Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Solutions feuille de TD 5

05/04/2024

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`https://lvzl.fr/teaching/2023-24/ca.html`

(⋆) exercice fondamental (⋆⋆) pour s'entraîner (⋆⋆⋆) pour aller plus loin 💻 sur machine

Exercice 1. (⋆) Construction de codes de Reed–Solomon.

Question 1.– Construire une matrice génératrice du code de Reed–Solomon de dimension 2 et de longueur 5 sur $\mathbb{F}_5$, dont les points d'évaluation sont $(0,1,2,3,4)$.

Question 2.– Construire une matrice de parité de ce même code.

Solutions de l'Exercice 1.

Solution Q1. Soit $\boldsymbol{x} = (0,1,2,3,4) \in \mathbb{F}_5^5$. Le code $\mathrm{RS}_2(\boldsymbol{x})$ est

$$\left\{ \left(f(0), f(1), f(2), f(3), f(4)\right) \mid f \in \mathbb{F}_5[x], \deg(f) < 2 \right\}$$

Une matrice génératrice de ce code consiste donc en l'évaluation des polynômes 1 et x en les points d'évaluation $\boldsymbol{x}$:

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

Solution Q2. On a vu dans le cours que pour $n = q$, on a $\mathrm{RS}_k(\boldsymbol{x})^\perp = \mathrm{RS}_{q-k}(\boldsymbol{x})$. Par conséquent, ici, une matrice de marité de $\mathrm{RS}_2(\boldsymbol{x})$ est une matrice génératrice de $\mathrm{RS}_2(\boldsymbol{x})^\perp = \mathrm{RS}_3(\boldsymbol{x})$, qui est donc (par exemple)

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

Exercice 2. (⋆) Existence de codes de Reed–Solomon.

Question 1.– Existe-t-il un code de Reed–Solomon permettant d'encoder 3 symboles de $\mathbb{F}_7$ et de corriger 2 erreurs sur les mots de codes créés ? Si oui, en donner une construction explicite (longueur, dimension, points d'évaluation).

Question 2.– Existe-t-il un code de Reed–Solomon permettant d'encoder au moins 2 symbole de $\mathbb{F}_7$ et de corriger 3 erreurs sur les mots de codes créés ? Si oui, en donner une construction explicite (longueur, dimension, points d'évaluation).

Solutions de l'Exercice 2.

Solution Q1. Oui, un tel code existe.

On souhaite encoder trois symboles, donc le code doit être de dimension au moins égale à 3. Par ailleurs, pour corriger 2 erreurs, il faut que la distance minimale soit au moins égale à 5. Comme tout code de Reed–Solomon esr MDS, cela correspond à fixer une longueur $n = k + d - 1 = 3 + 5 - 1 = 7$, ce qui est possible sur $\mathbb{F}_7$.

Par exemple, on peut choisir $\boldsymbol{x} = (0,1,2,3,4,5,6)$ ou $\boldsymbol{x} = (3,1,4,0,2,6,5)$.

Solution Q2. Non, un tel code n'existe pas.

S'il existait, sa dimension serait $k \geq 2$ et sa distance minimale $d \geq 2 \times 3 + 1 = 7$, donc on aurait $n = k + d - 1 \geq 8$. Comme nous sommes sur $\mathbb{F}_7$, on ne peut pas trouver 8 points d'évaluations distincts. Construire un code de Reed–Solomon avec ces paramètres est donc impossible.

Exercice 3. ($\star\star$) Codes de Reed–Solomon projectifs.

Dans cet exercice, on s'intéresse à une extension des codes de Reed–Solomon, appelés codes de Reed-Solomon projectifs. Pour cela, on note $\mathbb{F}_q[x]_{<k}$ l'ensemble des polynômes à coefficients dans $\mathbb{F}_q$ dont le degré est strictement inférieur à k. Puis, pour $P(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_q[x]_{<k}$, on définit $\nu_\infty(P) \coloneqq a_{k-1}$.

On note enfin $\boldsymbol{x} = (x_1, \ldots, x_q)$ une liste ordonnée de tous les éléments de $\mathbb{F}_q$.

Question 1.– Soit

$$\begin{array}{rccc} \phi_k & : \mathbb{F}_q[X]_{<k} & \to & \mathbb{F}_q^{q+1} \\ & f & \mapsto & (f(x_1), \ldots, f(x_q), \nu_\infty(f)) \end{array}$$

Vérifier que, pour tout $0 \leq k \leq q+1$, l'application ϕ_k est un endomorphisme injectif de $\mathbb{F}_q[X]_{<k}$ dans $\mathbb{F}_q^{q+1}$.

Le code de Reed-Solomon projectif de dimension k sur $\mathbb{F}_q$ est simplement l'image de ϕ_k. C'est donc un code de longueur $n = q+1$ et de dimension k. On le note $\mathrm{PRS}_k(\boldsymbol{x})$.

Question 2.– Dans cette question, on prend un exemple de paramètres. Donner une matrice génératrice de $\mathrm{PRS}_k(\boldsymbol{x})$ pour $q = 5$, $k = 3$ et $\boldsymbol{x} = (0,1,2,3,4)$.

Question 3.– Dans cette question, on revient au cas général. Démontrer que la distance minimale de $\mathrm{PRS}_k(\boldsymbol{x})$ est exactement $q - k$.

Solutions de l'Exercice 3.

Solution Q1. On a vu dans le cours que l'application d'évaluation est $\mathbb{F}_q$-linéaire. Par ailleurs, ν_∞ est également $\mathbb{F}_q$-linéaire : on a $\nu_\infty(f + \lambda g) = f_{k-1} + \lambda g_{k-1} = \nu_\infty(f) + \lambda\nu_\infty(g)$ pour tous $\lambda \in \mathbb{F}_q$ et tous $f, g \in \mathbb{F}_q[x]_{<k}$.

Par conséquent, ϕ_k est $\mathbb{F}_q$-linéaire.

Pour savoir si ϕ_k est injective, calculons son noyau. Soit $f \in \ker(\phi_k)$. Alors :

- si $k \leq q$, le polynôme f est de degré $\leq k-1 \leq q-1$ et admet q racines (les x_i), donc f est nul ;
- si $k = q+1$, alors le polynôme f a pour racines tous les x_i et est de degré $\leq k-1 = q$, donc il est de la forme $\lambda \prod_{i=1}^{q}(x - x_i)$ où λ est le coefficient dominant de f. On a donc $\lambda = \nu_\infty(f) = 0$ par hypothèse. Donc f est nul.

Dans tous les cas $\ker(\phi_k) = \{0\}$ donc ϕ_k est injective.

Solution Q2. La famille $(1, x, x^2)$ est libre dans $\mathbb{F}_q[x]_{<k}$, donc son image par ϕ_k est une base de $\mathrm{PRS}_k(\boldsymbol{x})$. En particulier, la matrice

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

est donc une matrice génératrice de ce code.

Solution Q3. à terminer
