Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs – Feuille de TD 5

Éléments de solutions

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.

Solutions de l'Exercice 1.

Solution Q1. Si $\{\boldsymbol{a}_i\}_{1 \le i \le k_1}$ et $\{\boldsymbol{b}_j\}_{1 \le j \le k_2}$ sont deux bases de $\mathcal{C}_1$ et $\mathcal{C}_2$, alors les $\boldsymbol{a}_i \otimes \boldsymbol{b}_j$ sont indépendants, donc ils forment une base de $\mathcal{C}_1 \otimes \mathcal{C}_2$. On a donc $\dim \mathcal{C}_1 \otimes \mathcal{C}_2 = k_1 k_2$.

Solution Q2. Si $\boldsymbol{a}$ et $\boldsymbol{b}$ sont des mots de poids respectifs d_1 et d_2 dans $\mathcal{C}_1$ et $\mathcal{C}_2$, alors on note que $\boldsymbol{a} \otimes \boldsymbol{b}$ a un poids $d_1 d_2$. Par ailleurs, on observe que toute ligne de $\boldsymbol{c} \in \mathcal{C}_1 \otimes \mathcal{C}_2$ est un mot de $\mathcal{C}_1$, et que toute colonne est un mot de $\mathcal{C}_2$. Si $\boldsymbol{c} \neq \boldsymbol{0}$, il y a donc au moins d_2 lignes non-nulles dans $\boldsymbol{c}$ (sinon on aurait des colonnes non-nulles de poids $< d_2$) et chacune de ces lignes a un poids $\ge d_1$. Par conséquent de poids de $\boldsymbol{c}$ est $\ge d_1 d_2$.

Solution Q3. En utilisant la borne de Singleton sur $\mathcal{C}_1$ et $\mathcal{C}_2$, on a :

$$n_1 n_2 \ge (k_1 + d_1 - 1)(k_2 + d_2 - 1) = k_1 k_2 + d_1 d_2 - 1 + (k_1 - 1)(d_2 - 1) + (k_2 - 1)(d_1 - 1).$$

Pour que $\mathcal{C}_1 \otimes \mathcal{C}_2$ soit MDS, il faut donc que $(k_1-1)(d_2-1) = (k_2-1)(d_1-1) = 0$ et que $\mathcal{C}_1$ et $\mathcal{C}_2$ soient MDS.

Comme on suppose $d_1, d_2 \geq 2$, ceci implique que $k_1 = 1$ et $k_2 = 1$, autrement dit que le code $\mathcal{C}_1 \otimes \mathcal{C}_2$ est un code de répétition.

Solution Q4.

1. Soit $\boldsymbol{c} \in \mathcal{C} \coloneqq \mathcal{C}_1 \otimes \mathcal{C}_2$. Supposons que l'on souhaite retrouver $c_{i,j}$, avec $(i,j) \in [1,n]^2$. On sait que la ligne $\boldsymbol{c}_{(i,*)} \in \mathbb{F}_q^n$ de $\boldsymbol{c}$ est un mot de $\mathcal{C}_1 = \mathrm{RS}_k(\boldsymbol{x})$. Ce code est MDS, donc est de localité égale à sa dimension k. Il existe donc un ensemble de reconstruction $S = \{(i,s_1), \ldots, (i,s_k)\} \subseteq \{(i,r), r \in [1,n]\}$, de cardinal k, permettant de retrouver $\boldsymbol{c}_{(i,*)}$.
2. Même raisonnement que pour 1., en raisonnant avec les colonnes.

Exercice 2. Codes Reed–Muller binaires.

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

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

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 $r \leq m$:

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

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 $0 \leq r \leq m$, 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 $\mathbb{F}_2^m = \{P_1,\ldots,P_n\}$, on a :

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

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 $e_1 + \cdots + e_m \leq m-1$, 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.

Solutions de l'Exercice 2.

Solution Q1. La dimension de $\mathcal{F}(m)$ est égale au nombre de choix pour les $(e_1,\dots,e_m)$, c'est-à-dire 2^m.

