Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Feuille de TD 2

26 novembre 2021

Exercices de TD

Exercice 1. Codes elliptiques.

Soit $\mathcal{E}$ une courbe elliptique sur $\mathbb{F}_q$ d'équation de Weierstrass

$$y^2 = x^3 + ax + b\,,$$

où $a, b \in \mathbb{F}_q$ sont tels que $4a^3 + 27b^2 \neq 0$. On suppose également que la caractéristique $\mathbb{F}_q$ n'est ni 2, ni 3.

On note $P_\infty = [0 : 1 : 0]$ l'unique point à l'infini de $\mathcal{E}$ (on considère que $Z = 0$ est la droite à l'infini). On note également $P_1, \ldots, P_n$ les points affines de $\mathcal{E}(\mathbb{F}_q)$, et on définit $\mathcal{P} := (P_1, \ldots, P_n)$. Enfin, pour $r \geq 0$, on considère le code de Goppa (code géométrique)

$$\mathcal{C}_\mathcal{E}(\mathcal{P}, rP_\infty) := \{\mathrm{ev}_\mathcal{P}(f), f \in L(rP_\infty)\} \subseteq \mathbb{F}_q^n\,.$$

Question 1.– Donner une majoration de la longueur n du code $\mathcal{C}_\mathcal{E}(\mathcal{P}, rP_\infty)$ en fonction de q.

On rappelle que l'espace de Riemann-Roch $L(D)$ associé au diviseur D sur la courbe $\mathcal{E}$ est défini par

$$L(D) = \{f \in \mathbb{F}_q(\mathcal{E}) \mid (f) \geq -D\} \cup \{0\}\,,$$

où $\mathbb{F}_q(\mathcal{E}) = \mathrm{Frac}(\mathbb{F}_q[X, Y, Z]/(F))$ est le corps de fonctions de la courbe $\mathcal{E}$, et

$$F(X, Y, Z) = X^3 + aXZ^2 + bZ^3 - Y^2Z$$

est le polynôme homogène la définissant.

Question 2.– Pour $r \geq 1$, quelle est la dimension du code $\mathcal{C}_\mathcal{E}(\mathcal{P}, rP_\infty)$?

Dans $\mathbb{F}_q(\mathcal{E})$, on considère maintenant les fonctions $x = X/Z$ et $y = Y/Z$.

Question 3.– Démontrer que P_∞ est un pôle de x et de y.

On note $v_P(f)$ la valuation d'une fonction rationnelle f en un point $P \in \mathcal{E}(\mathbb{F}_q)$.

Question 4.– Démontrer que $v_{P_\infty}(x) = -2$ et $v_{P_\infty}(y) = -3$.

Indication : on pourra utiliser l'une de ces deux méthodes au choix.
(1) Calculer une uniformisante u et essayer d'exprimer x comme le produit d'un inversible et d'une puissance de u.
(2) Utiliser la formule $\sum_{P \in \mathcal{E}} v_P(x) = 0$.

Question 5.– En déduire qu'une base de l'espace de Riemann-Roch $L(rP_\infty)$ est

$$\left\{x^i y^j \in \mathbb{F}_q(\mathcal{E}) \mid j \in \{0, 1\},\, i \in \{0, \ldots, r\} \text{ et } 2i + 3j \leq r\right\}.$$

Vérifier que la dimension obtenue est en accord avec la **Question 2**.

Question 6.– En déduire la forme d'une matrice génératice du code $\mathcal{C}_{\mathcal{E}}(\mathcal{P}, rP_\infty)$.

Question 7.– Application : pour $\mathcal{E} : y^2 = x^3 + x + 1$ définie sur $\mathbb{F}_5$:

1. Calculer l'ensemble des points de $\mathcal{E}$.
2. Donner une matrice génératrice de $\mathcal{C} = \mathcal{C}_{\mathcal{E}}(\mathcal{P}, rP_\infty)$ pour $r = 5$.
3. Donner un mot de poids minimal du code $\mathcal{C}$.

Exercice 2. Code trace et théorème de Delsarte.

Soit $\mathbb{F}_{q^m}$ une extension de $\mathbb{F}_q$ et $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_{q^m}$. On note k la dimension de $\mathcal{C}$ sur $\mathbb{F}_{q^m}$ et d sa distance minimale. Pour $x \in \mathbb{F}_{q^m}$, on note également $\mathrm{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}} \in \mathbb{F}_q$ la trace de x. Le **code trace** est alors

$$\mathrm{Tr}(\mathcal{C}) \coloneqq \{\mathrm{Tr}(\boldsymbol{c}) \coloneqq (\mathrm{Tr}(c_1), \ldots, \mathrm{Tr}(c_n)) \mid \boldsymbol{c} \in \mathcal{C}\} \subseteq \mathbb{F}_q^n .$$

On définit également le **sous-code sur un sous-corps** $\mathcal{C}_{|\mathbb{F}_q}$ comme

$$\mathcal{C}_{|\mathbb{F}_q} \coloneqq \mathcal{C} \cap \mathbb{F}_q^n .$$

Dans cet exercice, on propose de démontrer un résultat dû à Delsarte [1] :

$$\mathrm{Tr}(\mathcal{C}^\perp) = (\mathcal{C}_{|\mathbb{F}_q})^\perp .$$

Question 1.– Démontrer que $\mathrm{Tr}(\mathcal{C}^\perp) \subseteq (\mathcal{C}_{|\mathbb{F}_q})^\perp$.

