Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Algorithmes Arithmétiques II – Solutions feuille de TD 2

26/09/2023

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`https://lvzl.fr/teaching/2023-24/aa.html`

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

Exercice 1. ($\star\star$) 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.

Solutions de l'Exercice 1.

Solution Q1. Voir Algorithme 1.

Solution Q2.

1. On a $B(X) = X + X^2 + X^3 + X^6$.

Algorithme 1 : Algorithme d'Euclide

Entrée : deux polynômes $A, B \in \mathbb{F}[X]$
Sortie : trois polynômes $R, U, V \in \mathbb{F}_q[X]$ tels que $AU + BV = R$ et R est le pgcd de A et B

Initialiser $R_0 \leftarrow A$, $R_1 \leftarrow B$, $U_0 \leftarrow 1$, $U_1 \leftarrow 0$, $V_0 \leftarrow 0$ et $V_1 \leftarrow 1$.
Tant que $R_1 \neq 0$ **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 $R = R_0$, $U = U_1$ et $V = V_1$.

2. Une exécution de l'algorithme de Berlekamp–Massey donne :

k	ℓ_k	$P_k(X)$
0	0	1
1	0	1
2	2	1
3	2	$X+1$
4	2	$X+1$
5	3	X^3+X+1
6	3	X^3+X^2+1
7	3	X^3+X^2+1
8	3	X^3+X^2+1

3. On a

$$A(X) = X^2 \times B(X) + (X^5 + X^4 + X^3)$$
$$B(X) = (X+1) \times (X^5 + X^4 + X^3) + (X^2 + X)$$
$$(X^5 + X^4 + X^3) = (X^3 + X + 1) \times (X^2 + X) + X$$

C'est-à-dire :

k	R_k	U_k	V_k
0	X^8	1	0
1	$X + X^2 + X^3 + X^6$	0	1
2	$X^5 + X^4 + X^3$	1	X^2
3	$X^2 + X$	$X+1$	$X^3 + X^2 + 1$
4	X	$X^4 + X^3 + X^2$	$X^6 + X^5 + X^4 + X^3 + X + 1$

4. On observe que pour $k = 3$, on a $\deg R_3 = 2 < 4$, $\deg V_3 = 3 < 4$, et

$$U_3(X)X^8 + V_3(X)B(X) = R_3(X)$$

Autrement dit,

$$V_3(X)B(X) \equiv R_3(X) \mod X^8 \text{ avec } \deg R_3 < 4$$

Le polynôme V_3 est donc un polynôme de connexion de $\boldsymbol{b}$.

Solution Q3. Pour tout i (avant l'arrêt), on a

$$\deg R_{i-1} = \deg Q_i + \deg R_i \quad \text{et} \quad \deg V_{i+1} = \deg Q_i + \deg V_i\,.$$

Donc :

$$\deg V_{i+1} + \deg R_i = \deg V_i + \deg R_{i-1} = \cdots = \deg V_1 + \deg R_0 = 0 + \deg(A)$$

Puis,

$$\deg V_k + \deg R_{k-1} = 2n$$

Solution Q4. La suite $(\deg V_i)_i$ est strictement croissante (avant l'arrêt). On a donc $V_k(X)B(X) \equiv R_k(X) \mod X^{2n}$, avec $\deg R_k < n$ et $\deg V_k \leq 2n - n = n$.

Solution Q5. Si l'on cherche un polynôme de connexion de degré $< n$ d'une suite $\boldsymbol{b}$ dont les $2n$ premiers termes sont $(b_0, \ldots, b_{2n-1})$, on peut :

(i) calculer les polynômes $A(X) = X^{2n}$ et $B(X) = \sum_{i=0}^{2n-1} b_i X^i$,

(ii) exécuter les itérations de l'algorithme d'Euclide étendu, avec comme entrées $A(X)$ et $B(X)$, jusqu'à ce que $R_k(X)$ ait degré $\leq n-1$,
(iii) retourner le coefficient de Bézout $V_k(X)$ associé à $B(X)$.

La complexité de l'algorithme correspond asymptotiquement à celle de l'exécution de l'algorithme d'Euclide (tronquer à $\deg(R_k) \leq n-1$ fait seulement gagner un facteur constant). Elle est donc en $O(n^2)$ opérations dans $\mathbb{F}$.

Remarque. Avec des algorithmes avancés, on peut calculer le pgcd de deux polynômes en temps $O(M(2n)\log n)$, où $M(n)$ représente la complexité de la mutiplication de deux polynômes de degré $\leq n$ sur $\mathbb{F}$.

Exercice 2. $(\star\star\star)$ 💻 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 $O(tn^2)$.