Partiel de M.A.O. Calcul Formel Durée : 3 heures

Lundi 16 avril 2018
Master 1 M.F.A., Orsay

L'accès à internet et l'utilisation des téléphones portables sont interdits. Les documents et notes de cours sont interdits, à l'exception du livre "Calcul mathématique avec Sage". En revanche l'aide de Sage et une version pdf de ce livre sont disponibles sur les ordinateurs. Ce partiel est une épreuve de mathématiques. Avant d'utiliser l'ordinateur, il convient de se demander s'il n'est pas possible d'obtenir par un raisonnement simple ce qui pourrait être obtenu par un calcul plus complexe fait par ordinateur. A titre indicatif, dans les questions signalées par le signe ($\star$), on s'attend à une réponse utilisant de façon essentielle l'ordinateur ; pour les autres, on s'attend davantage à une réponse argumentée, utilisant éventuellement l'ordinateur mais de façon plus marginale.
Dans tous les cas, si vous utilisez l'ordinateur, vous devez recopier les lignes de code Sage que vous avez utilisées (en faisant attention à l'indentation), et ce que leur exécution a renvoyé ; il est également indispensable d'expliquer les calculs que vous faites faire à l'ordinateur. Il est parfois indiqué que certaines commandes de Sage ne doivent pas être utilisées ; en cas de doute n'hésitez pas à poser des questions pendant l'épreuve.

Le sujet est composé d'un seul problème, découpé en cinq parties. Les questions sont de difficulté inégale ; il est possible d'admettre le résultat de certaines pour traiter les suivantes.

Le but de ce problème est d'étudier quelques algorithmes de calcul d'une suite définie par une relation de récurrence, et d'en voir des applications. On note $\mathbb{K}$ un corps, d un entier strictement positif, et $a_0, \ldots, a_{d-1}$ des éléments de $\mathbb{K}$. On considère la suite $(u_n)_{n\geq 0}$ définie par la donnée de $u_0, u_1, \ldots, u_{d-1} \in \mathbb{K}$ et la relation de récurrence

$$u_{n+d} = a_{d-1}u_{n+d-1} + \ldots + a_1 u_{n+1} + a_0 u_n \text{ pour tout } n \geq 0. \quad (1)$$

Dans tout le problème on suppose $\mathbb{K}$, d, $a_0, \ldots, a_{d-1}$, $u_0, \ldots, u_{d-1}$ connus. Etant donné un entier $N \geq d$, on cherche à calculer soit le terme u_N (parties 2 et 3), soit tous les termes u_i avec $i \leq N$ (parties 1 et 4). On prendra garde au fait que d et N peuvent être *tous les deux* très grands : le coût des algorithmes devra toujours être exprimé en fonction de d et de N. On supposera seulement que N/d est très grand, si bien que $O(N+d) = O(N)$ par exemple.

Partie 1 : Approche naïve

1. Soit $n \geq 0$; supposons connus u_n, u_{n+1}, $\ldots$, u_{n+d-1}. En utilisant la relation de récurrence (1), quel est le coût du calcul de u_{n+d}, en opérations arithmétiques dans $\mathbb{K}$ (additions, multiplications, soustractions ou divisions) ?

2. En utilisant l'algorithme issu de la question 1, quel est le coût en opérations arithmétiques dans $\mathbb{K}$ du calcul d'un vecteur contenant les termes u_d, u_{d+1}, …, u_N ?
3. ($\star$) Dans cette question on s'intéresse à un exemple particulier : la suite (u_n) d'entiers relatifs définie par la relation de récurrence (1) avec $d = 3$, $a_0 = 2$, $a_1 = 3$, $a_2 = -5$, $u_0 = 0$, $u_1 = 2$, $u_2 = 3$. Ecrire un programme qui prend en entrée un entier N, et renvoie un vecteur contenant, pour i allant de 0 à N, le reste dans la division euclidienne de u_i par 13. Combien y a-t-il d'entiers i compris (au sens large) entre 0 et 100 pour lesquels u_i est divisible par 13 ?

Partie 2 : Approche matricielle

Dans toute la suite du problème on considère la matrice suivante :

$$M = \begin{bmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{d-1} \end{bmatrix}$$

et on identifie tout n-uplet $(x_1, \dots, x_d)$ de réels à la matrice *ligne* $[x_1\, x_2\, \dots\, x_d]$.

