D-finitude : algorithmes et applications

Alin Bostan

Frédéric Chyzak

Bruno Salvy

Table des matières

Introduction

Les séries D-finies sont les séries solutions d'équations différentielles linéaires à coefficients polynomiaux. Les suites P-récursives sont les solutions de récurrences linéaires à coefficients polynomiaux. Des notions analogues sont obtenues en remplaçant les opérateurs de dérivation et de décalage classiques par leurs q-analogues. Tous ces objets partagent de nombreuses propriétés qui sont décrites dans le cadre de la « D-finitude ». Le but de ce domaine est d'amener les systèmes de calcul formel à traiter de manière algorithmique un grand nombre de suites et de fonctions spéciales. En effet, on peut estimer qu'environ 60% des fonctions décrites dans le formulaire édité par Abramowitz & Stegun [1] appartiennent à cette classe, ainsi qu'un quart des suites de l'encyclopédie de Sloane [16, 17].

D'une certaine manière, les suites ou séries D-finies sont des analogues non-commutatifs des nombres algébriques : le rôle du polynôme minimal est joué par un opérateur linéaire. Ore [10] a décrit une version non-commutative de la division euclidienne et de l'algorithme d'Euclide étendu pour ces opérateurs linéaires (connus sous le nom de *polynômes de Ore*). Comme dans le cas commutatif, ces algorithmes rendent effectives plusieurs propriétés de clôture (voir [18]). Il s'ensuit que des identités entre ces fonctions ou ces suites peuvent être prouvées voire calculées automatiquement. Une partie du succès du pacquetage Gfun [13] provient d'une implantation de ces opérations. Une autre partie vient de la possibilité de découvrir de telles identités expérimentalement, avec des approximants de Padé-Hermite sur des séries formelles [2] à la place de l'algorithme LLL sur des nombres réels.

La découverte de la D-finitude d'une série est aussi notable du point de vue de la complexité : plusieurs opérations importantes peuvent être effectuées sur les séries D-finies à un coût moindre que sur des séries formelles arbitraires. Ceci comprend la multiplication, mais aussi l'évaluation à des points rationnels par scindage binaire [3]. Une application typique est l'évaluation numérique de π dans les systèmes de calcul formel.

D'autre part, le comportement local des solutions d'équations différentielles linéaires au voisinage de leurs singularités est bien compris [7] et des implantations d'algorithmes calculant les développements correspondants sont disponibles [20, 22]. Ceci donne accès au comportement asymptotique de nombreuses suites ou à des preuves analytiques que des suites ou fonctions ne peuvent être solutions de telles équations [8]. Des résultats de nature plus algébriques sont obtenus par la théorie de Galois différentielle [14, 15], qui partage naturellement de nombreuses sous-routines avec les algorithmes sur les séries D-finies.

Les applications réellement spectaculaires de la D-finitude proviennent du cadre multivarié : on travaille alors avec des suites ou des séries multivariées, ou avec des suites de séries ou de polynômes,... Elles obéissent alors à des systèmes d'opérateurs

linéaires qui peuvent être différentiels, aux différences, aux q-différences, ou de types mixtes, avec la contrainte supplémentaire qu'un nombre fini de conditions initiales est suffisant pour spécifier la solution. Il s'agit là d'un analogue non-commutatif des systèmes polynomiaux avec un nombre fini de solutions. Il s'avère que, comme dans le cas polynomial, des bases de Gröbner fournissent des réponses algorithmiques à de nombreuses questions de décision, en donnant un accès à des formes normales dans des espaces vectoriels quotient de dimension finie. Ceci a été observé d'abord dans le cadre différentiel [**9, 19**], puis étendu au cadre plus général des algèbres de Ore multivariées [**6**].

Une observation cruciale de Zeilberger [**24, 11**] est qu'une élimination dans ce contexte non-commutatif permet de calculer des intégrales ou des sommes définies. Cette opération s'appelle la *création télescopique*. Dans le cadre hypergéométrique (c'est-à-dire lorsque le quotient est un espace vectoriel de dimension 1), un algorithme rapide pour ce calcul est connu sous le nom d'algorithme rapide de Zeilberger [**23**]. Dans un cadre plus général, les bases de Gröbner sont utiles dans cette élimination. Ceci est vrai en différentiel [**12, 21**] et dans une large mesure dans le cas multivarié plus général [**6**]. En outre, l'algorithme rapide de Zeilberger a été généralisé aux algèbres de Ore par Chyzak [**4, 5**]. Cependant, de nombreuses questions d'efficacité demeurent, et des phénomènes de non-minimalité des opérateurs calculés ne sont pas encore complètement compris.

Ce cours présente une partie de ces algorithmes et de leurs applications. Les chapitres sont extraits du cours « Algorithmes efficaces en calcul formel » du Master Parisien de Recherche en Informatique (2006-2007). Le cours complet est disponible à l'url http://mpri.master.univ-paris7.fr/C-2-22.html.

Bibliographie

[1] Abramowitz (Milton) and Stegun (Irene A.) (editors). – *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. – Dover Publications Inc., New York, 1992, xiv+1046p. Reprint of the 1972 edition.

[2] Beckermann (Bernhard) and Labahn (George). – A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM Journal on Matrix Analysis and Applications*, vol. 15, n° 3, July 1994, pp. 804–823.

[3] Chudnovsky (D. V.) and Chudnovsky (G. V.). – Approximations and complex multiplication according to Ramanujan. In *Ramanujan revisited*, pp. 375–472. – Academic Press, Boston, MA, 1988.

[4] Chyzak (Frédéric). – *Fonctions holonomes en calcul formel*. – PhD Thesis, École polytechnique, 1998, 227p.

[5] Chyzak (Frédéric). – An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Mathematics*, vol. 217, n° 1-3, 2000, pp. 115–134.

[6] Chyzak (Frédéric) and Salvy (Bruno). – Non-commutative elimination in Ore algebras proves multivariate holonomic identities. *Journal of Symbolic Computation*, vol. 26, n° 2, August 1998, pp. 187–227.

[7] Fabry (E.). – *Sur les intégrales des équations différentielles linéaires à coefficients rationnels*. – Thèse de doctorat ès sciences mathématiques, Faculté des Sciences de Paris, July 1885.

[8] Flajolet (Philippe), Gerhold (Stefan), and Salvy (Bruno). – On the non-holonomic character of logarithms, powers, and the nth prime function. *The Electronic Journal of Combinatorics*, vol. 11, n° 2, April 2005. – A2, 16 pages.

[9] Galligo (André). – Some algorithmic questions on ideals of differential operators. In Caviness (Bob F.) (editor), *Proceedings EUROCAL'85. Lecture Notes in Computer Science*, vol. 204, pp. 413–421. – Springer-Verlag, 1985.

[10] Ore (Oystein). – Theory of non-commutative polynomials. *Annals of Mathematics*, vol. 34, 1933, pp. 480–508.

[11] Petkovšek (Marko), Wilf (Herbert S.), and Zeilberger (Doron). – $A = B$. – A. K. Peters, Wellesley, MA, 1996, xii+212p.

[12] Saito (Mutsumi), Sturmfels (Bernd), and Takayama (Nobuki). – *Gröbner deformations of hypergeometric differential equations*. – Springer-Verlag, Berlin, 2000, viii+254p.

[13] Salvy (Bruno) and Zimmermann (Paul). – Gfun : a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, vol. 20, n° 2, 1994, pp. 163–177.

[14] Singer (Michael F.). – Liouvillian solutions of n-th order homogeneous linear differential equations. *American Journal of Mathematics*, vol. 103, n° 4, 1981, pp. 661–682.

[15] Singer (Michael F.). – Algebraic relations among solutions of linear differential equations. *Transactions of the American Mathematical Society*, vol. 295, n° 2, 1986, pp. 753–763.

[16] Sloane (N. J. A.). – *The On-Line Encyclopedia of Integer Sequences*. – 2006. Published electronically at http://www.research.att.com/~njas/sequences/.

[17] Sloane (N. J. A.) and Plouffe (S.). – *The Encyclopedia of Integer Sequences*. – Academic Press, 1995.

[18] Stanley (Richard P.). – *Enumerative combinatorics*. – Cambridge University Press, 1999, vol. 2, xii+581p.

[19] Takayama (Nobuki). – Gröbner basis and the problem of contiguous relations. *Japan Journal of Applied Mathematics*, vol. 6, n° 1, 1989, pp. 147–160.

[20] Tournier (Évelyne). – *Solutions formelles d'équations différentielles*. – Doctorat d'État, Université scientifique, technologique et médicale de Grenoble, 1987.

[21] Tsai (Harrison). – *Algorithms for algebraic analysis*. – PhD thesis, University of California at Berkeley, Spring 2000.

[22] van Hoeij (Mark). – Formal solutions and factorization of differential operators with power series coefficients. *Journal of Symbolic Computation*, vol. 24, n° 1, 1997, pp. 1–30.

[23] Wilf (Herbert S.) and Zeilberger (Doron). – Rational function certification of multisum/integral/"q" identities. *Bulletin of the American Mathematical Society*, vol. 27, n° 1, July 1992, pp. 148–153.

[24] Zeilberger (Doron). – A holonomic systems approach to special functions identities. *Journal of Computational and Applied Mathematics*, vol. 32, n° 3, 1990, pp. 321–368.

CHAPITRE 1

Algorithmique des séries D-finies

Résumé

Les séries D-finies se calculent rapidement. L'équation différentielle linéaire les définissant fournit une structure de données adaptée sur laquelle plusieurs opérations utiles sont algorithmiques.

Les séries D-finies (c'est-à-dire solutions d'équations différentielles linéaires à coefficients polynomiaux) ont des coefficients qui satisfont une récurrence linéaire, ce qui permet d'en calculer les N premiers en $O(N)$ opérations, donc plus vite que la plupart des autres séries. Il est de ce fait crucial de reconnaître les séries qui sont D-finies et de disposer des équations différentielles les définissant. De plus, les coefficients des séries D-finies forment des suites qui sont appelées P-récursives, dont l'algorithmique est évidemment étroitement liée à celle des séries D-finies.

L'importance de ces séries et suites provient d'une part de leur algorithmique spécifique, et d'autre part de leur omniprésence dans les applications. Ainsi, le *Handbook of Mathematical Functions*, référence importante en physique, chimie et mathématiques appliquées, comporte environ 60% de fonctions solutions d'équations différentielles linéaires ; de même, les suites P-récursives forment environ un quart des plus de 100 000 suites référencées dans la version en ligne de l'*Encyclopedia of Integer Sequences* de N. Sloane.

1. Équations différentielles et récurrences

Définition 1. Une série formelle $A(X)$ à coefficients dans un corps $\mathbb{K}$ est dite *différentiellement finie* (ou D-finie) lorsque ses dérivées successives A, A', …, engendrent un espace vectoriel de dimension finie sur le corps $\mathbb{K}(X)$ des fractions rationnelles.

De manière équivalente, cette série est solution d'une équation différentielle linéaire à coefficients dans $\mathbb{K}(X)$: si c'est le cas alors l'équation différentielle permet de récrire toute dérivée d'ordre supérieur à celui de l'équation en termes des dérivées d'ordre moindre (en nombre borné par l'ordre). À l'inverse, si l'espace est de dimension finie, alors pour r suffisamment grand, $A, A', \ldots, A^{(r)}$ sont liées et une relation de liaison entre ces dérivées est une équation différentielle linéaire.

Définition 2. Une suite $(a_n)_{n\geq 0}$ d'éléments d'un corps $\mathbb{K}$ est appelée suite *polynomialement récursive* (ou P-récursive) si elle satisfait une récurrence de la forme

$$p_r(n)a_{n+r} + p_{r-1}(n)a_{n+r-1} + \cdots + p_0(n)a_n = 0, \qquad n \geq 0, \tag{1}$$

où les p_i sont des polynômes de $\mathbb{K}[X]$.

Dans la suite, $\mathbb{K}$ aura toujours caractéristique nulle. On peut donc penser sans rien perdre aux idées à $\mathbb{K} = \mathbb{Q}$.

1.1. Méthode naïve. Le résultat qu'il s'agit de considérer d'un point de vue algorithmique est le suivant.

THÉORÈME 1. *Une série formelle est D-finie si et seulement si la suite de ses coefficients est P-récursive.*

DÉMONSTRATION. Soit $A(X) = a_0 + a_1 X + \cdots$ une série D-finie et

$$q_0(X)A^{(r)}(X) + \cdots + q_r(X)A(X) = 0 \tag{2}$$

une équation différentielle qui l'annule. En notant $[X^n]f(X)$ le coefficient de X^n dans la série $f(X)$, on a les relations

$$\begin{aligned} [X^n]f'(X) &= (n+1)[X^{n+1}]f(X) \quad (n \geq 0), \\ [X^n]X^k f(X) &= [X^{n-k}]f(X) \quad (n \geq k). \end{aligned} \tag{3}$$

Par conséquent, l'extraction du coefficient de X^n de (2) fournit une récurrence linéaire sur les a_n valide dès lors que $n \geq n_0 := \max_{0\leq i\leq r} \deg q_i$. Pour obtenir une récurrence valide pour tout $n \geq 0$, il suffit de multiplier cette récurrence par le polynôme $n(n-1)\cdots(n-n_0+1)$.

À l'inverse, soit (a_n) une suite vérifiant la récurrence (1). Les identités analogues à (3) sont maintenant

$$\sum_{n\geq 0} n^k a_n X^n = \left(X\frac{d}{dX}\right)^k A(X), \quad \sum_{n\geq 0} a_{n+k}X^n = (A(X) - a_0 - \cdots - a_{k-1}X^{k-1})/X^k,$$

où A est la série génératrice des coefficients a_n et la notation $(Xd/dX)^k$ signifie que l'*opérateur d'Euler* $\theta = Xd/dX$ est appliqué k fois. En multipliant (1) par X^n et en sommant pour n allant de 0 à ∞, puis en multipliant par une puissance de X on obtient donc une équation différentielle linéaire de la forme

$$q_0(X)A^{(r)}(X) + \cdots + q_r(X)A(X) = p(X),$$

où le membre droit provient des conditions initiales. Il est alors possible, quitte à augmenter l'ordre de l'équation de 1, de faire disparaître ce membre droit, par une dérivation et une combinaison linéaire. □

EXERCICE 1. Estimer la complexité d'un algorithme direct utilisant cette idée, en nombre d'opérations dans $\mathbb{K}$.

Un algorithme plus efficace pour passer d'une équation différentielle d'ordre élevé à la récurrence linéaire satisfaite par les coefficients des solutions est donnée en §1.3.

1.2. Exemples d'applications.

EXEMPLE 1. Pour calculer une racine du polynôme $P_N(x)$ défini par la série génératrice

$$\sum_{n\geq 0} P_n(x)\frac{z^n}{n!} = \left(\frac{1+z}{1+z^2}\right)^x,$$

lorsque N est grand, il n'est pas nécessaire de calculer ce polynôme. Il suffit d'observer que cette série vérifie une équation différentielle linéaire d'ordre 1 (avec x en paramètre), ainsi que la série génératrice des dérivées des P_n, et d'utiliser les récurrences que l'on en déduit sur ces polynômes pour en calculer des valeurs. Ces valeurs permettent alors d'appliquer une méthode de Newton par exemple pour

résoudre le polynôme. Cette idée peut aussi être combinée avec la méthode de scindage binaire décrite au cours suivant.

EXEMPLE 2. Le cas particulier des récurrences d'ordre 1 donne lieu aux suites *hypergéométriques*, qui jouent un rôle important dans la sommation symbolique abordée dans un cours ultérieur.

1.3. Algorithme plus efficace. Vue l'importance du passage de l'équation différentielle à la récurrence, il est souhaitable de maîtriser le coût de cette conversion. Il est possible d'obtenir la récurrence plus efficacement que par la méthode naïve. Afin d'exprimer les estimations de complexité, on utilisera la notation classique $\mathsf{M}(n)$ pour la coût arithmétique (exprimé en nombres d'opérations dans $\mathbb{K}$) de la multiplication de deux polynômes dans $\mathbb{K}[X]$ de degré au plus n. Il est classique [6] que $\mathsf{M}(n)$ peut être pris dans $O(n^{1,59})$ par l'algorithme de Karatsuba ou bien dans $O(n \log n \log\log n)$, via la transformée de Fourier rapide (FFT).

1.3.1. *Cas d'un opérateur donné en $\theta = Xd/dX$.* Si l'équation différentielle linéaire de départ est donnée non pas comme un polynôme en X et $\partial = d/dX$, mais comme un polynôme en X et $\theta = Xd/dX$, alors la conversion en récurrence est assez facile : partant de

$$\sum_{\substack{0\le j\le m\\ 0\le i\le r}} a_{ij} X^j \theta^i,$$

les relations (3) donnent l'opérateur de récurrence

$$\sum a_{ij} S_n^{-j} n^i = \sum a_{ij} (n-j)^i S_n^{-j}.$$

De cette conversion découle le résultat de complexité suivant.

PROPOSITION 1. *La récurrence satisfaite par les coefficients des séries solutions d'une équation différentielle linéaire de degré r en θ et m en X se calcule en $O(m\,\mathsf{M}(r))$ opérations sur les coefficients.*

Par rapport au nombre rm de coefficients du résultat, cette complexité est quasi-optimale, car essentiellement linéaire en rm si la FFT est utilisée.

La preuve utilise la formule ci-dessus et l'observation que calculer les coefficients du polynôme $P(X-j)$ connaissant ceux du polynôme $P(X)$ de degré r ne requiert que $O(\mathsf{M}(r))$ opérations.

1.3.2. *Cas général.* Quitte à le multiplier au préalable par une puissance de X égale au plus à son degré en d/dX, il est toujours possible de récrire un polynôme en X et ∂ en un polynôme en X et θ. Cette récriture peut elle-même être effectuée assez rapidement.

