

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

Lundi 15 avril 2019
Master 1 M.F., 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.

Cet examen 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.

Les modalités d'utilisation de Sage sont les suivantes. Il est inutile de recopier sur votre copie les lignes de code Sage que vous avez utilisées. En revanche vous *devez* inscrire sur votre copie le résultat du calcul, et toutes les explications utiles (notamment toute justification mathématique de la façon dont vous avez fait votre programme). Vous devez aussi, le cas échéant, faire le lien dans votre copie entre le résultat brut donné par Sage et l'interprétation mathématique qui vous est demandée.
Vous disposez d'une feuille de calcul Sage nommée `copie-partiel-NOM-PRENOM.ipynb`. Vous devez remplacer NOM et PRENOM par les vôtres, aussi bien dans le nom de ce fichier qu'en tête du fichier lui-même. Cette feuille de calcul sera corrigée en même temps que votre copie ; il est donc conseillé de commenter raisonnablement vos programmes, et de veiller à leur lisibilité. Vous pouvez créer des feuilles de calcul auxiliaires, *qui ne seront pas corrigées* et peuvent vous servir de brouillon électronique. En tout état de cause veuillez suivre attentivement les consignes qui vous seront données pendant l'épreuve, et en cas de doute n'hésitez pas à poser des questions.

Dans tout le problème, on note $\mathbb{K}$ un corps sur lequel les opérations arithmétiques (addition, soustraction, multiplication, division) sont implémentées. On note n un entier strictement positif (dont on imagine qu'il est susceptible d'être très grand), et on fixe n éléments x_1, $\ldots$, x_n *deux à deux distincts* de $\mathbb{K}$. On considère les deux problèmes suivants :

Evaluation : Etant donné $P \in \mathbb{K}[X]$ de degré $< n$, calculer $P(x_1)$, $\ldots$, $P(x_n)$.

Interpolation : Etant donnés $y_1, \ldots, y_n \in \mathbb{K}$, déterminer un polynôme $P \in \mathbb{K}[X]$ de degré $< n$ tel que $P(x_k) = y_k$ pour tout $k \in \{1, \ldots, n\}$.

On rappelle que le problème d'interpolation possède une solution unique (puisque x_1, $\ldots$, x_n sont deux à deux distincts) : étant donnés $y_1, \ldots, y_n \in \mathbb{K}$ il existe un unique polynôme $P \in \mathbb{K}[X]$ de degré $< n$ tel que $P(x_k) = y_k$ pour tout $k \in \{1, \ldots, n\}$.

Le but de ce problème est d'étudier quelques algorithmes qui résolvent l'un ou l'autre de ces problèmes. Lorsqu'on évoquera le coût d'un algorithme, il s'agira toujours de son coût en nombre d'opérations arithmétiques dans $\mathbb{K}$. Dans les questions utilisant Sage, on n'utilisera pas (sauf éventuellement pour vérifier les résultats) la fonction `lagrange_polynomial` qui résout le problème de l'interpolation.

Les parties sont indépendantes les unes des autres, sauf mention explicite du contraire. Au sein de chaque partie, il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes.

Partie 1 : Algèbre linéaire

Dans cette partie on considère les vecteurs colonnes

$$Y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad \text{et} \quad A = \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

qui appartiennent à $M_{n,1}(\mathbb{K})$, où les a_i sont les coefficients de P : on note $P(X) = a_{n-1}X^{n-1}+\ldots+a_1X+a_0$. On introduit aussi la matrice de Vandermonde $M = [x_i^{j-1}]_{1\leq i,j\leq n} \in M_n(\mathbb{K})$. On rappelle que son déterminant est donné par la formule $\det M = \prod_{1\leq i<j\leq n}(x_j - x_i)$.

1. Quel est le coût du calcul de M à partir de $x_1, \ldots, x_n$?
2. Traduire à l'aide de M, A et Y la propriété suivante :

