

Codes Correcteurs

Exercice 12.1. — Soit $C(n, k)$ un code linéaire binaire de longueur n et de dimension k qui corrige au maximum t erreurs. Le poids du mot m — le nombre de composantes non nulles de m — est noté $\text{wt}(m)$. On note $x \cdot y$ le produit bit à bit des mots x et y ,

1. Montrer que $\text{wt}(x) = \sum_{i=1}^n x_i$.
2. Montrer que : $\text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2\text{wt}(x \cdot y)$.
3. En déduire que la différence entre deux mots est une distance.
4. En déduire que $\text{wt}(x + y) \equiv \text{wt}(x) + \text{wt}(y) \pmod{2}$.

Exercice 12.2. — Soit \mathcal{C} un code linéaire binaire de paramètres $[n, k, 5]$.

1. Montrer que \mathcal{C} contient un mot y de poids 5.
2. Montrer que $x \mapsto x + y$ réalise une bijection de \mathcal{C} .
3. En déduire que \mathcal{C} contient exactement 2^{k-1} mots de poids pair et 2^{k-1} mots de poids impair dans \mathcal{C} .

Exercice 12.3. — La distance minimale d'un code est la distance minimale entre deux mots de code distincts. Trouver la distance minimale d du code C dans les cas suivants :

$$C = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\} \subset (\mathbb{F}_2)^4 \tag{1}$$

$$C = \{10000, 01010, 00001\} \subset (\mathbb{F}_2)^5 \tag{2}$$

$$C = \{000000, 101010, 010101\} \subset (\mathbb{F}_2)^6. \tag{3}$$

Dans chaque cas, indiquer le nombre d'erreurs que l'on peut détecter et corriger.

Exercice 12.4. — \mathcal{C} désigne un code linéaire de longueur n , sur l'alphabet binaire $\{0, 1\} \subset \mathbb{Z}$, de dimension k et de distance minimale 5.

1. (a) Montrer que \mathcal{C} contient un mot b de poids 5.
 (b) Montrer que $\varphi_b : x \mapsto x + b$ est une bijection de \mathcal{C} . En déduire que \mathcal{C} contient autant de mots de poids pair que de mots de poids impair.
2. Soit $i \in \{1, \dots, n\}$. Posons $A_i = \{x \in \mathcal{C}, x_i = 0\}$, $B_i = \{x \in \mathcal{C}, x_i = 1\}$.
 (a) Montrer que $\sum_{x \in \mathcal{C}} x_i = |B_i|$.
 (b) Supposons $B_i \neq \emptyset$ et soit $b \in B_i$. Montrer que $\varphi_b : x \mapsto x + b$ réalise une bijection entre A_i et B_i .
 (c) En déduire que soit $|B_i| = 2^{k-1}$, soit $|B_i| = 0$.
3. (a) En déduire que $\sum_{x \in \mathcal{C}} \text{wt}(x) = \sum_{i=1}^n \sum_{x \in \mathcal{C}} x_i = 2^{k-1}(n - s)$, où s est un entier compris entre 0 et n .
 (b) Montrer que \mathcal{C} contient au moins $2^{k-1} - 1$ mots de poids supérieur à 6.
 (c) En déduire que

$$5 \cdot 2^{k-1} + 6 \cdot (2^{k-1} - 1) \leq \sum_{x \in \mathcal{C}} \text{wt}(x) \leq 2^{k-1}n.$$

- (d) En déduire que $\frac{3}{2^{k-2}} \geq 11 - n$.

Exercice 12.5. — Montrer que si C est un code binaire de longueur 10 et de distance 3, alors $|C| \leq 93$. Un code est maximal si on ne peut lui ajouter de mots sans que la condition de distance minimale soit violée. Montrer que si C est maximal alors il contient au moins 19 mots.

Exercice 12.6. — Construire un code binaire de longueur 3, de distance minimale 2 et ayant quatre mots. Si C est un code binaire de longueur 3 et de distance 2, montrer que C a au plus quatre mots. Quels sont tous les codes linéaires de dimension 2 et de longueur 3 sur \mathbb{F}_2 ?