Une première observation est que de la commutation

$$(\theta - i)X^i = X^i\theta$$

se déduit en multipliant à droite par ∂^i la relation

$$X^{i+1}\partial^{i+1} = (\theta - i)X^i\partial^i = (\theta - i)(\theta - i + 1)\cdots\theta.$$

Étant donnés des polynômes $a_i(X)$ de degré au plus $m+r$, il s'agit donc maintenant de calculer des polynômes $b_i(X)$ tels que

$$\sum_{i=0}^{r} a_i(X)X^i\partial^i = \sum_{i=0}^{r} a_i(X)(\theta - i + 1)\cdots\theta = \sum_{i=0}^{r} b_i(X)\theta^i.$$

Récrire le polynôme sous la forme

$$\sum_{j=0}^{m+r} X^j \sum_{i=0}^{r} a_{ij} X^i \partial^i$$

s'effectue en nombre linéaire d'opérations et montre qu'il suffit de savoir traiter efficacement le cas où les a_i (et donc aussi les b_i) sont constants. La transition des uns vers les autres se calcule alors par évaluation-interpolation sur $\theta = 0, 1, 2, \ldots$. Soit B le polynôme à calculer. Les premières identités obtenues par évaluation sont

$$a_0 = b_0, \quad a_0 + a_1 = \sum b_i, \quad a_0 + 2a_1 + 2a_2 = \sum 2^i b_i,$$

et plus généralement

$$e^X \sum a_i X^i = \sum \frac{B(i)}{i!} X^i,$$

ce qui montre que les valeurs de B en $0, \ldots, r$ peuvent être obtenues en $O(\mathsf{M}(r))$ opérations à partir des coefficients a_i, et par suite les coefficients de B peuvent être déterminés en $O(\mathsf{M}(r) \log r)$ opérations en utilisant des techniques d'interpolation rapide [6, Ch. 10].

THÉORÈME 2. *Le calcul des N premiers termes d'une série solution d'une équation différentielle linéaire d'ordre r en ∂ à coefficients des polynômes de degré au plus m requiert un nombre d'opérations arithmétiques borné par*

$$O\left((m+r)\mathsf{M}(r)\left(\log r + \frac{N}{r}\right)\right).$$

La première partie de l'estimation provient des estimations ci-dessus, la seconde de la complexité du calcul des N premiers termes d'une suite solution d'une récurrence linéaire d'ordre au plus $m + r$ avec des coefficients de degré au plus r, qui sera vue au cours 2.

2. Somme et produit

THÉORÈME 3. *L'ensemble des séries D-finies à coefficients dans un corps $\mathbb{K}$ est une algèbre sur $\mathbb{K}$. L'ensemble des suites P-récursives d'éléments de $\mathbb{K}$ est aussi une algèbre sur $\mathbb{K}$.*

DÉMONSTRATION. Les preuves pour les suites et les séries sont similaires. Les preuves pour les sommes sont plus faciles que pour les produits, mais dans le même esprit. Nous ne donnons donc que la preuve pour le produit $h = fg$ de deux séries D-finies f et g. Par la formule de Leibniz, toutes les dérivées de h s'écrivent comme combinaisons linéaires de produits entre une dérivée $f^{(i)}$ de f et une dérivée $g^{(j)}$ de g. Les dérivées de f et de g étant engendrées par un nombre fini d'entre elles, il en va de même pour les produits $f^{(i)}g^{(j)}$, ce qui prouve la D-finitude de h. □

EXERCICE 2. Faire la preuve pour le cas du produit de suites P-récursives.

En outre, cette preuve permet de borner l'ordre des équations : l'ordre de l'équation satisfaite par une somme est borné par la somme des ordres des équations satisfaites par les sommants, et l'ordre de l'équation satisfaite par un produit est borné par le produit des ordres.

Cette preuve donne également un algorithme pour trouver l'équation différentielle (resp. la récurrence) cherchée : il suffit de calculer les dérivées (resp. les décalées)

successives en les récrivant sur un ensemble fini de générateurs. Une fois leur nombre suffisant (c'est-à-dire au pire égal à la dimension plus 1), il existe une relation linéaire entre elles. À partir de la matrice dont les lignes contiennent les coordonnées des dérivées successives (resp. des décalés successifs) sur cet ensemble fini de générateurs, la détermination de cette relation se réduit alors à celle du noyau de la transposée.

Exemple 3. L'identité de Cassini sur les nombres de Fibonacci s'écrit

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^n.$$

Pour calculer le membre droit de cette égalité, le point de départ est simplement la récurrence définissant les nombres de Fibonacci :

$$F_{n+2} = F_{n+1} + F_n,$$

qui exprime que tous les décalés de F_n sont des combinaisons linéaires de F_n et F_{n+1}. Les produits qui interviennent dans l'identité de Cassini s'expriment donc *a priori* comme combinaison linéaire de F_n^2, F_nF_{n+1} et F_{n+1}^2 et donc le membre de gauche vérifie une récurrence d'ordre borné par 4. Le calcul est assez simple et donne une récurrence d'ordre 2 :

$$\begin{aligned} u_n &= F_{n+2}F_n - F_{n+1}^2 = F_{n+1}F_n + F_n^2 - F_{n+1}^2, \\ u_{n+1} &= F_{n+2}F_{n+1} + F_{n+1}^2 - F_{n+2}^2 = F_{n+1}^2 - F_n^2 - F_nF_{n+1} \\ &= -u_n. \end{aligned}$$

La preuve de l'identité est alors conclue en observant que $u_0 = 1$.

En réalité, ce calcul donne plus que la preuve de l'identité : il détermine le membre droit à partir du membre gauche. Si le membre droit est donné, le calcul est bien plus simple : comme le membre gauche vérifie une récurrence d'ordre au plus 4 et le membre droit une récurrence d'ordre 1, leur différence vérifie une récurrence d'ordre au plus 5. Il n'est pas nécessaire de calculer cette récurrence. Il suffit de vérifier que ses 5 conditions initiales sont nulles. Autrement dit, vérifier l'identité pour $n = 0, \dots, 4$ la prouve !

Exercice 3. De la même manière, montrer que $\sin^2 x + \cos^2 x = 1$, avec et sans calcul.

3. Produit d'Hadamard

Corollaire 1. *Si $f = \sum_{n\geq 0} a_n X^n$ et $g = \sum_{n\geq 0} b_n X^n$ sont deux séries D-finies, alors leur produit d'Hadamard*

$$f \odot g = \sum_{n\geq 0} a_n b_n X^n$$

l'est aussi.

La preuve est également un algorithme : des deux équations différentielles se déduisent deux récurrences satisfaites par les suites (a_n) et (b_n) ; d'après la section précédente, le produit (a_nb_n) vérifie alors une récurrence linéaire, dont se déduit enfin l'équation différentielle satisfaite par sa série génératrice.

EXEMPLE 4. Les polynômes de Hermite ont pour série génératrice

$$\sum_{n\geq 0} H_n(x)\frac{z^n}{n!} = \exp(z(2x-z)).$$

À partir de là, la détermination du membre droit de l'identité suivante due à Mehler est entièrement algorithmique :

$$\sum_{n\geq 0} H_n(x)H_n(y)\frac{z^n}{n!} = \frac{\exp\left(\frac{4z(xy-z(x^2+y^2))}{1-4z^2}\right)}{\sqrt{1-4z^2}}.$$

4. Séries algébriques

THÉORÈME 4. *Si la série $Y(X)$ annule un polynôme $P(X,Y)$ de degré d en Y, alors elle est solution d'une équation différentielle linéaire d'ordre au plus d.*

DÉMONSTRATION. La preuve est algorithmique. Quitte à diviser d'abord P par son pgcd avec sa dérivée P_Y par rapport à Y, il est possible de le supposer premier avec P_Y. En dérivant $P(X,Y)=0$ et en isolant Y', il vient

$$Y' = -\frac{P_X}{P_Y}.$$

Après inversion de P_Y modulo P via un calcul de pgcd étendu, cette identité se récrit

$$Y' = R_1(Y) \bmod P,$$

où R_1 est un polynôme en Y de degré au plus d et à coefficients dans $\mathbb{K}(X)$. Ceci signifie que Y' s'écrit comme combinaison linéaire de $1, Y, Y^2, \ldots, Y^{d-1}$ à coefficients dans $\mathbb{K}(X)$. Dériver à nouveau cette équation, puis récrire Y' et prendre le reste de la division par P mène à nouveau à une telle combinaison linéaire pour Y'' et plus généralement pour les dérivées successives de Y. Les $d+1$ vecteurs $Y, Y', \ldots, Y^{(d)}$ sont donc linéairement dépendants et la relation de liaison est l'équation cherchée. □

EXEMPLE 5. Les dénombrements d'arbres mènent naturellement à des équations algébriques sur les séries génératrices. Ainsi, la série génératrice des nombres de Catalan (nombre d'arbres binaires à n sommets internes) vérifie

$$y = 1 + zy^2;$$

la série génératrice des nombres de Motzkin (nombre d'arbres unaires-binaires à n sommets internes) vérifie

$$y = 1 + zy + zy^2.$$

Dans les deux cas, il est aisé d'obtenir d'abord une équation différentielle puis une récurrence qui permet de calculer efficacement ces nombres par la technique de scindage binaire. Dans le cas des nombres de Catalan, la récurrence est d'ordre 1, la suite est donc hypergéométrique et s'exprime aisément.

EXERCICE 4. Trouver une formule explicite des nombres de Catalan. Récrire le résultat en termes de factorielles, puis de coefficients binomiaux.

EXERCICE 5. À l'aide d'un système de calcul formel, calculer une récurrence linéaire satisfaite par les coefficients de la série y solution de

$$y = 1 + zy + zy^7.$$

Les mêmes arguments que ci-dessus mènent à une autre propriété de clôture des séries D-finies.

COROLLAIRE 2. *Si f est une série D-finie et y une série algébrique sans terme constant, alors $f \circ y$ est D-finie.*

La preuve consiste à observer que les dérivées successives de $f \circ y$ s'expriment comme combinaisons linéaires des $f^{(i)}(y)y^j$ pour un nombre fini de dérivées de f (par D-finitude) et de puissances de y (par la même preuve que pour le théorème 4). Cette preuve fournit encore un algorithme.

EXEMPLE 6. À l'aide d'un système de calcul formel, calculer une récurrence linéaire satisfaite par les coefficients du développement en série de Taylor de

$$\exp\left(\frac{1-\sqrt{1-4z}}{2}\right).$$

5. Limitations

En général, la composition de deux séries D-finies n'est pas D-finie. Voici trois résultats plus forts, dont la preuve repose sur la théorie de Galois différentielle et dépasse le cadre de ce cours.

THÉORÈME 5.
1. *Les séries f et $1/f$ sont simultanément D-finies si et seulement si f'/f est algébrique.*
2. *Les séries f et $\exp(\int f)$ sont simultanément D-finies si et seulement si f est algébrique.*
3. *Soit g algébrique de genre supérieur ou égal à 1, alors f et $g \circ f$ sont D-finies si et seulement si f est algébrique.*

EXERCICE 6. Prouver le sens "si" de ces trois propriétés.

Exercices

EXERCICE 7 (Opérations de clôture pour les équations différentielles linéaires à coefficients constants). Soient $f(X)$ et $g(X)$ solutions des équations différentielles linéaires homogènes

$$a_m f^{(m)}(X) + \cdots + a_0 f(X) = 0, \qquad b_n g^{(n)}(X) + \cdots + b_0 g(X) = 0,$$

avec $a_0, \ldots, a_m, b_0, \ldots, b_n$ des coefficients rationnels.

1. Montrer que $f(X)g(X)$ et $f(X)+g(X)$ sont solutions d'équations différentielles du même type.

Si le polynôme $a_m X^m + \cdots + a_0$ se factorise sur $\mathbb{C}$ en

$$a_m(X-\alpha_1)^{d_1}\cdots(X-\alpha_k)^{d_k},$$

on rappelle qu'une base de l'espace des solutions de

$$a_m f^{(m)}(X) + \cdots + a_0 f(X) = 0$$

est donnée par $\left\{e^{\alpha_1 X}, Xe^{\alpha_1 X}, \ldots, X^{d_1-1}e^{\alpha_1 X}, \ldots,\ e^{\alpha_k X}, Xe^{\alpha_k X}, \ldots, X^{d_k-1}e^{\alpha_k X}\right\}$.

2. Montrer qu'une équation satisfaite par $f(X)+g(X)$ peut être calculée à l'aide de l'algorithme d'Euclide.
3. Montrer qu'une équation satisfaite par $f(X)g(X)$ peut être obtenue par un calcul de résultant.

EXERCICE 8 (Puissance symétrique d'équation différentielle). Soient m et d deux entiers naturels et soient $a(X), b(X)$ deux polynômes dans $\mathbb{Q}[X]$ de degrés au plus d.

Q1. Montrer qu'il existe une équation différentielle $\mathcal{E}_m$ linéaire homogène d'ordre $m+1$, à coefficients dans $\mathbb{Q}[X]$, qui admet $\phi(X)^m$ comme solution, quelle que soit la solution $\phi(X)$ de l'équation différentielle

$$(\mathcal{E}_1) \qquad y''(X) + a(X)y'(X) + b(X)y(X) = 0.$$

On admettra que pour toute base (ϕ_1, ϕ_2) de solutions de $\mathcal{E}_1$, les fonctions $\phi_1^i \phi_2^{m-i}$, $i = 0, \ldots, m$ sont linéairement indépendantes.

Q2. Montrer que si $a = 0$, alors $\mathcal{E}_2 : y'''(X) + 4b(X)y'(X) + 2b'(X)y(X) = 0$.

Q3. Expliciter un algorithme pour calculer $\mathcal{E}_m$, en ramenant le calcul final à un calcul sur des matrices de polynômes.

Q4. Estimer la complexité de cet algorithme en nombres d'opérations dans $\mathbb{Q}$ en fonction de m et d.

Q5. Pour m fixé, on associe à une fonction y de X des fonctions L_k par les valeurs initiales

$$L_0(X) = y(X), \quad L_1(X) = y'(X)$$

et la relation de récurrence

$$L_{k+1}(X) = L_k'(X) + ka(X)L_k(X) + k(m-k+1)b(X)L_{k-1}(X).$$

(a) Montrer que lorsque $y = \phi^m$, pour $0 \leq k \leq m$,

$$L_k(X) = m(m-1)\ldots(m-k+1)\phi^{m-k}(X)\phi'(X)^k,$$

et $L_{m+1}(X) = 0$.

(b) Montrer que $L_{m+1}(X) = 0$ n'est autre que l'équation $\mathcal{E}_m$.

(c) En déduire des bornes sur les degrés des coefficients de $\mathcal{E}_m$ et un algorithme de complexité $O(m^3\mathsf{M}(d))$ pour le calcul de $\mathcal{E}_m$.

Q6. * Montrer que si $a, b \in \mathbb{Q}$, alors $\mathcal{E}_m$ est à coefficients constants et qu'on peut calculer $\mathcal{E}_m$ en $O(\mathsf{M}(m)\log m)$ opérations dans $\mathbb{Q}$.

Notes

Les propriétés de clôture des séries D-finies ont été décrites avec leurs applications par Stanley dans [13] ainsi que dans son livre [14], et par Lipshitz dans [9].

L'utilisation des séries D-finies pour les séries algébriques en combinatoire est exploitée à de nombreuses reprises par Comtet dans son livre [4], où il utilise l'algorithme décrit dans la preuve du Théorème 4. L'histoire de cet algorithme est compliquée. Il était connu d'Abel qui l'avait rédigé dans un manuscrit de 1827 qui n'a pas été publié. Ce manuscrit est décrit (p. 287) dans les œuvres complètes d'Abel [1]. Ensuite, ce résultat a été retrouvé par Sir James Cockle en 1860 et popularisé par le révérend Harley en 1862 [7]. Quelques années plus tard, il est encore retrouvé par Tannery [15] dans sa thèse, dont le manuscrit est remarquablement clair et disponible sur le web (à l'url http://gallica.bnf.fr).

Les limitations de la dernière section ne sont pas très connues. Elles sont dues à Harris et Sibuya pour la première [8] et à Singer pour les deux autres [11].

En ce qui concerne les algorithmes et les implantations, la plupart des algorithmes présentés dans ce cours sont implantés dans le package `gfun` de Maple [10]. L'algorithme rapide de la section 1.3 provient essentiellement de [3], qui donne une variante légèrement plus efficace (d'un facteur constant). L'exercice 4 est tiré d'une réponse à un "défi" [5].

Bibliographie

[1] Abel (Niels Henrik). – *Œuvres complètes. Tome II.* – Éditions Jacques Gabay, Sceaux, 1992, vi+716p. Edited and with notes by L. Sylow and S. Lie, Reprint of the second (1881) edition. Disponible en ligne à http://gallica.bnf.fr.

[2] Abramowitz (Milton) and Stegun (Irene A.) (editors). – *Handbook of mathematical functions with formulas, graphs, and mathematical tables.* – Dover Publications Inc., New York, 1992, xiv+1046p. Reprint of the 1972 edition.

[3] Bostan (Alin). – *Algorithmique efficace pour des opérations de base en Calcul formel.* – PhD thesis, École polytechnique, December 2003.

[4] Comtet (L.). – *Analyse Combinatoire.* – PUF, Paris, 1970. 2 volumes.

[5] Flajolet (Philippe) and Salvy (Bruno). – The Sigsam challenges : Symbolic asymptotics in practice. *SIGSAM Bulletin*, vol. 31, n° 4, December 1997, pp. 36–47.

[6] von zur Gathen (J.) and Gerhard (J.). – *Modern computer algebra.* Cambridge University Press, New York, 2nd edition, 2003.

[7] Harley (Rev. Robert). – On the theory of the transcendental solution of algebraic equations. *Quarterly Journal of Pure and Applied Mathematics*, vol. 5, 1862, pp. 337–360.

[8] Harris (William A.) and Sibuya (Yasutaka). – The reciprocals of solutions of linear ordinary differential equations. *Advances in Mathematics*, vol. 58, n° 2, 1985, pp. 119–132.

[9] Lipshitz (L.). – *D*-finite power series. *Journal of Algebra*, vol. 122, n° 2, 1989, pp. 353–373.

