60.24M

SESSION 2006

Filière MP (groupe I)

Épreuve commune aux ENS de Paris, Lyon et Cachan

Filière PC (groupe I)

Épreuve commune aux ENS de Paris et Lyon

MATHÉMATIQUES - INFORMATIQUE

Durée : 4 heures

L'usage de calculatrices électroniques de poche à alimentation autonome, non imprimantes et sans document d'accompagnement, est autorisé. Cependant, une seule calculatrice à la fois est admise sur la table ou le poste de travail, et aucun échange n'est autorisé entre les candidats.

Préambule

La simplification automatique d'intégrales est une fonctionnalité appréciée des utilisateurs de logiciels de calcul formel. Par exemple, pour intégrer les fractions rationnelles, les "recettes" bien connues (décomposition en éléments simples, changement de variable trigonométrique) se transforment aisément en des algorithmes qui sont implantés dans tous les logiciels du marché. La plupart des logiciels vont bien plus loin et même si l'on ne peut pas espérer disposer d'un algorithme qui simplifie toutes les intégrales, de nombreuses familles d'intégrales peuvent actuellement être traitées.

Dans ce problème on s'intéresse à la famille des intégrales dites hyperelliptiques, c'est-à-dire celles qui sont de la forme $\int_{x_0}^{x} \frac{h(u)\mathrm{d}u}{\sqrt{D(u)}}$, où h et D sont des polynômes. Certaines de ces intégrales peuvent se réécrire sous la forme $\log(a(x)+b(x)\sqrt{D(x)})$, où $a(x)$ et $b(x)$ sont des polynômes. Dans ce cas, on parle d'intégrale pseudo-hyperelliptique.

Le but du problème est de comprendre une version simplifiée d'un algorithme qui permet de calculer $a(x)$ et $b(x)$ lorsqu'une telle forme existe. L'algorithme repose sur l'utilisation de fractions continues de polynômes. L'étude des propriétés mathématiques et algorithmiques de celles-ci constitue une part importante du problème.

Les parties 1 et 2 sont complètement indépendantes. La partie 4 s'appuie sur la partie 3 qui utilise les notions introduites dans les deux premières parties.

1 Séries de Laurent formelles

Soit K un corps commutatif que l'on suppose de caractéristique différente de 2.

Une **série de Laurent formelle** sur K est une suite d'éléments $(a_i)_{i\in\mathbb{Z}}$ de K indexée par $\mathbb{Z}$, telle qu'il existe un entier n (positif ou négatif) vérifiant : si $i < n$, alors $a_i = 0$. Si la suite n'est pas identiquement nulle, quitte à changer n, on peut supposer que a_n est non nul, ce qu'on fera toujours par la suite. L'entier n est alors appelé la **valuation** de la série formelle. Par convention, la série nulle a pour valuation $+\infty$.

Une telle série de Laurent formelle est notée $\sum_{i\geq n} a_i z^i$, où z est une indéterminée. On insiste sur le fait que ceci n'est qu'une notation : même si les a_i sont des réels ou des complexes, on ignore totalement les questions de rayon de convergence. Si $a(z)$ est une série de Laurent formelle, on note $\mathrm{val}(a(z))$ sa valuation.

Soient $a(z) = \sum_{i\geq n_a} a_i z^i$ et $b(z) = \sum_{i\geq n_b} b_i z^i$ deux séries de Laurent formelles. On définit pour tout i dans $\mathbb{Z}$, $d_i = a_i + b_i$ et $c_i = \sum_{j+k=i} a_j b_k$.