Exercice 12.7. — Soit H une matrice sur \mathbb{F}_q à r lignes et n colonnes. Notons aussi H l'application linéaire de $(\mathbb{F}_q)^n$ dans $(\mathbb{F}_q)^r$ qui lui est associée. Supposons que cette application soit surjective (la matrice est de rang r). Alors le noyau de H est un sous-espace vectoriel de dimension $n - r$ de $(\mathbb{F}_q)^n$, c'est-à-dire un code linéaire $C(n, k)$ de longueur n et de dimension $k = n - r$. La matrice H est la matrice de contrôle de $C(n, k)$.

Montrer que l'ensemble E formé des mots dans $(\mathbb{F}_q)^n$ dont les $k - 1$ dernières composantes sont nulles est un sous-espace vectoriel ; quelle est sa dimension ? Montrer qu'il existe un élément non nul dans $C(n, k) \cap E$. En déduire la borne de Singleton sur la distance minimale : $d \leq n + 1 - k$.

Montrer qu'il existe un mot du code $C(n, k)$ de poids p si, et seulement si, il existe p colonnes de H linéairement dépendantes. En déduire une méthode pour déterminer la distance minimale d de $C(n, k)$ à partir de l'étude des colonnes de sa matrice de contrôle H .

Soit le code linéaire binaire dont une matrice de contrôle est : $H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$.

Déterminer le rang de cette matrice, la longueur du code associé et sa dimension. Calculer la borne de Singleton et la distance minimale de ce code. Combien d'erreurs peut-il détecter, corriger ? Expliciter le code associé à H .

Exercice 12.8. — Dans l'exercice , nous avons représenté un code par le noyau d'une application linéaire de $(\mathbb{F}_q)^n$ dans $(\mathbb{F}_q)^r$. Par commodité, l'usage est de représenter ce code par l'image d'une application linéaire de $(\mathbb{F}_q)^{n-r}$ dans $(\mathbb{F}_q)^n$ de la manière suivante :

1. Considérons la matrice et l'espace vectoriel suivants :

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad C = \{m \in (\mathbb{F}_2)^n \mid m = eG \text{ avec } e \in (\mathbb{F}_2)^n\}.$$

Vérifier que le code linéaire binaire C ainsi obtenu est bien le code associé à la matrice de contrôle H introduite dans l'exercice . G est la matrice génératrice du code C .

2. Coder les mots $(1, 0, 1)$, $(0, 1, 0)$ et $(1, 1, 1)$.
3. Déterminer une base du code linéaire C , une autre matrice génératrice et une autre matrice de contrôle de C .

Exercice 12.9. — Soit C le code linéaire ternaire (sur \mathbb{F}_3) dont une matrice génératrice est

$$G = \begin{pmatrix} 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 \end{pmatrix}.$$

1. Expliciter les paramètres de ce code et tous ses mots. Coder le message $v = (12)$.
2. Montrer que le code C est aussi engendré par la matrice $G' = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 2 \end{pmatrix}$.
3. Coder le même message v avec G' .
4. Construire une matrice de contrôle H de C et calculer la distance minimale.
5. La matrice H permet de définir l'application syndrôme de $(\mathbb{F}_3)^5$ dans $(\mathbb{F}_3)^2$ qui associe un mot m à son syndrôme $s(m)$. Si le syndrôme $s(m)$ est non nul, une erreur est détectée. Montrer que deux mots ont le même syndrôme si, et seulement si, leur différence est un mot du code.
6. On reçoit le mot $m = (12121)$. Est-il correct ; si non, trouver un autre mot ayant le même syndrôme et décoder m .

Exercice 12.10. — Soit C le code linéaire binaire de matrice génératrice

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

1. Combien de mots a le code C ?
2. Trouver une matrice A telle que $[IA]$ engendre un code C' équivalent à C .
3. En déduire une matrice de contrôle H de C' puis de C . Quelle est la distance minimale de C ?
4. Si le mot (111110) est reçu, quel est le mot émis.
5. Le mot (111111) est-il un mot du code ? Quel est le mot de C le plus proche ?

