Université Paris 8 Année 2022–2023

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Feuille de TD 2

29/09/2022

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

`www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/algorithmes-arithmetiques.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

---

Exercice 1. $(\star)$ Suite vectorielle et LFSR.

Soit $\boldsymbol{u} = (u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire scalaire non-nulle, produite par un LFSR de dimension L. On note $P(X) = \sum_{j=0}^{d} c_j X^j$ le polynôme de connexion du LFSR. On rappelle qu'on a donc

$$\sum_{j=0}^{d} c_j u_{n-j} = 0, \quad c_0 = 1\,.$$

Soit maintenant $\boldsymbol{v} = (v_k)$ une suite définie par

$$\forall k \in \mathbb{N}, \quad \boldsymbol{v}_k \coloneqq (u_k, u_{k+1}, \ldots, u_{k+L-1})^\top \in \mathbb{F}^L\,.$$

Question 1.– Démontrer que $\boldsymbol{v}$ est une suite récurrente linéaire sur $\mathbb{F}^L$. En donner une description sous forme de suite itérée, dont on précisera la matrice $\boldsymbol{A}$.

Question 2.– Que vaut $\det(\boldsymbol{A})$? En déduire une condition suffisante pour que la suite $\boldsymbol{u}$ ne soit pas nulle à partir d'un certain rang.

Question 3.– À l'aide des questions précédentes, démontrer que si le corps $\mathbb{F}$ est de cardinal q fini (*i.e.* $\mathbb{F} = \mathbb{F}_q$), alors la suite $\boldsymbol{u}$ a une période $\leq q^L - 1$.

Exercice 2. $(\star\star)$ 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 $\boldsymbol{b} \in \mathbb{F}^{\mathbb{N}}$, en utilisant l'algorithme d'Euclide étendu.

Pour cela, on considère les $2n$ premiers termes de la suite $\boldsymbol{b}$, 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 $P(X)B(X) \mod X^{2n}$ 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 $\boldsymbol{b} = (0,1,1,1,0,0,1,0)$.

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 $\boldsymbol{b}$ 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 3. $(\star)$ 💻 Implantation du calcul du polynôme de connexion par l'algorithme d'Euclide.

Question 1.– Implanter l'algorithme d'Euclide étendu, puis l'algorithme de calcul de polynôme de connexion vu dans l'Exercice 2.

Question 2.– Calculer les polynômes de connexion minimaux des suites données dans le fichier `challenges_lfsr.txt` (le même que pour l'exercice du TD1 où vous deviez implanter l'algorithme de Berlekamp–Massey).

Question 3.– Comparer expérimentalement la complexité de votre nouvel algorithme avec celle de l'algorithme de Berlekamp–Massey.

Exercice 4. $(\star\star\star)$ 💻 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 $\boldsymbol{A} \in \mathbb{F}^{n\times n}$ du système a $\leq t$ coefficients non-nuls sur chaque ligne.

Question 1.– Implanter 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.– Implanter une méthode de Horner pour calculer $Q(\boldsymbol{A})\boldsymbol{b}$ en temps $O(ndt)$ et espace $O(nt)$, où $Q(X) \in \mathbb{F}[X]$ est de degré d et $\boldsymbol{b} \in \mathbb{F}^n$.

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

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

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

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

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

Question 6.– En utilisant l'algorithme de Wiedemann, implanter une fonction `get_kernel_element(A)` qui calcule en temps $O(tn^2)$ et espace $O(nt)$ une solution du système $\boldsymbol{Ax} = \boldsymbol{0}$, où $\boldsymbol{A} \in \mathbb{F}^{n\times n}$ 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 $O(tn^2)$.