MPRI 2-22 le 6 février 2007

RÉVISION

1. Polynômes de Graeffe

Soit $\mathbb{K}$ un corps et soit $f \in \mathbb{K}[X]$ un polynôme unitaire de degré $d \geq 1$. Pour $N \geq 1$, on appelle le *N-ième polynôme de Graeffe* $G_N(f)$ l'unique polynôme unitaire de degré d de $\mathbb{K}[X]$ dont les racines sont les puissances N-ièmes des racines de f.

(1) Montrer qu'on peut déterminer $G_N(f)$ par un calcul de résultant, en $O(\mathsf{M}(dN))$ opérations dans $\mathbb{K}$.

(2) Prouver que $G_N(f)$ est le polynôme caractéristique de X^N modulo f et en déduire un algorithme de complexité $O(\mathsf{M}(d)\log(N) + d\,\mathsf{M}(d))$.

(3) Si N est une puissance de 2, montrer qu'il est possible de calculer $G_N(f)$ en $O(\mathsf{M}(d)\log(N))$ opérations dans $\mathbb{K}$.

2. Solutions polynomiales et rationnelles

(1) Trouver toutes les solutions polynomiales $x(k) \in \mathbb{Q}[k]$ de la récurrence

$$(1-k)^2 x(k+1) - k^2 x(k) = -2(1-k)^2 + 1.$$

(2) Montrer que les solutions dans $\mathbb{Q}(t)$ de l'équation différentielle

$$(1-t^2)y''(t) - 2ty'(t) + 6y(t) = 0$$

sont toutes de la forme $c(1-3t^2)$, avec $c \in \mathbb{Q}$.

3. Sommes indéfinies et définies

(1) À l'aide de l'algorithme de Gosper, montrer que

$$\sum_{k=1}^{n} \frac{k \cdot k!}{n^k} \binom{n}{k} = n.$$

(2) Dérouler l'algorithme de création téléscopique de Zeilberger afin de calculer la somme $\sum_k \binom{n}{k}^2$.

4. Bases de Gröbner

(1) Soit

$$G = \left\{ X^2 + \frac{3}{2}XY + \frac{1}{2}Y^2 - \frac{3}{2}X - \frac{3}{2}Y, \quad XY^2 - X, \quad Y^3 - Y \right\}.$$

Montrer que pour l'ordre *grevlex* (ordre du degré, raffiné par l'ordre lexicographique inverse) avec $X > Y$, G est une base de Gröbner de l'idéal $I = \langle G \rangle \subset \mathbb{C}[X,Y]$ engendré par G.

(2) En déduire que $\mathcal{B} = \{1,\ X,\ Y,\ XY,\ Y^2\}$ est une base de l'espace vectoriel $A = \mathbb{C}[X,Y]/I$ sur $\mathbb{C}$.

(3) Écrire la table de multiplication de l'algèbre A sur la base $\mathcal{B}$.

(4) Déterminer la matrice, dans la base $\mathcal{B}$, de la multiplication par $X\cdot : A \to A$ et son polynôme minimal.

(5) En déduire que $I \cap \mathbb{C}[X] = (X^4 - 2X^3 - X^2 + 2X)$.

SOLUTIONS

1. Polynômes de Graeffe

(1) On a $G_N(f)(T) = \mathrm{Res}_X(T - X^N, f(X))$, d'où

$$G_N(f)(T^N) = \mathrm{Res}_X(T^N - X^N, f(X)) = (X^N - 1) \otimes f.$$

Or, le produit composé de polynômes de degrés d et N peut se calculer en $O(\mathsf{M}(dN))$ opérations dans $\mathbb{K}$ (cf. Cours 3). Remarquons que ce résultat est quasi-optimal en d, par rapport à la taille de la sortie ($G_N(f)$ a d coefficients).

(2) Les coefficients de $g = X^N \bmod f$ peuvent se calculer en $O(\mathsf{M}(d)\log(N))$ opérations dans $\mathbb{K}$ (cf. Cours 4). La multiplication par X modulo f admet comme valeurs propres les racines de f. Par un résultat classique d'algèbre linéaire, la multiplication par X^N modulo f admet comme valeurs propres les puissances N-ièmes des racines de f, son polynôme caractéristique vaut donc $G_N(f)$. Il reste à montrer que le polynôme caractéristique χ_g de la multiplication par g modulo f peut se calculer en $O(d\mathsf{M}(d))$ opérations.