Exercice 12.11. — Soit C le code linéaire sur \mathbb{F}_5 de matrice génératrice $G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}$

1. Donner la longueur n , la dimension k et le nombre de mots de C .
2. Est-ce que C est un code systématique ?
3. Montrer que $H = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix}$ est une matrice de contrôle de C .
4. Calculer la distance minimale d de C , la capacité de correction t et montrer que C est MDS (*Maximum Distance Separable* — sa distance minimale atteint la borne de Singleton).
5. Faire la table de décodage contenant tous les vecteurs erreurs possibles de poids $\leq t$. Décoder les mots (1, 1, 1, 1) et (1, 1, 0, 1).
6. Calculer le syndrôme de (2, 3, 1, 1). Que peut-on en déduire ?

Exercice 12.12. — Soit C le code linéaire binaire de longueur 6 dont une matrice génératrice est

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

1. Calculer la distance minimale et la capacité de correction de C .
2. Si le mot (110110) est reçu, quel est le mot émis.

Exercice 12.13. — Soit C le code linéaire binaire dont une matrice génératrice est G .

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

1. Quelle est sa dimension ?
2. Montrer qu'une matrice normalisée est G' .
3. En déduire une matrice de contrôle H de C . Quelle est la distance minimale de C ?
4. Quel est le syndrôme du mot $v = (010101)$?
5. Décoder le mot v .

Exercice 12.14. — Soit C le code linéaire sur \mathbb{F}_5 de matrice génératrice G .

$$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 0 & 4 \\ 1 & 1 & 1 & 1 & 4 & 0 \end{pmatrix}, \quad G' = \begin{pmatrix} 1 & 0 & 4 & 3 & 3 & 1 \\ 0 & 1 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

1. Quelle est sa dimension ? Combien de mots a le code ?
2. Montrer qu'une matrice normalisée de C est G' .
3. En déduire une matrice de contrôle H de C .
4. Quelle est la capacité de correction de C ?
5. Décoder le mot (432100).

Exercice 12.15. — Soit C le code linéaire ternaire dont une matrice génératrice est G .

$$G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 & 1 \\ 2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 & 0 & 1 \end{pmatrix}, \quad G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{pmatrix}.$$

1. Montrer que G' est matrice normalisée associée à G .
2. Construire une matrice de contrôle.
3. Quelle est la distance minimale ?

Exercice 12.16. — Soit C le code linéaire binaire de matrice de contrôle

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

1. Montrer que C est MDS.
2. Construire la table de décodage et décoder successivement 1111111, 1101011, 0110110, 0111110.

Exercice 12.17. — On considère le code C dont la matrice de contrôle H est formée de n vecteurs colonnes distincts non nuls de $(\mathbb{F}_2)^4$.

1. Montrer que $n \leq 14$
2. Quelle est la capacité de correction de H .
3. Construire un code binaire de longueur 10, contenant 64 mots et de distance 3. (comparer avec l'exercice)

Exercice 12.18. — On considère le code C_p sur \mathbb{F}_p de matrice génératrice

$$G := \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 & 3 & 2 \end{pmatrix}.$$

1. Quelles sont les longueurs et dimension de C_p . Montrer que $d \leq 3$.
2. Pour $p = 2, 3, 5$, trouver des matrices de contrôle pour C_p .
3. Pour $p = 2, 3, 5$, trouver les distances minimales.
4. Pour $p = 5$, on reçoit le mot $(1, 1, 1, 2, 3, 4)$. Quel était le mot émis ?

Exercice 12.19. — Soit $\alpha \in \mathbb{F}_8$, tel que $\alpha^3 = \alpha + 1$. On considère le code C_8 sur \mathbb{F}_8 de matrice de contrôle $H = (\alpha \ \alpha^2 \ \dots \ \alpha^7)$.

1. Quelles sont les caractéristiques du code C_8 ?
2. Donner une matrice génératrice de C_8 .

Exercice 12.20. — Soit $\alpha \in \mathbb{F}_{2^n}$. On considère le code sur \mathbb{F}_2 de matrice de contrôle généralisée

$$H = (\alpha \ \alpha^2 \ \dots \ \alpha^{2^n-1})$$

c'est-à-dire le code linéaire sur \mathbb{F}_2 de longueur $2^n - 1$ dont les mots vérifient $\sum_{i=1}^{2^n-1} c_i \alpha^i = 0$.

1. Montrer que la distance minimale de C est 3 si et seulement si α est primitif.
2. On considère $n = 3$ et $\alpha^3 = \alpha + 1$. Donner une matrice génératrice de C .