ÉNS de Lyon
2018-2019

Agrégation
Option C

TD Codes correcteurs

1 Codes

Exercice 1 — Un exemple — Soit C le code binaire défini par

$$C = \{(0000101), (0011101), (1111100), (1111111), (0101011)\}.$$

Suposons que la probabilité d'erreur de transmission de chaque bit est $p = 1/4$ (chaque bit est transmis indépendamment). Déterminer, selon le principe du maximum de vraisemblance, le mot du code dont l'envoi donne lieu à la réception de mot suivant :

(a) (1101001) ;
(b) (0110101).

Exercice 2 — Code de parité — On suppose que l'on veut transmettre un message de n bits. On rajoute à la fin du message un bit de parité : 0 s'il y a un nombre pair de 1 dans le message, 1 sinon. Le destinataire reçoit donc $n + 1$ bits.

1. Montrer que s'il y a exactement une erreur dans la transmission des n premiers bits, le destinataire peut s'en apercevoir, mais pas corriger.
2. Montrer que le destinataire ne détecte pas forcément s'il y a plus d'une erreur de transmission.

Exercice 3 — Code de répétition — On suppose que l'on veut transmettre un message de k bits. Pour cela, on répète n fois chacun des bits. Par exemple ($n = 3$) pour transmettre le message [01] on envoie [000111]. Vérifier que cela permet de corriger les erreurs lorsque leur nombre est $< n/2$.

Exercice 4 — Calculer le taux d'information du code de parité, du code de répétition.

Exercice 5 — Montrer que la distance de Hamming sur $\mathbb{F}_q^n$ est une distance.

Exercice 6 — Calculer la distance minimale du code de parité et du code de répétition.

Exercice 7 — Soit C un code donné comme une partie de $\mathbb{F}_q^n$, avec $\mathrm{Card}(C) = q^k$.

1. Quel est le cardinal d'une boule de rayon t dans $\mathbb{F}_q^n$?
2. En déduire une inégalité sur t, k et n si C est t-correcteur.

2 Codes linéaires

Soit C un code linéaire de longueur n et dimension k sur $\mathbb{F}_q$ (autrement dit C est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k). On note d la distance minimale de C. On dit que C est de type (n, k, d).

Exercice 8 — Montrer que le code de parité et le code de répétition sont des codes linéaires sur $\mathbb{F}_2$, et déterminer leur type.

Exercice 9 — Borne de Singleton — Soit $f : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ une application de contrôle pour C (c'est-à-dire une application linéaire de noyau C). On note M la matrice de f dans les bases canoniques (matrice de contrôle de C).

1. Montrer que d est le plus grand entier tel que $d-1$ colonnes distinctes de M soient toujours linéairement indépendantes.
2. En considérant le rang de M, montrer que $d \leq n - k + 1$.

Exercice 10 — Décodage — Soit $C \subset \mathbb{F}_q^n$ un code correcteur de dimension k, et M une matrice de contrôle de C. On suppose qu'on a envoyé un message $m \in C$. Notre correspondant a reçu $m' = m + e$ avec $e \in \mathbb{F}_q^n$, et il veut retrouver e.

1. Comment trouver Me ?
2. On suppose que C est t-correcteur. Soit u un antécédent de Me par M, avec $w(u) \leq t$. Montrer que si $w(e) \leq t$ alors $e = u$.

En pratique, si t est grand il n'est pas facile de trouver un u qui convient. Un problème est donc d'élaborer des codes où le décodage est facile.

Exercice 11 — Code de Hamming de longueur 7 — On prend ici $q = 2$. On note C le code linéaire donné par la matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

1. Montrer que C est un sous-espace de $\mathbb{F}_2^7$ stable par permutation cyclique des coordonnées.
2. Vérifier que C est un code correcteur de longueur 7 et de dimension 4.
3. Montrer que la distance minimale de C est 3, et que C est 1-correcteur.
4. Comparer le taux d'information de C à celui d'un code de répétition qui serait 1-correcteur.

5. Vérifier que $\mathbb{F}_2^7$ est réunion disjointe des boules centrées en les points de C et de rayon 1. Le code C est donc parfait.
6. On pose $s(x_0, \ldots, x_6) = (x_0 + x_2 + x_3 + x_4, x_1 + x_3 + x_4 + x_5, x_2 + x_4 + x_5 + x_6)$. Montrer que $C = \ker s$.
7. En considérant les colonnes de la matrice de s, montrer que s induit une bijection de l'ensemble des mots de poids 1 dans $\mathbb{F}_2^7$, sur l'ensemble $\mathbb{F}_2^3 \setminus \{0\}$.
8. En déduire un algorithme de décodage permettant de retrouver m lorsque l'on a reçu $m' = m + e$ avec $\omega(e) = 1$.

