Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Feuille de TD 2

Éléments de solutions

26 novembre 2021

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 $\mathcal{C}$.

Solutions de l'Exercice 1.

Solution Q1. La borne de Hasse-Weil donne $|\mathcal{E}(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$. Comme les points d'évaluation sont distincts du point à l'infini, on obtient $n \leq q + 2\sqrt{q}$.

Solution Q2. Si $k > 2g - 2 = 0$, d'après le théorème de Riemann-Roch on a

$$\dim \mathcal{C} = \deg(kP_\infty) - g + 1 = k\,.$$

Solution Q3. Commençons par y. Au point à l'infini on a $Y = 1$ et $Z = 0$, donc P_∞ est bien un pôle de $y = Y/Z$.

Pour $x = X/Z$, on a *a priori* une forme indéterminée « $\frac{0}{0}$ ». Levons l'indétermination en utilisant l'équation de la courbe. On obtient (dans $\mathbb{F}_q(\mathcal{E})$) :

$$\frac{X}{Z} = \frac{X^3}{ZX^2} = \frac{ZY^2 - aXZ^2 - bZ^3}{ZX^2} = \frac{Y^2 - aXZ - bZ^2}{X^2}$$

et, avec cette écriture de x, on observe que $P_\infty = [0:1:0]$ est bien un pôle de x.

Solution Q4. Utilisons d'abord la **première indication**. On commence par chercher une uniformisante u en P_∞, c'est-à-dire une fonction rationnelle $u \in \mathbb{F}_q(\mathcal{E})$ telle que $v_{P_\infty} = 1$. Pour cela, il suffit de choisir u de la forme $f(X,Z)/Y$ avec $f(X,Z) = 0$ une équation de droite non-tangente à $\mathcal{E}$ en P_∞. Calculons donc l'équation de la tangente à $\mathcal{E}$ en P_∞ :

$$\begin{aligned} 0 &= \frac{\partial F}{\partial X}(P_\infty) \cdot X + \frac{\partial F}{\partial Y}(P_\infty) \cdot (Y - 1) + \frac{\partial F}{\partial Z}(P_\infty) \cdot Z \\ &= 0 + 0 + 1 \times Z = Z \end{aligned}$$

On peut donc prendre $u = \frac{X}{Y}$ par exemple. Ensuite, on essaie d'exprimer x (respectivement, y) sous la forme wu^d où $w \in \mathbb{F}_q(\mathcal{E})$ n'a ni pôle ni zéro en P_∞ (donc, w est de valuation 0) et où d sera donc la valuation de x (respectivement, y). Commençons par $x = X/Z$. On a :

$$x = \frac{X}{Z} = \frac{X^3}{ZX^2} = \frac{X^3}{ZX^2} = \frac{ZY^2 - aXZ^2 - bZ^3}{ZX^2} = \frac{Y^2 - aXZ - bZ^2}{X^2} = \left(1 - \frac{aXZ + bZ^2}{Y^2}\right)\frac{Y^2}{X^2} = wu^{-2}\,.$$

Comme $w := 1 - \frac{aXZ+bZ^2}{Y^2}$ a pour évaluation 1 en P_∞, on obtient $v_{P_\infty}(x) - 2$. Pour aller plus rapidement avec y, on peut observer que

$$y = \frac{Y}{Z} = \frac{Y}{X} \cdot \frac{X}{Z} = w^{-1}x \quad \Longrightarrow \quad v_{P_\infty}(y) = v_{P_\infty}(w^{-1}) + v_{P_\infty}(x) = -1 - 2 = -3\,.$$

Si l'on veut suivre la **seconde indication**, on procède ainsi. On a $v_{P\infty}(x) = -2$. Pour le vérifier (par exemple), on note que $\sum_P v_P(x) = 0$, et pour les points $P = [p_x : p_y : p_z] \neq P_\infty$, on a

$$v_P(x) = \begin{cases} 0 & \text{si } p_x \neq 0 \\ 1 & \text{si } b \neq 0, p_x = 0, p_z = 1 \text{ et } p_y = \pm\sqrt{b} \\ 2 & \text{si } b = 0, p_x = 0, p_y = 0 \text{ et } p_z = 0 \end{cases}$$

De manière similaire, $v_{P_\infty}(y) = -3$.