Solution Q2. Il faut compter le nombre de $(e_1,\dots,e_m)$ tels que que $\sum_{i=1}^m e_i \leq r$. Pour une somme $\ell = \sum_{i=1}^m e_i$ fixée dans $[0,r]$, il y a $\binom{m}{\ell}$ choix de $(e_1,\dots,e_m)$ possible, correspondant à la position des ℓ « 1 » sur les m indices possibles. Au total, on obtient donc :

$$\dim \mathcal{F}_r(m) = \sum_{\ell=0}^{r} \binom{m}{\ell}.$$

Solution Q3. Il faut évaluer les monômes 1, x_1, x_2 et x_3 sur les points de $\mathbb{F}_2^3$. On obtient :

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Solution Q4. La longueur du code est égale au nombre de points dans $\mathbb{F}_2^r$, c'est-à-dire 2^r. L'application d'évaluation est injective (car les monômes sont de degré partiel ≤ 1), donc $\dim \mathrm{RM}_q(m,r) = \dim \mathcal{F}_r(m) = \sum_{\ell=0}^r \binom{m}{\ell}$.

Solution Q5. Pour $r=0$, on obtient un code de répétition de longueur 2^r.

Solution Q6.

- Pour $m=1$, on a bien $\sum_{x\in\mathbb{F}_2} x^0 = 1+1 = 0$
- Supposons le résultat vrai pour $m-1$. Soient $(e_1,\dots,e_m) \in \{0,1\}^m$ tels que $\sum_{i=1}^m e_i \leq m-1$. Deux acs se présentent :
  - — ou bien tous les e_i sont nuls, alors on a :

$$\sum_{x\in\mathbb{F}_2^m} \prod_{i=1}^m x_i^{e_i} = \sum_{x\in\mathbb{F}_2^m} 1 = 2^m = 0.$$

  - — ou bien il existe un indice j tel que $e_j = 1$. Alors

$$\sum_{x\in\mathbb{F}_2^m} \prod_{i=1}^m x_i^{e_i} = \sum_{x_j\in\mathbb{F}_2} \left(\sum_{(x_1,\dots,x_{j-1},x_{j+1},x_m)\in\mathbb{F}_2^{m-1}} \prod_{i\in[1,m]\setminus\{j\}} x_i^{e_i} \right) x_j^1$$

    Remarquons que $\sum_{i\in[1,m]\setminus\{j\}} e_i \leq m-2$, donc par hypothèse de récurrence, le terme $\sum_{(x_1,\dots,x_{j-1},x_{j+1},x_m)\in\mathbb{F}_2^{m-1}} \prod_{i\in[1,m]\setminus\{j\}} x_i^{e_i}$ est nul. Puis, $\sum_{x\in\mathbb{F}_2^m} \prod_{i=1}^m x_i^{e_i} = 0$.

Solution Q7. Rappelons qu'une base de $\mathrm{RM}(m,r)$ est formée des vecteurs d'évaluation des monômes $\prod_{i=1}^m x_i^{e_i}$, où $\sum_{i=1}^m e_i \leq r$.

Soient donc $(e_1,\dots,e_m)$ et $(e'_1,\dots,e'_m)$ tels que $\sum_{i=1}^m e_i \leq r$ et $\sum_{i=1}^m e'_i \leq m-r-1$. Montrons que le produit scalaire des vecteurs d'évaluation des monômes $\prod_{i=1}^m x_i^{e_i}$ et $\prod_{i=1}^m x_i^{e'_i}$ est nul. Ce produit scalaire vaut :

$$\sum_{x\in\mathbb{F}_2^m} \prod_{i=1}^m x_i^{e_i} \prod_{j=1}^m x_j^{e'_j} = \sum_{x\in\mathbb{F}_2^m} \prod_{i=1}^m x_i^{e_i+e'_i}.$$

Notons que $x_i^{e_i+e'_i} = x_i^{e_i+e'_i \bmod 2}$ car $a^2 = a$ dans $\mathbb{F}_2$. Par conséquent, le produit scalaire vaut

$$\sum_{\boldsymbol{x}\in\mathbb{F}_2^m} \prod_{i=1}^{m} x_i^{b_i}$$

où les $b_i \in \{0,1\}$ et $\sum_{i=1}^m b_i \leq \sum_{i=1}^m e_i + e'_i \leq r + m - r - 1 = m - 1$. En utilisant la question précédente, on en déduit que le produit scalaire est nul.