[10] Salvy (Bruno) and Zimmermann (Paul). – Gfun : a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, vol. 20, n° 2, 1994, pp. 163–177.

[11] Singer (Michael F.). – Algebraic relations among solutions of linear differential equations. *Transactions of the American Mathematical Society*, vol. 295, n° 2, 1986, pp. 753–763.

[12] Sloane (N. J. A.). – *The On-Line Encyclopedia of Integer Sequences.* – 2006. Published electronically at http://www.research.att.com/~njas/sequences/.

[13] Stanley (R. P.). – Differentiably finite power series. *European Journal of Combinatorics*, vol. 1, n° 2, 1980, pp. 175–188.

[14] Stanley (Richard P.). – *Enumerative combinatorics.* – Cambridge University Press, 1999, vol. 2, xii+581p.

[15] Tannery (Jules). – *Propriétés des intégrales des équations différentielles linéaires à coefficients variables.* – Thèse de doctorat ès sciences mathématiques, Faculté des Sciences de Paris, 1874. Disponible en ligne à http://gallica.bnf.fr.

CHAPITRE 2

Récurrences linéaires à coefficients polynomiaux

Résumé

Pour calculer les n premiers termes d'une suite P-récursive, l'algorithme direct par déroulement de la récurrence est quasi-optimal vis-à-vis de n. En effet, sa complexité arithmétique (resp. binaire) est linéaire en n (resp. quasi-quadratique en n). Le n-ième terme d'une telle suite peut être calculé plus rapidement que l'ensemble des n premiers termes, en essentiellement $\sqrt{n}$ opérations arithmétiques et n opérations binaires.

Le calcul du n-ième terme d'une suite P-récursive, donnée par la récurrence à coefficients polynomiaux

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0, \qquad (n \in \mathbb{N}), \tag{1}$$

intervient fréquemment en combinatoire et pour calculer des troncatures de séries, ainsi que comme étape clé dans le meilleur algorithme connu pour la factorisation déterministe d'entiers. Si les coefficients $p_i(n)$ ont degré au plus d en n, l'algorithme naïf par déroulement de la récurrence (1) a complexité arithmétique $O(rdn)$ et complexité binaire $O\big(rn^2\,\mathsf{I}(d\log n)\big)$. Ici, par $\mathsf{I}(N)$ on note le nombre d'opérations binaires requises pour la multiplication de deux entiers de tailles binaires au plus N[1]. Ces complexités sont quasi-optimales vis-à-vis de n, pour le calcul de tous les n premiers termes. Pour le calcul du n-ième terme seul, la technique des *pas de bébés / pas de géants* décrite en section 2 permet d'atteindre une meilleure complexité arithmétique, en $O\big(r^2\mathsf{M}(\sqrt{dn}\,)\log dn + r^\omega\mathsf{M}(\sqrt{dn}\,)\log n\big)$. Le gain en racine de n est typique de la technique.

Cette technique n'est pas bien adaptée pour abaisser la complexité binaire du calcul du n-ième terme, lorsque les coefficients des polynômes p_i sont entiers. En revanche, la méthode du *scindage binaire* de la section 3 fournit une complexité binaire quasi-optimale, en $O\big(r^\omega\,\mathsf{I}(dn\log n)\log n\big)$. Notons que le scindage binaire n'abaisse en rien la complexité arithmétique, mais améliore pourtant la complexité binaire jusqu'à la rendre quasi-linéaire en la taille de sa sortie.

Dans le cas spécifique d'ordre $r = 1$, une suite u est dite *hypergéométrique*. Remarquons que la définition se récrit sous la forme suivante, plus facile à mémoriser :

$$\frac{u_{n+1}}{u_n} = -\frac{p_0(n)}{p_1(n)}.$$

Autrement dit, le quotient de deux termes successifs de la suite est donné par l'évaluation d'une fraction rationnelle fixée, sauf peut-être en un nombre fini de valeurs de n. Les suites P-récursives et encore plus les suites hypergéométriques joueront un rôle important dans des chapitres ultérieurs.

[1] En particulier on peut prendre $\mathsf{I}(N)$ dans $O(N\log N\log\log N)$ si l'on utilise l'algorithme de type FFT de Schönhage-Strassen [4, Th. 8.24].

1. Calcul naïf de $n!$ et de suites P-récursives

La définition de la factorielle comme produit,

$$n! = 1 \times 2 \times \cdots \times n,$$

montre que $n!$ peut être calculé en $n-1$ opérations arithmétiques.

L'estimation de la complexité binaire de cette méthode repose sur la *formule de Stirling* :

$$\log n! = n \log n - n \log e + \frac{1}{2} \log n + O(1), \qquad n \to \infty.$$

En particulier, nous retiendrons l'équivalence $\log n! \sim n \log n$ qui donne la taille de $n!$. La k-ième étape du produit multiplie $k!$ par $k+1$, et donc un entier de taille $\log k! \sim k \log k$ avec un entier de taille $\log(k+1) \sim \log k$. Ce produit déséquilibré coûte donc moins de $ck\,\mathsf{I}(\log k)$ opérations binaires pour une certaine constante c. Le calcul complet de la factorielle par la méthode naïve effectue donc

$$\sum_{k=1}^{n} ck\,\mathsf{I}(\log k) = O\big(n^2\,\mathsf{I}(\log n)\big)$$

opérations binaires. Ces complexités arithmétique et binaire sont quasi-optimales pour le calcul conjoint des nombres $1!$, $2!$, …, $n!$.

Pour une suite P-récursive donnée par une récurrence de la forme (1), le calcul de u_{n+r} à partir des r valeurs précédentes de la suite demande $O(rd)$ opérations arithmétiques pour l'évaluation des polynômes (par exemple par le schéma de Horner) puis $O(r)$ opérations pour effectuer la combinaison linéaire des u_{n+i}. Calculer u_n à partir des valeurs initiales $u_0, \ldots, u_{r-1}$ demande donc $O(rdn)$ opérations.

Une première amélioration, utilisée au Cours précédent dans la preuve du Th. 2, vient de l'observation que les coefficients p_i peuvent être évalués sur les entiers $0, 1, 2 \ldots, n$ en utilisant des techniques d'évaluation multipoint rapide. La complexité $O(rdn)$ pour le calcul de u_n peut ainsi être abaissée à $O\big(r\mathsf{M}(d)\big(n/d + \log d\big)\big)$.

La complexité binaire par cette méthode découle de nouveau essentiellement de la croissance de u_n. Pour estimer celle-ci, il est agréable de faire apparaître u_n comme le quotient v_n/w_n des suites définies par les récurrences

$$v_{n+r} + p_{r-1}(n)v_{n+r-1} \cdots + p_0(n)v_n = 0, \qquad p_r(n)w_{n+r} = w_{n+r-1}, \qquad (n \in \mathbb{N}),$$

et les conditions initiales $v_i = u_i$ et $w_i = 1$ quand $0 \le i < r$. Par une vision matricielle, v_n est donné comme première coordonnée du vecteur V_n de la suite vectorielle définie par la récurrence du premier ordre

$$V_{n+1} = A(n)V_n \quad \text{avec} \quad A(n) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -p_0(n) & & \cdots & & -p_{r-1}(n) \end{pmatrix}.$$

La matrice $A(n)$ s'écrit sous la forme $A_\delta n^\delta + A_{\delta-1} n^{\delta-1} + \ldots$, pour des matrices constantes A_i et un entier δ entre 0 et d. Il s'ensuit que sa norme est bornée par $r2^\ell(d+1)n^d$, avec le choix de norme $||M|| = \max_{1 \le i \le r}(\sum_{j=1}^{r} |m_{ij}|)$ sur les matrices. Ici ℓ représente un majorant commun pour les tailles binaires des coefficients

des p_i et des conditions initiales $u_0, \dots, u_{r-1}$. Les majorations

$$|v_n| \le ||V_n|| \le ||A(n)|| \cdots ||A(1)||\,||U_0|| \le r^n (n!)^d (d+1)^n 2^{\ell n} \ell$$

fournissent la borne $O(dn \log n + n\ell + n \log r)$ sur la taille $\log |v_n|$. Par le même raisonnement, la taille du dénominateur w_n est du même ordre, si bien que par le même type d'argument que pour la factorielle, la complexité binaire du calcul naïf de u_n est $O\big(rn^2\, \mathsf{I}(d \log n + \ell + \log r)\big)$.

2. Pas de bébés et pas de géants

On sait que le n-ième terme d'une récurrence linéaire à coefficients constants peut être calculé en complexité arithmétique $O(\log n)$. Dans le cas des coefficients polynomiaux, les choses se compliquent : à ce jour, on ne connaît pas d'algorithme polynomial en $\log n$. L'exemple typique en est le calcul du n-ième terme de la factorielle $u_n = n!$, qui vérifie la récurrence à coefficients polynomiaux $u_{n+1} = (n+1)u_n$ pour $n \ge 0$. Une solution efficace utilise la technique des *pas de bébés et pas de géants* et requiert un nombre d'opérations arithmétiques en $\sqrt{n}$ (à des facteurs logarithmiques près). Pour simplifier la présentation, supposons que n est un carré parfait. L'idée de l'algorithme est de poser

$$P(X) = (X+1)(X+2)\cdots(X+n^{1/2}),$$

afin d'obtenir la valeur de u_n à l'aide de l'équation

$$u_n = \prod_{j=0}^{n^{1/2}-1} P\big(jn^{1/2}\big). \tag{2}$$

Cette égalité suggère la procédure suivante :

1. *Pas de bébés* : Calculer les coefficients de P, en $O\big(\mathsf{M}(\sqrt{n}\,) \log n\big)$ opérations arithmétiques (en construisant un arbre binaire de feuilles $X + i$).
2. *Pas de géants* : Évaluer P sur les points 0, $\sqrt{n}$, $2\sqrt{n}$, …, $(\sqrt{n}-1)\sqrt{n}$ et retrouver la valeur de u_n à l'aide de l'équation (2). En utilisant des techniques d'évaluation rapide, ceci se fait en $O\big(\mathsf{M}(\sqrt{n}\,) \log n\big)$ opérations.

Le coût total de cet algorithme est de $O\big(\mathsf{M}(\sqrt{n}) \log n\big)$ opérations arithmétiques. Si la FFT est utilisée pour la multiplication des polynômes, le gain par rapport à la méthode directe est de l'ordre de $\sqrt{n}$, à des facteurs logarithmiques près, typique pour la technique des pas de bébés et pas de géants.

Ce résultat se généralise au problème du calcul d'un terme d'une suite récurrente linéaire à coefficients polynomiaux. À cette fin, le polynôme à considérer est maintenant le polynôme matriciel

$$P(X) = A(X+m)\cdots A(X+2)A(X+1),$$

pour $m = (n/d)^{1/2}$. Le produit $A(n)\cdots A(1)$ est le produit de $(dn)^{1/2}$ évaluations de P, lequel a degré $(dn)^{1/2}$. Ces évaluations matricielles s'obtiennent en réalisant successivement les évaluations multipoints des r^2 coordonnées de la matrice P.

Exercice 1. Montrer que la complexité arithmétique de l'algorithme esquissé ci-dessus est en $O\big(r^2 \mathsf{M}(\sqrt{dn}\,) \log dn + r^\omega \mathsf{M}(\sqrt{dn}\,) \log n\big)$.

EXERCICE 2. Étant donné un polynôme $f \in \mathbb{K}[X]$ de degré 2 et un entier $N \geq 0$, quel est le nombre d'opérations dans $\mathbb{K}$ nécessaires pour déterminer le coefficient de X^N du polynôme f^N ? (Indication : La solution directe consiste à calculer tous les coefficients u_n de f^N modulo X^{N+1} par exponentiation binaire. Son coût est de $O\big(\mathsf{M}(N)\big)$ opérations arithmétiques. Une approche plus rapide repose sur le fait que les u_n satisfont une récurrence à coefficients polynomiaux d'ordre 2.)

2.1. Factorisation déterministe des entiers. Supposons que nous devons factoriser un entier N. Tester tous les diviseurs plus petits que $\sqrt{N}$ a un coût linéaire en $\sqrt{N}$ (dans ce paragraphe, par coût on entend complexité bit). Afin d'accélérer ce calcul, Strassen [5] propose de rassembler tous les entiers plus petits que $\sqrt{N}$ en $\sqrt[4]{N}$ blocs, chacun contenant $\sqrt[4]{N}$ entiers consécutifs. Soit c de l'ordre de $\sqrt[4]{N}$ et notons $f_0 = 1 \cdots c \bmod N$, $f_1 = (c+1) \cdots (2c) \bmod N$, ..., $f_{c-1} = (c^2 - c + 1) \cdots (c^2) \bmod N$. Si les valeurs $f_0, \ldots, f_{c-1}$ sont connues, alors il devient facile de déterminer un facteur de N, en prenant des pgcd de $f_0, \ldots, f_{c-1}$ avec N. Ainsi, la principale difficulté est de calculer les valeurs f_i.

Pour ce faire, on prend $\mathbb{K} = \mathbb{Z}/N\mathbb{Z}$ et F le polynôme $(X+1) \cdots (X+c) \in \mathbb{K}[X]$, qu'on évalue en les points $0, c, 2c, \ldots, c(c-1)$ en $O(\mathsf{M}(c) \log c)$ opérations de $\mathbb{K}$. Par les techniques d'évaluation-interpolation rapide, la complexité totale est de $O(\mathsf{M}(\sqrt[4]{N}) \log N)$ opérations modulo N, soit $O(\mathsf{M}(\sqrt[4]{N})\, \mathsf{I}(\log N) \log N)$ opérations bits. Notons qu'on ne connaît pas de meilleur algorithme déterministe ; l'existence d'un tel algorithme est un grand problème ouvert.

3. Scindage binaire

3.1. Cas de la factorielle. Pour exploiter la multiplication rapide d'entiers, l'idée consiste à équilibrer les produits en calculant $P(a,b) = (a+1)(a+2) \cdots b$ récursivement par

$$P(a,b) = P(a,m)P(m,b) \quad \text{où} \quad m = \left\lfloor \frac{a+b}{2} \right\rfloor.$$

Appelons $C(a,b)$ (resp. $\mathsf{I}(a,b)$) le coût binaire du calcul de $P(a,b)$ (resp. de ab). Il résulte immédiatement de la méthode que ce coût vérifie l'inégalité

$$C(a,b) \leq C(a,m) + C(m,b) + \mathsf{I}\big(\log P(a,m), \log P(m,b)\big).$$

Sous l'hypothèse raisonnable que la complexité de la multiplication d'entiers est croissante avec la taille des entiers, le coût du calcul de $P(a,m)$ est inférieur au coût du calcul de $P(m,b)$, d'où la nouvelle inégalité

$$C(a,b) \leq 2C(m,b) + \mathsf{I}\big(P(m,b)\big).$$

L'utilisation de l'inégalité précédente donne les inégalités successives

$$\begin{aligned} C(0,n) &\leq 2C(n/2,n) + \mathsf{I}\big(\log P(n/2,n)\big) \\ &\leq 4C(3n/4,n) + 2\,\mathsf{I}\big(\log P(3n/4,n)\big) + \mathsf{I}\big(\log P(n/2,n)\big) \\ &\leq \cdots \\ &\leq 2^k C(n - 2^{-k}n, n) + 2^k\,\mathsf{I}\big(\log P(n-2^{-k}n,n)\big) + \cdots + \mathsf{I}\big(\log P(n/2,n)\big), \end{aligned}$$

pour tout entier positif k. L'entier $P(n-2^{-k}n, n)$ est le produit de $2^{-k}n$ facteurs de taille bornée par $\log n$; il a donc pour taille $2^{-k}n \log n$. Par sous-additivité de la

fonction I, la dernière inégalité devient

$$C(0,n) \leq 2^k C(n/2^k, n) + k\,\mathsf{I}(n\log n).$$

En choisissant finalement d'arrêter la récursion lorsque $n - 2^{-k}n$ et n diffèrent d'au plus un, ce qui impose k de l'ordre de $\log n$, on aboutit à la borne

$$C(0,n) \leq O(\log n) + \mathsf{I}(n\log n)\log n$$

donc à une complexité binaire dans $O\big(\mathsf{I}(n\log n)\log n\big)$. Si la multiplication utilisée est la FFT, cette complexité s'écrit $O(n\log^3 n \log\log n)$; si la multiplication est d'exposant de n strictement plus grand que 1, elle s'écrit $O\big(\mathsf{I}(n\log n)\big)$.

3.2. Récurrences d'ordre 1. La factorielle de la section précédente suit la récurrence $u_{n+1} = (n+1)u_n$. On considère ici tout d'abord les solutions de récurrences de la forme

$$u_{n+1} = p(n)u_n, \qquad p \in \mathbb{Z}[X].$$

Si p a degré d, $\log p(n)$ est dans $O(d\log n)$, si bien que la taille de u_n est $O(dn\log n)$.

De même, pour toute récurrence de la forme

$$u_{n+1} = \frac{p(n)}{q(n)}u_n, \qquad p, q \in \mathbb{Z}[X],$$

on peut pour calculer u_n appliquer séparément la même technique de scindage binaire sur le numérateur et le dénominateur. Si d est le maximum des degrés de p et q, le calcul produit deux entiers de taille $O(dn\log n)$ en un nombre d'opérations binaires en $O\big(\mathsf{I}(dn\log n)\log n\big)$. Ensuite, si le dénominateur est non nul, la méthode de Newton permet d'effectuer la division finale en $O\big(\mathsf{I}(dn\log n)\big)$ opérations binaires.

3.3. Calcul de $e = \exp(1)$. Le point de départ est la suite (e_n) donnée par

$$e_n = \sum_{k=0}^{n} \frac{1}{k!}.$$

Cette suite converge vers e. Plus précisément, il est classique que le terme de reste dans $e - e_n$ se majore par une série géométrique de sorte que

$$0 \leq e - e_n \leq \frac{1}{n\,n!}.$$

Pour calculer N décimales de e par cette série, il suffit de rendre $\frac{1}{n\,n!}$ inférieur à 10^{-N}. Il s'ensuit qu'il suffit de prendre N de sorte que $n\,n!$ et 10^N soient du même ordre, c'est-à-dire d'avoir N proportionnel à $n\log n$. Il suffit donc de prendre $n = O(N/\log N)$ termes dans la série.

