Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Exercices complémentaires

13 janvier 2022

Exercice 1. Codes juxtaposés.

Soient $\mathcal{A} \subseteq \mathbb{F}_q^n$ et $\mathcal{B} \subseteq \mathbb{F}_q^m$ deux codes linéaires définis sur le même alphabet $\mathbb{F}_q$. On note $\mathcal{A} \oplus \mathcal{B}$ le code :

$$\mathcal{A} \oplus \mathcal{B} = \{(\boldsymbol{a}, \boldsymbol{b}) \mid \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}\}$$

où $(\boldsymbol{a}, \boldsymbol{b})$ représente la concaténation (ou juxtaposition) des vecteurs $\boldsymbol{a}$ et $\boldsymbol{b}$.

Question 1.– Quelle est la longueur de $\mathcal{A} \oplus \mathcal{B}$, en fonction de celles de $\mathcal{A}$ et $\mathcal{B}$?

Question 2.– Quelle est la dimension de $\mathcal{A} \oplus \mathcal{B}$, en fonction de celles de $\mathcal{A}$ et $\mathcal{B}$?

Question 3.– Quelle est la distance minimale de $\mathcal{A} \oplus \mathcal{B}$, en fonction de celles de $\mathcal{A}$ et $\mathcal{B}$?

Question 4.– Déterminer une matrice génératrice de $\mathcal{A} \oplus \mathcal{B}$ en fonction de matrices génératrices (quelconques) de $\mathcal{A}$ et $\mathcal{B}$.

Question 5.– Exprimer $(\mathcal{A} \oplus \mathcal{B})^\perp$ en fonction de $\mathcal{A}^\perp$ et $\mathcal{B}^\perp$.

Question 6.– On note $m\mathcal{A} \coloneqq \underbrace{\mathcal{A} \oplus \cdots \oplus \mathcal{A}}_{m \text{ fois}}$. À partir des questions précédentes, donner les paramètres de $m\mathcal{A}$ en fonction de ceux de $\mathcal{A}$.

Puis, répondre aux questions suivantes :

1. Si $\mathcal{A}$ est MDS, le code $m\mathcal{A}$ peut-il être MDS ? Si oui, sous quelle(s) condition(s) ?
2. Si $\mathcal{A}$ a pour paramètres fixes $[n, k, d]$, quel est le comportement asymptotique des paramètres relatifs (R, δ) de la famille de codes $m\mathcal{A}$ lorsque $m \to \infty$?

Exercice 2. Produit de Schur.

Pour $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^n$, on note

$$\boldsymbol{a} \star \boldsymbol{b} \coloneqq (a_1 b_1, \ldots, a_n b_n) \in \mathbb{F}_q^n$$

le produit terme à terme des vecteurs $\boldsymbol{a}$ et $\boldsymbol{b}$, aussi appelé produit de Schur. On note $\boldsymbol{a}^{\star 2} \coloneqq \boldsymbol{a} \star \boldsymbol{a}$ le carré de Schur de $\boldsymbol{a}$.

Si $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$ sont deux codes linéaires de même alphabet et même longueur, on définit alors le code produit de Schur :

$$\mathcal{A} \star \mathcal{B} \coloneqq \mathrm{Vect}_{\mathbb{F}_q}\{\boldsymbol{a} \star \boldsymbol{b} \mid \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}\}\,.$$

De même, on définit le code carré de Schur $\mathcal{A}^{\star 2} = \mathcal{A} \star \mathcal{A}$.

Question 1.– Si $\mathcal{C} \subseteq \mathbb{F}_q^n$ est un code quelconque et $\mathcal{R}$ est le code de répétition de longueur n sur $\mathbb{F}_q$, que vaut $\mathcal{C} \star \mathcal{R}$?

Question 2.– Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$. Démontrer que $\mathcal{C} \star \mathcal{C}^\perp$ est toujours inclus dans le code de parité de longueur n sur $\mathbb{F}_q$.

Question 3.– Soit $\mathcal{C} = \mathcal{A} \star \mathcal{B}$ où $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$.

1. Soit $i \in \{1, \dots, n\}$. Dans quel cas a-t-on $c_i = 0$ pour tout $\boldsymbol{c} \in \mathcal{C}$?
2. En déduire une condition nécessaire et suffisante pour que $\mathcal{C} = \{\mathbf{0}\}$.

Question 4.– Soient $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$ deux codes. On note $a = \dim \mathcal{A}$ et $b = \dim \mathcal{B}$.

