Université Paris 8 Année 2022–2023

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Solutions feuille de TD 1

23/09/2021

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

`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. ($\star$) Polynôme de connexion minimal.

Soit $\boldsymbol{u} \in \mathbb{F}^{\mathbb{N}}$ une suite récurrente linéaire sur un corps $\mathbb{F}$.

Question 1.– Démontrer que l'ensemble des polynômes de connexion de $\boldsymbol{u}$ forme un idéal de $\mathbb{F}[X]$.

Question 2.– En déduire qu'il existe un unique polynôme de connexion de $\boldsymbol{u}$ dont le degré est minimal, et tel que $P(0) = 1$.

Solutions de l'Exercice 1.

Solution Q1. Notons $\mathcal{R}(\boldsymbol{u})$ l'ensemble des polynômes de connexion de la suite $\boldsymbol{u}$ de série formelle $U(X)$. Par définition, comme on peut écrire $U \times 0 = 0$, le polynôme nul est dans $\mathcal{R}(\boldsymbol{u})$. Soient maintenant $P, Q \in \mathcal{R}(\boldsymbol{u})$, et $\lambda \in \mathbb{F}$. On note L_P et L_Q les nombres de termes initiaux associés au polynôme P et Q. Alors, pour $L = \max\{L_P, L_Q\} + 1$ et pour tout $n \geq L$ on a :

$$\sum_{i=0}^{\max\{\deg P, \deg Q\}} (p_i + q_i)\, u_{n-i} = 0 + 0 = 0, \quad \sum_{i=0}^{d} (\lambda p_i) u_{n-1} = 0 \quad \text{et} \quad \sum_{i=1}^{d+1} p_{i-1}\, u_{n-i} = \sum_{i=0}^{d} p_i\, u_{n-1-i} = 0\,.$$

Autrement dit, $P + Q$, λP et XP sont dans $\mathcal{R}(\boldsymbol{u})$.

Remarque : plus formellement, en travaillant dans l'anneau des séries formelles $\mathbb{F}[\![X]\!]$, on pouvait simplement noter que pour tout $A \in \mathbb{F}[X]$, on a $UPA = QA$, donc PA est un polynôme de connexion de la suite $\boldsymbol{u}$.

Solution Q2. L'anneau $\mathbb{F}[X]$ est euclidien, donc ses idéaux sont principaux et engendrés par un polynôme de degré minimal. Soit P un générateur de $\mathcal{R}(\boldsymbol{u})$. Pour montrer le résultat, quitte à diviser P par $P(0)$ il suffit d'établir que $P(0) \neq 0$. On observe alors que si l'on avait $P(0) = 0$, alors $P(X) = \sum_{i=0}^{d} p_i X^i$ s'écrirait $XA(X)$, et on vérifie aisément que $A(X)$ est dans $\mathcal{R}(\boldsymbol{u})$:

$$\sum_{i=0}^{d-1} a_i u_{n+1-i} = \sum_{i=1}^{d} p_{i-1}\, u_{n+1-i} = \sum_{i=0}^{d} p_i\, u_{n-i} = 0, \quad \forall n \geq L\,.$$

C'est contradictoire avec le fait que P soit de degré minimal dans $\mathcal{R}(\boldsymbol{u})$.

Exercice 2. ($\star$) LFSR d'une suite dont les premiers termes sont nuls.

Soit $\boldsymbol{u} \in \mathbb{F}^{\mathbb{N}}$ une suite récurrente linéaire telle que $u_0 = \cdots = u_{k-1} = 0$ et $u_k = 1$. On note $(\ell_n(\boldsymbol{u}))_{n \in \mathbb{N}}$ le profil de complexité linéaire de $\boldsymbol{u}$.

Question 1.– Pour tout $i \in \{1, \ldots, k\}$:

1. démontrer que $\ell_i(\boldsymbol{u}) = 0$;
2. expliciter un polynôme $P_i(X) \in \mathbb{F}[X]$ de degré minimal tel que $(P_i(X), \ell_i(\boldsymbol{u}))$ engendre $\boldsymbol{u}$ sur i termes.

Question 2.– Démontrer que $\ell_{k+1}(\boldsymbol{u}) = k+1$.

Question 3.– Soit $\boldsymbol{v} \in \mathbb{F}^{\mathbb{N}}$ la suite telle que $v_n = u_{k+n}$ pour tout $n \in \mathbb{N}$. Démontrer que $\ell_n(\boldsymbol{v}) = \ell_{n+k}(\boldsymbol{u}) - k$ pour tout $n \in \mathbb{N}$.

Solutions de l'Exercice 2.