Solution Q5. Soit $\mathcal{F} = \{x^i y^j \mid 0 \leq i \leq k, 0 \leq j \leq 1 \text{ et } 2i + 3j \leq k\}$. On vérifie aisément que $\mathcal{F}$ est une famille libre dans $\mathbb{F}_q(\mathcal{E})$.

Par ailleurs, chacun des $x^i y^j$ de $\mathcal{F}$ vérifie $v_{P_\infty}(x^i y^j) = i v_{P_\infty}(x) + j v_{P_\infty}(y) = -2i - 3j \geq -k$. On a également $v_P(x^i y^j) \geq 0$ pour $P \neq P_\infty$ donc le diviseur associé $(x^i y^j) \geq -kP_\infty$. Ainsi, $\mathcal{F} \subseteq L(kP_\infty)$.

Pour la dimension, il reste à compter le nombre de couples (i, j) d'entiers naturels tels que $2i + 3j \leq k$. On montre facilement (par exemple par récurrence) que ce nombre est k si $k \geq 1$ (et 1 si $k = 0$).

Solution Q6. Les lignes d'une matrice génératrice $\boldsymbol{G}$ est formée des évaluations sur $P_1, \ldots, P_n$ des fonctions $x^i y^j$ de $L(kP_\infty)$. C'est-à-dire :

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & \ldots & \ldots & 1 \\ x(P_1) & x(P_2) & \ldots & \ldots & x(P_n) \\ \vdots & \ldots & & \ldots & \vdots \\ x^{\lfloor r/2 \rfloor}(P_1) & \ldots & & \ldots & x^{\lfloor r/2 \rfloor}(P_n) \\ y(P_1) & \ldots & & \ldots & y(P_n) \\ yx(P_1) & \ldots & & \ldots & yx(P_n) \\ \vdots & \ldots & & \ldots & \vdots \\ yx^{\lfloor (r-3)/2 \rfloor}(P_1) & \ldots & & \ldots & yx^{\lfloor (r-3)/2 \rfloor}(P_n) \end{pmatrix}$$

Solution Q7.

1. Pour déterminer les points affines de la courbe, on identifie d'abord les carrés de $\mathbb{F}_5$:

y	0	1	2	3	4
y^2	0	1	4	4	1

   Puis, on cherche des $x \in \mathbb{F}_5$ tels que $x^3 + x + 1$ est un carré :

x	0	1	2	3	4
$x^3 + x + 1$	1	3	1	1	4

   On obtient donc 8 points affines (auxquels il faut ajouter le point à l'infini) :

   $$\mathcal{E}(\mathbb{F}_5) = \{[0:1:1], [0:4:1], [2:1:1], [2:4:1], [3:1:1], [3:4:1], [4:2:1], [4:3:1], [0:1:0]\}.$$

2. Pour $r = 5$, une base de l'espace de Riemann-Roch est :

   $$\{1, x, x^2, y, xy\}.$$

   On obtient donc la matrice génératrice :

   $$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 3 & 3 & 4 & 4 \\ 0 & 0 & 4 & 4 & 4 & 4 & 1 & 1 \\ 1 & 4 & 1 & 4 & 1 & 4 & 2 & 3 \\ 0 & 0 & 2 & 3 & 3 & 2 & 3 & 2 \end{pmatrix}$$

3. On connaît une borne sur la distance minimale du code :

   $$d_{\min}(\mathcal{C}) \geq n - \dim(\mathcal{C}) + 1 - g = n - r = 3.$$

   Remarquons maintenant en sommant la troisième ligne et le double de la cinquième ligne de $\boldsymbol{G}$ que le mot

   $$(0, 0, 3, 0, 0, 3, 2, 0)$$

   est dans le code. Cela correspond à l'évaluation de $x^2 + 2xy$ sur les points affines de la courbe.

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 $\mathcal{C}$.

Solutions de l'Exercice 2.

Solution Q1. Soit $\boldsymbol{h} \in \mathcal{C}^\perp$ et $\boldsymbol{x} = \mathrm{Tr}(\boldsymbol{h})$. Grâce à la linéarité de Tr, pour tout $\boldsymbol{c} \in \mathcal{C}_{|\mathbb{F}_q}$ on a

$$\langle \boldsymbol{x}, \boldsymbol{c} \rangle = \langle \mathrm{Tr}(\boldsymbol{h}), \boldsymbol{c} \rangle = \mathrm{Tr}(\langle \boldsymbol{h}, \boldsymbol{c} \rangle) = \mathrm{Tr}(0) = 0$$

car $\boldsymbol{h} \in \mathcal{C}^\perp$ et $\boldsymbol{c} \in \mathcal{C}_{|\mathbb{F}_q} \subseteq \mathcal{C}$.