La suite $(e_n)_{n\geq 0}$ vérifie $e_n - e_{n-1} = 1/n!$ et donc

$$n(e_n - e_{n-1}) = e_{n-1} - e_{n-2}.$$

Cette récurrence se récrit

$$\begin{pmatrix} e_n \\ e_{n-1} \end{pmatrix} = \frac{1}{n} \underbrace{\begin{pmatrix} n+1 & -1 \\ n & 0 \end{pmatrix}}_{A(n)} \begin{pmatrix} e_{n-1} \\ e_{n-2} \end{pmatrix} = \frac{1}{n!} A(n)A(n-1)\cdots A(2) \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Le calcul du produit de matrices peut alors être effectué par scindage binaire. Le calcul de e_N par ce procédé demande donc $O(\mathsf{I}(N\log N)\log N)$ opérations binaires.

Pour calculer n décimales de e, la première étape ci-dessus construit deux entiers de taille $O(N \log N) = O(n)$ en $O(\mathsf{I}(n) \log n)$ opérations binaires. Il faut ensuite effectuer une division qui ne demande que $O(\mathsf{I}(n))$ opérations par l'algorithme de Newton. L'ensemble du calcul est donc quasi-optimal. (En outre, le $\log n$ n'est pas présent pour des multiplications comme celle de Karatsuba dont l'exposant de complexité est supérieur à 1.)

Un autre exemple d'application est donné dans les notes.

3.4. Suites polynomialement récursives. Revenons à présent au cas d'une suite P-récursive (1). On fait ici l'hypothèse que le coefficient de tête p_r ne s'annule pas sur les entiers $0, \dots, n-r$, où n est l'indice du terme maximal que l'on souhaite calculer. On garde les notations d pour une borne sur les degrés des polynômes p_i, et ℓ pour une borne sur la taille de leurs coefficients lorsque ceux-ci sont entiers.

THÉORÈME 1. *La complexité binaire de la méthode du scindage binaire pour calculer u_n est en $O(r^\omega\, \mathsf{I}(dn \log n + \ell n + n \log r) \log n)$.*

Comme précédemment, cette dernière complexité descend à $O(r^\omega\, \mathsf{I}(dn \log n + \ell n + n \log r))$ si l'exposant α de la complexité $\mathsf{I}(m) = m^\alpha$ est supérieur à 1.

EXERCICE 3. Vérifier les formules de ce théorème.

Exercices

EXERCICE 4 (Calcul efficace de coefficients trinomiaux centraux). Soit $\mathsf{I} : \mathbb{N} \to \mathbb{N}$ la fonction définie par $\mathsf{I}(n) = \lfloor n \log(n+1) \log(\log(n+3)) \rfloor$ pour tout $n \geq 1$. On rappelle qu'il est possible de multiplier des entiers de n chiffres binaires en $O(\mathsf{I}(n))$ opérations binaires et des polynômes de degré n à coefficients dans un anneau arbitraire en $O(\mathsf{I}(n))$ opérations arithmétiques dans l'anneau.

Soit $N \in \mathbb{N}$ et soit $P = \sum_{i=0}^{2N} p_i X^i \in \mathbb{Z}[X]$ le polynôme $P(X) = (1+X+X^2)^N$.

1. Montrer que $O(\mathsf{I}(N))$ opérations binaires suffisent pour déterminer la parité de tous les coefficients de P.
   Indication : un entier n est pair si et seulement si $n = 0$ dans $\mathbb{Z}/2\mathbb{Z}$.
2. Montrer que P vérifie une équation différentielle linéaire d'ordre 1 à coefficients polynomiaux. En déduire que les p_i suivent une récurrence d'ordre 2 que l'on précisera.
3. Donner un algorithme qui calcule p_N en $O(\mathsf{I}(N \log N) \log N)$ opérations binaires.

EXERCICE 5 (Calcul rapide de factorielle et de coefficients binomiaux centraux). Cet exercice montre comment calculer certaines suites récurrentes linéaires plus vite que par la méthode de scindage binaire.

Soit $N \in \mathbb{N}$ et soit $Q = \sum_{i=0}^{2N} q_i X^i \in \mathbb{Z}[X]$ le polynôme $Q(X) = (1+X)^{2N}$.

1. Montrer que q_N peut être calculé en utilisant uniquement des additions d'entiers du triangle de Pascal, c'est-à-dire l'identité suivante :
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \qquad k \geq 1, n \geq 1.$$
   Quelle est la complexité binaire de cet algorithme ?

On admet que le calcul de tous les nombres premiers inférieurs à N peut être effectué en $O(N \log N / \log\log N)$ opérations binaires, qu'il existe au plus $3N/\log(N)$ tels nombres premiers et que la multiplicité avec laquelle apparaît le nombre premier p dans la factorisation de $N!$ vaut

$$\mathrm{ind}(p, N) = \sum_{i=1}^{\infty} \left[\frac{N}{p^i}\right],$$

où la notation $[x]$ représente la partie entière de x.

2. Montrer que le calcul de $\mathrm{ind}(p, N)$ peut être effectué en $O(\mathsf{I}(\log N)\log N)$ opérations binaires.
3. Montrer que la décomposition en facteurs premiers de $N!$ peut être effectuée en $O(\mathsf{I}(N)\log N)$ opérations binaires, ainsi que celle de q_N.
4. Montrer que $N!$ et q_N peuvent alors être reconstruits en respectivement $O(\mathsf{I}(N\log N)\log\log N)$ et $O(\mathsf{I}(N)\log N)$ opérations binaires.

Notes

L'algorithme par pas de bébés et pas de géants a été introduit par Strassen [5] et généralisé dans [2] au problème du calcul d'un terme d'une suite P-récursive.

L'exercice 2 est inspiré de [3, Pb. 4].

Le raisonnement de §3.3 se généralise au calcul des sommes convergentes de suites hypergéométriques. En particulier, c'est ainsi que les systèmes de calcul formel calculent rapidement π par une formule découverte par les frères Chudnovsky :

$$\frac{1}{\pi} = \frac{12}{C^{3/2}} \sum_{n=0}^{\infty} \frac{(-1)^n (6n)!(A+nB)}{(3n)!n!^3 C^{3n}}$$

où $A = 13591409$, $B = 545140134$ et $C = 640320$.

La partie de l'exercice 5 consacrée au calcul de $N!$ est due à P. Borwein [1].

Bibliographie

[1] Borwein (Peter B.). – On the complexity of calculating factorials. *Journal of Algorithms*, vol. 6, n° 3, 1985, pp. 376–380.

[2] Chudnovsky (D. V.) and Chudnovsky (G. V.). – Approximations and complex multiplication according to Ramanujan. In *Ramanujan revisited*, pp. 375–472. – Academic Press, Boston, MA, 1988.

[3] Flajolet (Philippe) and Salvy (Bruno). – The Sigsam challenges : Symbolic asymptotics in practice. *SIGSAM Bulletin*, vol. 31, n° 4, December 1997, pp. 36–47.

[4] von zur Gathen (J.) and Gerhard (J.). – *Modern computer algebra*. Cambridge University Press, New York, 2nd edition, 2003.

[5] Strassen (V.). – Einige Resultate über Berechnungskomplexität. *Jber. Deutsch. Math.-Verein.*, vol. 78, n° 1, 1976/77, pp. 1–8.

CHAPITRE 3

Résolution d'équations différentielles linéaires

Résumé

Les solutions polynomiales ou rationnelles d'équations différentielles linéaires s'obtiennent en utilisant des développements en série et la structure des ensembles de séries solutions.

L'objectif de ce cours est de décrire des algorithmes permettant de calculer les solutions polynomiales et rationnelles d'une équation de la forme

$$Ly(x) = \sum_{k=0}^{n} a_k(x) y^{(k)}(x) = 0, \tag{1}$$

où les coefficients a_k, $k = 0, \dots, n$ sont des polynômes à coefficients dans un corps $\mathbb{K}$. De manière équivalente (voir §1), ces algorithmes permettront de résoudre le système

$$Y'(x) = A(x)Y(x), \tag{2}$$

où $A(x)$ est une matrice de fractions rationnelles de $\mathbb{K}(x)$ et Y un vecteur.

Ces algorithmes seront utilisés dans un cours ultérieur pour le calcul d'intégrales définies.

1. Système et équation

L'équivalence entre équation linéaire d'ordre n et système linéaire d'ordre 1 sur des vecteurs de taille n est classique. Nous détaillons les calculs en jeu.

L'équation (1) est transformée en une équation de la forme (2), en posant $Y = (y_0, \dots, y_{n-1})^T$ où $y_i = y^{(i)}$ pour $i = 0, \dots, n-1$. La matrice A est alors une matrice compagnon

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \\ -\frac{a_0}{a_n} & \dots & \dots & \dots & -\frac{a_{n-1}}{a_n} \end{pmatrix}. \tag{3}$$

À l'inverse, pour toute matrice A intervenant dans un système de type (2), une équation différentielle de type (1) peut être obtenue pour n'importe quelle combinaison linéaire à coefficients dans $\mathbb{K}$ des coordonnées d'une solution Y. En effet, les dérivées successives $Y, Y', Y'', \dots$ sont des vecteurs dans un espace de dimension n où n est la taille de la matrice. Il existe donc un $k \leq n$ tel que $Y, \dots, Y^{(k)}$ soient liés sur $\mathbb{K}$. Multiplier à gauche par un vecteur constant donne l'équation cherchée.

EXERCICE 1. Trouver une équation différentielle linéaire satisfaite par y_1 solution de

$$y_1' = xy_1 - y_2, \quad y_2' = y_1 - xy_2.$$

2. Solutions séries et singularités

Avant de rechercher le développement en série de solutions de l'équation (1) ou du système (2), il est utile de localiser les singularités. Le point de départ est une version du théorème de Cauchy sur les équations différentielles :

THÉORÈME 1. *Si $A(x)$ est une fonction de $\mathbb{C}$ dans $\mathbb{C}^{n\times n}$ analytique dans une région simplement connexe R du plan complexe, alors l'équation*

$$Y'(x) = A(x)Y(x)$$

possède une unique solution telle que $Y(\alpha) = U$ pour tout $\alpha \in R$ et $U \in \mathbb{C}^n$. Cette solution est analytique dans R.

L'application de ce résultat à l'équation (2) montre qu'en tout point où A est analytique (développable en série entière), il existe une base de solutions séries entières convergentes. Au vu de la matrice compagnon (3), il en va de même pour les solutions de l'équation (1) en tout point où le coefficient de tête a_n est non-nul. *A contrario*, les seuls points où le système (2) peut ne pas admettre de solution série sont les racines de a_n.

DÉFINITION 1. On dit que $\alpha \in \mathbb{C}$ est un point *ordinaire* de l'équation (1) si $a_n(\alpha) \neq 0$. On dit qu'il est *singulier* dans le cas contraire.

EXEMPLE 1. La fraction rationnelle $y = 1/(1-x)$ est solution de l'équation

$$(1-x)y'(x) - y(x) = 0.$$

Le complexe $\alpha = 1$ est singularité de la solution et donc nécessairement point singulier de l'équation, ce qui s'y traduit par l'annulation du coefficient de tête.

EXEMPLE 2. Le polynôme x^{10} est solution de l'équation

$$10xy'(x) - y(x) = 0.$$

La solution n'a pas de point singulier complexe, mais le complexe $\alpha = 0$ est point singulier de l'équation ; le théorème de Cauchy ne s'y applique pas.

Une autre conséquence utile de ce théorème est que les fonctions D-finies ne peuvent avoir qu'un nombre fini de singularités (les racines du coefficient de tête). Il s'en déduit des résultats négatifs.

EXEMPLE 3. La fonction $1/\sin x$ ne satisfait pas d'équation différentielle linéaire à coefficients polynomiaux.

EXEMPLE 4. La suite des nombres de Bernoulli, qui interviennent en particulier dans la formule d'Euler-Maclaurin, ne peut être solution d'une récurrence linéaire à coefficients polynomiaux, puisque la série génératrice exponentielle

$$\sum_{n=0}^{\infty} B_n \frac{z^n}{n!} = \frac{z}{\exp(z)-1}$$

a une infinité de pôles (aux $2ik\pi$, $k \in \mathbb{Z}^\star$).

Le théorème ci-dessus entraîne aussi la possibilité de développer les solutions en série. Soit

$$\lambda := \min_k(\mathrm{val}(a_k) - k), \quad \mu := \max_k(\deg(a_k) - k),$$

où $\mathrm{val}(p(x))$ désigne le plus grand entier m tel que x^m divise $p(x)$, que l'on appelle la *valuation* de p. Alors les coefficients de l'équation (1) se récrivent

$$a_k(x) = \sum_{i=\lambda}^{\mu} a_{k,i} x^{i+k}.$$

Ceci permet de définir les polynômes

$$u_i(x) = \sum_{k=0}^{n} a_{k,i} x(x-1)\cdots(x-k+1),$$

de sorte que si $y = \sum_{m=-K}^{\infty} y_i x^i$ ($K \in \mathbb{Z}$) est une série de Laurent solution de (1), ses coefficients satisfont la récurrence

$$u_\lambda(i-\lambda)y_{i-\lambda} + \cdots + u_\mu(i-\mu)y_{i-\mu} = 0 \tag{4}$$

pour tout $i \in \mathbb{Z}$ (les y_i d'indice inférieur à $-K$ sont supposés nuls).

Définition 2. Le polynôme u_λ s'appelle *polynôme indiciel* de l'équation (1) à l'origine ; le polynôme u_μ est son *polynôme indiciel à l'infini*.

En changeant la variable x en $x + \alpha$ dans l'équation, le même calcul fournit deux polynômes. C'est un exercice de montrer que le polynôme indiciel à l'infini est inchangé. L'autre s'appelle le polynôme indiciel en α.

Proposition 1. *Si 0 est un point ordinaire pour l'équation (1), alors pour tout $U = (u_0, \ldots, u_{n-1}) \in \mathbb{C}^n$, les coefficients du développement en série de la solution y de (1) telle que $y^{(k)}(0) = u_k$, $k = 0, \ldots, n-1$ sont donnés par la récurrence linéaire (4).*

Démonstration. Il suffit de prouver que le coefficient de tête de la récurrence, à savoir $u_\lambda(i-\lambda)$, ne s'annule pas pour $i - \lambda = n, n+1, \ldots$, ce qui permet alors le calcul de $y_{i+\lambda}$ à partir des précédents. En effet, lorsque l'origine est ordinaire, le coefficient a_n est tel que $a_n(0) \neq 0$ et donc $\mathrm{val}(a_n) - n = -n$ est minimal. Donc $\lambda = n$ et $u_\lambda(x) = a_n(0)x(x-1)\cdots(x-n+1)$, ce qui permet de conclure. □

En effectuant le changement de variable $x \mapsto x + \alpha$, le même raisonnement s'applique à tout point α ordinaire.

3. Solutions polynomiales

S'il existe une solution polynomiale de degré N, l'équation (4) avec $i - \mu = N$ montre que $u_\mu(N) = 0$. Ceci fournit un procédé pour trouver les degrés possibles des solutions polynomiales.

Supposons d'abord que l'origine est un point ordinaire de l'équation. Alors une solution polynomiale est une solution dont le développement en série n'a que des coefficients nuls à partir du degré N. D'après la récurrence (4), il suffit que les coefficients des degrés $N+1$ à $N + \mu - \lambda$ le soient. L'idée est alors de constater que cette observation se ramène à un calcul d'algèbre linéaire. Voici le détail de l'algorithme :

1. Calculer la récurrence (4) ;
2. Calculer la plus grande racine entière positive N de u_μ. Si N n'existe pas, il n'existe pas de solution polynomiale non-nulle ;
3. Pour $0 \leq i \leq n-1$, utiliser la récurrence pour calculer une série solution
$$y_i = x^i + \sum_{j=n}^{N+\mu-\lambda} y_{i,j} x^j + O(x^{N+\mu-\lambda+1});$$
4. Former la matrice $M = [y_{i,j}]$, $0 \leq i < n$, $N+1 \leq j \leq N+\mu-\lambda$;
5. Calculer une base B du noyau de la transposée M^t ;
6. L'ensemble des $c_0 y_0 + \cdots + c_{n-1} y_{n-1}$ pour $(c_0, \ldots, c_{n-1})$ dans B forme une base de l'espace des solutions polynomiales.

Si l'origine n'est pas un point ordinaire de l'équation, il n'est pas garanti que la récurrence (4) permette de calculer les séries solutions. Deux approches sont alors possibles : soit on étend les calculs précédents pour s'adapter au cas singulier, soit, plus simplement, on trouve un point ordinaire (il y en a au moins un parmi $0, 1, \ldots, \deg(a_n)$ et on effectue les calculs en ce point.)

4. Solutions rationnelles

Les solutions rationnelles ne peuvent avoir de pôle (zéro de leur dénominateur) qu'en une singularité de l'équation. De la même manière que pour les degrés des solutions polynomiales, les multiplicités possibles des pôles sont données par les racines entières négatives du polynôme indiciel en ces singularités. Ceci conduit à un algorithme simple, essentiellement dû à Liouville, pour calculer les solutions rationnelles de (1).

1. En toute racine α de a_n :
   - calculer le polynôme indiciel $p_\alpha(n)$;
   - calculer la plus petite racine entière négative N_α de p_α, s'il n'en existe pas, faire $N_\alpha := 0$;
2. Former le polynôme $P = \prod_{a_n(\alpha)=0} (x-\alpha)^{-N_\alpha}$;
3. Effectuer le changement de fonction inconnue $y = Y/P$ et réduire au même dénominateur ;
4. Chercher une base B des solutions polynomiales de cette nouvelle équation. Une base des solutions rationnelles est formée des fractions $\{b/P, b \in B\}$.