Question 1.1

1. Montrer que $(d_i)_{i\in\mathbb{Z}}$ est une série de Laurent formelle et que $\mathrm{val}(d(z)) \geq \min\big(\mathrm{val}(a(z)), \mathrm{val}(b(z))\big)$, avec égalité si $\mathrm{val}(a(z)) \neq \mathrm{val}(b(z))$. On dit alors que $d(z)$ est la **somme** de $a(z)$ et $b(z)$ et on note $d(z) = a(z) + b(z)$.
2. Montrer que, pour tout i, c_i est en fait défini par une somme finie. Quel est le nombre maximal de termes non nuls dans cette somme ? Montrer que $(c_i)_{i\in\mathbb{Z}}$ est une série de Laurent formelle et que $\mathrm{val}(c(z)) = \mathrm{val}(a(z)) + \mathrm{val}(b(z))$. On dit alors que $c(z) = \sum c_i z^i$ est le **produit** de $a(z)$ et $b(z)$ et on note $c(z) = a(z)b(z)$.
3. Montrer que toute série de Laurent formelle non identiquement nulle est produit d'une série de la forme z^d et d'une série de valuation nulle.

Question 1.2 Montrer que les séries de Laurent formelles munies de cette addition et ce produit forment un anneau commutatif (ayant un élément unité). On notera 0 le neutre pour l'addition, 1 le neutre pour la multiplication, et par extension on notera n l'élément $1 + \cdots + 1$ répété n fois.

Question 1.3 Montrer qu'une série de Laurent formelle $a(z)$ non nulle est inversible et que $\mathrm{val}(a(z)^{-1}) = -\mathrm{val}(a(z))$. L'ensemble des séries de Laurent formelles est donc un corps. On notera classiquement $1/a(z)$ l'inverse de $a(z)$.

Question 1.4 Écrire dans un pseudo-langage de haut niveau une fonction qui prend en entrée les k premiers coefficients a_0, a_1, …, a_{k-1} d'une série formelle $a(z) = \sum_{i\geq 0} a_i z^i$, de valuation nulle, et retourne les k premiers coefficients de l'inverse de $a(z)$. On supposera que les opérations élémentaires (additions, soustractions, multiplications, inverses) dans le corps K font partie intégrante du langage.

Soit $a(z)$ une série de Laurent formelle non nulle, de valuation paire, et dont le premier terme non nul vaut 1. Ainsi $a(z)$ s'écrit $a(z) = z^{2k}(1 + \alpha_1 z + \alpha_2 z^2 + \cdots)$, où k est dans $\mathbb{Z}$. On définit les suites $(B_j)_{j\geq 0}$ et $(E_j)_{j\geq 0}$ de séries de Laurent formelles par $B_0(z) = 1$, puis

$$\left\{\begin{array}{rcl} E_j(z) & = & B_j(z)^2 - a(z)/z^{2k} \\ B_{j+1}(z) & = & B_j(z) - \frac{E_j(z)}{2B_j(z)}, \end{array}\right. \qquad \text{pour } j \geq 0.$$

(La division par 2 est possible car K est de caractéristique différente de 2.)

Question 1.5 Montrer que, pour tout $j \geq 0$, $B_j(z)$ et $E_j(z)$ sont bien définies, que la valuation de $B_j(z)$ est 0 et que celle de $E_j(z)$ vaut au moins 2^j.

Question 1.6 Montrer que, pour tout entier n, il existe un indice j à partir duquel tous les B_j ont les mêmes n premiers termes. En déduire qu'il existe une série de Laurent formelle $b(z)$ telle que $a(z) = b(z)^2$. On note alors $b(z) = \sqrt{a}(z)$ une telle série dont le premier terme non nul vaut 1.

Dans la situation où une suite de séries de Laurent formelles $(f_j(z))_{j\geq 0}$ est telle que $\mathrm{val}(f_j(z))$ tend vers l'infini, on dira que la suite $(f_j(z))_{j\geq 0}$ tend vers 0. Plus généralement, s'il existe une série de Laurent formelle $g(z)$ telle que $\mathrm{val}(f_j(z) - g(z))$ tend vers l'infini, on dira que la suite $(f_j(z))_{j\geq 0}$ tend vers $g(z)$. On a ainsi montré dans les questions précédentes que la suite $(E_j(z))_{j\geq 0}$ tend vers 0 et que la suite $(B_j(z))_{j\geq 0}$ tend vers $\sqrt{a}(z)/z^k$.