$$P(x_k) = y_k \text{ pour tout } k \in \{1, \ldots, n\}.$$

3. En déduire un algorithme qui résout le problème de l'évaluation. Quel est son coût ?
4. Reprendre la question précédente avec le problème de l'interpolation.
5. ($\star$) Dans cette question seulement on pose $\mathbb{K} = \mathbb{Q}$, $n = 2$, $x_i = i$ et $y_i = 3^i$ pour tout $i \in \{1, \ldots, n\}$. Calculer la matrice M puis, en suivant l'algorithme de la question 4, déterminer le polynôme P solution du problème d'interpolation. Recopier sur la copie le coefficient de X dans P. *On rappelle que l'utilisation de la commande* `lagrange_polynomial` *est interdite, sauf éventuellement pour vérifier les résultats.*
6. ($\star$) Reprendre la question précédente avec $n = 10$ au lieu de $n = 2$.
7. Dans cette question seulement, on note ω une racine primitive n-ième de l'unité dans $\mathbb{K}$, c'est-à-dire un élément d'ordre n dans le groupe multiplicatif $\mathbb{K}^*$. On suppose aussi que $x_i = \omega^{i-1}$ pour tout $i \in \{1, \ldots, n\}$ et on note $M_\omega = [\omega^{(i-1)(j-1)}]_{1\leq i,j\leq n}$ la matrice de Vandermonde associée.
   (a) Si $\mathbb{K}$ est un corps fini $\mathbb{F}_q$, donner une condition nécessaire et suffisante portant sur q et n pour qu'un tel ω existe dans $\mathbb{F}_q$.
   (b) Montrer que $M_\omega M_{\omega^{-1}} = nI_n$, avec $M_{\omega^{-1}} = [\omega^{-(i-1)(j-1)}]_{1\leq i,j\leq n}$.

(c) En déduire, si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, que M_ω est inversible et déterminer son inverse.

(d) Si $\mathbb{K}$ n'est pas un sous-corps de $\mathbb{C}$, quelle hypothèse peut-on faire sur $\mathbb{K}$ pour obtenir quand même le résultat de la question précédente ?

(e) Expliquer pourquoi, si on est sous les hypothèses de la question (c) ou de la question (d) et si on sait résoudre le problème de l'évaluation avec un certain coût lorsque $x_i = \omega^{i-1}$, alors on peut résoudre le problème de l'interpolation avec le même coût pour ces mêmes points.

Partie 2 : Interpolation de Lagrange

Dans cette partie on étudie un algorithme pour résoudre le problème de l'interpolation. On pose pour $k \in \{1, \dots, n\}$:

$$L_k(X) = \prod_{\substack{1 \le \ell \le n \\ \ell \neq k}} \Big(X - x_\ell\Big).$$

On rappelle qu'étant donnés $y_1, \dots, y_n \in \mathbb{K}$, l'unique solution P du problème d'interpolation est alors donnée par :

$$P(X) = \sum_{k=1}^{n} \frac{y_k}{L_k(x_k)} L_k(X). \tag{1}$$

On considère aussi le polynôme

$$L(X) = \prod_{\ell=1}^{n} \Big(X - x_\ell\Big).$$

8. ($\star$) Dans cette question seulement on note $p = 641$ (qui est un nombre premier), et $\mathbb{K} = \mathbb{F}_p$. Pour tout $k \in \mathbb{Z}$ on note $\overline{k}$ la classe de k modulo p, qui appartient à $\mathbb{F}_p$. On choisit $n = 100$ et pour $i \in \{1, \dots, n\}$ on pose $x_i = \overline{i}$ et $y_i = \overline{3^i}$. En utilisant la formule (1) calculer le polynôme interpolateur P, et recopier sur la copie le coefficient de X^2 dans P. *Les questions qui suivent consistent à déterminer une méthode efficace pour mener à bien ce calcul ; ici une méthode naïve sera acceptée.*
9. En supposant $L(X)$ connu, comment peut-on (pour $k \in \{1, \dots, n\}$ donné) calculer $L_k(X)$? Quel est le coût de ce calcul ?
10. Quel est le coût du calcul du produit de deux polynômes, l'un étant de degré 1 et l'autre de degré j ?
11. Déterminer un algorithme, fondé sur la formule (1), qui résout le problème de l'interpolation en $O(n^2)$ opérations arithmétiques dans $\mathbb{K}$.