Il suffit de calculer les d premières sommes de Newton de χ_g (car le passage sommes de Newton $\to$ coefficients se fait en $O(\mathsf{M}(d))$ opérations, cf. Cours 3). On commence par calculer en $O(\mathsf{M}(d))$ les d premières sommes de Newton $N_i(f) = \sum_{f(\alpha)=0} \alpha^i$ de f. Les polynômes $g_k = g^k \bmod f$ se calculent itérativement pour $k = 1, \ldots, d$ en $O(d\mathsf{M}(d))$ opérations. La k-ième somme de Newton de χ_g vaut $\sum_{f(\alpha)=0} g(\alpha)^k = \sum_{f(\alpha)=0} g_k(\alpha)$ et se calcule en $O(d)$ opérations à partir des coefficients de g_k et des sommes de Newton $N_i(f)$.

Remarquons que le coût total est quasi-optimal par rapport à N.

(3) Si N est une puissance de 2, on peut donner un algorithme de complexité quasi-optimale à la fois par rapport à d et à N. Tout repose sur la remarque que $G_2(f)(T^2)$ s'écrit

$$\prod_{f(\alpha)=0} (T^2 - \alpha^2) = \prod_{f(\alpha)=0} (T - \alpha) \prod_{f(\alpha)=0} (T + \alpha) = (-1)^d f(T) f(-T)$$

et donc peut être calculé en 1 multiplication en degré d. Par le même raisonnement, $G_{2^k}(f)$ se calcule à partir de $G_{2^{k-1}}(f)$ en $O(\mathsf{M}(d))$.

2. Solutions polynomiales et rationnelles

(1) Si $x(k) = \alpha k^d + \beta k^{d-1} + \cdots$, alors $x(k+1) = \alpha k^d + (\alpha d + \beta) k^{d-1} + \cdots$, d'où

$$(1-k)^2 x(k+1) - k^2 x(k) = \alpha(d-2)k^{d-1} + \cdots.$$

Toute solution de l'équation homogène $(1-k)^2 x(k+1) - k^2 x(k) = 0$ a donc forcément degré 2 ; de même, toute solution de l'équation inhomogène donnée est de degré 1 avec $\alpha = 2$. Par coefficients indéterminés, on déduit aisément que la solution générale de l'équation homogène est $c(k-1)^2$ et que $x_0(k) = 2k-3$ est solution de l'équation inhomogène. donnée. En conclusion, la solution générale de l'équation initiale est

$$x(k) = c(k-1)^2 + 2k - 3.$$

(2) Si $y(t)$ est une solution rationnelle de $(1-t^2)y''(t) - 2ty'(t) + 6y(t) = 0$, alors les possibles pôles de $y(t)$ sont en $t \in \{-1, +1\}$. Traitons le cas de $t = 1$. Le changement de variable $t \leftarrow t - 1$ fournit l'équation $L_1(y) = (1-t^2)y''(t) - 2ty'(t) + 6y(t)$. L'équation indicielle en $t = 1$ est le coefficient de $t^{\rho-1}$ dans $L_1(t^\rho)$, elle vaut donc $2\rho^2$. Son unique racine étant 0, $y(t)$ n'a pas de pôle en $t = 1$. Le même raisonnement montre que $y(t)$ n'a pas de pôle en $t = -1$, par conséquent $y(t)$ est une solution polynomiale. Son degré d est donné par les racines du coefficient de t^ρ dans $L_1(t^\rho)$. Ce coefficient vaut $(\rho+3)(2-\rho)$, donc $d = 2$. La solution se déduit par coefficients indéterminés.

3. Sommes indéfinies et définies

(1) Le terme général $t(k) = \frac{k \cdot k!}{n^k}\binom{n}{k}$ est hypergéométrique (en k), car $r(k) = t(k+1)/t(k)$ vaut $(k+1)(n-k)/nk$, qui est une fraction rationnelle en k. On cherche une somme indéfinie hypergéométrique $z(k)$ de $t(k)$. Cf. Cours 18, une telle somme doit être un multiple de $t(k)$ et l'égalité $z(k+1)-z(k) = t(k)$ mène à l'équation (dite de Gosper)

$$y(k+1)r(k) - y(k) = 1,$$

dont on cherche une solution rationnelle $y(k)$ valant le rapport inconnu $z(k)/t(k)$. L'algorithme d'Abramov (Cours 18) prédit le dénominateur k de $y(k)$. Le numérateur $x(k) = ky(k)$ satisfait l'équation

