

## Feuille d'exercices n° 6

### Codes correcteurs et codes correcteurs linéaires : notions fondamentales

**Exercice 1.** Montrer que si  $\mathcal{C}$  est un code parfait binaire de longueur  $n$  et de distance minimale 7 alors  $n = 7$  ou  $n = 23$ .

**Exercice 2 (sur les isométries de  $A^n$  avec  $A = \mathbb{F}_2$ ).** Soit l'alphabet à deux éléments  $A = \{0, 1\}$ . On munit l'espace  $A^n$  avec  $n \geq 1$  de la distance de Hamming, et on considère le groupe  $G$  des isométries de  $A^n$ .

1. Montrer qu'il existe une application injective

$$\Phi : \mathfrak{S}_n \times (\mathfrak{S}_A)^n \rightarrow G.$$

2. Montrer que toute translation  $\tau_a : A^n \rightarrow A^n, x \in A^n \mapsto x + a$  est une isométrie, de la forme  $(s_1, \dots, s_n) \in (\mathfrak{S}_A)^n$  en identifiant un élément  $(s_1, \dots, s_n) \in (\mathfrak{S}_A)^n$  et l'image  $\Phi(\text{Id}; s_1, \dots, s_n)$  définie ci-dessus.
3. Montrer que la seule isométrie qui fixe le vecteur  $0 \in A^n$  et tous les vecteurs de la base canonique de  $A^n$  est l'identité de  $A^n$ . *Indication* : raisonner par récurrence sur le poids des éléments de  $A^n$ . En déduire que  $\Phi$  est surjective ; donner le nombre d'éléments de  $G$ .
4. Montrer la formule  $\sigma\tau_a\sigma^{-1} = \tau_{\sigma(a)}$  pour tout  $\sigma \in \mathfrak{S}_n$  et  $a \in A^n$ . En déduire que le sous-groupe des translations est distingué dans  $G$ , et exhiber une structure de produit semi-direct sur  $\mathfrak{S}_n \times (\mathfrak{S}_A)^n$  qui fasse de  $\Phi$  un isomorphisme (pour les produits semi-directs, cf. par exemple le *Cours d'algèbre* de D. Perrin chez Ellipses, chapitre 1).

**Exercice 3.** Montrer que si  $\mathcal{C}$  est un code linéaire sur  $\mathbb{F}_q$  alors l'une des deux propositions suivantes, et une seule, est vraie :

- (a) Tous les mots de codes commencent par 0 ;
- (b) Exactement une fraction  $1/q$  des mots de codes commencent par 0.

**Exercice 4 (borne de Plotkin).** Soit  $\mathcal{C}$  un  $[n, k, d]$ -code linéaire sur  $\mathbb{F}_q$ .

1. Montrer que la somme des poids de tous les mots de codes est majorée par  $n(q-1)q^{k-1}$
2. En déduire que la distance minimum  $d$  de  $\mathcal{C}$  est majorée par :

$$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}.$$

**Exercice 5.** Soit  $\mathbb{F}_p$  le corps à  $p$  éléments pour  $p$  premier et  $p$  impair. Montrer qu'il existe  $a$  et  $b$  dans  $\mathbb{F}_p$  tels que  $a^2 + b^2 = -1$ . En déduire un exemple de  $[8, 4]$ -code auto-dual dans  $\mathbb{F}_p$  pour un tel  $p$ . Préciser cet exemple dans  $\mathbb{F}_7$ .

**Exercice 6.** Quelle est la distance minimale du code linéaire sur  $\mathbb{F}_{11}$  dont la matrice de parité est :

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}$$

**Exercice 7.** Construire la table des syndromes du code à test de parité et du code par triple vérification. Rappel : le code par test de parité  $\mathbb{F}_2^7 \rightarrow \mathbb{F}_2^8$  rajoute un bit de parité égal à la somme des 7 premiers bits

transmis; le code par triple vérification est défini par  $f : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2^6, (x_1, x_2, x_3) \mapsto (x_1, x_2, x_3, a, b, c)$  avec  $a, b, c$  tels que

$$x_1 + x_2 + c = x_1 + x_3 + b = x_2 + x_3 + a = 0.$$

**Exercice 8.** Soit  $G$  la matrice génératrice d'un code  $\mathcal{C}$  sur  $\mathbb{F}_2$  :

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

Déterminer si les mots suivants appartiennent à  $\mathcal{C}$  et, si non, en décoder les erreurs :

$$(1, 1, 0, 1, 0, 1, 1) ; \quad (0, 1, 1, 0, 1, 1, 1) ; \quad (0, 1, 1, 1, 0, 0, 0).$$

**Exercice 9.** Soit  $\mathcal{C}$  un  $[n, k]$ -code linéaire sur  $\mathbb{F}_q$  de matrice génératrice  $M \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ . On considère les opérations suivantes sur les lignes ou colonnes de  $M$ .

- (i). Échanger deux lignes  $l$  et  $l'$  de  $M$
  - (ii). Multiplier une ligne  $l$  de  $M$  par un scalaire  $k$  non nul
  - (iii). Remplacer une ligne  $l$  par la somme de  $l$  et d'une autre ligne  $l'$ .
  - (iv). Échanger deux colonnes  $c$  et  $c'$  de  $M$
  - (v). Multiplier une colonne  $c$  de  $M$  par un scalaire  $k$  non nul
1. Soit  $\mathcal{C}'$  le code de matrice génératrice obtenu à partir de  $M$  par un nombre quelconque d'opérations sur les lignes de  $M$ . Montrer que les mots de codes de  $\mathcal{C}'$  et de  $\mathcal{C}$  sont les mêmes (seule la correspondance entre messages et mots de code change).
  2. Soit  $\mathcal{C}'$  le code de matrice génératrice obtenu à partir de  $M$  par un nombre quelconque d'opérations sur les colonnes de  $M$ . Montrer que  $\mathcal{C}'$  est un  $[n, k]$  dont on décrira les mots de codes par rapport à ceux de  $\mathcal{C}$ .