Partie 3 : Evaluation sur une suite géométrique

Dans cette partie on fixe un élément $\zeta \in \mathbb{K}^*$ et on pose $x_i = \zeta^{i-1}$ pour tout $i \in \{1, \ldots, n\}$. On suppose toujours que $x_1, \ldots, x_n$ sont deux à deux distincts. On cherche à évaluer un polynôme $P(X) = a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ aux points x_i. Pour cela on note

$$\lambda_i = \zeta^{i(i-1)/2} \text{ pour tout } i \in \mathbb{N}, \text{ et } b_i = \frac{a_i}{\lambda_i} \text{ pour tout } i \in \{0, \ldots, n-1\}.$$

12. Vérifier qu'on a
$$\zeta^{ij} = \frac{\lambda_{i+j}}{\lambda_i \lambda_j} \text{ pour tous } i, j \in \mathbb{N}.$$

13. En déduire que
$$P(x_i) = \frac{1}{\lambda_{i-1}} \sum_{j=0}^{n-1} \lambda_{i-1+j}\, b_j \text{ pour tout } i \in \{1, \ldots, n\}.$$

14. Rappeler pour quel nombre réel α l'algorithme de Karatsuba permet de calculer le produit de deux polynômes de degré $\leq t$ à coefficients dans $\mathbb{K}$ en $O(t^\alpha)$ opérations arithmétiques dans $\mathbb{K}$.
15. A l'aide de la question 13, proposer un algorithme qui résout le problème de l'évaluation aux points x_i en $O(n^\alpha)$ opérations arithmétiques dans $\mathbb{K}$, où α est défini à la question 14.

Partie 4 : Application à la multiplication de matrices à coefficients polynomiaux

Soient $R, S \in M_n(\mathbb{K}[X])$ deux matrices $n \times n$ à coefficients dans $\mathbb{K}[X]$. Le but de cette partie est de donner un algorithme fondé sur l'évaluation et l'interpolation pour calculer le produit RS. On suppose connu un entier $d \geq 2$ tel que les coefficients de R et S soient de degré $< d$. On prendra garde au fait que n et d peuvent tous les deux être grands : les complexités des algorithmes étudiés dans cette partie seront des fonctions de ces deux variables.

On note $\alpha \geq 1$ le nombre réel tel que l'algorithme de Karatsuba permet de calculer le produit de deux polynômes de degré $\leq t$ à coefficients dans $\mathbb{K}$ en $O(t^\alpha)$ opérations arithmétiques dans $\mathbb{K}$. *On rappelle que la question 14 ci-dessus demandait d'expliciter la valeur de α, mais ce n'est pas nécessaire pour la suite.*

16. Déterminer le coût du calcul de RS si on effectue naïvement le produit matriciel et qu'on calcule par l'algorithme de Karatsuba tous les produits de polynômes qui apparaissent.

On suppose maintenant qu'on dispose dans $\mathbb{K}$ de $2d$ éléments $x_1, \ldots, x_{2d}$ deux à deux distincts pour lesquels on sait résoudre le problème de l'interpolation et celui de l'évaluation avec un coût en $O(d^\alpha)$, les polynômes P mis en jeu dans ces deux problèmes étant de degré $< 2d$. *Concernant l'évaluation, la question 15 fournit en effet de tels points.*

17. Proposer un algorithme qui calcule le produit RS en $O(dn^3 + d^\alpha n^2)$ opérations arithmétiques dans $\mathbb{K}$.

Remarque : mis en œuvre plus efficacement, les algorithmes de type évaluation-interpolation permettent souvent de réaliser des gains de complexité beaucoup plus spectaculaires.

Partie 5 : Compléments

Les questions de cette partie sont plus ouvertes ; pour chacune la réponse attendue tient en quelques lignes, il n'est pas utile de faire de longs développements très détaillés.

18. Soit A un anneau (commutatif et unitaire). On souhaite généraliser les résultats de la partie 1 en remplaçant partout $\mathbb{K}$ par A. Pour y parvenir, quelle hypothèse peut-on faire sur les éléments $x_1, \ldots, x_n$ de A ?
19. Soit $\mathbb{K} = \mathbb{F}_q$ un corps fini. Supposons qu'on sache résoudre efficacement le problème de l'évaluation, en tous les points de $\mathbb{K}$, de tout polynôme $P \in \mathbb{K}[X]$ de degré $< q$ (c'est-à-dire lorsque $n = q$ et $\{x_i, 1 \leq i \leq n\} = \mathbb{F}_q$). Comment peut-on alors évaluer efficacement en tous les points de $\mathbb{K}$ un polynôme $Q \in \mathbb{K}[X]$ de degré d beaucoup plus grand que q ?
20. Les algorithmes de type évaluation-interpolation comme celui présenté dans la partie 4 permettent de manipuler efficacement des polynômes, en remplaçant les opérations dans $\mathbb{K}[X]$ par des opérations dans $\mathbb{K}$. Quel est l'analogue permettant de manipuler efficacement de grands entiers ?