Université Paris 8 Année 2021–2022

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Feuille de TD 1

22/09/2021

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

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/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.

Question 1.– Démontrer que l'ensemble des polynômes de connexion P 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 $P(0) = 1$.

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 $i \in \{1, \dots, k\}$:

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

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 ?

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 ?

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 suites dont les premiers termes sont donnés par :

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

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

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

Pour les deux premières questions de cet exercice, les fonctions à implémenter doivent être génériques et être exécutables sur n'importe quel corps effectif $\mathbb{F}$.

Question 1.– Implanter les fonctions suivantes.

1. Une fonction `triangular_solve(T, b)` qui calcule une solution éventuelle d'un système linéaire $\boldsymbol{T}\boldsymbol{x} = \boldsymbol{b}$, 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.
2. Une fonction `right_kernel(T)` qui calcule une base du noyau à droite d'une matrice échelonnée $\boldsymbol{T} \in \mathbb{F}^{n\times n}$.
3. Une fonction `gaussian_elimination(A, b)` qui effectue l'éimination gaussienne sur la matrice $\boldsymbol{A} \in \mathbb{F}^{n\times n}$ et le vecteur $\boldsymbol{b} \in \mathbb{F}^n$.

Question 2.– Écrire une fonction `solve_system(A, b)` qui calcule l'ensemble des solutions du système d'équations $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$, 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.

Question 3.– 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 4.– 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'exécution de l'algorithme.