Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Feuille de TD 3

03 décembre 2021

Exercice 1. Codes de Tamo-Barg.

Dans cet exercice, on s'intéresse à la construction des polynômes g utiles à la définition des codes de Tamo-Barg.

Pour rappel, on se donne $g \in \mathbb{F}_q[x]$ tel que $\deg g = r+1$. On considère ensuite des éléments $y_1, \dots, y_s \in \mathbb{F}_q$ tels que pour tout $j \in [1, s]$, l'équation $g(x) = y_j$ admet exactement $r+1$ solutions

$$\mathcal{A}_j = \{a_{j,1}, \dots, a_{j,r+1}\} \subseteq \mathbb{F}_q \,.$$

Pour $0 \leq \ell \leq s$, on construit alors l'espace de fonctions polynomiales :

$$\mathcal{F}_\ell \coloneqq \mathrm{span}_{\mathbb{F}_q}\{x^i g(x)^j \mid 0 \leq i \leq r-1, 0 \leq j \leq \ell - 1\}$$

et le vecteur d'évaluation

$$\boldsymbol{a} = (a_{1,1}, \dots, a_{1,r+1}, a_{2,1}, \dots, \dots, a_{s,1}, \dots, a_{s,r+1}) \in \mathbb{F}_q^{s(r+1)} \,.$$

Le code de Tamo-Barg associé à ces grandeurs est alors :

$$\mathrm{TB}_{r,s,\ell}(\boldsymbol{a}) \coloneqq \{\mathrm{ev}_{\boldsymbol{a}}(f) \mid f \in \mathcal{F}_\ell\} \subseteq \mathbb{F}_q^{s(r+1)} \,.$$

Question 1.– Soit H un sous-groupe multiplicatif de $\mathbb{F}_q^\times$ et $A \subseteq \mathbb{F}_q^\times$ une classe d'équivalence « modulo H ». Démontrer que

$$\prod_{a \in A} (X - a) = X^{|H|} - \lambda_A \,.$$

pour un certain $\lambda_A \in \mathbb{F}_q^\times$. En déduire la construction d'une classe de codes de Tamo-Barg dont on explicitera le polynôme g, la localité r et la longueur n.

Question 2.– Soit G un sous-groupe additif de $\mathbb{F}_q$ et $B \subseteq \mathbb{F}_q$ une classe d'équivalence « modulo G ». Démontrer que le polynôme

$$\prod_{u \in G} (X - u)$$

est constant sur B. En déduire la construction d'une classe de codes de Tamo-Barg dont on explicitera le polynôme g, la localité r et la longueur n.

Dans la question suivante (indépendante des deux premières), on souhaite donner une borne inférieure $m_{q,r}$ sur la longueur maximale d'un code de Tamo-Barg de localité r sur $\mathbb{F}_q$.

Question 3.– [difficile] Démontrer qu'il existe un polynôme de degré $r+1$ qui est constant sur au moins $\binom{q}{r+1}/q^r$ sous-ensembles disjoints de taille $r+1$ de $\mathbb{F}_q$. En déduire que $m_{q,r} \geq \frac{q(1-r/q)^r}{r!}$.

Exercice 2. Localité du code de Hadamard.

On reprend la définition du code de Hamming q-aire vu dans un exercice précédent. Pour rappel, si $P_1, \ldots, P_n$ est l'ensemble des points de $\mathbb{P}^{\ell-1}(\mathbb{F}_q)$, on définit une matrice $\boldsymbol{M}$ dont les colonnes sont les coordonnées des points P_i dans un système de représentation standard :

$$\boldsymbol{M} = \begin{pmatrix} P_1 & P_2 & \cdots & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{\ell \times n}.$$

Le code de Hamming $\mathcal{H}_q(\ell) \subseteq \mathbb{F}_q^n$ est alors le code qui admet $\boldsymbol{M}$ comme matrice de contrôle.

Le code de Hadamard est alors défini comme $\mathrm{Had}_q(\ell) = \mathcal{H}_q(\ell)^\perp$. Autrement dit, c'est le code qui admet $\boldsymbol{M}$ comme matrice génératrice.

Question 1.– Rappeler les paramètres n, k, d du code de Hadamard $\mathrm{Had}_q(\ell)$. Quelle est sa distance duale ?

Question 2.– Démontrer que $\mathrm{Had}_q(\ell)$ a localité $r = 2$ pour tout ℓ.

Question 3.– Pour un certain indice $i \in [1, n]$ fixé, combien d'ensembles de reconstruction disjoints i admet-il ?