Raisonnons par l'absurde et supposons que $\mathrm{Tr}(\mathcal{C}^\perp) \neq (\mathcal{C}_{|\mathbb{F}_q})^\perp$.

Question 2.– Démontrer qu'il existe $\boldsymbol{u} \in \mathrm{Tr}(\mathcal{C}^\perp)^\perp$ et $\boldsymbol{v} \in \mathcal{C}$ tels que $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \neq 0$.

Question 3.– En déduire que, pour ces mots $\boldsymbol{u}$ et $\boldsymbol{v}$, il existe $\gamma \in \mathbb{F}_{q^m}^\times$ tel que $\langle \boldsymbol{u}, \mathrm{Tr}(\gamma \boldsymbol{v}) \rangle \neq 0$. Conclure la preuve du théorème de Delsarte.

Question 4.– Applications.

1. Donner une minoration de la dimension et de la distance minimale de $\mathcal{C}_{|\mathbb{F}_q}$ en fonction des paramètres de $\mathcal{C}$.
2. Expliquer comment calculer efficacement une base (= lignes d'une matrice génératrice) de $\mathcal{C}_{|\mathbb{F}_q}$ en fonction d'une base de $\mathcal{C}$.

Quelques exercices fondamentaux (pour s'entraîner)

Exercice 3. Notions fondamentales sur les codes.

Dans tout l'exercice, on considère $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code linéaire de dimension k et de distance minimale d. Pour $J \subset \{1, \ldots, n\}$ et $\boldsymbol{x} \in \mathbb{F}_q^n$, on note $\boldsymbol{x}_{|J} \in \mathbb{F}_q^{|J|}$ le mot issu de $\boldsymbol{x}$ en ne gardant que les coordonnées indexées par $j \in J$.

On définit ensuite le code $\mathcal{C}$ *poinçonné* en $I \subset \{1, \ldots, n\}$ comme

$$\mathrm{Punct}_I(\mathcal{C}) \coloneqq \{\boldsymbol{c}_{[1,n]\setminus I},\ \boldsymbol{c} \in \mathcal{C}\}$$

et le code $\mathcal{C}$ *raccourci* sur $I \subset \{1, \ldots, n\}$ comme

$$\mathrm{Short}_I(\mathcal{C}) \coloneqq \{\boldsymbol{c}_{[1,n]\setminus I} \mid \boldsymbol{c} \in \mathcal{C} \text{ et } \boldsymbol{c}_{|I} = \boldsymbol{0}\} .$$

Question 1.– Déterminer les paramètres (longueur, borne sur la dimension, borne sur la distance minimale) de $\mathrm{Punct}_I(\mathcal{C})$ en fonction de n, k, d et $\ell = |I|$.

Question 2.– Déterminer les paramètres (longueur, borne sur la dimension, borne sur la distance minimale) de $\mathrm{Short}_I(\mathcal{C})$ en fonction de n, k, d et $\ell = |I|$.

Question 3.– Démontrer que $\mathrm{Punct}_I(\mathcal{C}^\perp) = \mathrm{Short}_I(\mathcal{C})^\perp$.

Exercice 4. Codes MDS.

On rappelle qu'un code MDS (*maximum distance separable*) est un code dont les paramètres n, k, d satisfont avec égalité la borne de Singleton $d \leq n - k + 1$.

Question 1.– Soit $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ où les x_i sont deux-à-deux distincts, et $\boldsymbol{y} \in (\mathbb{F}_q^\times)^n$. Démontrer que le code de Reed-Solomon généralisé de dimension k défini comme

$$\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \coloneqq \{(y_1 f(x_i), \ldots, y_n f(x_n)) \mid f \in \mathbb{F}_q[X], \deg f < k\} \quad \subseteq \mathbb{F}_q^n$$

est un code MDS.

Soit maintenant $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code MDS quelconque de dimension k.

Question 2.– Démontrer que si $\mathcal{C}$ est MDS, alors $\mathcal{C}^\perp$ est également MDS.

On note $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ une matrice génératrice de $\mathcal{C}$.

Question 3.– Démontrer que toute sous-matrice de $\boldsymbol{G}$ de taille $k \times k$ est inversible. En déduire que, étant donné un mot $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G} \in \mathcal{C}$, la connaissance de n'importe quel sous-ensemble de k symboles de $\boldsymbol{c}$ permet de retrouver exactement $\boldsymbol{m}$.

Question 4.– Supposons que $\boldsymbol{G} = [\, \boldsymbol{I}_k \mid \boldsymbol{A} \,]$ soit sous forme systématique.

1. Démontrer que la matrice $\boldsymbol{A} \in \mathbb{F}_q^{k \times (n-k)}$ ne contient aucun zéro.
2. Plus généralement, démontrer que tous les mineurs de $\boldsymbol{A}$ sont non-nuls.

Références

[1] Philippe Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 21(5) :575–576, 1975.