$$\left(1 - \frac{k}{n}\right) x(k+1) - x(k) = k.$$

Cette dernière admet la solution constante évidente $x(k) = -n$. Par conséquent, l'équation de Gosper admet comme solution $y(k) = -n/k$ et donc

$$z(k) = t(k)y(k) = -\frac{k!}{n^{k-1}}\binom{n}{k}$$

est une somme indéfinie de $t(k)$. En sommant l'égalité $z(k+1) - z(k) = t(k)$ sur $k = 1, 2, \ldots, n$ on obtient l'ídentité de l'énoncé.

(2) Soit $F(n,k) = \binom{n}{k}^2$. Le principe de la création téléscopique est la recherche d'une récurrence de la forme $\sum_{j=0}^{J} a_j(n)F(n+j,k) = G(n,k+1) - G(n,k)$. Il n'existe aucune récurrence de cette forme avec $J = 0$, c'est-à-dire que $\binom{n}{k}^2$ n'est pas indéfiniment sommable. Ceci se vérifie à l'aide de l'algorithme de Gosper, qui revient à montrer que l'équation $(n-k)^2x(k+1) - k^2x(k) = 1$ n'admet pas de solution polynomiale (Prouvez-le !) Traitons le cas $J = 1$. On cherche $a_0(n), a_1(n) \in \mathbb{Q}[n]$ tels que $a_0(n)F(n,k) + a_1(n)F(n+1,k)$ soit hypergéométrique indéfiniment sommable, c'est-à-dire tels qu'il existe $G(n,k) \in \mathbb{Q}(n)[k]$ vérifiant l'identité

$$a_0(n)F(n,k) + a_1(n)F(n+1,k) = G(n,k+1) - G(n,k).$$

Notons $t(k)$ le terme gauche de cette égalité. La somme indéfinie hypergéométrique $G(n,k)$ de $t(k)$ doit être de la forme $R(k)t(k)$, où $R(k)$ est une solution rationnelle de l'équation de Gosper

$$R(k+1)\left(\frac{a_0(n-k)^2 + a_1(n+1)^2}{a_0(n-k+1)^2 + a_1(n+1)^2}\right) \cdot \left(\frac{n+1-k}{k+1}\right)^2 - R(k) = 1.$$

L'algorithme d'Abramov prédit que $R(k)$ doit avoir la forme

$$R(k) = \frac{k^2}{a_0(n-k+1)^2 + a_1(n+1)^2} \cdot x(k),$$

où $x(k)$ est une solution polynomiale de l'équation

$$(n-k+1)^2x(k+1) - k^2x(k) = a_0(n-k+1)^2 + a_1(n+1)^2.$$

Une étude similaire à celle de l'exercice 2 (1) montre que la solution $x(k)$ est forcément de degré 1 et la méthode des coefficients indéterminés fournit la solution $\alpha = -3(n+1), \beta = 2, a_0 = -2(2n+1), a_1 = n+1$. Autrement dit, $F(n,k) = \binom{n}{k}^2$ satisfait la récurrence

$$-2(2n+1)F(n,k) + (n+1)F(n+1,k) = G(n,k+1) - G(n,k),$$

avec $G(n,k) = R(k)t(k) = (2k-3n-3)\binom{n}{k-1}^2$. En sommant sur k, on déduit que $f(n) = \sum_k \binom{n}{k}^2$ vérifie la récurrence $-2(2n+1)f(n)+(n+1)f(n+1) = 0$, avec $f(0) = 1$, d'où on tire $f(n) = \binom{2n}{n}$.

4. Bases de Gröbner

(1) Cf. le critère de Buchberger, il suffit de prouver que les S-polynômes $\mathrm{Spoly}(f_1, f_2)$, $\mathrm{Spoly}(f_1, f_3)$ et $\mathrm{Spoly}(f_2, f_3)$ se réduisent à 0 modulo l'ensemble $\mathcal{G} = \{f_1, f_2, f_3\}$. (Rappelons qu'on dit que g se réduit à zéro modulo $\mathcal{G}$ s'il admet une écriture $g = \sum_i a_i f_i$ avec $\mathrm{multideg}_{grevlex}(g) \geq \mathrm{multideg}_{grevlex}(a_i f_i)$ pour tout i). En effet, les termes de tête de f_1, f_2, f_3 étant X^2, XY^2, Y^3, on obtient que

