Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Feuille de TD 5

17 décembre 2021

Exercice 1. Codes produits.

Pour $\boldsymbol{a} \in \mathbb{F}_q^n$ et $\boldsymbol{b} \in \mathbb{F}_q^m$, on note

$$\boldsymbol{a} \otimes \boldsymbol{b} = \begin{pmatrix} b_1 a_1 & \cdots & b_1 a_n \\ \vdots & & \vdots \\ b_m a_1 & \cdots & b_m a_n \end{pmatrix}$$

et on assimile cette matrice à un vecteur dans $\mathbb{F}_q^{nm}$.

Soit $\mathcal{C}_1$ et $\mathcal{C}_2$ deux codes sur $\mathbb{F}_q$ de paramètres respectifs $[n_1, k_1, d_1]$ et $[n_1, k_2, d_2]$. On définit le code produit

$$\mathcal{C}_1 \otimes \mathcal{C}_2 = \mathrm{Vect}_{\mathbb{F}_q}\{\boldsymbol{a} \otimes \boldsymbol{b} \mid \boldsymbol{a} \in \mathcal{C}_1, \boldsymbol{b} \in \mathcal{C}_2\} \subseteq \mathbb{F}_q^{n_1 \times n_2}.$$

Question 1.– Démontrer que $\dim(\mathcal{C}_1 \otimes \mathcal{C}_2) = k_1 k_2$.

Question 2.– Démontrer que $\mathrm{d}_{\min}(\mathcal{C}_1 \otimes \mathcal{C}_2) = d_1 d_2$.

Question 3.– Le code $\mathcal{C}_1 \otimes \mathcal{C}_2$ peut-il être MDS ? Si oui, sous quelles contraintes ?

Question 4.– Dans cette question on suppose $\mathcal{C}_1 = \mathcal{C}_2 = \mathrm{RS}_k(\boldsymbol{x}) \subseteq \mathbb{F}_q^n$. Le code $\mathcal{C}_1 \otimes \mathcal{C}_2$ a donc longueur n^2, dimension k^2 et distance minimale $(n-k+1)^2$.

1. Démontrer que $\mathcal{C}_1 \otimes \mathcal{C}_2$ a localité k.
2. Démontrer tout indice $i \in [1, n^2]$ admet (au moins) 2 ensembles de reconstruction disjoints, de cardinal k.

Exercice 2. Codes Reed–Muller binaires.

On considère l'ensemble des fonctions polynomiales sur le corps $\mathbb{F}_2$, dites *fonctions booléennes* :

$$\mathcal{F}(m) := \mathrm{Vect}_{\mathbb{F}_2}\{(x_1, \ldots, x_m) \mapsto x_1^{e_1} x_2^{e_2} \ldots x_m^{e_m} \mid \forall i \in \{1, \ldots, m\},\ e_i \in \{0,1\}\}.$$

Notons que le degré *individuel* en x_i des fonctions boolénnes est borné par 1, car $x^2 = x$ dans $\mathbb{F}_2$.

On considère ensuite l'ensemble des fonctions booléennes de degré *total* borné par $r \leq m$:

$$\mathcal{F}_r(m) := \{f \in \mathcal{F}(m), \deg(f) \leq r\}.$$

Question 1.– Quelle est la dimension de l'expace vectoriel $\mathcal{F}(m)$?

Question 2.– Démontrer que la dimension de $\mathcal{F}_r(m)$, pour $0 \le r \le m$, est :

$$\sum_{i=0}^{r} \binom{m}{i}$$

Le code de Reed–Muller est le code d'évaluation des fonctions boolénnes de degré borné, sur tous les points de $\mathbb{F}_2^m$. Formellement, si $\mathbb{F}_2^m = \{P_1, \dots, P_n\}$, on a :

$$\mathrm{RM}(m, r) := \{\boldsymbol{c} = (f(P_1), \dots, f(P_n)) \mid P \in \mathcal{F}_r(m)\}\,.$$

Question 3.– Donner une matrice génératrice de $\mathrm{RM}(3, 1)$.

Question 4.– Donner la longueur et la dimension de $\mathrm{RM}(m, r)$ en fonction de m et r.

Question 5.– Reconnaître le code $\mathrm{RM}(m, 0)$ comme un code « connu ».

On souhaite maintenant caractériser le code dual d'un code de Reed–Muller binaire.

Question 6.– Démontrer (par exemple par récurrence sur m), que si $e_1 + \cdots + e_m \le m - 1$, alors

$$\sum_{\boldsymbol{x} \in \mathbb{F}_2^m} \prod_{i=1}^{m} x_i^{e_i} = 0\,.$$

Question 7.– En déduire que $\mathrm{RM}(m, r)^\perp = \mathrm{RM}(m, m - r - 1)$.

On s'intéresse maintenant à la distance minimale de $\mathrm{RM}(m, r)$.

Question 8.– Démontrer que l'évaluation du monôme $\prod_{i=1}^{r} x_i$ fournit un mot de code de $\mathrm{RM}(m, r)$ de poids 2^{m-r}.

Question 9.– Démontrer que la distance minimale de $\mathrm{RM}(m, r)$ est 2^{m-r}.

On s'intéresse enfin aux propriétés de localité du code $\mathrm{RM}(m, r)$.

Question 10.– En utilisant les Questions 7 et 9, donner une borne inférieure sur la localité de $\mathrm{RM}(m, r)$.

Question 11.– Déduire de la question précédente la localité de $\mathrm{RM}(m, r)$, en fournissant un ensemble de reconstruction pour chaque coordonnée du code.