La preuve de l'algorithme se réduit à observer que P est un multiple du dénominateur de toute solution rationnelle. Cet algorithme permet également de trouver les solutions rationnelles du système (2), en se ramenant à une équation. Il existe aussi d'autres algorithmes plus directs.

Notes

Les idées de base de l'algorithme de recherche de solutions rationnelles sont dues à Liouville [3] qui donne également une méthode par coefficients indéterminés pour trouver les solutions polynomiales. La présentation qui utilise les récurrences donne un algorithme de même complexité mais fait mieux ressortir la structure du calcul [1].

La recherche de solutions d'équations différentielles linéaires ne s'arrête pas aux solutions rationnelles. En utilisant la théorie de Galois différentielle, il existe une algorithmique sophistiquée de recherche de solutions *liouvilliennes* (c'est-à-dire formées par l'application répétée d'exponentielles, d'intégrales et de prise de racines de polynômes). Les calculs se ramènent à la recherche présentée ici de solutions rationnelles pour des équations (les *puissances symétriques*, voir Ex. 8 pour l'ordre 2) formées à partir de l'équation de départ [4, 5, 6].

Bibliographie

[1] Abramov (Sergei A.), Bronstein (Manuel), and Petkovšek (Marko). – On polynomial solutions of linear operator equations. In Levelt (A. H. M.) (editor), *Symbolic and Algebraic Computation*. pp. 290–296. – ACM Press, New York, 1995. Proceedings of ISSAC'95, July 1995, Montreal, Canada.

[2] Ince (E. L.). – *Ordinary differential equations*. – Dover Publications, New York, 1956, viii+558p. Reprint of the 1926 edition.

[3] Liouville (Joseph). – Second mémoire sur la détermination des intégrales dont la valeur est algébrique. *Journal de l'École polytechnique*, vol. 14, 1833, pp. 149–193.

[4] Marotte (F. M.). – *Les équations différentielles linéaires et la théorie des groupes*. – PhD thesis, Faculté des Sciences de Paris, 1898.

[5] Singer (Michael F.). – Liouvillian solutions of n-th order homogeneous linear differential equations. *American Journal of Mathematics*, vol. 103, n° 4, 1981, pp. 661–682.

[6] Singer (Michael F.) and Ulmer (Felix). – Linear differential equations and products of linear forms. *Journal of Pure and Applied Algebra*, vol. 117/118, 1997, pp. 549–563.

CHAPITRE 4

Solutions rationnelles de récurrences

Résumé

Un petit noyau d'algorithmes relativement simples permet de trouver les solutions polynomiales et rationnelles de récurrences linéaires. La résolution dans ces classes « élémentaires » est la base de toute une algorithmique sur les suites, qui sera étudiée en détail au cours suivant.

Ce cours porte sur la résolution d'une relation de récurrence linéaire en ses solutions polynomiales et rationnelles, c'est-à-dire en ses suites solutions dont le terme général est donné par l'évaluation d'un polynôme, respectivement d'une fraction rationnelle, en l'indice de la suite. La résolution dans ces classes « élémentaires » est la base de toute une algorithmique sur les suites. Au cours 5 l'algorithme de Gosper pour la sommation indéfinie se ramène à des résolutions en solutions rationnelles. Il en est de même pour d'autres applications, telles la résolution de récurrences dans des classes de solutions plus complexes (sommes emboîtées, quotients de sommes), ou encore la désingularisation et la factorisation d'une récurrence.

Les questions de complexité ne sont pas abordées ici. Le corps $\mathbb{K}$ qui est utilisé dans certains énoncés a toujours caractéristique nulle, et on peut penser que $\mathbb{K}$ est le corps $\mathbb{Q}$ sans que cela limite la portée des idées de ce cours. Le terme « constante » est employé pour désigner un élément du corps $\mathbb{K}$: une constante est alors indépendante de l'indice de sommation (k sur les exemples donnés plus haut).

Pour fixer la notation, la récurrence dont on cherche les solutions est

$$Lu(n) = \sum_{k=0}^{m} a_k(n)u(n+k), \tag{1}$$

où les $a_k(n)$ sont des polynômes de $\mathbb{K}[n]$, de degrés au plus d.

1. Solutions polynomiales

Le cœur technique de ce cours est dans cette section, organisée par généralité croissante. Les sections qui suivent, bien plus courtes, montrent l'application de la recherche de solutions polynomiales à la recherche de solutions rationnelles.

1.1. Équation homogène. Il s'agit ici de trouver les polynômes $P(n)$ tels que $LP(n) = 0$. Une première observation simple est que L est une application linéaire de $\mathbb{K}[n]_D$, l'espace vectoriel des polynômes de degré au plus D, dans $\mathbb{K}[n]_{D+d}$, pour tout $D \in \mathbb{N}$. Les noyaux des restrictions de L à $\mathbb{K}[n]_D$ pour $D = 0, 1, \ldots$ forment une suite croissante d'espaces vectoriels stationnaire à partir d'un certain indice D_0. L'algorithme consiste donc à trouver une borne sur cet indice (c'est-à-dire sur le degré maximal des polynômes solutions) et à calculer une base de l'espace correspondant.

Exemple 1. Observons que la récurrence

$$Lu(n) = nu(n+1) - (n+100)u(n) = 0$$

a pour solution le polynôme $u(n) = n(n+1)\cdots(n+99)$ de degré 100. Notre but dans cet exemple est de montrer que l'ensemble des solutions polynomiales de cette récurrence est exactement l'ensemble des multiples de u par une constante.

L'application de l'opérateur L sur un monôme n^d donne

$$Ln^d = (d-100)n^d + \cdots,$$

où les points de suspension correspondent à des termes de degré au plus $d-1$. Par linéarité, un polynôme f de degré d autre que 100 est tel que Lf a aussi degré d. Il s'ensuit que les solutions polynomiales ne peuvent avoir que degré 100, d'où le résultat annoncé.

Cet exemple se généralise. Pour y voir plus clair, il est plus commode de récrire les décalages $u(n+k)$ de la suite initiale en terme de différences finies. Ainsi, on note $\Delta u(n) = u(n+1) - u(n)$ et, par récurrence, $\Delta^{k+1}u(n) = (\Delta^k u)(n+1) - (\Delta^k u)(n)$. La récurrence à annuler prend la forme

$$Lu = \sum_{k=0}^{m} b_k(n)\Delta^k u = 0$$

pour de nouveaux polynômes b_k. L'opérateur Δ fait décroître de 1 exactement le degré des polynômes. Ainsi

$$\deg(\Delta^k P) \leq \max(\deg P - k, 0),$$

avec égalité tant que $\Delta^k P \neq 0$, et donc $\deg(LP) \leq \deg P + \max_k\{\deg(b_k) - k\}$. Soient alors

$$b := \max_k\{\deg(b_k) - k\}, \qquad E := \{\, k \mid \deg(b_k) - k = b \,\}.$$

Ces quantités vont servir à fournir une borne sur le degré des solutions.

Exemple 2. La récurrence de l'exemple précédent se récrit

$$(n\Delta - 100)(u_n) = 0;$$

l'entier b vaut 0 et l'ensemble E est $\{0, 1\}$.

Soit D le degré d'une solution. La discussion distingue deux cas :
— soit $D + b < 0$, et alors $-(b+1)$ est une borne sur D ;
— sinon le coefficient de degré $D + b$ dans $L(n^D + \cdots)$ vaut

$$\sum_{k\in E} \mathrm{lc}(b_k)D(D-1)\cdots(D-k+1),$$

où lc désigne le coefficient de tête (*leading coefficient*). Cette expression, vue comme un polynôme en D, s'appelle *le polynôme indiciel* de la récurrence, lequel est non nul.

Cette discussion mène au résultat suivant.

Proposition 1. *Une borne sur le degré des solutions polynomiales de l'opérateur $L = \sum b_k(n)\Delta^k$ est donnée par le maximum de $-(b+1)$ et de la plus grande racine entière positive du polynôme indiciel de L.*

Un algorithme simple consiste alors à calculer cette borne et à rechercher ensuite les solutions par un calcul d'algèbre linéaire.

EXERCICE 1. Trouver les solutions polynomiales de la récurrence

$$3u(n+2) - nu(n+1) + (n-1)u(n) = 0.$$

1.2. Équation inhomogène. L'opérateur L étant un endomorphisme linéaire de $\mathbb{K}[n]$, l'équation inhomogène $Lu(n) = Q(n)$ ne peut avoir de solutions polynomiales que si Q est un polynôme. La discussion qui précède montre qu'une borne sur le degré de ces solutions est donnée par le maximum de $\deg(Q) - b$ et de la borne obtenue pour la partie homogène. Le reste du calcul est à nouveau réduit à de l'algèbre linéaire en dimension finie. Une autre manière d'aboutir à cette borne consiste à appliquer $\Delta^{\deg Q+1}$ aux deux membres de l'équation inhomogène pour la rendre homogène et appliquer le calcul précédent.

EXERCICE 2. Montrer que pour $\alpha = 0$ la récurrence

$$3u(n+2) - nu(n+1) + (n-1)u(n) = -2(n-\alpha)^3$$

n'a pas de solution, alors que pour $\alpha = 5$, elle en a.

1.3. Équation inhomogène paramétrée. Le problème est ici de trouver s'il existe un polynôme $u(n)$ et des constantes $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ tels que

$$Lu(n) = \lambda_1 Q_1(n) + \cdots + \lambda_k Q_k(n),$$

les polynômes Q_i étant donnés. La borne sur le degré de $u(n)$ vient d'être donnée. Il ne reste qu'à observer que les équations qu'il faut ensuite résoudre sont linéaires non seulement en les coefficients du polynôme, mais aussi en les λ_i. Une fois encore, le problème est ainsi réduit à un calcul d'algèbre linéaire.

EXERCICE 3. Résoudre en (u, λ, μ) la récurrence

$$3u(n+2) - nu(n+1) + (n-1)u(n) = \lambda n^3 + \mu n^2.$$

2. Solutions rationnelles : Algorithme d'Abramov

2.1. Équation homogène. Le problème est maintenant de trouver les solutions rationnelles de l'équation $Lu(n) = 0$. L'algorithme procède en deux temps : d'abord le calcul d'un multiple des dénominateurs des solutions, ensuite un changement de fonction inconnue pour ramener la recherche du numérateur à celle de solutions polynomiales d'une nouvelle équation linéaire, problème qui vient d'être traité.

Pour trouver un multiple du dénominateur, on peut observer que les pôles de $u(n), u(n+1), \dots, u(n+m)$ sont décalés les uns des autres. Si u n'a pas deux pôles différant d'un entier, il ne peut donc y avoir de solution rationnelle que si le dénominateur Q de u vérifie

$$Q(n) \mid a_0(n), \quad Q(n+1) \mid a_1(n), \dots, \quad Q(n+m) \mid a_m(n),$$

et donc dans ce cas un multiple du dénominateur est donné par

$$\operatorname{pgcd}\big(a_0(n), a_1(n-1), \dots, a_m(n-m)\big).$$

En général cependant, il peut y avoir des racines de Q qui diffèrent d'un entier et cet argument n'est plus valable. Or, si α et β sont deux racines de Q telles que $\alpha - \beta = k \in \mathbb{N}$ est maximal, alors nécessairement $a_0(\alpha) = 0$ et $a_m(\beta - m) = 0$. L'algorithme suivant utilise cette idée pour fournir un multiple de Q.

Multiple du dénominateur

Entrée : la récurrence $Lu(n) = 0$, avec L donné par l'équation (1) ;

Sortie : un multiple du dénominateur des solutions rationnelles.

1. Calculer le polynôme
$$R(h) = \operatorname{Res}_n\big(a_0(n+h), a_m(n-m)\big);$$
2. Si R n'a pas de racines dans $\mathbb{N}$, alors renvoyer le polynôme 1 ; sinon, soit $h_1 > h_2 > \cdots > h_m \geq 0$ ses racines entières positives. Initialiser Q à 1, A à $a_0(n)$, B à $a_m(n-m)$;
3. Pour $i = 1, \dots, m$ faire
$$g(n) := \operatorname{pgcd}\big(A(n+h_i), B(n)\big) ;$$
$$Q(n) := g(n)g(n-1)\cdots g(n-h_i)Q(n) ;$$
$$A(n) := A(n)/g(n-h_i) ;$$
$$B(n) := B(n)/g(n) ;$$
4. Renvoyer Q.

Le polynôme dans l'étape (1) est un résultant particulier qui peut se calculer efficacement comme une somme composée.

Il est possible de raffiner un peu cet algorithme pour obtenir des multiples de degré moindre du dénominateur, c'est ce que fait Abramov dans [2] et aussi dans certains cas en tenant compte de tous les a_i dans [1]. Une manière plus directe d'aboutir à ces raffinements à été donnée par van Hoeij [3].

Exercice 4. Trouver les solutions rationnelles des récurrences suivantes :
$$(n+1)u_{n+1} - nu_n = 0,$$
$$(n+1)(n+3)u_{n+2} - 2(n+2)nu_{n+1} + (n-1)(n+1)u_n = 0,$$
$$(n+3)(n+2)(n^2+6n+4)u(n+2) - (n+1)(3n^3+27n^2+64n+48)u(n+1) + 2n^2(n^2+8n+11)u(n) = 0.$$

2.2. Équation inhomogène. Comme pour les solutions polynomiales, l'image d'une fraction rationnelle par L étant une fraction rationnelle, il ne peut y avoir de solution rationnelle de l'équation inhomogène que si le membre droit est rationnel. Dans ce cas, réduire l'équation au même dénominateur mène à une équation pour laquelle un multiple du dénominateur des solutions rationnelles est obtenu en considérant la partie homogène. Après changement de fonction inconnue, le calcul se ramène à la recherche de solutions polynomiales d'une équation inhomogène.

2.3. L'ordre 1. Lorsque la récurrence est d'ordre 1, il est en outre possible de prédire des facteurs du numérateur. En effet, dans la récurrence
$$a(n)u(n+1) + b(n)u(n) = c(n),$$
si b et c ont une racine commune, qui n'est pas un pôle de u et qui n'est pas une racine de a, alors elle est nécessairement racine de $u(n+1)$. De même, si $a(n)$ et $c(n)$ ont une racine commune qui n'est pas un pôle de $u(n+1)$ et qui n'est pas racine de b, alors elle est racine de $u(n)$.

Ces calculs préalables permettent de réduire le degré des coefficients de l'équation dont on recherche ensuite les solutions polynomiales.

2.4. Équation inhomogène paramétrée. Le même argument que ci-dessus mène à une conclusion similaire : un multiple du dénominateur s'obtient par les méthodes du cas homogène, et le changement de fonction inconnue ramène à la résolution d'une équation inhomogène paramétrée.

Bibliographie

[1] Abramov (S. A.). – Rational solutions of linear differential and difference equations with polynomial coefficients. *USSR Computational Mathematics and Mathematical Physics*, vol. 29, n° 11, 1989, pp. 1611–1620. – Translation of the Zhurnal vychislitel'noi matematiki i matematicheskoi fiziki.

[2] Abramov (S. A.). – Rational solutions of linear difference and q-difference equations with polynomial coefficients. In Levelt (A. H. M.) (editor), *Symbolic and Algebraic Computation*. pp. 285–289. – ACM Press, New York, 1995. Proceedings of ISSAC'95, July 1995, Montreal, Canada.

[3] van Hoeij (Mark). – Rational solutions of linear difference equations. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock)*. pp. 120–123. – ACM, New York, 1998.

CHAPITRE 5

Sommation indéfinie et définie de suites hypergéométriques

Résumé

Les algorithmes vus au Cours 4 sont appliqués pour trouver les sommes indéfinies de suites hypergéométriques, pour la recherche de solutions hypergéométriques de récurrences linéaires et pour trouver des sommes définies de suites hypergéométriques.

Voici quelques exemples de sommes dont le traitement algorithmique est détaillé dans ce cours.

$$\sum_{k=1}^{n} \frac{k-1}{k(k+1)} 2^k = \frac{2^{n+1}}{n+1} - 1,$$

$$\sum_{k=0}^{n} \frac{(3k)!}{k!\,(k+1)!\,(k+2)!\,27^k} = \frac{(81n^2+261n+200)(3n+2)!}{40(n+2)!\,(n+1)!\,n!\,27^n} - \frac{9}{2},$$

$${}_2F_1\left(\left.\begin{matrix} a, b \\ c \end{matrix}\right| 1\right) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k k!} = \frac{\Gamma(c-a-b)\Gamma(c)}{\Gamma(c-a)\Gamma(c-b)},$$

$$\sum_{k\in\mathbb{Z}} (-1)^k \binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!\,b!\,c!}.$$

Les deux premières sont calculées à l'aide de sommes *indéfinies*, c'est-à-dire des analogues discrets de la primitive ; pour les deux suivantes, il n'existe pas de somme indéfinie hypergéométrique, mais ces sommes *définies*, où toutes les valeurs possibles de l'indice de sommation sont parcourues, peuvent être calculées automatiquement. Les deux dernières sommes sont classiques ; la première est due à Gauss, la seconde à Dixon. Dans la dernière, on adopte la convention que les binomiaux $\binom{a}{b}$ sont nuls lorsque $b < 0$ ou $b > a$.

Une chaîne complète d'algorithmes permettant de trouver les membres droits des identités ci-dessus est détaillée dans ce cours et dans le suivant.

1. Sommation hypergéométrique indéfinie. Algorithme de Gosper

La recherche de formes closes pour la sommation est souvent naturellement posée en terme de suites hypergéométriques. Après quelques définitions et propriétés de ces suites, nous abordons leur sommation.

1.1. Suites hypergéométriques.

Définition 1. On appelle *suite hypergéométrique* une suite P-récursive vérifiant une récurrence linéaire *d'ordre 1*.