2 Fractions continues

Une **fraction continue** sur un corps commutatif L est une suite d'éléments $a = (a_i)_{i\geq 0}$ tels que $a_i \neq 0$ si $i > 0$. La fraction continue a étant donnée, on s'intéresse à l'expression

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

Plus précisément, on note $[a_0, \ldots, a_k]$ la valeur de l'expression

$$a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_k}}},$$

que l'on appelle **convergent** d'ordre k, ou k-ème convergent de a. De manière plus formelle, pour $k = 0$ on a $[a_0] = a_0$, puis on définit un convergent d'ordre $k+1$ à partir d'un convergent d'ordre k par

$$[a_0, \ldots, a_{k-1}, a_k, a_{k+1}] = [a_0, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}].$$

Question 2.1 Montrer que pour toute fraction continue $(a_i)_{i\geq 0}$, pour tout $k > 0$, le k-ème convergent peut s'écrire $\frac{p_k}{q_k}$ où les suites p_k et q_k sont définies par $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$ et pour tout $k \geq 2$,

$$\begin{cases} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2}. \end{cases}$$

Question 2.2 Écrire un programme (dans un pseudo-langage de haut niveau) qui, étant donnés les $k+1$ premiers termes d'une fraction continue $(a_i)_{i\geq 0}$, calcule la valeur de son k-ème convergent en effectuant une unique inversion. On supposera que les opérations élémentaires dans le corps L font partie intégrante du langage. Évaluer le nombre d'additions et de multiplications dans L effectuées lors d'une exécution du programme.

Question 2.3 Soit $(a_i)_{i\geq 0}$ une fraction continue et soit C_k son k-ème convergent. Montrer que pour tout $k > 0$, $C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$, où la suite $(q_i)_{i\geq 0}$ est définie comme à la question 2.1.

Question 2.4 Dans cette question (et uniquement dans cette question), on suppose que le corps L est le corps des rationnels $\mathbb{Q}$. On suppose de plus que les a_i sont des entiers strictement positifs. Montrer que la suite des convergents tend vers une limite réelle.

3 Fractions continues de polynômes

Dorénavant, on prend comme corps $L = K(x)$ le corps des fractions rationnelles à coefficients dans le corps K.

On s'intéresse aux fractions continues sur $K(x)$ d'une forme particulière : on considère uniquement les fractions continues $(a_i(x))_{i\geq 0}$ telles que pour tout i, le terme $a_i(x)$ est un polynôme et de plus, si $i > 0$, alors ce polynôme est de degré au moins 1. Une telle fraction continue est appelée **fraction continue de polynômes** sur K. Ses convergents sont donc des fractions rationnelles à coefficients dans K.

Dans la suite, afin d'alléger les notations, il nous arrivera de noter simplement f un polynôme $f(x)$ appartenant à $K[x]$. De même, on notera couramment F une série de Laurent formelle $F(z)$.

À tout polynôme $U(x)$ appartenant à $K[x]$, on peut associer une série de Laurent formelle notée $\varphi(U)$, définie de la manière suivante : si $U(x) = u_0 + u_1 x + \cdots + u_d x^d$, alors

$$\varphi(U)(z) = U(1/z) = u_d z^{-d} + u_{d-1} z^{-d+1} + \cdots + u_1 z^{-1} + u_0.$$

L'opérateur φ est clairement un morphisme injectif d'anneau, et on peut donc l'étendre en un morphisme injectif du corps des fractions rationnelles dans le corps des séries de Laurent formelles comme suit : si U et V sont deux polynômes avec $V \neq 0$, alors $\varphi(\frac{U}{V}) = \varphi(U)/\varphi(V)$. Insistons sur le fait que ce dernier quotient est à comprendre comme le produit de la série de Laurent formelle $\varphi(U)$ avec l'inverse de la série de Laurent formelle $\varphi(V)$ (cela n'a rien à voir avec une fraction rationnelle).

