Université Paris 13 Année 2021–2022

M2 Mathématiques des données

# Codes correcteurs – Feuille de TD 1

19 novembre 2021

## Exercice 1. Algorithme de décodage de codes de Reed-Solomon.

Dans cet exercice, on étudie l'algorithme de Gao [1] qui permet de décoder les codes de Reed-Solomon jusqu'au rayon de décodage unique.

On considère donc $\mathcal{C} = \mathrm{RS}(\boldsymbol{x}, k) \subseteq \mathbb{F}_q^n$ le code de Reed-Solomon évalué sur les points $\boldsymbol{x} = (x_1, \ldots, x_n)$ où les $x_i \in \mathbb{F}_q$ sont deux à deux distincts. **On suppose que $n$ et $k$ sont pairs pour éviter la manipulation de parties entières.** La méthode de Gao pour décoder dans $\mathcal{C}$ est décrite dans l'Algorithme 2. Celui-ci prend en entrée un mot transmis $\boldsymbol{y} \in \mathbb{F}_q^n$, tel que $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$, où $\boldsymbol{c}$ est un mot de $\mathcal{C}$ et $\boldsymbol{e}$ est une erreur de poids $\mathrm{wt}(\boldsymbol{e}) \leq t \coloneqq \frac{n-k}{2}$. Le but de l'exercice est de démontrer que l'algorithme retourne le message associé à $\boldsymbol{c}$, c'est-à-dire les coefficients du polynôme $C \in \mathbb{F}_q[X]_{<k}$ tel que $c_i = C(x_i)$ pour tout $i = 1, \ldots, n$.

Dans tout l'exercice, on note $Y(X)$ le polynôme interpolateur des points $(x_i, y_i)$, c'est-à-dire le polynôme $Y(X) \in \mathbb{F}_q[X]$ de plus petit degré tel que $y_i = Y(x_i)$. On note également $C(X) \in \mathbb{F}_q[X]$ le polynôme interpolateur des $(x_i, c_i)$. Enfin, on note $A(X) = (X - x_1) \ldots (X - x_n)$ et $E(X) = (X - x_{j_1}) \ldots (X - x_{j_w})$ où $\{j_1, \ldots, j_w\}$ sont les indices des erreurs présentes dans $\boldsymbol{e}$. Autrement dit $E(x_j) = 0$ si et seulement si $e_j \neq 0$.

L'algorithme de Gao (Algorithme 2) utilise une variante tronquée de l'algorithme d'Euclide étendu, décrite dans l'Algorithme 1.

**Algorithme 1 :** Algorithme d'Euclide tronqué, aussi noté `partial_xgcd`

**Entrée :** deux polynômes $A, B \in \mathbb{F}_q[X]$ tels que $\deg A = n$ et $\deg B \leq n - 1$, et un entier $s \leq n - 1$
**Sortie :** trois polynômes $R, U, V \in \mathbb{F}_q[X]$ tels que $UA + BV = R$ et $\deg R < s$

Initialiser $R_0 = A$, $R_1 = B$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$ et $V_1 = 1$.
**Tant que** $\deg R_1 \geq s$ **faire**
  Calculer le quotient $Q$ de la division euclidienne de $R_0$ par $R_1$.
  Mettre à jour $(R_0, R_1) \leftarrow (R_1, R_0 - QR_1)$.
  Mettre à jour $(U_0, U_1) \leftarrow (U_1, U_0 - QU_1)$.
  Mettre à jour $(V_0, V_1) \leftarrow (V_1, V_0 - QV_1)$.
**Retourner** $R = R_1$, $U = U_1$ et $V = V_1$.

**Algorithme 2 :** Algorithme de Gao [1] pour le décodage des codes de Reed-Solomon

**Entrée :** un mot $\boldsymbol{y} \in \mathbb{F}_q^n$ tel que $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$, $\boldsymbol{c} \in \mathcal{C}$ et $\mathrm{wt}(\boldsymbol{e}) \leq \frac{n-k}{2}$
**Sortie :** le message $\boldsymbol{m}$ initial

Calculer $A(X) = (X - x_1)(X - x_2) \cdots (X - x_n)$.
Calculer $Y(X)$ le polynôme interpolateur des points $\{(x_i, y_i)\}_{1 \leq i \leq n}$.
Calculer $s = (k + n)/2$.
Effectuer $(R, U, V) \leftarrow$ `partial_xgcd`$(A, Y, s)$.
Calculer $C(X) = \frac{R(X)}{V(X)}$.
**Retourner** les coefficients de $C$.

**Question 1.–** Donner des bornes (ou la valeur exacte lorsque c'est possible) sur les degrés des polynômes $A(X)$, $C(X)$, $E(X)$ et $Y(X)$.

**Question 2.–** Démontrer que $Y(X)E(X) \equiv C(X)E(X) \mod A(X)$. En déduire qu'il existe un couple de polynômes $(N, E) \in \mathbb{F}_q[X]$ tel que

$$Y(X)E(X) \equiv N(X) \mod A(X), \quad \deg E \leq \tfrac{n-k}{2}, \quad \deg N \leq k - 1 + \tfrac{n-k}{2}\,. \tag{1}$$

**Question 3.–** Démontrer que si $(N, E)$ et $(N', E')$ sont deux couples de solutions de (1), alors on a

$$\frac{N}{E} = \frac{N'}{E'} = C(X)\,.$$

**Note.** L'équation (1) est parfois appelée « équation-clé » pour le décodage. Observons qu'on peut l'exprimer comme un système d'équations linéaires à $(\deg N + 1) + \deg E \leq n - 1$ inconnues (le polynôme $E$ est unitaire) et $n$ équations. On peut résoudre ce système par une élimination Gaussienne en temps $O(n^3)$. Dans cet exercice, on va chercher à résoudre l'équation-clé par des divisions euclidiennes de polynômes.

**Question 4.–** Dans l'algorithme d'Euclide étendu, on a $U_i A + V_i B = R_i$ à chaque étape de l'algorithme. Démontrer la relation suivante sur les degrés de certains de ces polynômes :

$$\deg V_i + \deg R_{i-1} = \deg A\,.$$

**Question 5.–** Démontrer que pour $s = \frac{n+k}{2}$, le triplet de sortie $(R, U, V)$ de la procédure `partial_xgcd`$(A, Y, s)$ est tel que $(N = R, E = V)$ vérifie l'équation (1).

**Question 6.–** Conclure sur la correction de l'algorithme et donner une borne sur sa complexité en fonction de $n$.

# Références


[1] Shuhong Gao. A New Algorithm for Decoding Reed-Solomon Codes. In Vijay K. Bhargava, H. Vincent Poor, Vahid Tarokh, and Seokho Yoon, editors, *Communications, Information and Network Security*, pages 55–68. Springer US, 2003.