Une telle récurrence, de la forme

$$u_{n+1} = \frac{P(n)}{Q(n)} u_n, \tag{1}$$

où P et Q sont des polynômes admet une solution explicite à l'aide de la fonction Γ. Cette fonction est classiquement définie pour $\Re(z) > 0$ par l'intégrale d'Euler

$$\Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t}\, dt.$$

Une intégration par parties montre l'équation fonctionnelle

$$\Gamma(z+1) = z\Gamma(z).$$

Une première conséquence de cette équation est de fournir un prolongement méromorphe de Γ à $\mathbb{C} \setminus \mathbb{Z}^-$. Grâce à la valeur facile à calculer $\Gamma(1) = 1$, cette équation montre aussi que pour tout entier positif n, $\Gamma(n+1) = n!$. Enfin, l'équation fonctionnelle permet de résoudre la récurrence (1) sous la forme

$$u_n = u_0 \left(\frac{\mathrm{lc}(P)}{\mathrm{lc}(Q)}\right)^n \prod_{P(\alpha)=0} \frac{\Gamma(n-\alpha)}{\Gamma(-\alpha)} \prod_{Q(\beta)=0} \frac{\Gamma(-\beta)}{\Gamma(n-\beta)},$$

où $\mathrm{lc}(p)$ désigne le coefficient de tête du polynôme p.

Cette formule est valable tant que les valeurs des points où est évaluée Γ ne sont pas des entiers négatifs ou nuls, c'est-à-dire pour $\alpha \notin \mathbb{N}$ et $\beta \notin \mathbb{N}$. Elle continue d'être valable lorsque $\alpha \in \mathbb{N}$ à condition d'interpréter le premier quotient comme une limite : d'après l'équation fonctionnelle, pour k et n deux entiers positifs ou nuls,

$$\lim_{s \to k} \frac{\Gamma(n-s)}{\Gamma(-s)} = \begin{cases} 0, & \text{si } n > k\,; \\ (-1)^n \frac{k!}{(k-n)!}, & \text{si } n \leq k. \end{cases}$$

Cette limite correspond bien à ce qui est attendu : si $k \in \mathbb{N}$ est une racine de P, alors $u_{k+1} = 0$ et par suite $u_n = 0$ pour $n > k$.

Lorsque $\beta \in \mathbb{N}$, la même limite peut être utilisée tant que $n \leq \beta$, et la suite cesse d'être définie pour $n > \beta$.

Les suites hypergéométriques jouent un rôle important en analyse classique, où elles apparaissent comme coefficients de Taylor des séries introduites par la définition suivante.

Définition 2. On appelle *série hypergéométrique généralisée* et on note

$${}_pF_q\left(\left.\begin{matrix} a_1, \ldots, a_p \\ b_1, \ldots, b_q \end{matrix}\right| x\right)$$

la série

$$\sum_{n \geq 0} \frac{(a_1)_n \cdots (a_p)_n}{(b_1)_n \cdots (b_q)_n} \frac{x^n}{n!},$$

où la notation $(a)_n$ représente le produit $a(a-1)\cdots(a-n+1)$.

Des cas particuliers de séries qui s'expriment à l'aide de séries hypergéométriques généralisées sont les séries $\exp(x)$, $\log(1+x)$, les dilogarithmes et polylogarithmes, les fonctions J_ν de Bessel, les fonctions d'Airy, etc.

Exercice 1. Récrire l'identité de Dixon en terme de valeur d'une ${}_3F_2$ en 1.

1.2. Algorithme de Gosper. Étant donnée une suite hypergéométrique $u(n)$, le problème de sommation indéfinie hypergéométrique de $u(n)$ consiste à déterminer s'il existe une autre suite hypergéométrique $U(n)$ telle que $U(n+1)-U(n)=u(n)$ et si oui, la calculer.

Une observation simple est formulée dans le lemme suivant.

LEMME 1. *Si $U(n)$ est une suite hypergéométrique et L un opérateur de récurrence linéaire à coefficients polynomiaux, alors il existe une fraction rationnelle $r(n)$ telle que $LU(n)=r(n)U(n)$.*

DÉMONSTRATION. $r(n)$ n'est autre que le reste de la division euclidienne de L par le polynôme unitaire de degré 1 donnant la récurrence qui annule $U(n)$. Plus explicitement, si $U(n)$ est hypergéométrique, par définition, il existe une fraction rationnelle $R(n)$ telle que $U(n+1)=R(n)U(n)$ et donc par récurrence $U(n+k)=R(n+k-1)\cdots R(n)U(n)$ pour tout k. Le résultat s'en déduit additionnant les contributions. □

Ce lemme entraîne qu'une somme hypergéométrique $U(n)$ de $u(n)$ doit être le produit de $u(n)$ par une fraction rationnelle $R(n)$. Diviser la récurrence $U(n+1)-U(n)=u(n)$ par $u(n)$ réduit alors le calcul à celui de la recherche de solutions rationnelles de l'équation inhomogène

$$R(n+1)\frac{u(n+1)}{u(n)}-R(n)=1, \tag{2}$$

d'ordre 1, problème traité dans la section précédente, particulièrement en 2.3. L'algorithme ainsi obtenu est connu sous le nom d'algorithme de Gosper [**3**].

EXERCICE 2. Calculer une somme indéfinie de $\frac{2^k(k-1)}{k(k+1)}$.

EXEMPLE 1. L'algorithme de Gosper permet également de donner des réponses négatives. Voici en détail comment il permet de prouver par l'absurde que $\sum_{k=1}^{n}1/k!$ n'est pas hypergéométrique.

Si $S(n)$ est une telle somme, elle doit être le produit de $1/n!$ par une fraction rationnelle $r(n)$. Cette fraction satisfait donc la récurrence

$$S(n+1)-S(n)=\frac{1}{(n+1)!}=\frac{r(n+1)}{(n+1)!}-\frac{r(n)}{n!}.$$

En chassant les dénominateurs, il reste

$$r(n+1)-(n+1)r(n)=1.$$

Le résultat de l'algorithme « Multiple du dénominateur » d'Abramov montre que r doit être un polynôme : les pôles de plus petite partie réelle de r doivent être annulés par 1. Enfin, r ne peut pas non plus être un polynôme : son terme de plus haut degré ne disparaît pas par évaluation de la récurrence.

1.3. Sommation paramétrée. Étant données k suites hypergéométriques $u_1(n),\dots,u_k(n)$, il s'agit de déterminer, si elles existent, une suite hypergéométrique $S(n)$ et des constantes $\lambda_1,\dots,\lambda_k$ telles que

$$S(n+1)-S(n)=\lambda_1u_1(n)+\cdots+\lambda_ku_k(n).$$

D'après la discussion précédente, si $\lambda_i\lambda_j\neq 0$ alors u_i et u_j sont similaires au sens où $u_i(n)/u_j(n)$ est rationnel. Il suffit donc de considérer le cas où tous les u_i sont similaires à une même suite $u(n)$. Dans ce cas, le membre droit de (2) est remplacé

par une combinaison linéaire des λ_i à coefficients des fractions rationnelles et la méthode de la section précédente s'applique.

2. Sommation hypergéométrique définie. Algorithme de Zeilberger

Les suites considérées dans cette section sont hypergéométriques en deux variables, c'est-à-dire que

$$\frac{u(n+1,k)}{u(n,k)} \quad \text{et} \quad \frac{u(n,k+1)}{u(n,k)}$$

sont deux fractions rationnelles en n et k. Le problème de sommation définie hypergéométrique est de déterminer si

$$U(n) = \sum_k u(n,k)$$

est hypergéométrique et si oui, le trouver. La somme porte sur toutes les valeurs $k \in \mathbb{Z}$, étant entendu que bien souvent ces sommes ont en fait un support fini. Plus précisément, l'intervalle de sommation s'arrête aux *bornes naturelles* de sommation, indices où par hypothèse la suite et toutes ses décalées par rapport à l'autre indice (n) s'annulent.

Exemple 2. Des sommes simples traitées par cet algorithme sont

$$\sum_k \binom{n}{k} = 2^n, \quad \sum_k \binom{n}{k}^2 = \binom{2n}{n}.$$

Dans ces deux exemples, en dehors de $k \in \{0, \dots, n\}$, les binomiaux sont nuls.

Du point de vue de la P-récursivité, il n'est pas seulement utile de déterminer $U(n)$ s'il est hypergéométrique, mais plus généralement de trouver une récurrence linéaire à laquelle il obéit. C'est ce que réalise l'algorithme de Zeilberger. Trouver si la somme est hypergéométrique se ramène alors à la recherche de solutions hypergéométriques de récurrences linéaires, problème qui est traité par l'algorithme de Petkovšek dans la section suivante.

2.1. Principe de la création téléscopique. On cherche un opérateur

$$(S_k - 1)Q(n,k,S_n,S_k) - P(n,S_n) \tag{3}$$

qui annule la suite $u(n,k)$ à sommer (S_n et S_k désignent les opérateurs de décalage en n et k, $S_n u(n,k) = u(n+1,k)$ et $S_k u(n,k) = u(n,k+1)$). Une fois un tel opérateur trouvé, la sommation sur k est aisée, et l'hypothèse de bornes naturelles conduit à l'égalité

$$P(n,S_n)U(n) = 0.$$

Exemple 3. En suivant ce modèle, voici une preuve compliquée que

$$U(n) = \sum_k \binom{n}{k} = 2^n.$$

Le point de départ est l'opérateur de l'identité du triangle de Pascal

$$S_n S_k - S_k - 1,$$

qui se récrit

$$(S_k - 1)(S_n - 1) + (S_n - 2).$$

En termes plus explicites, cet opérateur se traduit

$$\binom{n+1}{k+1} - \binom{n+1}{k} - \binom{n}{k+1} + \binom{n}{k} + \binom{n+1}{k} - 2\binom{n}{k} = 0.$$

En sommant sur $k \in \mathbb{Z}$, les premiers termes se téléscopent deux à deux, et il reste

$$U(n+1) - 2U(n) = 0.$$

La fin de la preuve provient de la condition initiale $S(0) = 1$.

2.2. Algorithme de Zeilberger. Il reste à voir comment trouver les opérateurs P et Q de l'équation (3) dans le cas général. L'idée de Zeilberger est que cette équation

$$P(n, S_n)u(n,k) = (S_k - 1)Q(n, k, S_n, S_k)u(n,k)$$

signifie que Qu est une somme hypergéométrique *indéfinie* de $P(n, S_n)u$ par rapport à k.

L'algorithme procède alors incrémentalement sur le degré de P en S_n. Pour $m = 1, 2, \ldots$, il faut chercher s'il existe des $\lambda_i(n)$ (les coefficients de P) tels que

$$\lambda_1(n)u(n,k) + \lambda_2(n)u(n+1,k) + \cdots + \lambda_m(n)u(n+m,k)$$

ait une somme hypergéométrique. L'algorithme pour cela a été présenté dans la section précédente.

2.3. Terminaison. L'algorithme ne termine pas en général. Les premiers, Wilf et Zeilberger ont délimité une classe importante, les suites *proprement hypergéométriques* sur lesquelles la terminaison et par conséquent le succès sont garantis. Ces suites sont de la forme

$$u(n,k) = P(n,k)Z^k \frac{\prod_{i=1}^{\ell}(a_i n + b_i k + c_i)!}{\prod_{i=1}^{m}(u_i n + v_i k + d_i)!},$$

où les a_i, b_i, u_i et v_i sont des *entiers*, ℓ et m sont des entiers positifs, P est un polynôme et Z une constante.

PROPOSITION 1. *L'algorithme de Zeilberger termine si $u(n,k)$ est proprement hypergéométrique.*

La preuve est un peu longue et n'a pas été abordée dans le cours. L'idée est de prouver un résultat légèrement plus fort, à savoir l'existence d'un polynôme $A(n, S_k, S_n)$ qui ne dépend pas de k et annule $u(n,k)$. Une division euclidienne de A par $S_k - 1$ permet d'en déduire un couple (P, Q) tel que l'opérateur (3) annule $u(n,k)$ *et de plus* Q ne dépend pas de k. L'existence de A est obtenue en considérant les monômes en n, S_n, S_k par degré total croissant et leur action sur $u(n,k)$. L'application de ces monômes sur $u(n,k)$ produit un multiple rationnel de $u(n,k)$. Comme les coefficients a_i, b_i, u_i et v_i sont des entiers, le nombre de nouveaux facteurs de ces fractions rationnelles finit par croître moins vite que le nombre de monômes, et il s'ensuit l'existence d'une relation de liaison. La partie technique de la preuve se concentre donc sur l'étude soigneuse des facteurs de ces fractions rationnelles et de leur nombre.

Cette proposition ne donne qu'une condition suffisante pour l'existence d'un $P(n, S_n)$ et conséquemment pour la terminaison de l'algorithme de Zeilberger. Il existe des suites qui ne sont pas proprement hypergéométriques et pour lesquelles l'algorithme fonctionne quand même. Cela a donné lieu à une série de travaux,

et le dernier mot revient à un travail récent d'Abramov [1] où il donne un test algorithmique de terminaison de l'algorithme.

3. Solutions hypergéométriques. Algorithme de Petkovšek

Si $Lu(n) = 0$ avec $u(n)$ hypergéométrique, il existe deux polynômes P et Q satisfaisant

$$u(n+1) = \frac{P(n)}{Q(n)} u(n),$$

et on peut prendre Q unitaire. Le reste de la division euclidienne de L par $S_n - P/Q$, une fois réduit au même dénominateur donne une condition nécessaire et suffisante d'existence de solution hypergéométrique. Ce reste s'écrit

$$\begin{aligned}(4)\quad & a_m(n)P(n+m-1)P(n+m-2)\cdots P(n) \\ & \quad + a_{m-1}(n)Q(n+m-1)P(n+m-2)\cdots P(n) \\ & \qquad + \cdots + a_0(n)Q(n+m-1)\cdots Q(n) = 0.\end{aligned}$$

Si on savait prédire que $\operatorname{pgcd}\big(P(n), Q(n+i)\big) = 1$ pour $i = 0, \ldots, m-1$, alors on en déduirait facilement que $P(n)$ divise $a_0(n)$ et $Q(n+m-1)$ divise $a_m(n)$. Ceci nous donnerait un algorithme : toute paire de facteurs unitaires de $a_0(n)$ et $a_m(n-m+1)$ donne un candidat pour $Q(n)$ et un candidat pour P à une constante près, il suffit alors d'injecter ces candidats dans (4) et chercher s'il existe une constante permettant de satisfaire l'équation. En bouclant sur les facteurs de a_0 et a_m, le travail est terminé.

En général, il se peut très bien que $P(n)$ et $Q(n+i)$ aient des facteurs communs. La solution trouvée par Petkovšek consiste à recourir à une décomposition plus forte de la fraction rationnelle. On cherche une solution telle que

$$\frac{u(n+1)}{u(n)} = Z \frac{A(n)}{B(n)} \frac{C(n+1)}{C(n)},$$

où Z est une constante, A, B, C sont des polynômes unitaires, $\operatorname{pgcd}(A, C) = 1$, $\operatorname{pgcd}\big(B(n), C(n+1)\big) = 1$ et $\operatorname{pgcd}\big(A(n), B(n+i)\big) = 1$ pour tout $i \in \mathbb{N}$. Cette décomposition des fractions rationnelles est parfois appelée décomposition de Gosper-Petkovšek.

Exercice 3. Montrer que toute fraction rationnelle peut se décomposer sous la forme ci-dessus. Donner un algorithme calculant les polynômes A, B, C et la constante Z correspondant à une fraction rationnelle donnée en entrée. (Indice : s'inspirer de l'algorithme d'Abramov.)

Avec cette décomposition, l'équation (4) devient

$$\begin{aligned}(5)\quad & Z^m a_m(n)A(n+m-1)\cdots A(n)C(n+m) + \\ & \quad Z^{m-1} a_{m-1}(n)B(n+m-1)A(n+m-2)\cdots A(n)C(n+m-1) \\ & \qquad + \cdots + a_0(n)B(n+m-1)\cdots B(n)C(n) = 0.\end{aligned}$$

Les contraintes de la décomposition permettent de déduire immédiatement

$$A(n) | a_0(n), \qquad B(n+m-1) | a_m(n).$$

L'algorithme de Petkovšek s'en déduit : pour chaque paire (A, B) de facteurs de a_0 et a_m, le coefficient de tête du polynôme membre gauche de (5) donne une équation

polynomiale sur Z, une fois Z ainsi fixé, il reste à chercher les solutions polynomiales C de l'équation, s'il en existe.

Exercice 4. Résoudre ainsi

$$(n-1)u(n+2) - (n^2+3n-2)u(n+1) + 2n(n+1)u(n) = 0,$$
$$u(n+2) - (2n+1)u(n+1) + (n^2-2)u(n) = 0.$$

Bien qu'il n'ait pas été traité ici, le cas inhomogène n'est pas difficile : le membre droit doit être hypergéométrique et, outre les solutions hypergéométriques de la partie homogène, la solution doit être le produit du membre droit par une fraction rationnelle. Ceci ramène le problème à la recherche de solutions rationnelles.

Notes

Le livre [4] est une bonne introduction aux questions abordées dans ce cours. L'algorithme de Petkovšek possède des extensions intéressantes, par réduction de l'ordre, à une classe plus large de solutions, appelées *solutions d'Alembertiennes*. Ces extensions n'ont pas été décrites dans le cours, elle le sont dans [2].

De nombreuses généralisations de l'algorithme de Zeilberger sont possibles : par exemple la suite à sommer peut ne pas être hypergéométrique, tout en étant toujours P-récursive, ou il peut s'agir d'une suite de fonctions D-finies et l'on cherche une équation différentielle satisfaite par la somme définie, etc. Ces questions seront abordées dans un chapitre ultérieur du cours.

Bibliographie

[1] Abramov (S. A.). – When does Zeilberger's algorithm succeed ? *Advances in Applied Mathematics*, vol. 30, n° 3, 2003, pp. 424–441.

[2] Abramov (Sergei A.) and Petkovšek (Marko). – D'alembertian solutions of linear differential and difference equations. In *Proceedings of the international symposium on Symbolic and algebraic computation*. pp. 169–174. – ACM Press, 1994.

[3] Gosper (R. William). – Decision procedure for indefinite hypergeometric summation. *Proceedings of the National Academy of Sciences USA*, vol. 75, n° 1, January 1978, pp. 40–42.