Solution Q2. Si l'on suppose que $\mathrm{Tr}(\mathcal{C}^\perp) \neq (\mathcal{C}_{|\mathbb{F}_q})^\perp$, d'après la Q1 il existe $\boldsymbol{u} \in \mathrm{Tr}(\mathcal{C}^\perp)^\perp \setminus \mathcal{C}_{|\mathbb{F}_q}$. Comme $\boldsymbol{u} \notin \mathcal{C}$, il existe $\boldsymbol{v} \in \mathcal{C}^\perp$ tel que $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \neq 0$.

Solution Q3. La forme linéaire trace est non-dégénérée. Comme $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \neq 0$, il existe $\gamma \in \mathbb{F}_{q^m}^\times$ tel que $\mathrm{Tr}(\gamma \langle \boldsymbol{u}, \boldsymbol{v} \rangle) \neq 0$. Autrement dit,

$$\langle \boldsymbol{u}, \mathrm{Tr}(\gamma \boldsymbol{v}) \rangle \neq 0 .$$

C'est en contradiction avec le fait que $\boldsymbol{u} \in \mathrm{Tr}(\mathcal{C}^\perp)^\perp$.

Solution Q4.

1. On note $k = \dim_{\mathbb{F}_{q^m}} \mathcal{C}$. Alors, $\dim_{\mathbb{F}_{q^m}} \mathcal{C}^\perp = n - k$, donc $\dim_{\mathbb{F}_q} \mathcal{C}^\perp = m(n-k)$. Par conséquent, la dimension de $\mathrm{Tr}(\mathcal{C}^\perp)$ sur $\mathbb{F}_q$ est plus petite que $m(n-k)$, puis d'après le théorème de Delsarte :

$$\dim(\mathcal{C}_{|\mathbb{F}_q}) \geq n - m(n-k) .$$

Quant à la distance minimale, on a la borne $\mathrm{d}_{\min}(\mathcal{C}_{|\mathbb{F}_q}) \geq d = \mathrm{d}_{\min}(\mathcal{C})$ car $\mathcal{C}_{|\mathbb{F}_q} \subseteq \mathcal{C}$. On n'a pas mieux généralement, car il se peut qu'un mot de pôids minimal de $\mathcal{C}$ ait ses coefficients sur $\mathbb{F}_q$.

2. Pour construire une base de $\mathcal{C}_{|\mathbb{F}_q}$, on procède comme suit :
   - — on calcule une base $\mathcal{B}$ de $\mathcal{C}^\perp$ à partir d'une base de $\mathcal{C}$ (sur une matrice : calcul d'un noyau),
   - — on en déduit une base $\mathcal{B}'$ de $\mathrm{Tr}(\mathcal{C}^\perp)$: pour cela, il faut réduire la famille génératrice obtenue en décomposant chaque $\boldsymbol{b} \in \mathcal{B}$ sur une base de $\mathbb{F}_{q^m}/\mathbb{F}_q$,
   - — une nouvelle fois, on calcule une base de l'orthogonal à $\mathrm{Tr}(\mathcal{C}^\perp)$ (par arpport au produit scalaire sur $\mathbb{F}_q$), par un calcul de noyau. Le résultat est bien une base de $\mathcal{C}_{|\mathbb{F}_q}$ d'après le théorème de Delsarte.

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 $J \subset \{1, \dots, n\}$ 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 $I \subset \{1, \dots, n\}$ 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 $I \subset \{1, \dots, n\}$ 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 $\mathrm{Punct}_I(\mathcal{C}^\perp) = \mathrm{Short}_I(\mathcal{C})^\perp$.

Solutions de l'Exercice 3.

Solution Q1.

