Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Feuille de TD 5

05/04/2024

Le corrigé de certains exercices sera disponible à l'adresse suivante :

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

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

En cours d'écriture (version du 5 avril 2024)

Exercice 1. $(\star)$ 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.

Exercice 2. $(\star)$ 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).

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 $\nu_\infty(P) := a_{k-1}$.

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 $q - k$.