Les codes $\mathrm{RM}(m,r)$ et $\mathrm{RM}(m, m-r-1)$ sont donc orthogonaux. Il reste à démontrer que la somme de leur dimension est égale à leur longueur. On a :

$$\begin{aligned}\dim \mathrm{RM}(m,r) + \dim \mathrm{RM}(m,m-r-1) &= \sum_{i=0}^{r}\binom{m}{i} + \sum_{j=0}^{m-r-1}\binom{m}{j} = \sum_{i=0}^{r}\binom{m}{i} + \sum_{j=0}^{m-r-1}\binom{m}{m-j} \\ &= \sum_{i=0}^{r}\binom{m}{i} + \sum_{j'=r+1}^{m}\binom{m}{j'} = \sum_{i=0}^{m}\binom{m}{i} = 2^m\end{aligned}$$

Solution Q8. Le monôme $\prod_{i=1}^r x_i$ s'annule exactement sur les points $\boldsymbol{x} \in \mathbb{F}_2^r$ tels que $x_i = 0$ pour au moins un $i \in [1,r]$. Donc, les points sur lesquels ce monôme ne s'annule pas sont $\{(1,\dots,1,x_{r+1},\dots,x_m) \mid (x_{r+1},\dots,x_m) \in \mathbb{F}_2^{m-r}\}$. Il y en a 2^{m-r} donc le poids du vecteur d'évluation de $\prod_{i=1}^r x_i$ est 2^{m-r}.

Solution Q9. D'après la question précédente, il faut démontrer que tout mot non-nul de $\mathrm{RM}(m,r)$ est de poids au moins 2^{m-r}. On le démontre par récurrence sur r.

- Pour $r = 0$, c'est évident car $\mathrm{RM}(r,0)$ est le code de répétition (de distance minimale égale à $n = 2^m$).
- Supposons le résultat vrai pour $r-1$. Soit $\boldsymbol{c} \in \mathrm{RM}(m,r)$ le vecteur d'évaluation d'un polynôme $f(x_1,\dots,x_m)$. Le degré total de f est majoré par r. Si ce degré est $< r$, alors on applique l'hypothèse de récurrence, et le poids de $\boldsymbol{c}$ est donc $\geq 2^{m-(r-1)} > 2^{m-r}$. Supposons maintenant que $\deg f = r$.
  à terminer

Solution Q10. On utilise le fait que la localité d'un code est plus grande que $d^\perp - 1$. Notons ici ℓ la localité de $\mathrm{RM}(m,r)$. On a donc :

$$\ell \geq 2^{m-(m-r-1)} - 1 = 2^{r+1} - 1\,.$$

Solution Q11. Supposons que l'on souhaite reconstruire un symbole c_i d'un mot $\boldsymbol{c} \in \mathrm{RM}(m,r)$, tel que c_i est l'évaluation de f en un point $\boldsymbol{a} = (a_1,\dots,a_m) \in \mathbb{F}_2^m$. Ici, on va chercher un mot de $\mathrm{RM}(m,r)^\perp = \mathrm{RM}(m, m-r-1)$ de poids $d^\perp = 2^{r+1}$ dont le support contient i (rappel : ce mot définit une équation de parité de poids 2^{r+1} qui permet de calculer c_i avec $2^{r+1}-1$ autres valeurs c_j). De manière équivalente, cela correspond à chercher un polynôme de degré $\leq m-r-1$ qui ne s'annule pas sur exactement 2^{r+1}, y compris $\boldsymbol{a}$. On peut alors prendre le monôme :

$$f(x_1,\dots,x_m) = \prod_{i=1}^{m-r-1}(x_i + a_i + 1)$$

Ce monôme se n'annule pas sur $\boldsymbol{a}$, et par un raisonnement similaire à la question 8, le poids du vecteur d'évaluation associé est $2^{m-(m-r-1)} = 2^{r+1}$.

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 $\leq t$ de $\boldsymbol{y}$.

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

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

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.

Solutions de l'Exercice 3.

Solution Q1.