1. Le code $\mathrm{Punct}_I(\mathcal{C})$ a pour longueur $n - \ell$.
2. Sa dimension est comprise entre $k - \ell$ et k. Pour le voir, on considère l'application

$$\begin{array}{rccc} \pi : & \mathbb{F}_q^n & \to & \mathbb{F}_q^{n-\ell} \\ & \boldsymbol{x} & \mapsto & \boldsymbol{x}_{|[1,n]\setminus I} \end{array}$$

   Cette application est linéaire, et $\mathrm{Punct}_I(\mathcal{C}) = \pi(\mathcal{C})$. Donc $\dim \pi(\mathcal{C}) \leq \dim(\mathcal{C}) = k$. Comme le noyau de π est de dimension ℓ, on a $\dim \pi(\mathcal{C}) \geq \dim \mathcal{C} - \ell = k - \ell$. Notons que la dimension de $\mathrm{Punct}_I(\mathcal{C})$ est égale à k si aucun mot non-nul de $\mathcal{C}$ n'a pour support un sous-ensemble de I.
3. La distance minimale de $\mathrm{Punct}_I(\mathcal{C})$ est comprise entre $d - \ell$ et d. En effet, l'application π ne peut que faire décroître le poinds des mots, d'au plus ℓ unités. Par ailleurs, si tout les mots de poids minimaux de $\mathcal{C}$ sont nuls sur $\mathcal{C}$, la distance minimale de $\mathrm{Punct}_I(\mathcal{C})$ reste égale à d.

Solution Q2. à venir

Solution Q3. à venir

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.

Solutions de l'Exercice 4.

Solution Q1. Pour $\boldsymbol{y} = (1, \ldots, 1)$, le code $\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ est un code de Reed-Solomon classique ; il est donc MDS. Maintenant, si $\boldsymbol{y} \neq (1, \ldots, 1)$, le $\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ est l'image d'un code de Reed-Solomon par l'application

$$\phi : (a_1, \ldots, a_n) \mapsto (y_1, \ldots, y_n)$$

L'application ϕ est une isométrie de $\mathbb{F}_q^n$: plus particulièrement, c'est un isomorphisme qui préserve la distance de Hamming. Ainsi, $\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) = \phi(\mathrm{RS}_k(\boldsymbol{x}))$ est un code de même dimension et même distance minimale que $\mathrm{RS}_k(\boldsymbol{x})$; il est donc MDS.

Solution Q2. Supposons que $\mathcal{C}$ est MDS. Pour démontrer que $\mathcal{C}^\perp$ est MDS, il suffit de démontrer que $\mathcal{C}^\perp$ a distance $n - (n - k) + 1 = k + 1$. Supposons le contraire. Alors, il existe un ensemble I de cardinal k qui contient le support d'un mot de $\mathcal{C}^\perp$. Si $\boldsymbol{G}$ est une matrice génératrice de $\mathcal{C}$, cela signifie que les colonnes indexées par I sont liées. La sous-matrice $I \times I$ de $\boldsymbol{G}$ est donc singulière, et ses lignes sont donc également liées : il en existe une combinaison linéaire qui mène au vecteur nul. Par conséquent, il existe un mot de $\mathcal{C}$ qui est nul sur I ; c'est contradictoire avec le fait que $d = n - k + 1$.

Solution Q3. On suit le même raisonnement que la question précédente. Si $\boldsymbol{G}$ admet une sous-matrice singulière, alors on peut construire un mot non-nul de $\mathcal{C}$ de poids $\leq n - k$, ce qui est en contradiction avec la distance minimale $d = n - k + 1$ d'un code MDS.

Par conséquent, si l'on connaît la restriction $\boldsymbol{c}_{|I}$ où $|I| = k$, alors on peut peut retrouver $\boldsymbol{m}$ en résolvant le système linéaire $\boldsymbol{m}\boldsymbol{G}_{|I} = \boldsymbol{c}_{|I}$, car la sous-matrice $\boldsymbol{G}_{|I}$ est inversible.

Solution Q4.

1. Si $\boldsymbol{A}$ contenait un 0 à la ligne i, cette ligne aurait $k - 1 + 1 = k$ zéros (les $k - 1$ autres provenant de $\boldsymbol{I}_k$). C'est en contradiction avec la distance minimale $d = n - k + 1$ du code.
2. Supposons qu'un mineur de $\boldsymbol{A}$ soit nul, et notons I et J les coordonnées des colonnes et des lignes impliquées. Alors, il existe une combinaison linéaire des lignes indexées par J qui est nulle sur I. Cette combinaison linéaire produit un mot ayant $|I| + (k - |I|)$ zéros : les coordonnées indexées par I et celles indexées par $[1, k] \setminus J$ (sur la partie identité de $\boldsymbol{G}$).

Références

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