Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Solutions 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 :

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

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 :

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

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 $m_{q,r} \geq \frac{q(1-r/q)^r}{r!}$.

Solutions de l'Exercice 1.

Solution Q1. Soit $A = \alpha H = \{\alpha h \mid h \in H\}$. Comme H est un groupe, par le théorème de Lagrange on a $h^{|H|} = 1$ pour tout $h \in H$. Par conséquent $a^{|H|} = \alpha^{|H|}$ pour tout $a \in A$. Le polnyôme $\prod_{a \in A}(X - a) - X^{|H|} + \alpha^{|H|}$ s'annule donc sur tout $a \in A$. Il s'ensuit :

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

On peut donc construire un code de Tamo-Barg de localité $r = |H| - 1$ et longueur $n = sr$ avec $s \leq \frac{q-1}{r}$, en choisissant $g(X) = X^{|H|}$.

Solution Q2. On peut écrire $B = \beta + G = \{\beta + v, v \in G\}$. Puis, pour $P(X) = \prod_{u \in G}(X - u)$, on a pour tout $b = \beta + v$:

$$P(b) = \prod_{u \in G}(\beta + v - u) = \prod_{w \in G}(\beta + w)$$

qui est indépendant de v. On obtient donc une classe de codes de Tamo-Barg pour $g(X) = P(X)$, de localité $r = p^e - 1$ (G est un $\mathbb{F}_p$-espace vectoriel, car $\mathbb{F}_q = \mathbb{F}_{p^\ell} \simeq \mathbb{F}_p^\ell$) et de longueur $n = sr$ avec $s \leq p^{\ell - e}$.

Solution Q3. Considérons l'ensemble M des polynômes unitaires de $\mathbb{F}_q[X]$ ayant $r+1$ racines distinctes. L'ensemble M est de cardinal $\binom{q}{r+1}$, car ce sont les polynômes de la forme $(X - \alpha_1)\dots(X - \alpha_{r+1})$. Dans M, on définit la classe d'équivalence $f \equiv g$ si et seulement si $f - g$ est une constante. Alors, le nombre de classes d'équivalence est plus petit que q^r, car une classe d'équivalence est déterminée par les coefficients $a_1, \dots, a_r$ des polynômes $X^{r+1} + a_r X_r + \dots + a_1 X + a_0$ y figurant.

Par conséquent, il existe une classe d'équivalence ayant plus de $\binom{q}{r+1}/q^r$ éléments, et n'importe quel représentant f de la classe est constant sur les zéros des autres représentants de la classe. Notons les zéros de deux représentants d'une même classe forment deux ensembles disjoints (sinon, un certain $X - \alpha$ divise $f - g$ qui est une constante, ce qui mène à une contradiction). Donc f est constant sur au moins $\binom{q}{r+1}/q^r$ ensembles disjoints de taille $r+1$.

Un calcul donne ensuite :

$$m_{q,r} \geq (r+1)\frac{\binom{q}{r+1}}{q^r} \geq \frac{(q-r)^{r+1}}{r!\, q^r} \geq \frac{q(1 - r/q)^r}{r!}\,.$$

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 $P_1, \dots, P_n$ 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 ?

Solutions de l'Exercice 2.

Solution Q1. On a vu dans un exercice précédent sur le code de Hamming q-aire, que le code de Hamming $\mathcal{H}_q(\ell)$ a pour longueur $n = \frac{q^\ell - 1}{q-1}$, dimension $n - \ell$, distance minimale 3 et distance duale $q^{\ell-1}$.

Pour le code de Hadamard, on a donc :

— longueur $n = \frac{q^\ell-1}{q-1}$,
— dimension $k = \ell$,
— distance minimale $d = q^{\ell-1}$,
— distance duale $d^\perp = 3$.

Solution Q2. **Rappel de l'exercice sur le code de Hamming.** Les mots du code de Hadamard sont les vecteurs d'évaluation des formes linéaires sur les $P_1, \dots, P_n$. En effet, tout mot $\boldsymbol{c} \in \mathrm{Had}_q(\ell)$ est une combinaison linéaire des lignes de la matrice $\boldsymbol{M}$. La i-ème ligne $\boldsymbol{m}_i$ de $\boldsymbol{M}$ correspond à l'évaluation de la forme $X_i : \boldsymbol{x} \mapsto x_i$ sur les points $P_1, \dots, P_n$. On peut donc écrire $c_j = \sum_{i=1}^{\ell} \lambda_i X_i(P_j)$.

Supposons maintenant que l'on veuille reconstruire le symbole c_j. On choisit un point $P_s \neq P_j$ et on définit $P_t = P_j - P_s$ de sorte que $P_j = P_s + P_t$. Alors, par linéarité on a

$$c_j = c_s + c_t$$

donc on peut reconstruire c_j à l'aide de deux autres symboles du mot de code.

Solution Q3. L'indice $i \in [1, n]$ a admet autant d'ensembles de reconstruction de cardinal 2, qu'un point P_i admet de paires d'autres points $\{P_s, P_t\}$ alignés avec P_i, deux-à-deux disjointes.

Comptons ces paires. Il y a $|\mathbb{P}^{\ell-2}(\mathbb{F}_q)| = \frac{q^{\ell-1}-1}{q-1}$ droites passant par P_i, et sur chacune de ces droites, $\lfloor \frac{q}{2} \rfloor$ paires disjointes possibles. On obtient donc un total de

$$\left\lfloor \frac{q}{2} \right\rfloor \frac{q^{\ell-1} - 1}{q - 1}.$$