Exercice 12 — Code de Hamming étendu de longueur 8 — En reprenant les notations de l'exercice précédent, on considère le code C' de longueur 8 obtenu en ajoutant à la fin de chaque vecteur de C un bit de parité. Quelle est la dimension de C' ? Combien d'erreurs C' peut-il corriger (resp. détecter) ?

3 Codes cycliques

Dans toute la suite V désigne l'espace vectoriel $\mathbb{F}_q^n$, et C est un sous-espace vectoriel de dimension k de V. On supposera que q et n sont premiers entre eux.

On note σ l'endomorphisme de V défini par $\sigma(x_0, \ldots, x_{n-1}) = (x_{n-1}, x_0, \ldots, x_{n-2})$. On dit que le code C est cyclique si $\sigma(C) = C$.

Exercice 13 —

1. Vérifier que V est isomorphe à $\mathbb{F}_q[X]/(X^n - 1)$ par $(x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i X^i$.
2. Montrer que via cet isomorphisme, l'application σ correspond à $P \mapsto XP$.
3. En déduire que les sous-espaces vectoriels de V stables par σ sont en bijection avec les idéaux de $\mathbb{F}_q[X]$ contenant $X^n - 1$, puis qu'ils sont en bijection avec les polynômes unitaires f de $\mathbb{F}_q[X]$ divisant $X^n - 1$.

Exercice 14 — Soit C un sous-espace vectoriel de V non nul stable par σ. On désigne par $v = (a_0, \ldots, a_r, 1, 0 \ldots, 0)$ le vecteur non nul de C ayant le plus de zéros à droite, et dont le premier coefficient non nul en partant de la droite est égal à 1.

1. Montrer que v est uniquement déterminé, que $a_0 \neq 0$, et que C a pour base les $\sigma^k(v), 0 \leq k \leq m$ pour une valeur de m à déterminer.
2. Montrer que par la bijection de l'exercice précédent, C correspond à l'idéal engendré par le polynôme $f = a_0 + a_1 X + \cdots + a_r X^r + X^{r+1}$.
3. Réciproquement, montrer que si C correspond à l'idéal engendré par le polynôme $f = a_0 + a_1 X + \cdots + X^{r+1}$, alors le vecteur v correspondant est $(a_0, \ldots, a_r, 1, 0 \ldots, 0)$.
4. Exprimer la dimension de C en fonction du degré de f.
5. Quel est l'idéal correspondant au code de Hamming de longueur 7 ?

Exercice 15 — On rappelle qu'on suppose n et q premiers entre eux. On note K un corps de décomposition de $X^n - 1$ sur $\mathbb{F}_q$.

1. Vérifier que $X^n - 1$ est à racines simples dans une clôture algébrique de $\mathbb{F}_q$.
2. Soit α une racine primitive n-ième de 1 dans K (justifier son existence). Vérifier que dans $K[X]$ on a l'égalité : $X^n - 1 = \prod_{i \in \mathbb{Z}/n\mathbb{Z}} (X - \alpha^i)$.
3. En déduire que les diviseurs unitaires de $X^n - 1$ dans $K[X]$ sont en bijection naturelle avec les parties S de $\mathbb{Z}/n\mathbb{Z}$. On notera g_S le polynôme associé à S.
4. À quelle condition sur S le polynôme g_S est-il à coefficients dans $\mathbb{F}_q$? À quelle condition est-il irréductible sur $\mathbb{F}_q$?
5. Montrer que s'il existe des entiers a et s tels que $a+1, a+2, \ldots, a+s$ sont dans S, alors la distance minimale du code correcteur associé à g_S est au moins $s+1$ (on utilisera l'identification $V \cong \mathbb{F}_q[X]/(X^n - 1)$).

Exercice 16 — Codes de Hamming —

On prend ici $q = 2$ et $n = 2^s - 1$. Soit S la plus petite partie de $\mathbb{Z}/(2^s - 1)\mathbb{Z}$ stable par multiplication par 2 et contenant 1.

1. Montrer que S est de cardinal s.
2. On appelle code de Hamming de degré n le code associé à g_S. Vérifier qu'il est 1-correcteur et parfait.
3. On ne suppose plus que n est de la forme $2^s - 1$. Quels sont les ensembles S possibles dans les cas suivants :
   (a) $q = 2$ et $n = 23$.
   (b) $q = 3$ et $n = 11$.
4. Construire les codes associés à déterminer leurs types.

On voit apparaître ici le code binaire de Golay G_{23} et le code ternaire de Golay G_{11} qui sont les seuls codes parfaits non triviaux t-correcteurs avec $t > 1$.