4. Démontrer que pour tous $n \geq i \geq 0$ on a

$$(u_n, u_{n+1}, \dots, u_{n+d-1}) = (u_i, u_{i+1}, \dots, u_{i+d-1})M^{n-i}. \tag{2}$$

5. Notons $V_n \in M_{n,1}(\mathbb{K})$ la première colonne de la matrice M^n. Déduire de la question précédente qu'on a, pour tous $n \geq i \geq 0$:

$$u_n = (u_i, u_{i+1}, \dots, u_{i+d-1})V_{n-i}.$$

6. En utilisant la question 5 avec $i = 0$, proposer un algorithme pour calculer u_N. Quel est son coût en opérations arithmétiques dans $\mathbb{K}$? *Comme annoncé dans le préambule, on demande la dépendance de ce coût par rapport aux deux paramètres d et N.*
7. ($\star$) Dans cette question on considère à nouveau l'exemple de la question 3. En utilisant l'algorithme de la question précédente, écrire un programme qui prend en entrée un entier N, et renvoie le reste dans la division euclidienne de u_N par 13. *On pourra utiliser librement la fonction de Sage qui permet de calculer des puissances.* Combien vaut ce reste quand $N = 200$?

Partie 3 : Approche modulaire

Notons $P = X^d - a_{d-1}X^{d-1} - \ldots - a_1 X - a_0 \in \mathbb{K}[X]$. Pour tout $n \geq 0$, on note

$$V_n = \begin{bmatrix} v_0^{(n)} \\ v_1^{(n)} \\ \vdots \\ v_{d-1}^{(n)} \end{bmatrix}$$

la première colonne de la matrice M^n, déjà considérée à la question 5. On va travailler dans le quotient $\mathbb{K}[X]/(P)$; on note x la classe de X dans ce quotient.

8. Démontrer que pour tout $n \geq 0$ on a :
$$x^n = v_0^{(n)} + v_1^{(n)} x + \ldots + v_{d-1}^{(n)} x^{d-1}.$$
9. Rappeler brièvement comment on peut calculer le produit de deux éléments de $\mathbb{K}[X]/(P)$ (représentés par le vecteur de leurs coordonnées dans la base $(1, x, \ldots, x^{d-1})$), et quel est le coût de ce calcul en opérations arithmétiques dans $\mathbb{K}$.
10. Déduire des questions précédentes une variante plus efficace de l'algorithme de la question 6. Quel est son coût en opérations arithmétiques dans $\mathbb{K}$?
11. ($\star$) Reprendre la question 7 en implémentant l'algorithme de la question 10.

Partie 4 : Calcul efficace des premiers termes

On revient maintenant à l'objectif de la partie 1 : calculer tous les termes u_i avec $i \leq N$. On va utiliser les résultats des parties 2 et 3, dont on conserve les notations. Pour tout $n \geq 0$ on pose

$$Q_n(X) = \left(u_{2d-2} + u_{2d-3}X + \ldots + u_0 X^{2d-2}\right)\left(v_0^{(n)} + v_1^{(n)} X + \ldots + v_{d-1}^{(n)} X^{d-1}\right) \in \mathbb{K}[X]$$

et on note $q_0^{(n)}$, …, $q_{3d-3}^{(n)}$ les coefficients de Q_n, de telle sorte que $Q_n(X) = \sum_{i=0}^{3d-3} q_i^{(n)} X^i$.

12. Démontrer que pour tout $n \geq 0$ et tout $i \in \{0, \ldots, d-1\}$ on a
$$u_{n+i} = q_{2d-2-i}^{(n)}.$$
13. Dans cette question seulement, on suppose qu'on sait effectuer chacun des calculs suivants en $O(d \log d)$ opérations arithmétiques dans $\mathbb{K}$:
    - Calculer u_d, u_{d+1}, …, u_{2d-2}.
    - Multiplier deux polynômes de degré $\leq 2d$ à coefficients dans $\mathbb{K}$.
    - Multiplier deux éléments de $\mathbb{K}[X]/(P)$.

    Sous ces hypothèses, déterminer un algorithme permettant de calculer u_d, u_{d+1}, …, u_N en $O(N \log d)$ opérations arithmétiques dans $\mathbb{K}$.
14. Comparer le coût de l'algorithme de la question 13 à celui de la question 2. Peut-on encore espérer améliorer notablement l'algorithme de la question 13 ?

15. ($\star$) Reprendre à nouveau la question 7, cette fois en implémentant l'algorithme de la question 13.

Partie 5 : Application à l'évaluation d'un polynôme sur une suite arithmétique

16. Soit $P \in \mathbb{K}[X]$, $\alpha, \beta \in \mathbb{K}$, avec $\alpha \neq 0$. Pour tout $n \geq 0$ on pose $u_n = P(\alpha n + \beta)$. Démontrer que la suite (u_n) satisfait une relation de récurrence de la forme (1), avec $d = \deg P + 1$. Expliciter les coefficients $a_0, \ldots, a_{d-1}$; dépendent-ils de P ?