1. Démontrer que
$$\dim(\mathcal{A} \star \mathcal{B}) \leq \min\{ab, n\}\,.$$
2. Démontrer que
$$\dim(\mathcal{A}^{\star 2}) \leq \min\left\{\frac{a(a+1)}{2}, n\right\}\,.$$

Question 5.– Plus difficile : démontrer que $\dim(\mathcal{A} \star \mathcal{B}) \geq \min\{n, \dim(\mathcal{A}) + \mathrm{d}_{\min}(\mathcal{B}^\perp) - 2\}$.

Question 6.– Soit $\mathcal{C} = \mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \subseteq \mathbb{F}_q^n$.

1. Reconnaître $\mathcal{C}^{\star 2}$ comme un code de Reed–Solomon.
2. Comparer la dimension de $\mathcal{C}^{\star 2}$ avec les bornes démontrées dans les questions précédentes.

Exercice 3. Codes $(\mathcal{U}, \mathcal{U}+\mathcal{V})$.

Soient $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_2^n$ deux codes binaires. On définit le code « $\mathcal{U}, \mathcal{U}+\mathcal{V}$ » comme
$$\mathcal{C} = \{(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) \mid \boldsymbol{u} \in \mathcal{U}, \boldsymbol{v} \in \mathcal{V}\} \subseteq \mathbb{F}_2^{2n}$$

Question 1.– Quelle est la dimension de $\mathcal{C}$?

Question 2.– Donner une matrice génératrice de $\mathcal{C}$ en fonction de matrices génératrices $\boldsymbol{G}_\mathcal{U} \in \mathbb{F}$ et $\boldsymbol{G}_\mathcal{V}$ de $\mathcal{U}$ et $\mathcal{V}$.

Question 3.– On s'intéresse à la distance minimale du code $\mathcal{C}$.

1. Démontrer qu'il existe un mot de $\mathcal{C}$ de poids $2\,\mathrm{d}_{\min}(\mathcal{U})$.
2. Démontrer qu'il existe un mot de $\mathcal{C}$ de poids $\mathrm{d}_{\min}(\mathcal{V})$.
3. Soit $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v})$ un mot non-nul de $\mathcal{C}$. Démontrer que $\mathrm{wt}(\boldsymbol{c}) \geq \min\{2\,\mathrm{d}_{\min}(\mathcal{U}), \mathrm{d}_{\min}(\mathcal{V})\}$. On distinguera les cas selon si $\boldsymbol{v}$ est nul ou non-nul.
4. Conclure sur la distance minimale de $\mathcal{C}$.

On s'intéresse au problème de décodage dans le code $(\mathcal{U}, \mathcal{U}+\mathcal{V})$. Soit $\boldsymbol{y} = \boldsymbol{y} + \boldsymbol{e}$ où $\boldsymbol{c} \in \mathcal{C}$ et $\boldsymbol{e} \in$ est un mot de poids $\leq t = \lfloor (\mathrm{d}_{\min}(\mathcal{C}) - 1)/2 \rfloor$.

Pour cela, on suppose que l'on peut décoder les codes $\mathcal{U}$ et $\mathcal{V}$ jusque leur rayon de décodage unique.

Question 4.– Écrivons $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2)$ et $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2)$ où les mots $\boldsymbol{y}_i, \boldsymbol{e}_i$ ont longueur n. Calculer $\boldsymbol{y}_1 + \boldsymbol{y}_2$, puis démontrer que l'on peut retrouver $\boldsymbol{e}_2$ en résolvant un problème de décodage dans le code $\mathcal{V}$.

Question 5.– Une fois avoir obtenu e_2, en déduire comment retrouver e_1.

Exercice 4. Codes hermitiens.

Dans cet exercice, on considère un corps fini $\mathbb{F}_q$ et son extension quadratique $\mathbb{F}_{q^2}$. La courbe hermitienne $\mathcal{H}_q$ est la courbe projective plane définie sur $\mathbb{F}_{q^2}$ par l'équation

$$Y^{q+1} + ZX^q + Z^qX = 0\,.$$

On admet que le genre de la courbe $\mathcal{H}_q$ est $g = \frac{q(q-1)}{2}$.

Points rationnels. On souhaite déterminer les points rationnels de $\mathcal{H}_q$.

Question 1.– Combien de points à l'infini ($Z = 0$) la courbe $\mathcal{H}_q$ possède-t-elle ?

Question 2.– Combien de points de la forme $P = [0 : y : z]$ la courbe $\mathcal{H}_q$ possède-t-elle ?

Question 3.– Soit $\alpha \in \mathbb{F}_q$.