On définit aussi un opérateur ψ qui à toute série de Laurent formelle $f(z)$ associe un polynôme : si f est de valuation strictement positive, alors $\psi(f) = 0$, et si f est de valuation d négative ou nulle, avec $f(z) = \sum_{i\geq d} f_i z^i$, alors $\psi(f)(x) = f_0 + f_{-1}x + \cdots + f_d x^{-d}$. Ainsi pour tout polynôme U à coefficients dans K, on a $\psi(\varphi(U)) = U$.

Question 3.1 Propriétés élémentaires de φ et ψ.

1. Si U est un polynôme de degré d, quelle est la valuation de $\varphi(1/U)$?
2. Si $a(z)$ et $b(z)$ sont des séries de Laurent formelles, vérifier que $\psi(a(z) + b(z)) = \psi(a(z)) + \psi(b(z))$. Donner un exemple de séries de Laurent formelles $a(z)$ et $b(z)$ telles que $\psi(a(z)b(z)) \neq \psi(a(z))\psi(b(z))$. Ainsi ψ est un morphisme additif mais pas multiplicatif des séries de Laurent formelles vers les polynômes.
3. À quelle condition une série de Laurent formelle $f(z)$ vérifie-t-elle $f(z) = \varphi(\psi(f(z)))$?

Question 3.2 Soit $(a_i)_{i\geq 0}$ une fraction continue de polynômes. Montrer qu'il existe une série de Laurent formelle $F(z)$ telle que les images par φ des convergents de $(a_i)_{i\geq 0}$ tendent vers $F(z)$ au sens défini à la fin de la partie 1 : si C_k est le k-ème convergent, alors la valuation de $F - \varphi(C_k)$ tend vers l'infini lorsque k tend vers l'infini. On pourra s'aider de la question 2.3.

Réciproquement, à toute série de Laurent formelle F qui n'est pas l'image par φ d'une fraction rationnelle, on souhaite associer une fraction continue dont les images par φ des convergents tendent vers F. Pour cela, on introduit les suites suivantes : on pose $\alpha_0 = F$, puis pour tout $k \geq 0$,

$$a_k = \psi(\alpha_k), \quad \text{et} \quad \alpha_{k+1} = \frac{1}{\alpha_k - \varphi(a_k)}.$$

Question 3.3 Montrer que la suite $(a_i)_{i\geq 0}$ est bien définie et que pour tout $i \geq 1$, le degré de a_i est au moins 1. La suite $(a_i)_{i\geq 0}$ est donc une fraction continue de polynômes. Montrer que les images par φ de ses convergents tendent vers F. Pour cela, on pourra démontrer que, pour tout $k \geq 1$, on a

$$F = \frac{\alpha_{k+1}\varphi(p_k) + \varphi(p_{k-1})}{\alpha_{k+1}\varphi(q_k) + \varphi(q_{k-1})},$$

où les suites $(p_k)_{k\geq 0}$ et $(q_k)_{k\geq 0}$ sont définies à partir de la suite $(a_i)_{i\geq 0}$ comme dans la question 2.1.

Question 3.4 Lemme de meilleure approximation.

Soit $F(z)$ une série de Laurent formelle qui n'est pas l'image par φ d'une fraction rationnelle. On considère sa fraction continue associée et $(p_k)_{k\geq 0}$ et $(q_k)_{k\geq 0}$ les suites définies à partir de cette fraction continue comme dans la question 2.1.