[4] Petkovšek (Marko), Wilf (Herbert S.), and Zeilberger (Doron). – $A = B$. – A. K. Peters, Wellesley, MA, 1996, xii+212p.

CHAPITRE 6

Équations fonctionnelles linéaires et polynômes tordus

Résumé

Une certaine variété de polynômes non commutatifs fournit une représentation unifiée pour une large classe d'équations fonctionnelles linéaires. Celle-ci s'avère bien adaptée pour les calculs. Nous réinterprétons nombre des algorithmes vus dans ce cours dans ce point de vue.

1. Des polynômes non commutatifs pour calculer avec des opérateurs linéaires

Dans les années 1930, le mathématicien Oystein Ore (1899–1968) s'est intéressé à la résolution de systèmes linéaires reliant des dérivées $f_i^{(j)}(x)$, des décalées $f_i(x+j)$, ou les substitutions $f_i(q^j x)$ de fonctions inconnues $f_i(x)$. À cette fin, il a introduit de nouvelles familles de polynômes en une variable ayant la propriété que cette variable ne commute pas avec les coefficients des polynômes. Ce défaut de commutativité reflète une sorte de loi de Leibniz.

Rappelons la relation de Leibniz pour deux fonctions quelconques f et g :

$$(fg)'(x) = f'(x)g(x) + f(x)g'(x).$$

En notant D l'opérateur de dérivation, M celui qui à une fonction f associe la fonction donnée par $M(f)(x) = xf(x)$, I l'opérateur identité sur les fonctions, et $\circ$ la composition d'opérateurs, la règle de Leibniz donne, pour $f(x) = x$ et g quelconque,

$$(D \circ M)(g) = D\big(M(g)\big) = M\big(D(g)\big) + g = (M \circ D + I)(g).$$

L'identité étant vérifiée par toute g, on obtient l'égalité $D \circ M = M \circ D + I$ entre opérateurs linéaires différentiels. D'autres opérateurs vérifient des analogues de la règle de Leibniz : l'opérateur Δ de différence finie, donné par $\Delta(f)(x) = f(x+1) - f(x)$; l'opérateur $S = \Delta + I$ de décalage, donné par $S(f)(x) = f(x+1)$; pour une constante q fixée autre que 0 et 1, l'opérateur H de dilatation, donné par $H(f)(x) = f(qx)$. On a les relations :

$$\Delta(fg)(x) = f(x+1)\Delta(g)(x) + \Delta(f)(x)g(x),$$
$$(fg)(x+1) = f(x+1)g(x+1), \qquad (fg)(qx) = f(qx)g(qx),$$

qui mènent aux relations $\Delta \circ M = (M + I) \circ \Delta + I$, $S \circ M = (M + I) \circ S$, $H \circ M = Q \circ M \circ H$ entre opérateurs linéaires, après avoir introduit un nouvel opérateur Q donné par $Q(f)(x) = qf(x)$.

Le point de vue d'Ore est d'abstraire ces différents contextes d'opérateurs dans un même moule algébrique.

Définition. *Soit A un anneau commutatif unitaire de caractéristique zéro, que nous supposons muni d'un endomorphisme injectif σ et d'une σ-dérivation δ, au sens où pour tout a et tout b de A,*

$$\sigma(a+b) = \sigma(a) + \sigma(b), \qquad \sigma(ab) = \sigma(a)\sigma(b), \qquad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

Pour une nouvelle variable ∂, on appelle anneau de polynômes tordus *l'algèbre sur A engendrée par ∂ et les relations, pour tout a de A,*

$$\partial a = \sigma(a)\partial + \delta(a).$$

On note cet anneau $A\langle\partial; \sigma, \delta\rangle$.

(La terminologie « polynôme tordu » est la traduction de l'anglais « *skew polynomial* », où « skew » signifie « de biais », « oblique ». Certains auteurs ont proposé la traduction « polynôme gauche », où « gauche » a le sens de « voilé », par opposition à « plan ». Mais nous voulons éviter ici toute confusion avec des notions algébriques de multiple, module, fraction, etc, pour lesquelles « gauche » a le sens opposé de « droite ».)

Des choix adéquats de σ et δ nous font retrouver les quelques exemples donnés plus haut. Pour simplifier la notation, nous supposons que A peut s'identifier à un bon espace de fonctions. On a alors, en notant 0 l'application qui à toute fonction associe la fonction constante nulle :

- $\mathbb{Q}(x)\langle\partial; I, D\rangle$ représente l'algèbre des opérateurs différentiels linéaires ;
- $\mathbb{Q}(x)\langle\partial; S, 0\rangle$ représente l'algèbre des opérateurs de récurrence ;
- $\mathbb{Q}(x)\langle\partial; S, \Delta\rangle$ représente l'algèbre des opérateurs de différence finie ;
- $\mathbb{Q}(x)\langle\partial; H, 0\rangle$ pour $q \in \mathbb{Q}(x) \setminus \{0, 1\}$ représente l'algèbre des opérateurs de q-dilatation ;
- $\mathbb{Q}(x)\langle\partial; I, 0\rangle$ n'est autre que l'anneau commutatif $\mathbb{Q}(x)[\partial]$ des polynômes usuels.

Toutes ces algèbres d'opérateurs sont à coefficients dans $\mathbb{Q}(x)$; on dispose aussi d'analogues pour $A = \mathbb{Q}[x]$ et $A = \mathbb{Q}[x, x^{-1}]$.

On fera attention à la notation. Si la composition entre opérateurs est notée par $\circ$, nous ne ferons qu'une simple juxtaposition pour le produit de polynômes tordus, et nous noterons 1 l'élément neutre pour le produit de polynômes tordus. Néanmoins, on fera l'abus de notation de noter de la même façon, D_x, la dérivation par rapport à x quel que soit l'anneau A, et I, sans indice, pour l'identité de n'importe quel A. De plus, nous noterons simplement x pour M. Ainsi, on a :

- $\partial x = x\partial + 1$ dans $\mathbb{Q}(x)\langle\partial; I, D\rangle$;
- $\partial x = (x+1)\partial$ dans $\mathbb{Q}(x)\langle\partial; S, 0\rangle$;
- $\partial x = (x+1)\partial + 1$ dans $\mathbb{Q}(x)\langle\partial; S, \Delta\rangle$;
- $\partial x = qx\partial$ dans $\mathbb{Q}(x)\langle\partial; H, 0\rangle$;
- $\partial x = x\partial$ dans $\mathbb{Q}(x)\langle\partial; I, 0\rangle = \mathbb{Q}(x)[\partial]$.

Le cas $\delta = 0$ est fréquent, et on écrit alors $A\langle\partial; \sigma\rangle$, sans référence au 0. De même que dans le cas commutatif on définit les polynômes de Laurent, dont l'algèbre est notée $A[X, X^{-1}]$, et dans laquelle $XX^{-1} = X^{-1}X = 1$, le cas où σ est inversible et autre que l'identité permet de représenter des opérateurs qui possèdent un inverse. Dans ce cas, on notera $A\langle\partial, \partial^{-1}; \sigma\rangle$ l'algèbre où $\partial a = \sigma(a)\partial$, $\partial^{-1}a = \sigma^{-1}(a)\partial^{-1}$, $\partial\partial^{-1} = \partial^{-1}\partial = 1$.

Pour finir de se détacher de la notation en termes d'opérateurs, on fait agir les anneaux de polynômes tordus sur les espaces de fonctions, au sens de l'action d'un anneau sur un module. Rappelons qu'un module M sur un anneau A est

un ensemble non vide, muni d'une loi + en faisant un groupe additif, stable sous l'action d'une produit externe par les éléments de A, tel que l'action par produit externe par 1 soit l'identité, et vérifiant les formules $(PQ)\cdot f = P\cdot(Q\cdot f)$ et $(P+Q)\cdot f = (P\cdot f)+(Q\cdot f)$. Un anneau de polynômes tordus n'a pas d'action unique sur un espace de fonctions donné, mais dans la suite de ce texte, nous adoptons les conventions qu'un anneau de la forme $A\langle\partial;\sigma\rangle$ agit par $\partial\cdot f = \sigma(f)$ pour une extension convenable de σ, qu'un anneau de la forme $A\langle\partial;\sigma,\delta\rangle$ agit par $\partial\cdot f = \delta(f)$ pour une extension convenable de δ, et que les coefficients dans A agissent par simple multiplication, $a\cdot f = af$.

Munis de cette notation générique, nous allons maintenant réexprimer des algorithmes déjà vus et petit à petit introduire de nouveaux calculs.

2. Clôtures par morphismes entre anneaux de polynômes tordus

Dans cette section, nous sommes amenés à considérer simulanément des fonctions de x et des fonctions d'une autre variable. Aussi indiquerons-nous en indice de D, S, ∂, σ, δ, etc, la variable à laquelle ces objets font référence. De plus, les anneaux A qui servent à construire les anneaux de polynômes tordus sont de la forme $\mathbb{Q}[x]$ ou $\mathbb{Q}[x,x^{-1}]$.

2.1. Récurrence sur les coefficients extraits d'une série D-finie et série génératrice d'une suite P-récursive. On a déjà vu que lorsqu'une série $f=\sum_{n\geq 0}u_n x^n$ est D-finie, ses coefficients vérifient une relation de récurrence finie, autrement dit, que la suite $c=(u_n)_{n\geq 0}$ est P-récursive. La preuve repose sur les identités

$$xf = \sum_{n\geq 1} u_{n-1}x^n = \sum_{n\geq 1}(\partial_n^{-1}\cdot c)(n)\,x^n$$

et

$$D_x(f) = f' = \sum_{n\geq 0}(n+1)u_{n+1}x^n = \sum_{n\geq 0}\big((n+1)\partial_n\cdot c\big)(n)\,x^n,$$

où nous avons introduit l'anneau $\mathbb{Q}[n]\langle\partial_n,\partial_n^{-1};S_n\rangle$. Par récurrence, ceci donne

$$\begin{aligned} x^\alpha D_x^\beta(f) &= \sum_{n\geq\alpha}\Big(\partial_n^{-\alpha}\big((n+1)\partial_n\big)^\beta\cdot c\Big)(n)\,x^n \\ &= \sum_{n\geq\alpha}\big((n+1-\alpha)\cdots(n+\beta-\alpha)\partial_n^{\beta-\alpha}\cdot c\big)(n)\,x^n. \end{aligned}$$

Pour une série f solution de l'équation différentielle

$$a_r(x)f^{(r)}(x)+\cdots+a_0(x)f(x)=0$$

où les a_i sont dans $\mathbb{Q}[x]$, nous obtenons ainsi une récurrence sur c, valable pour des n assez grands. Cette récurrence s'exprime en termes de polynômes tordus de la façon suivante. On représente l'opérateur différentiel associé à l'équation par le polynôme tordu $L=a_r(x)\partial_x^r+\cdots+a_0(x)$ dans $\mathbb{Q}[x]\langle\partial_x;I,D_x\rangle$ sur $\mathbb{Q}$. De la sorte, l'équation différentielle s'écrit $L\cdot f=0$. On introduit aussi l'algèbre $\mathbb{Q}[n]\langle\partial_n,\partial_n^{-1};S_n\rangle$ et le morphisme d'algèbres μ défini par $\mu(x)=\partial_n^{-1}$ et $\mu(\partial_x)=(n+1)\partial_n$. Alors, la

suite c des coefficients satisfait à la récurrence représentée par l'image $\mu(L)$. Pour comprendre pour quels n cette récurrence est valide, écrivons

$$\mu(L) = b_p(n)\partial_n^p + \cdots + b_q(n)\partial_n^q$$

pour $p \leq q$ et $b_p b_q \neq 0$. Alors, la récurrence prend la forme

$$\big(\mu(L)\cdot u\big)(n) = b_p(n)u_{n+p} + \cdots + b_q(n)u_{n+q} = 0$$

et est vérifiée pour tout n si $p \geq 0$ et pour tout $n \geq -p$ si $p < 0$.

De façon duale, une suite P-récursive u a une série génératrice $f = \sum_{n\geq 0} u_n x^n$ D-finie, ce que nous allons retrouver en termes de polynômes tordus. Pour ce point, nous supposons en fait que la suite u est prolongée aux indices négatifs par $u_n = 0$ pour $n < 0$, et qu'elle est P-récursive sur $\mathbb{Z}$ tout entier. Ceci ne constitue aucune perte de généralité : une récurrence valable pour la suite initiale devient valable pour la suite prolongée après multiplication par un polynôme de la forme $(n+1)(n+2)\dots(n+r)$. Les formules

$$\sum_{n\in\mathbb{Z}} n u_n x^n = x\partial_x \cdot f \qquad \text{et} \qquad \sum_{n\in\mathbb{Z}} u_{n+1}x^n = x^{-1}f$$

donnent par récurrence

$$\sum_{n\geq 0} n^\alpha u_{n+\beta}x^n = (x\partial_x)^\alpha x^{-\beta}\cdot f = x^{-\beta}(x\partial_x - \beta)^\alpha \cdot f,$$

et fournissent un autre morphisme, ν, de $\mathbb{Q}[n]\langle\partial_n; S_n\rangle$ dans $\mathbb{Q}[x,x^{-1}]\langle\partial_x; I, D_x\rangle$, donné par $\nu(n) = x\partial_x$ et par $\nu(\partial_n) = x^{-1}$. Pour une suite u solution de l'équation de récurrence

$$b_p(n)u_{n+r} + \cdots + b_0(n)u_n = 0$$

où les b_i sont dans $\mathbb{Q}[n]$, nous introduisons le polynôme tordu $P = b_p(n)\partial_n^r + \cdots + b_0(n)$ de $\mathbb{Q}[n]\langle\partial_n; S_n\rangle$. Pour obtenir une relation différentielle sur la série génératrice f, nous considérons $\nu(P)$ que nous écrivons

$$\nu(P) = a_0(x) + \cdots + a_r(x)\partial_x^r.$$

Alors la série f satisfait à la relation différentielle

$$a_0(x)f(x) + \cdots + a_r(x)f^{(r)}(x) = 0.$$

Algébriquement, les propriétés précédentes s'expriment par le fait que μ s'étend en un isomorphisme d'algèbres entre $\mathbb{Q}[x,x^{-1}]\langle\partial_x; I, D_x\rangle$ et $\mathbb{Q}[n]\langle\partial_n, \partial_n^{-1}; S_n\rangle$, dont l'inverse étend ν.

2.2. Séries binomiales.

Exercice 1. Une série binomiale est une série de la forme $\sum_{n\geq 0} u_n \binom{x}{n}$. Montrer que les solutions en série binomiale d'une équation fonctionnelle à différence

$$a_r(x)f(x+r) + \cdots + a_0(x)f(x) = 0$$

ont des coefficients u_n qui vérifient une récurrence et expliciter le morphisme entre algèbres de polynômes tordus correspondant.

2.3. Changements de variables. Lorsqu'une série D-finie $f(x)$ est solution d'une équation différentielle $L \cdot f = 0$ donnée par un polynôme tordu

$$L = L(x, \partial_x) = a_r(x)\partial_x^r + \cdots + a_0(x),$$

la série $f(\lambda x)$ est solution de l'équation différentielle associée à

$$L(\lambda x, \lambda^{-1}\partial_x) = a_r(\lambda x)\lambda^{-r}\partial_x^r + \cdots + a_0(\lambda x),$$

ce qui est encore le résultat d'un morphisme d'algèbres.

Lorsque f est une fonction D-finie, la fonction $z \mapsto f(1/z)$ est elle aussi D-finie, en z cette fois, pour autant que la fonction composée ait un sens. En effet, pour toute fonction g, notons $\tilde{g}(z) = g(1/z)$ (avec la même réserve de définition). Puisque $g(x) = \tilde{g}(1/x)$, par dérivation on a $g'(x) = -\tilde{g}'(1/x)/x^2$, ce qui est l'évaluation en $z = 1/x$ de $-z^2\partial_z \cdot \tilde{g}$. Autrement dit, on a $\widetilde{g'} = -z^2\partial_z \cdot \tilde{g}$, d'où par récurrence $\widetilde{g^{(\beta)}} = (-z^2\partial_z)^\beta \cdot \tilde{g}$. Ainsi, $\tilde{f}$ est D-finie, donnée comme vérifiant l'équation différentielle associée à l'image de L par le morphisme de $\mathbb{Q}[x]\langle\partial_x; I, D_x\rangle$ dans $\mathbb{Q}[z, z^{-1}]\langle\partial_z; I, D_z\rangle$ qui envoie x sur z^{-1} et ∂_x sur $-z^2\partial_z$.

Exercice 2. Plus généralement, la fonction obtenue par substitution rationnelle de la variable, donnée par $h(u) = f\big(r(u)\big)$, est encore D-finie. Nous laissons en exercice le soin de montrer ce résultat par la même approche dans le cas où la dérivée r' s'exprime comme une fraction rationnelle en r.

3. Division euclidienne

Dans cette section et les suivantes, nous nous appuyons sur des propriétés particulières des anneaux de polynômes tordus quand l'anneau A de la construction est un corps, que nous prendrons de la forme $\mathbb{Q}(x)$.

La commutation $\partial a = \sigma(a)\partial + \delta(a)$ dans $\mathbb{Q}(x)\langle\partial; \sigma, \delta\rangle$ permet d'écrire tout polynôme tordu sous la forme $a_0(x)+\cdots+a_r(x)\partial^r$, pour des fractions rationnelles a_i de $\mathbb{Q}(x)$ uniques. Une conséquence de l'injectivité de σ est l'existence d'un degré en ∂ bien défini, étant l'entier r de l'écriture précédente lorsque a_r est non nulle. En particulier, le degré d'un produit L_1L_2 de polynômes tordus est la somme des degrés des L_i. Il s'ensuit que la division euclidienne du cas commutatif, et toute la théorie qui en découle, se transpose avec peu d'altérations dans le cas tordu.