1. On a $\boldsymbol{y}^{\star 2} = \boldsymbol{c}^{\star 2} + \boldsymbol{e}^{\star 2} + 2\boldsymbol{c} \star \boldsymbol{e}$.
2. Ainsi, $\boldsymbol{y}^{\star 2} = \boldsymbol{c}^{\star 2} + \boldsymbol{e}'$ où $\boldsymbol{c}^{\star 2} \in \mathcal{C}^{\star 2}$ et $\boldsymbol{e}' = \boldsymbol{e}^{\star 2} + 2\boldsymbol{c} \star \boldsymbol{e}$.
3. On a
$$\mathrm{supp}(\boldsymbol{e}') \subseteq \mathrm{supp}(\boldsymbol{e}^{\star 2}) \cup \mathrm{supp}(\boldsymbol{c} \star \boldsymbol{e}) \subseteq \mathrm{supp}(\boldsymbol{e}) \cup (\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{e})) \subseteq \mathrm{supp}(\boldsymbol{e}).$$

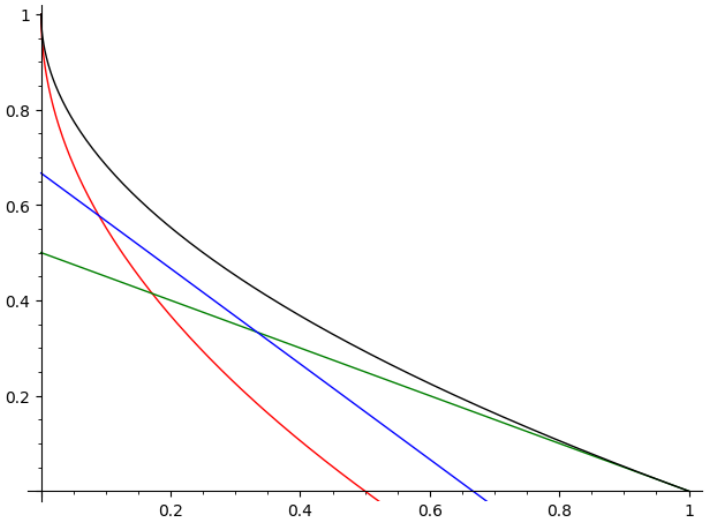

FIGURE 1 – Comparaison asymptotique, en fonction de $R = k/n$, des rayons de décodage relatifs t/n pour le décodage unique (en vert), le *power decoding* (en bleu), le décodage en liste de Sudan (en rouge), et la borne de Johnson (en noir).

Solution Q2. Pour tout $i \in \{1?\ldots, n\}$, on a $y_i E(x_i) = c_i E(x_i)$. Comme $E(x_j) = 0$ sur les cordonées $e'_j \neq 0$, on a également $y_i^2 E(x_i) = c_i^2 E(x_i)$. Le système obtenu est donc :

$$\begin{cases} Y(x_i)E(x_i) = C(x_i)E(x_i) \\ Y^2(x_i)E(x_i) = C^2(x_i)E(x_i) \end{cases}$$

Solution Q3. On pose $A = E$, $B_1 = CE$ et $B_2 = C^2E$. On obtient les contraintes sur les degrés :

$$\begin{cases} \deg A \leq t \\ \deg B_1 \leq t + k - 1 \\ \deg B_2 \leq t + 2k - 2 \end{cases}$$

Par ailleurs, on peut supposer que A est unitaire.

Solution Q4. C'est immédiat au vu de la question précédente.

Solution Q5.

1. Si $t \geq n - 2(k-1)$, alors le polynôme $B_2(X) = \prod_{i=1}^{n}(X - x_i)$ est de degré $n \leq t + 2k - 2$ et vérifie $B_2(x_i) = 0$ pour tout $i \in \{1, \ldots, n\}$. Le triplet $(0, 0, B_2)$ est donc une solution non-nulle du système.
2. Pour avoir un espace de solutions de dimension au plus 1, il est nécéssaire que

   $$\#\text{équations} + 1 \geq \#\text{inconnues}$$

   Dans notre cas, cela signifie qu'on doit imposer

   $$n + 1 \geq t + (t + k - 1) + (t + 2k - 2) \iff t \leq \frac{2n - 3k + 2}{3}.$$

   Notons que le polynôme A de contrinue qu'à $\leq t$ inconnues car il est supposé unitaire.
3. Pour simplifier on fait une analyse asymptotique ($n \to \infty$). Le rayon de Sudan est $1 - \sqrt{2R}$ et celui du décodage unique $\frac{1}{2}(1 - R)$. Pour le *power decoding*, on obtient $\frac{2}{3} - R$. On compare ces grandeurs en fonction de R dans la Figure 1.