1. Montrer que, pour tout $k \geq 1$, on a

$$\mathrm{val}(\varphi(p_k) - F\varphi(q_k)) = \deg q_{k+1} > \deg q_k.$$

2. Soient p et q deux polynômes et $k \geq 1$ un entier. Montrer qu'il existe deux polynômes a et b tels que

$$\begin{cases} q &= aq_{k-1} + bq_k \\ p &= ap_{k-1} + bp_k. \end{cases}$$

3. On suppose que p et q sont premiers entre eux, que $\deg q_{k-1} \leq \deg q < \deg q_k$, et que q n'est pas proportionnel à q_{k-1} (c'est-à-dire qu'il n'existe pas de $\lambda \in K$ tel que $q = \lambda q_{k-1}$). Montrer que a et b sont non nuls puis que $\mathrm{val}(\varphi(p) - F\varphi(q)) = \deg q_k - \deg a$.
4. En déduire le lemme de meilleure approximation : si p et q sont deux polynômes premiers entre eux tels que $\mathrm{val}(\varphi(p) - F\varphi(q)) > \deg q$, alors p/q est un convergent de la fraction continue associée à F.

Soit $D(x)$ un polynôme unitaire, de degré pair ≥ 2, qui n'est pas le carré d'un polynôme. Alors son image par φ est une série de Laurent formelle de valuation paire dont le premier terme non nul vaut 1, et d'après la question 1.6, il existe une série formelle dont le carré est $\varphi(D(x))$. Par abus de notation, on omet le φ, et l'on note simplement $\sqrt{D}$ cette série formelle. On vérifie alors sans difficultés que $\sqrt{D}$ n'est pas l'image par φ d'une fraction rationnelle.

Question 3.5 Écrire une fonction qui prend en entrée un polynôme $D(x)$ comme ci-dessus et qui retourne le polynôme $\psi(\sqrt{D})$. On pourra s'inspirer des suites $B_j(z)$ et $E_j(z)$ introduites en fin de partie 1. On suppose donnée une bibliothèque pour les opérations élémentaires sur les polynômes de $K[x]$ (mais pas sur les séries formelles qui sont des objets potentiellement de taille infinie). Quel est le degré maximal des polynômes manipulés ?

Afin d'étudier la fraction continue associée à $\sqrt{D}$, on introduit les suites P_k, Q_k, a'_k définies de la manière suivante. Soient $P_0 = 0$, $Q_0 = 1$, $a'_0 = \psi(\sqrt{D})$, puis pour tout $k \geq 0$, a'_k est le quotient dans la division euclidienne de $P_k + \psi(\sqrt{D})$ par Q_k, et

$$\begin{aligned} P_{k+1} &= a'_k Q_k - P_k \\ Q_{k+1} &= \frac{D - P_{k+1}^2}{Q_k}. \end{aligned}$$

Question 3.6 Le but de cette question est de démontrer que la suite $(a'_k)_{k\geq 0}$ donne la fraction continue $(a_k)_{k\geq 0}$ de polynômes associée à $\sqrt{D}$.

1. Montrer que P_k et Q_k sont des polynômes et que $Q_k \neq 0$ pour tout $k \geq 0$.
2. Soit $F(z)$ une série de Laurent formelle et Q un polynôme non nul. Montrer que $\psi(\frac{F}{\varphi(Q)})$ est égal au quotient dans la division euclidienne de $\psi(F)$ par Q. Pour cela, on pourra commencer par écrire F comme la somme de $\varphi(\psi(F))$ et d'une série de valuation strictement positive. En déduire que
$$a'_k = \psi\left(\frac{\varphi(P_k) + \sqrt{D}}{\varphi(Q_k)}\right).$$
3. Soit $(\alpha_k)_{k\geq 0}$ la suite correspondant à la fraction continue associée à $\sqrt{D}$, définie comme avant la question 3.3. Pour tout $k \geq 0$, montrer que $\alpha_k = \frac{\varphi(P_k)+\sqrt{D}}{\varphi(Q_k)}$ et $a_k = a'_k$, par récurrence sur k.

