)$ avec $c_1 = m_1 + m_3 + m_4$, $c_2 = m_1 + m_2 + m_3$ et $c_3 = m_2 + m_3 + m_4$. *Vous expliquerez vos calculs.*

1. Donnez la matrice génératrice G de ce code de Hamming.
2. Déduisez-en la matrice de contrôle H associée de sorte que le produit $H.{}^tG = [0]_{3,4}$.
3. Un récepteur reçoit les messages $\mathcal{R}_1 = 1010010$ et $\mathcal{R}_2 = 0010111$. Contrôlez l'intégrité de chacun de ces messages, corrigez-les si nécessaire (en supposant qu'une seule erreur ait pu se produire), et restituez pour chacun les messages d'origine $\mathcal{M}_1$ et $\mathcal{M}_2$.
4. Expliquez en quoi un tel $(7, 4)$-code de Hamming est un code linéaire *parfait*.

Exercice 8) Codes CRC
Voici un code CRC de degré $r = 3$ défini par son polynôme générateur $P_g = x^3 + x^2 + 1$.

1. On souhaite coder le message $m = 100101$. Commencez par mettre le message m sous la forme du polynôme P_m. Calculez le polynôme P_c obtenu par division de polynômes et déduisez-en le message codé c obtenu par ajout de redondance à m
2. On reçoit le message codé $c' = 1100101$. Contrôlez si c' est valide ou non ? Si oui, ôtez lui sa redondance afin de retrouver le message m' initial.

Exercices complémentaires

Exercice 9) Code de Hamming On considère le code de Hamming entièrement spécifié par la matrice de contrôle H suivante :

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

1. Le récepteur reçoit le message $\mathcal{R} = 1100001$. Vérifiez si le message reçu $\mathcal{R}$ est bien celui qui a été transmis.
2. Le cas échéant, proposez une correction de $\mathcal{R}$ qui corresponde au message $\mathcal{T}$ réellement transmis.
3. Trouvez la matrice génératrice G de ce même code de Hamming qui est entièrement conditionné par la matrice de contrôle H.
4. Déduisez-en la valeur du message $\mathcal{M} = x_1x_2x_3x_4$ codé en le message $\mathcal{T}$ par ajout de redondance.

Exercice 10) Codes CRC On considère le code CRC de degré $r = 2$ défini par son polynôme générateur $P_g = x^2 + x + 1$. Voici deux messages suivis de leur version codée transmise. Contrôlez l'intégrité de chacun des messages transmis. En cas d'échec, l'ARQ (*Automatic Repeat reQuest*) en redemande l'envoi.

1. message $\mathcal{M}_1 = 01101$ codé en $\mathcal{C}_1 = 0110110$.
2. message $\mathcal{M}_2 = 10111$ codé en $\mathcal{C}_2 = 1011111$.

Exercice 11) N° ISBN *(International Standard Book Number)* Ce numéro identifie chaque livre édité dans le monde [1]. Il comporte 10 chiffres $c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1$ séparés en quatre segments $A - B - C - D$. A identifie la communauté linguistique, B l'éditeur et C le numéro d'ouvrage chez l'éditeur. La clef de contrôle $D = c_1$ est soit un chiffre de 0 à 9, soit la lettre X qui représente alors 10. Le chiffre c_1 vérifie :

$$\sum_{i=1}^{10}(i \times c_i) \equiv 0 \mod 11$$

1. Le numéro ISBN : $212 - 345 - 680 - 2$ est-il valide ?
2. Complétez la séquence suivante pour en faire un numéro ISBN valide :

$$210 - 050 - 682 - ...$$

1. Depuis le 1er janvier 2007, les livres sont identifiés par un code-barres EAN-13 *(European Article Numbering)* qui commence par 978 ou 979 puis est suivi des 9 premiers chiffres du code ISBN mais dont le dernier chiffre est la clef de contrôle propre à ce code.