$$\mathrm{Spoly}(f_1, f_2) = Y^2 f_1 - X f_2 = \tfrac{3}{2}XY^3 + \tfrac{1}{2}Y^4 - \tfrac{3}{2}XY^2 - \tfrac{3}{2}Y^3 + X^2 = \tfrac{3Y}{2} f_2 + f_1,$$
$$\mathrm{Spoly}(f_2, f_3) = Y f_2 - X f_3,$$
$$\mathrm{Spoly}(f_1, f_3) = Y^3 f_1 - X^2 f_3,$$

fournissent de telles écritures.

(2) Cf. la question précédente, l'idéal initial $\mathrm{in}(I)$ de I est engendré par les monômes X^2, XY^2, Y^3. Une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}[X,Y]/I$ est fournie par les monômes de $\mathbb{C}[X,Y]$ qui n'appartiennent pas à $\mathrm{in}(I)$. La conclusion s'ensuit (faire un dessin de l'escalier asscocié !)

(3) Il suffit de calculer le reste de $b_1 b_2 \bmod \mathcal{G}$ pour tous $b_1, b_2 \in \mathcal{G}$. On obtient la table de multiplication suivante

$\times$	1	X	Y	XY	Y^2
1	1	X	Y	XY	Y^2
X	X	U	XY	V	X
Y	Y	XY	Y^2	X	Y
XY	XY	V	X	U	XY
Y^2	Y^2	X	Y	XY	Y^2

où

$$U = -\frac{3}{2}XY - \frac{1}{2}Y^2 + \frac{3}{2}X + \frac{3}{2}Y \quad \text{et} \quad V = \frac{3}{2}XY + \frac{3}{2}Y^2 - \frac{3}{2}X - \frac{1}{2}Y.$$

(4) On écrit les éléments de $X \cdot \mathcal{B} = \{X,\ X^2,\ XY,\ X^2Y,\ XY^2\}$ modulo $\mathcal{G}$. On a $X \bmod \mathcal{G} = X$, $X^2 \bmod \mathcal{G} = X^2 - f_1 = \frac{3}{2}X + \frac{3}{2}Y - \frac{3}{2}XY - \frac{1}{2}Y^2$, $XY \bmod \mathcal{G} = XY$, $X^2Y \bmod \mathcal{G} = X^2Y - f_1 Y = -\frac{3}{2}X - \frac{1}{2}Y + \frac{3}{2}XY + \frac{3}{2}Y^2$, et $XY^2 \bmod \mathcal{G} = XY^2$. La matrice de la multiplication par X dans la base $\mathcal{B}$ est donc

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 3/2 & 0 & -3/2 & 1 \\ 0 & 3/2 & 0 & -1/2 & 0 \\ 0 & -3/2 & 1 & 3/2 & 0 \\ 0 & -1/2 & 0 & 3/2 & 0 \end{pmatrix}.$$

Par définition, le polynôme minimal de cette matrice est égal au polynôme minimal de la multiplication par X dans A. Pour éviter le calcul du polynôme minimal d'une matrice 5×5, on peut raisonner différemment. On cherche une dépendence linéaire entre $1, X, X^2, \ldots$ dans l'algèbre quotient A. En utilisant la base $\mathcal{B}$, cela revient à chercher un élément du noyau de la matrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3/2 & 4 & 15/2 \\ 0 & 0 & 3/2 & 3 & 15/2 \\ 0 & 0 & -3/2 & -3 & -15/2 \\ 0 & 0 & -1/2 & -3 & -13/2 \end{pmatrix}$$

Un tel élément se trouve par élimination de Gauss ; il s'agit de $(0, 2, -1, -2, 1)^T$, qui correspond au polynôme minimal $m_X(T) = T^4 - 2T^3 - T^2 - 2T$.

(5) Par définition de l'anneau quotient, on a $m_X(X) = X^4 - 2X^3 - X^2 - 2X \in I$. L'idéal $I \cap \mathbb{C}[X]$ est principal, soit F son générateur unitaire. Par définition de l'anneau quotient, la multiplication par $F(X)$ dans A est l'application identiquement nulle, par conséquent $m_X(T)$ divise $F(T)$. Par ailleurs, $m_X \in I = (F)$ entraîne que F divise m_X. Donc $F = m_X$, d'où la conclusion.