4 Application aux intégrales pseudo-hyperelliptiques

Dans cette partie, le corps de base K est le corps des réels. On considère les intégrales de la forme
$$\int_{x_0}^{x} \frac{h(u)du}{\sqrt{D(u)}},$$
où h est un polynôme non nul et D un polynôme unitaire de degré pair, qui n'est pas un carré. On suppose (ici et partout dans cette section) que D est strictement positif sur l'intervalle fermé d'intégration, si bien que la fonction à intégrer est continue, et même C^∞.

Si le degré de D est 2, un changement de variables permet toujours de se ramener à l'intégration d'une fraction rationnelle, si bien que l'intégrale est facilement exprimable à l'aide des fonctions usuelles.

Si le degré de D est au moins 4, ce que l'on supposera désormais, il n'y a en général pas moyen d'exprimer une telle intégrale à l'aide des fonctions usuelles. Cependant, il existe des cas particuliers. Lorsque cette intégrale est égale à une expression de la forme $\log(a(x) + b(x)\sqrt{D(x)})$ où a et b sont des polynômes, on dit qu'on a affaire à une **intégrale pseudo-hyperelliptique** (ou intégrale pseudo-elliptique, si $\deg D = 4$).

La formule suivante
$$\int_{x_0}^{x} \frac{6udu}{\sqrt{u^4+4u^3-6u^2+4u+1}} = \log\Big(x^6+12x^5+45x^4+44x^3-33x^2+43+$$
$$(x^4+10x^3+30x^2+22x-11)\sqrt{x^4+4x^3-6x^2+4x+1}\Big) + C_0(x_0),$$

montre que de telles intégrales existent (il n'est pas demandé de refaire les calculs pour vérifier cette égalité).

Le but de cette partie est de montrer que, s'ils existent, les polynômes a et b peuvent être calculés à l'aide de la fraction continue de la série de Laurent formelle $\sqrt{D}$ (qui n'a a priori rien à voir avec la fonction $\sqrt{D(x)}$ qui intervient dans l'intégrale).

Question 4.1 Montrer que si l'on a une intégrale pseudo-hyperelliptique

$$\int_{x_0}^{x} \frac{h(u)du}{\sqrt{D(u)}} = \log\left(a(x) + b(x)\sqrt{D(x)}\right),$$

alors il existe une constante non nulle μ telle que $a(x)^2 - D(x)b(x)^2 = \mu$. (On pourra utiliser le fait que la fonction $\sqrt{D(x)}$ n'est pas égale à une fraction rationnelle.)

Question 4.2 En utilisant le lemme de meilleure approximation (question 3.4), montrer que a/b est, au signe près, un convergent de la fraction continue de la série de Laurent formelle $\sqrt{D}$.

Question 4.3 Montrer que pour tout $k \geq 1$, on a $p_{k-1}^2 - Dq_{k-1}^2 = (-1)^k Q_k$, où les polynômes Q_k, p_k et q_k sont définis à partir de la fraction continue de $\sqrt{D}$ comme dans les questions 2.1 et 3.6. Pour cela on pourra écrire α_k de deux manières différentes à l'aide des questions 3.3 et 3.6.3. En déduire qu'il existe un indice k tel que le polynôme $Q_k(x)$ est constant, puis que la fraction continue associée à $\sqrt{D}$ est quasi-périodique à partir d'un certain rang, c'est-à-dire périodique à partir d'un certain rang, modulo la multiplication des polynômes par des scalaires.

Question 4.4 Donner les principes d'un algorithme qui prend deux polynômes $D(x)$ et $h(x)$ en entrée, qui retourne $a(x)$ et $b(x)$ si l'intégrale $\int_{x_0}^{x} \frac{h(u)du}{\sqrt{D(u)}}$ est pseudo-hyperelliptique et vaut $\log(a(x) + b(x)\sqrt{D(x)})$, et qui ne termine pas s'il n'existe pas de solution. On suppose donnée une bibliothèque qui permet de calculer sur les polynômes réels (et on ignore les problèmes d'arrondis).