Solution Q6. Notons $\mathrm{Diag}(\boldsymbol{y})$ la matrice diagonale de taille $n \times n$ dont les éléments diagonaux sont donnés par $\boldsymbol{y}$. On vérifie alors que le système s'écrit comme

$$\begin{pmatrix} \mathrm{Diag}(\boldsymbol{y})\boldsymbol{V}_t(\boldsymbol{x}) & -\boldsymbol{V}_{t+k}(\boldsymbol{x}) & \boldsymbol{0} \\ \mathrm{Diag}(\boldsymbol{y}^{\star 2})\boldsymbol{V}_t(\boldsymbol{x}) & \boldsymbol{0} & -\boldsymbol{V}_{t+2k-1}(\boldsymbol{x}) \end{pmatrix} \cdot \boldsymbol{X} = \begin{pmatrix} (-\boldsymbol{y} \star \boldsymbol{x}^{\star t})^\top \\ (-\boldsymbol{y}^{\star 2} \star \boldsymbol{x}^{\star t})^\top \end{pmatrix}$$

où $\boldsymbol{X}$ est constitué successivement des coeffcients de A, B_1 et B_2.

Solution Q7.

1. Voir l'Algorithme 1.
2. On peut généraliser le *power decoding* a d'autres puissances que 2. POur cela, on écrit un système

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

dont les inconnues sont les polynômes $(A, B_1, \dots, B_\ell)$ où B_j a degré $\leq t + j(k-1)$. On obtient ℓn équations et $(\ell+1)t + (k-1)\frac{\ell(\ell+1)}{2}$ inconnues. En adaptant l'Algorithme 1, on peut alors corriger t erreurs si

$$t \leq \frac{\ell}{\ell+1} n - \frac{(k-1)\ell}{2}.$$

Asymptotiquement en n, la valeur maximale de t/n est donc approximativement $\ell/(\ell+1) - (\ell/2) \cdot R$.

Algorithme 1 : Algorithme de *power decoding* pour $\mathcal{C} = \mathrm{RS}_k(\boldsymbol{x})$

Entrée : $\boldsymbol{y} \in \mathbb{F}_q^n$ et $t \geq 1$

Sortie : $\boldsymbol{c} \in \mathcal{C}$ tel que $\mathrm{d_H}(\boldsymbol{c}, \boldsymbol{y}) \leq t$, ou un symbole d'erreur de décodage

Calculer l'ensemble S des solutions du système

$$\begin{pmatrix} \mathrm{Diag}(\boldsymbol{y})\boldsymbol{V}_t(\boldsymbol{x}) & -\boldsymbol{V}_{t+k}(\boldsymbol{x}) & \boldsymbol{0} \\ \mathrm{Diag}(\boldsymbol{y}^{\star 2})\boldsymbol{V}_t(\boldsymbol{x}) & \boldsymbol{0} & -\boldsymbol{V}_{t+2k-1}(\boldsymbol{x}) \end{pmatrix} \cdot \boldsymbol{X} = \begin{pmatrix} (-\boldsymbol{y} \star \boldsymbol{x}^{\star t})^\top \\ (-\boldsymbol{y}^{\star 2} \star \boldsymbol{x}^{\star t})^\top \end{pmatrix}$$

Si $\dim S \leq 1$
  Choisir $\boldsymbol{X}$ une solution aléatoire du système
  Construire (A, B_1, B_2) le triplet de polynômes correspondant.
  Si *A divise B_1 et B_2 et* $(B_1/A)^2 = B_2/A$
    Affecter $C = B_1/A$
    Si $\deg(C) \leq k-1$ *et* $\mathrm{d_H}(\mathrm{ev}_{\boldsymbol{x}}(C), \boldsymbol{y}) \leq t$
      Retourner C
Retourner un symbole d'erreur.

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.