1. Démontrer que si $\alpha \neq 0$, alors l'équation $y^{q+1} = \alpha$ admet exactement $q+1$ solutions dans $\mathbb{F}_{q^2}$.
2. Démontrer que l'équation $x^q + x = \alpha$ admet exactement q solutions dans $\mathbb{F}_{q^2}$.

Question 4.– Déduire des questions précédentes que $\mathcal{H}_q$ possède exactement $q^3 + 1$ points sur $\mathbb{F}_{q^2}$.

Valuation et espace de Riemann–Roch.

Question 5.– Démontrer la courbe $\mathcal{H}_q$ est lisse, c'est-à-dire que la tangente en tout point de $\mathcal{H}_q$ est bien définie.

Question 6.– Soit $P_\infty = [1 : 0 : 0]$. Calculer la tangente à $\mathcal{H}_q$ en P_∞. En déduire une uniformaisante.

Question 7.– Soit $x = X/Z$ et $y = Y/Z$. Démontrer que $v_{P_\infty}(x) = -(q+1)$ et que $v_{P_\infty}(y) = -q$.

Question 8.– On définit les deux fonctions rationnelles $x := X/Z \in \mathbb{F}_{q^2}(\mathcal{H}_q)$ et $y := Y/Z \in \mathbb{F}_{q^2}(\mathcal{H}_q)$. Démontrer que $v_{P_\infty}(x) = -(q+1)$ et que $v_{P_\infty}(y) = -q$.

Question 9.– Soit $m > q(q-1) - 2$. En déduire la forme de l'espace de Riemann–Roch $L(mP_\infty)$.

Code hermitien. Soit $\mathcal{P} = (P_1, \ldots, P_n)$ le vecteur constitué de la liste des points affines de $\mathcal{H}_q$. On définit le code hermitien $\mathcal{C}_m \subseteq \mathbb{F}_{q^2}^n$ comme le code géométrique de points d'évaluation $\mathcal{P}$ et de diviseur mP_∞, autrement dit :

$$\mathcal{C}_m := \{(f(P_1), \ldots, f(P_n)) \mid f \in L(mP_\infty)\}\,.$$

Question 10.– Déterminer les paramètres (longueur, dimension, distance minimale) de $\mathcal{C}_m$ en fonction de q et m. On donnera une borne inférieure sur ces paramètres lorsque la valeur exacte n'est pas connue.

Exercice 5. Codes concaténés.

Soit $\mathcal{A}$ un code sur l'alphabet $\mathbb{F}_{2^m}$, de paramètres $[N, K, D]_{2^m}$. Soit également $\mathcal{B}$ un code $[n, m, d]_2$, défini sur $\mathbb{F}_2$. On notera que la dimension sur $\mathbb{F}_2$ du code $\mathcal{B}$ est égale au degré d'extension du corps de base de $\mathcal{A}$.

On fixe également une application $\mathbb{F}_2$-linéaire et injective $\psi : \mathbb{F}_{2^m} \to \mathcal{B}$.

La concaténation du code (externe) $\mathcal{A}$ par le code (interne) $\mathcal{B}$ est alors définie comme

$$\mathcal{A} \square \mathcal{B} \coloneqq \{(\psi(a_1), \dots \psi(a_N)) \mid \boldsymbol{a} \in \mathcal{A}\} \subseteq \mathbb{F}_2^{Nn}.$$

Question 1.– Donner la dimension de $\mathcal{A} \square \mathcal{B}$ en tant qu'espace vectoriel sur $\mathbb{F}_2$.

Question 2.– Démontrer que la distance minimale de $\mathcal{A} \square \mathcal{B}$ est $\geq Dd$.

Question 3.– Donner un exemple de codes $\mathcal{A}$ et $\mathcal{B}$ pour lesquels $\mathcal{A} \square \mathcal{B}$ a distance minimale exactement Dd.

Question 4.– Soit $\boldsymbol{P} \in \mathbb{F}_2^{k \times n}$ la matrice de l'application linéaire ψ dans une certaine base de $\mathbb{F}_{2^m}/\mathbb{F}_2$. Notons que $\boldsymbol{P}$ est une matrice génératrice du code $\mathcal{B}$. Étant donnée une matrice génétrice $\boldsymbol{G} = (g_{i,j}) \in \mathbb{F}_{2^m}^{K \times N}$ de $\mathcal{A}$, déterminer une matrice génératrice de $\mathcal{A} \square \mathcal{B}$.

Question 5.– Démontrer que la distance minimale de $(\mathcal{A} \square \mathcal{B})^\perp$ est inférieure ou égale à la distance minimale de $\mathcal{B}^\perp$.