Solution Q1. En posant $P_i(X) = 1$, on obtient que $u_i = 0$ pour tout $i \in \{1, \ldots, k\}$. Donc, il n'y a pas besoin de terme initial pour la suite $\boldsymbol{u}$ jusqu'à l'ordre k, et $\ell_i(\boldsymbol{u}) = 0$.

Solution Q2. Comme $u_k = 1$, on ne peut pas exprimer u_k comme une combinaison linéaires des $\{u_i\}_{i \leq k-1}$ qui sont tous nuls. Par conséquent, on doit initialiser les $k+1$ premiers termes de la suite sans relation de récurrence, et $\ell_{k+1}(\boldsymbol{u}) = k+1$.

Solution Q3. Montrons que $\mathcal{R}_n(\boldsymbol{v}) = \{(P,L) \mid (P,L+k) \in \mathcal{R}_{n+k}(\boldsymbol{u})\}$. Ceci étant établi, on aura alors

$$\begin{aligned}
\ell_n(\boldsymbol{v}) &= \min\{L \mid (P,L) \in \mathcal{R}_n(\boldsymbol{v})\} \\
&= \min\{L \mid (P,L+k) \in \mathcal{R}_{n+k}(\boldsymbol{v})\} \\
&= \min\{L' \mid (P,L') \in \mathcal{R}_{n+k}(\boldsymbol{v})\} - k \\
&= \ell_{n+k}(\boldsymbol{u}) - k\,.
\end{aligned}$$

En notant U et V les séries formelles associées à $\boldsymbol{u}$ et $\boldsymbol{v}$, cela revient à démontrer que :

$$PU \mod X^{n+k} \text{ est de degré } \leq L+k-1 \quad \Longleftrightarrow \quad PV \mod X^n \text{ est de degré } \leq L-1\,.$$

Pour cela, observons que par définition de $\boldsymbol{v}$, on a $U(X) = X^k V(X)$. L'équivalence s'ensuit aisément.

Exercice 3. ($\star\star$) Exécution de l'algorithme de Berlekamp–Massey.

Question 1.– Dérouler l'algorithme de Berlekamp–Massey sur la suite binaire dont les 10 premiers termes sont :

$$(1,1,1,1,0,1,1,0,1,1)\,.$$

Question 2.– Si la suite se poursuit indéfiniment par la séquence périodique $(0,1,1)$, que dire de son polynôme de connexion minimal ?

Solutions de l'Exercice 3.

Solution Q1. On obtient la séquence de LFSR suivante

k	P_k	L_k
0	1	0
1	1	1
2	$X+1$	1
3	$X+1$	1
4	$X+1$	1
5	X^4+X+1	4
6	X^4+X+1	4
7	$X^4+X^3+X^2+X+1$	4
8	X^2+X+1	4
9	X^2+X+1	4

Solution Q2. Le polynôme de connexion minimal sera $1+X+X^2$, car :

— il est polynôme de connexion,
— il n'y a pas de polynôme de connexion ayant degré 1 ou 0 (les essayer tous, il y en a au plus 4).

Si le lien entre période et degré du polynôme de connexion a été vu, on peut aussi l'utiliser comme argument : comme la période de la suite est 3, le degré du polynôme de connexion doit vérifier $2^d - 1 \geq 3$, autrement dit $d \geq 2$.

Exercice 4. ($\star$) Premiers termes d'une suite définie par sa série formelle.

Soit $\boldsymbol{u} \in \mathbb{F}_2^{\mathbb{N}}$ la suite récurrente linéaire définie par la série formelle

$$U(X) = \frac{1 + X + X^2}{1 + X + X^3}.$$

Question 1.– Quel est l'ordre de la suite ? Combien de termes initiaux possède-t-elle ?

Question 2.– Donner les 15 premiers termes de la suite $\boldsymbol{u}$. Quelle est sa période ?

Solutions de l'Exercice 4.

Solution Q1. Le dénominateur $P(X) = 1 + X + X^3$ est un polynôme de connexion de la suite $\boldsymbol{u}$. Son degré est une borne supérieure sur l'ordre de la suite. Par ailleurs, comme P est irréductible sur $\mathbb{F}_2$, on a égalité.

Le nombre de termes initiaux se compte sur degré du numérateur de $U(X)$, c'est-à-dire 2.

Solution Q2. On utilise l'algorithme suivant pour développer $U(X)$ en $x = 0$.

Algorithme 1 : Développement d'une fraction rationnelle en 0.

```
u ← []
g(x) ← f(x)
Pour tout i allant de 0 à N − 1 faire
    Ajouter g(0) à la fin de u
    Remplacer g(x) par (g(x) − g(0))/x.
Retourner u
```

On obtient la séquence suivante :

$$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$$

Sa période est $7 = 2^3 - 1$.