Exercice 3. *Power decoding.*

Dans cet exercice, on s'intéresse au problème du décodage des codes de Reed–Solomon au delà du rayon de décodage unique $\lfloor \frac{d-1}{2} \rfloor$. On va étudier l'algorithme nommé *power decoding*, initialement introduit par Sidorenko, Schmidt et Bossert [1].

Soit donc $\mathcal{C} = \mathrm{RS}_k(\boldsymbol{x}) \subseteq \mathbb{F}_q^n$ un code de Reed-Solomon de longueur n et dimension k. On considère un mot reçu $\boldsymbol{y} \in \mathbb{F}_q^n$, et on cherche un mot de code $\boldsymbol{c} \in \mathcal{C}$ à distance $\le t$ de $\boldsymbol{y}$.

On introduit le produit de Schur (aussi nommé produit de Hadamard) de vecteurs :

$$\text{si } \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^n, \quad \text{alors } \boldsymbol{a} \star \boldsymbol{b} := (a_1 b_1, \dots, a_n b_n) \in \mathbb{F}_q^n\,.$$

L'idée est s'intéresser aux puissances successives de $\boldsymbol{y}$ pour ce produit de Schur. On va d'abord se focaliser sur $\boldsymbol{y}$ et $\boldsymbol{y}^{\star 2}$.

Question 1.– Supposons qu'il existe $\boldsymbol{c} \in \mathcal{C}$ et $\boldsymbol{e} \in \mathbb{F}_q^n$ de poids t tel que $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$.

1. Calculer $\boldsymbol{y}^{\star 2}$ en fonction de $\boldsymbol{c}$ et $\boldsymbol{e}$.
2. Démontrer que l'on peut exprimer $\boldsymbol{y}^{\star 2}$ comme un mot de $\mathcal{C}^{\star 2}$ bruité.
3. On note $\boldsymbol{e}'$ l'erreur associée. Démontrer que le support de erreur $\boldsymbol{e}'$ est inclus dans celui de $\boldsymbol{e}$.

Soit $E(X) \in \mathbb{F}_q[X]$ le polynôme annulateur de l'erreur $\boldsymbol{e}$. Par définition, $E(X) = \prod_{i \in \mathrm{supp}(\boldsymbol{e})}(X - x_i)$. On note également $Y(X) \in \mathbb{F}_q[X]$ et $C(X) \in \mathbb{F}_q[X]$ les polynômes interpolateurs de plus petit degré de $\boldsymbol{y}$ et $\boldsymbol{c}$, par rapport aux points d'évaluations définis par le vecteur $\boldsymbol{x}$.

Question 2.– En s'inspirant de l'algorithme de Berlekamp–Welch, écrire un système de deux équations clés impliquant les polynômes $E(X)$, $Y(X)$ et $C(X)$.

On considère le système d'équations suivant :

$$\begin{cases} y_i A(x_i) = B_1(x_i) & \forall i = 1, \dots, n, \\ y_i^2 A(x_i) = B_2(x_i) & \forall i = 1, \dots, n, \end{cases} \tag{1}$$

où les inconnues sont les coefficients des polynômes $A(X)$, $B_1(X)$, $B_2(X)$.

Question 3.– Comment relier le système d'équations (1) aux équations clés déterminées dans la question précédente ? Préciser les contraintes sur le degré des polynômes A, B_1, B_2.

Question 4.– Vérifier que le triplet $(A = E, B_1 = EC, B_2 = EC^2)$ est une solution du système (1).

Question 5.– Rayon de décodage.

1. Démontrer que si $t \geq n - 2(k-1)$, alors on peut trouver une autre solution au système, de la forme $(A = 0, B_1 = 0, B_2 \neq 0)$.
2. Quelle condition sur n, k et t doit-on imposer pour espérer obtenir un espace de solutions de dimension au plus 1 au système (1) ?
3. Comparer la borne obtenue au rayon de décodage unique de $\mathcal{C} = \mathrm{RS}_k(\boldsymbol{x})$, et au rayon de Sudan.

Question 6.– Réécrire le système (1) comme une équation matricelle $\boldsymbol{M}\boldsymbol{X} = \boldsymbol{b}$. On précisera $\boldsymbol{X}$ et $\boldsymbol{b}$ et on écrira $\boldsymbol{M}$ en fonction de $\boldsymbol{y}, \boldsymbol{y}^2$ et des matrices de Vandermonde

$$\boldsymbol{V}_r(\boldsymbol{x}) := \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & \dots & x_1^{r-1} \\ 1 & x_2 & x_2^2 & \dots & \dots & x_2^{r-1} \\ \vdots & & & & & \vdots \\ 1 & x_n & x_n^2 & \dots & \dots & x_n^{r-1} \end{pmatrix}.$$

Question 7.– Description de l'algorithme de *power decoding*.

1. À l'aide des questions précédentes, écrire formellement un algorithme qui prend en entrée $\boldsymbol{y} \in \mathbb{F}_q$ et $t \geq 1$, et qui retourne $\boldsymbol{c} \in \mathcal{C}$ tel que $\mathrm{d_H}(\boldsymbol{c}, \boldsymbol{y}) \leq t$. L'algorithme pourra éventuellement échouer, mais toute valeur retournée de l'algorithme devra être correcte.
2. Généraliser l'algorithme pour des puissances de $\boldsymbol{y}$ plus grandes que 2.

Références

[1] Georg Schmidt, Vladimir Sidorenko, and Martin Bossert. Collaborative decoding of interleaved reed-solomon codes and concatenated code designs. *IEEE Trans. Inf. Theory*, 55(7) :2991–3012, 2009.