

Algorithmes Arithmétiques II – Feuille de TD 2

26/09/2023

Le corrigé de certains exercices sera disponible à l'adresse suivante :

<https://lvz1.fr/teaching/2023-24/aa.html>

(★) exercice fondamental (★★) pour s'entraîner (★★★) pour aller plus loin  sur machine

Exercice 1. (★★) Calcul du polynôme de connexion par l'algorithme d'Euclide.

Dans cet exercice, on étudie une méthode permettant de calculer le polynôme de connexion minimal d'une suite scalaire $\mathbf{b} \in \mathbb{F}^{\mathbb{N}}$, en utilisant l'algorithme d'Euclide étendu.

Pour cela, on considère les $2n$ premiers termes de la suite \mathbf{b} , on note $B(X) = \sum_{i=0}^{2n-1} b_i X^i \in \mathbb{F}[X]$, et on cherche donc un polynôme de connexion $P(X)$ de degré $\leq n$ tel que $P(X)B(X) \pmod{X^{2n}}$ est de degré $< n$.

Question 1.– Rappeler l'algorithme d'Euclide étendu pour les polynômes.

Question 2.– Exemple : supposons que $\mathbb{F} = \mathbb{F}_2$, $n = 4$ et $\mathbf{b} = (0, 1, 1, 1, 0, 0, 1, 0)$.

1. Donner l'expression du polynôme $B(X)$.
2. Déterminer un polynôme de connexion de la suite, de degré < 4 . On pourra, si besoin, utiliser l'algorithme de Berlekamp–Massey.
3. Appliquer l'algorithme d'Euclide étendu à $A(X) = X^8$ et $B(X)$.
4. Commenter les résultats obtenus.

Dans le cas général, on exécute l'algorithme d'Euclide étendu sur les entrées $A(X) = X^{2n}$ et $B(X) = \sum_{i=0}^{2n-1} b_i X^i$. Les polynômes successivement calculés par l'algorithme sont notés R_i, Q_i, U_i, V_i et satisfont :

$$R_{i-1} = Q_i R_i + R_{i+1}, \quad U_{i-1} = Q_i U_i + U_{i+1}, \quad V_{i-1} = Q_i V_i + V_{i+1}$$

avec initialement $R_0 = A$ et $R_1 = B$.

On note $k \geq 1$ le premier indice pour lequel le reste $R_k(X)$ a degré $< n$. Autrement dit, on a également $\deg R_{k-1} \geq n$.

Question 3.– Quelle est la relation entre $\deg V_k$, $\deg R_{k-1}$ et $\deg A$?

Question 4.– Démontrer que V_k est un polynôme de connexion de la suite \mathbf{b} en étudiant notamment la croissance de la suite $(\deg(V_i))_i$.

Question 5.– Décrire un nouvel algorithme de calcul de polynôme de connexion, et en donner la complexité.

Exercice 2. (☆☆☆) Implantation de la résolution de système linéaire creux.

Dans cet exercice, on se donne comme objectif de résoudre effectivement un système linéaire creux en temps $O(tn^2)$ et espace $O(nt)$, où la matrice $A \in \mathbb{F}^{n \times n}$ du système a $\leq t$ coefficients non-nuls sur chaque ligne.

Question 1.– Planter une structure permettant de gérer et d’effectuer des opérations élémentaires sur des matrices creuses : création d’une matrice creuse aléatoire, somme de deux matrices, produit matrice-vecteur, échange de lignes/colonnes, etc.

Question 2.– Planter une méthode de Horner pour calculer $Q(A)\mathbf{b}$ en temps $O(ndt)$ et espace $O(nt)$, où $Q(X) \in \mathbb{F}[X]$ est de degré d et $\mathbf{b} \in \mathbb{F}^n$.

Question 3.– Planter une fonction qui calcule le pgcd et le ppccm de deux polynômes de degré $\leq d$ en temps $O(d^2)$.

Question 4.– En s’aidant de l’algorithme de Berlekamp–Massey :

1. planter une fonction qui calcule le polynôme annulateur d’une suite vectorielle itérée $\mathbf{v} = (A^k \mathbf{b})_{k \in \mathbb{N}}$;
2. planter une fonction qui calcule le polynôme annulateur de A .

Ces fonctions devront avoir une complexité en $O(tn^2)$ en temps et $O(nt)$ en espace.

Question 5.– Planter une fonction `get_one_solution(A, b)` qui calcule en temps $O(tn^2)$ et espace $O(nt)$ une solution particulière du système $A\mathbf{x} = \mathbf{b}$, où $A \in \mathbb{F}^{n \times n}$ est t -creuse et $\mathbf{b} \in \mathbb{F}^n \setminus \{\mathbf{0}\}$.

Question 6.– En utilisant l’algorithme de Wiedemann, planter une fonction `get_kernel_element(A)` qui calcule en temps $O(tn^2)$ et espace $O(nt)$ une solution du système $A\mathbf{x} = \mathbf{0}$, où $A \in \mathbb{F}^{n \times n}$ est t -creuse et non-inversible.

Question 7.– Donner les complexités expérimentales (en temps) des fonctions `get_one_solution(A, b)` et `get_kernel_element(A)`. On prendra garde de choisir des valeurs assez grandes de n et assez petites de t (relativement à n) pour observer la croissance en $O(tn^2)$.