Exercice 5. ($\star\star$) Implantation de l'algorithme de Berlekamp–Massey.

Question 1.– Implanter l'algorithme de Berlekamp-Massey vu en cours, sur un corps fini $\mathbb{F}_2$.

Question 2.– Tester votre fonction avec les 5 suites dont les premiers termes sont donnés dans le fichier `challenges_lfsr.txt`. Les trois premières séquences présentes dans ce fichier sont les suivantes :

1. $(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$
2. $(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$
3. $(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, \ldots$
   $\ldots 1, 1, 0, 0, 1, 1, 1, 0, 0)$

Question 3.– En produisant des suites linéaires récurrentes aléatoires d'ordre d, donner une estimation expérimentale de la complexité de l'algorithme de Berlekamp–Massey en fonction de d.

Solutions de l'Exercice 5.

Voir les scripts SageMath disponibles en ligne.

Exercice 6. 💻 ($\star\star\star$) Résolution de systèmes linéaires.

Les fonctions à implanter doivent être suffisamment génériques pour être exécutables sur n'importe quel corps effectif $\mathbb{F}$.

Question 1.– Implanter les fonctions suivantes.

1. Une fonction `right_kernel(T)` qui calcule une base du noyau à droite d'une matrice échelonnée $\boldsymbol{T} \in \mathbb{F}^{n\times n}$. On pourra supposer que les pivots de $\boldsymbol{T}$ sont sur sa diagonale.
2. Une fonction `triangular_solve(T, b)` qui calcule une solution éventuelle d'un système linéaire $\boldsymbol{Tx} = \boldsymbol{b}$, où $\boldsymbol{T} \in \mathbb{F}^{n\times n}$ est sous forme échelonnée. On traitera notamment le cas où le système n'admet aucune solution. Comme pour la question précédente, on pourra supposer que les pivots de $\boldsymbol{T}$ sont sur sa diagonale.
3. Une fonction `gaussian_elimination(A, b)` qui effectue l'élimination gaussienne sur la matrice $\boldsymbol{A} \in \mathbb{F}^{n\times n}$ et le vecteur $\boldsymbol{b} \in \mathbb{F}^n$. Si, dans les questions précédentes, on a supposé que les pivots de $\boldsymbol{T}$ sont sur sa diagonale, alors l'élimination gaussienne devra produire une matrice ayant cette propriété.

Question 2.– Écrire une fonction `solve_system(A, b)` qui calcule l'ensemble des solutions du système d'équations $\boldsymbol{Ax} = \boldsymbol{b}$, où $\boldsymbol{A} \in \mathbb{F}^{n\times n}$ et $\boldsymbol{b} \in \mathbb{F}^n$. On donnera les solutions sous la forme d'un espace affine, dont on décrira un élément particulier et une base de l'espace directeur.

Sur la page web du cours, vous pouvez retrouver des fichiers dont le nom a la forme `system<n>x<n>r<r>q<q>.txt`. Ces fichiers contiennent $n+2$ lignes :

— les n premières lignes sont composés de n chiffres entre 0 et $q-1$, représenant chacun un élément de $\mathbb{F}_q$: chacune de ce lignes représente une ligne de la matrice $\boldsymbol{A}$ du système ;
— la $(n+1)$-ème ligne est vide ;
— la dernière ligne représente $\boldsymbol{b}$ (elle est aussi constituée de n coefficients sur $\mathbb{F}_q$).

La valeur de r donnée dans le nom de fichier représente la dimension de l'espace directeur des solutions au système. Elle est d'ordre indicative, mais peut vous permettre de vérifier la cohérence de vos résultats.

Question 3.– Résoudre les systèmes linéaires donnés dans les fichiers mentionnés ci-dessus.

Question 4.– Implanter une fonction `solve_general_system(A, b)` qui traite le cas où le système n'est pas nécessairement carré, c'est-à-dire lorsque $\boldsymbol{A} \in \mathbb{F}^{m\times n}$ et $\boldsymbol{b} \in \mathbb{F}^m$.

Question 5.– Dans le cas où $\mathbb{F} = \mathbb{F}_2$, donner une estimation numérique la plus précise possible de la complexité de la résolution d'un système linéaire aléatoire de taille $n \times n$. On pourra

— ou bien incorporer des compteurs pour évaluer le nombre d'opérations (additions et multiplications) effectuées en fonction de n,
— ou bien mesurer le temps d'éxecution de l'algorithme.

Solutions de l'Exercice 6.

Voir les scripts SageMath disponibles en ligne.