La différence principale avec le cas commutatif est qu'on distingue division euclidienne à gauche et division euclidienne à droite. Vu notre interprétation en termes d'opérateurs linéaires, nous ne considèrerons que la division à droite, qui se fait en retranchant des multiples à gauche. Soit à diviser $A = a_r(x)\partial^r + \cdots + a_0(x)$ de degré r par $B = b_s(x)\partial^s + \cdots + b_0(x)$ de degré s. On suppose $s \leq r$. Alors,

$$\partial^{r-s}B = \sigma^{r-s}\big(b_s(x)\big)\partial^r + \text{termes d'ordre inférieur},$$

où la puissance de σ représente une itération (par composition), et ainsi

$$A - a_r(x)\sigma^{r-s}\big(b_s(x)\big)^{-1}\partial^{r-s}B$$

est de degré strictement inférieur à r. Cette étape de réduction est l'étape élémentaire de la division euclidienne. En itérant le procédé, on aboutit à un reste R de degré strictement inférieur à s. En regroupant les facteurs gauches, on obtient un quotient à gauche Q tel que $A = QB + R$.

Exemple 1. On considère l'anneau $\mathbb{Q}(n)\langle\partial_n; S_n\rangle$ des polynômes tordus représentant les opérateurs de décalage. La division de $A = (n^2-1)\partial_n^2 - (n^3+3n^2+n-2)\partial_n + (n^3+3n^2+2n)$, qui annule les combinaisons linéaires de $n!$ et n, par $B = n\partial_n^2 - (n^2+3n+1)\partial_n + (n^2+2n+1)$, qui annule les combinaisons linéaires $n!$ et 1, s'écrit

$$A = n^{-1}(n^2-1)B - n^{-1}(n^2+n+1)\big(\partial_n - (n+1)\big).$$

Le reste est multiple de $\partial_n - (n+1)$, qui représente la récurrence $u_{n+1} = (n+1)u_n$, vérifiée par la factorielle.

Notons une propriété de cette division : si A est multiplié à gauche par un facteur $m(x)$ sans que B ne soit changé, alors Q et R sont multipliés à gauche par le même facteur $m(x)$. Ceci ne vaut plus (en général) pour un facteur faisant intervenir ∂. On a la propriété analogue pour la multiplication à droite par un facteur $m(\partial)$.

La division euclidienne nous donne une nouvelle interprétation du calcul du N-ième terme d'une suite P-récursive $u = (u_n)$ relativement à $\mathbb{Q}(n)\langle\partial_n; S_n\rangle$. Supposons que u soit solution de l'équation de récurrence

$$a_r(n)u_{n+r} + \cdots + a_r(n)u_n = 0.$$

En déroulant la récurrence, on voit que u_N peut, pour tout N sauf annulation malvenue de a_r, se mettre sous la forme $\alpha_{r-1,N}u_{r-1} + \cdots + \alpha_{0,N}u_0$. Plus généralement, on a une relation qui récrit u_{n+N} en terme de u_{n+r-1}, …, u_n. Pour l'obtenir, associons à la récurrence sur u le polynôme tordu $P = a_r(n)\partial_n^r + \cdots + a_r(n)$. Pour un N donné, la division euclidienne de ∂_n^N par P s'écrit

$$\partial_n^N = Q_N(n)P + \alpha_{r-1,N}(n)\partial_n^{r-1} + \cdots + \alpha_{0,N}(n)$$

pour des fractions rationnelles $\alpha_{i,N}(n)$. Après application sur u et évaluation en n, nous obtenons

$$u_{n+N} = 0 + \alpha_{r-1,N}(n)u_{n+r-1} + \cdots + \alpha_{0,N}(n)u_n,$$

d'où le résultat annoncé pour $\alpha_{i,N} = \alpha_{i,N}(0)$.

Exercice 3. Nous laissons le lecteur se convaincre que la récriture d'une dérivée $f^{(N)}$ d'une fonction D-finie f décrite par une équation différentielle d'ordre r en terme de ses dérivées d'ordre strictement inférieur à r s'interprète de façon analogue comme le calcul d'un reste de division euclidienne.

Le même ingrédient se retrouve dans l'algorithme donnant la clôture par addition de deux fonctions D-finies ou de deux suites P-récursives : pour deux objets f et g à additionner, décrits comme solutions des équations respectives $L_f \cdot f = 0$ et $L_g \cdot g = 0$ pour des polynômes tordus de degrés respectifs r et s d'un anneau adéquat $A\langle\partial;\sigma,\delta\rangle$, l'algorithme exprime pour des i successifs $\partial^i \cdot (f+g)$ sous la forme $(\partial^i \bmod L_f)\cdot f + (\partial^i \bmod L_g)\cdot g$, où la notation $A \bmod B$ note le reste de la division euclidienne à droite de A par B. Lorsque suffisamment de i ont été considérés, l'algorithme qui a jusqu'à présent été donné calcule par de l'algèbre linéaire des cofacteurs a_0, …, a_{r+s} tels que

$$\sum_{i=0}^{r+s} a_i(\partial^i \bmod L_f) = 0 \qquad \text{et} \qquad \sum_{i=0}^{r+s} a_i(\partial^i \bmod L_g) = 0.$$

Notons que $P = \sum_{i=0}^{r+s} a_i \partial^i$ est un multiple commun à gauche de L_f et de L_g, puisque $P \bmod L_f = P \bmod L_g = 0$.

4. Recherche de solutions et factorisation d'opérateurs

Comme pour les anneaux de polynômes commutatifs usuels, une notion de factorisation est présente pour les anneaux de polynômes tordus. Une nuance importante réside dans le lien entre les « zéros » des polynômes tordus et la position des facteurs. Nous allons voir que la factorisation de polynômes tordus se relie aux algorithmes vus en cours pour la recherche de solutions polynomiales, rationnelles, et hypergéométriques dans le cas de récurrences.

Dans le cas d'un polynôme commutatif h se factorisant sous la forme fg pour des facteurs polynomiaux de degré au moins 2, tout zéro de f et tout zéro de g est zéro de h ; à l'inverse, quitte à se placer dans une clôture algébrique, tout zéro α de h en fournit un facteur $x - \alpha$ et un quotient exact $f(x)$ tel que $h(x) = f(x)(x - \alpha)$. Dans le cas tordu, une factorisation $L = PQ$ dans $A\langle\partial; \sigma, \delta\rangle$ (où A est un corps) a des propriétés différentes selon le facteur : une solution f de l'équation $Q \cdot f = 0$ est encore solution de $L \cdot f = 0$, car $L \cdot f = P \cdot (Q \cdot f) = P \cdot 0 = 0$; mais une solution g de P ne donne lieu à des solutions f de L que par la relation $Q \cdot f = g$. Inversement, une solution f de L donne lieu à un facteur droit d'ordre 1 de L, quitte à étendre A par f et tous ses itérés par σ et δ. Ce facteur est de la forme $\partial - (\partial \cdot f)/f$, c'est-à-dire $\partial - \delta(f)/f$ ou $\partial - \sigma(f)/f$ selon l'action de l'anneau de polynômes tordus sur les fonctions.

Les algorithmes de recherche de solutions dans des classes particulières fournissent donc implicitement, pour chaque solution trouvée, un facteur droit d'ordre 1. Plus précisément, dans le cas différentiel, une solution polynomiale ou rationnelle f d'une équation $L \cdot f = 0$ pour L dans l'anneau $\mathbb{Q}(x)\langle\partial_x; I, D_x\rangle$ fournit un facteur droit $D = \partial_x - D_x(f)/f$ où $D_x(f)/f$ est rationnel ; dans le cas à récurrence, une solution polynomiale, rationnelle ou hypergéométrique f d'une équation $L \cdot f = 0$ pour L dans l'anneau $\mathbb{Q}(x)\langle\partial_x; S_x\rangle$ fournit un facteur droit $D = \partial_x - S_x(f)/f$ où $S_x(f)/f$ est rationnel. Dans les deux cas, le quotient Q tel que $L = QD$ est aussi à coefficients rationnels.

Exercice 4. Un antimorphisme ϕ entre anneaux est une application $\mathbb{Q}$-linéaire qui renverse les produits : $\phi(PQ) = \phi(Q)\phi(P)$. Montrer l'existence d'antimorphismes $\mu : \mathbb{Q}(x)\langle\partial_x; I, D_x\rangle \to \mathbb{Q}(u)\langle\partial_u; I, D_u\rangle$ et $\nu : \mathbb{Q}(x)\langle\partial_x; S_x\rangle \to \mathbb{Q}(u)\langle\partial_u; S_u\rangle$, définis par les relations

$$\mu(x) = u, \quad \mu(\partial_x) = -\partial_u, \qquad \text{et} \qquad \nu(x) = -u, \quad \nu(\partial_x) = \partial_u.$$

Expliquer comment ces antimorphismes fournissent des facteurs gauches d'ordre 1 de polynômes tordus.

5. Algorithme d'Euclide

Rappelons qu'un idéal d'un anneau commutatif unitaire A est un sous-groupe additif de A clos par multiplication par les éléments de A. Il est classique que les anneaux commutatifs euclidiens — ceux dans lesquels l'existence d'un degré permet une division euclidienne — sont principaux — tout idéal peut être engendré par un unique générateur. C'est le cas des anneaux de polynômes commutatifs à coefficients dans un corps. Le p. g. c. d. p de deux polynômes f et g est alors l'unique polynôme

unitaire engendrant l'idéal (f,g), somme des idéaux (f) et (g). Il se calcule comme dernier reste non nul par l'algorithme d'Euclide.

Pour un anneau de polynômes tordus $A = K\langle\partial;\sigma,\delta\rangle$ sur un corps K, la situation est la même si on prend soin de ne considérer que des idéaux à gauche, c'est-à-dire avec la clôture par multiplication à gauche par les éléments de A. Les notions qui en découlent sont celles de divisions euclidiennes à droite et de plus grands communs diviseurs à droite (p. g. c. d. d.). Soient P_0 et P_1 deux polynômes de A. Si P_1 n'est pas nul, on écrit la division euclidienne de P_0 par P_1, sous la forme $P_0 = Q_0P_1 + P_2$. Tant que P_{i+2} n'est pas nul, on itère en divisant P_{i+1} par P_{i+2}. Soit j la valeur finale de i, telle que $P_{j+1} \neq 0$ et $P_{j+2} = 0$. Alors :

$$\begin{bmatrix} P_0 \\ P_1 \end{bmatrix} = \begin{bmatrix} Q_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \cdots = \begin{bmatrix} Q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} Q_j & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} P_{j+1} \\ 0 \end{bmatrix},$$

d'où on déduit que P_{j+1} divise P_0 et P_1 à droite : $P_0 = FP_{j+1}$ et $P_1 = GP_{j+1}$ pour des polynômes tordus F et G adéquats. Puis en inversant les matrices

$$\begin{bmatrix} P_{j+1} \\ 0 \end{bmatrix} = \begin{bmatrix} U & V \\ R & S \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \end{bmatrix} \qquad \text{pour} \qquad \begin{bmatrix} U & V \\ R & S \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q_j \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -Q_0 \end{bmatrix}.$$

En particulier, $P_{j+1} = UP_0 + VP_1$ est élément de l'idéal à gauche $AP_0 + AP_1$. Un élément quelconque $L = MP_0 + NP_1$ de cet idéal est aussi multiple de P_{j+1} : $L = (MF+NG)P_{j+1}$. En normalisant P_{j+1} pour le rendre unitaire, on obtient donc un p. g. c. d. d. distingué de P_0 et P_1. Par ailleurs, le polynôme tordu $RP_0 = -SP_1$ est un plus petit multiple commun à gauche (p. p. c. m. g.) de P_0 et P_1, par le même argument que dans le cas commutatif, en suivant de près les degrés tout au long de l'algorithme.

On a vu que les algorithmes de clôture par addition entre fonctions D-finies ou entre suites P-récursives renvoient un multiple commun à gauche des polynômes tordus L_f et L_g décrivant les deux objets f et g additionner. Comme ces algorithmes opèrent par degrés croissants, le polynôme renvoyé est de degré minimal en ∂, parmi ceux qui annulent la somme $f+g$. Le polynôme annulateur de la somme $f+g$ renvoyé par ces algorithmes est donc le p. p. c. m. g. de L_f et de L_g.

Exemple 2. Nous repartons des polynômes A et B de l'exemple 1 pour en calculer un p. g. c. d. d. et un p. p. c. m. g. On pose $P_0 = A$, $P_1 = B$; on a déjà calculé $P_2 = -n^{-1}(n^2+n+1)\big(\partial_n - (n+1)\big)$ avec $P_0 = n^{-1}(n^2-1)P_1 + P_2$. Il vient ensuite

$$P_1 = \left(-\frac{n(n+1)}{n^2+3n+3}\partial_n + \frac{n(n+1)}{n^2+n+1}\right) P_2 + 0.$$

Ainsi, le p. g. c. d. d. unitaire est $\partial_n - (n+1)$. Remarquons qu'il annule les solutions communes de A et B, à savoir les multiples de $n!$. Le p. p. c. m. g unitaire s'obtient par renormalisation de $Q_1P_0 = (Q_1Q_0+1)P_1$:

$$\partial_n^3 - \frac{n^3+6n^2+8n+5}{n^2+n+1}\partial_n^2 + \frac{2n^3+9n^2+13n+7}{n^2+n+1}\partial_n - \frac{(n^2+3n+3)(n+1)}{n^2+n+1}.$$

Notons que ses solutions sont toutes les solutions de A et B : les combinaisons linéaires de $n!$, n et 1.

6. Relations de contiguïté

Un grand nombre de fonctions spéciales sont en fait des fonctions $f_n(x)$ d'une variable continue x et d'une variable discrète n. Les familles de telles fonctions dont

l'intérêt a été relevé, par exemple par la physique mathématique, sont telles que la dépendance en x est liée à la dépendance en n. Il apparaît que très fréquemment, la fonction $f_{n+\alpha}(x)$, pour $\alpha = \pm 1$, est reliée à la fonction $f_n(x)$ et à ses dérivées. C'est le cas pour la classe importante des *fonctions hypergéométriques*, c'est-à-dire, essentiellement, pour les séries génératrices de suites hypergéométriques, et pour des fonctions limites de fonctions hypergéométriques, dont un certain nombre de familles de polynômes orthogonaux classiques, et pour des généralisations.

Dans cette section, nous considérons des fonctions D-finies paramétrées et résolvons algorithmiquement des problèmes tels que la détermination d'une relation de la forme

$$f_{n+1}(x) = \sum_{i=0}^{r-1} a_i(x) f_n^{(i)}(x)$$

pour la suite de polynômes

$$f_n(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k}^2 \binom{n+k}{k}^2 x^k.$$

Ici, la relation explicite est

$$\begin{aligned} f_{n+1}(x) = {} & 12\frac{x^3(x+1)}{(n+1)^3} f_n'''(x) + 4\frac{x^2(2n+2xn+11+14x)}{(n+1)^3} f_n''(x) \\ & - 4\frac{x(5xn^2-n^2-4n-6+2xn-9x)}{(n+1)^3} f_n'(x) - \frac{16xn-n-1+4x}{n+1} f_n(x). \end{aligned}$$

L'opérateur différentiel linéaire implicitement au membre droit s'appelle un *opérateur de montée* ; un opérateur qui donnerait $f_{n-1}(x)$ s'appelle un *opérateur de descente*. Une relation linéaire entre les decalées $f_{n+i}(x)$ et ne faisant intervenir aucune dérivation s'appelle une *relation de contiguïté*.

6.1. Fonction hypergéométrique de Gauss. La plus simple des fonctions hypergéométriques est la fonction hypergéométrique de Gauss, définie par

$$F(a,b;c;x) = \sum_{k\geq 0} \frac{(a)_k (b)_k}{(c)_k} \frac{x^k}{k!} \qquad \text{avec} \qquad (s)_n = s(s+1)\cdots(s+n-1) = \frac{\Gamma(s+n)}{\Gamma(s)}.$$

(Ici, la fonction $\Gamma(s)$ est la fonction classique qui interpole la factorielle.)

Oublions la dépendance en b et c du coefficient de x^k dans cette somme, coefficient que nous notons $u_{a,k}$. Nous avons

$$u_{a,k+1} = \frac{(a+k)(b+k)}{(c+k)(k+1)} u_{a,k} \qquad \text{et} \qquad u_{a+1,k} = \left(\frac{k}{a}+1\right) u_{a,k}.$$

La première de ces identités nous fournit le polynôme tordu

$$(c+k)(k+1)\partial_k - (a+k)(b+k)$$

qui annule u. Pour $k=-1$, cette récurrence impose $u_{a,-1}=0$, ce qui permet d'étendre la suite u à toute valeur $k\in\mathbb{Z}$ tout en continuant de vérifier la récurrence. Par le morphisme qui effectue le passage à la série génératrice, nous obtenons

$$\begin{aligned} & (c+x\partial_x)(x\partial_x+1)x^{-1} - (a+x\partial_x)(b+x\partial_x) \\ & \quad = \big((x\partial_x)^2 + (c+1)x\partial_x + c\big)x^{-1} - \big((x\partial_x)^2 + (a+b)x\partial_x + ab\big) \\ & \quad = x(1-x)\partial_x^2 + \big(c-(a+b+1)x\big)\partial_x - ab. \end{aligned}$$

Notons L ce polynôme tordu en ∂_x. La deuxième identité sur u donne, après sommation, $F(a+1,b;c;x) = (a^{-1}x\partial_x + 1)\cdot F(a,b;c;x)$; c'est-à-dire qu'un opérateur de montée est donné par le polynôme tordu $L_\uparrow = a^{-1}x\partial_x + 1$.

Définissons $G(a,b;c;x)$ comme étant $F(a+1,b;c;x)$. Supposons qu'il existe un inverse V de $L_\uparrow$ modulo L à droite. Alors $VL_\uparrow - 1$ est un multiple à gauche de L, qui annule donc F. Ainsi, $F = VL_\uparrow \cdot F = V \cdot G$, autrement dit, V représente un opérateur de descente de G. On obtient un opérateur de descente pour F par un simple décalage arrière de a dans V. La division euclidienne

$$L = Q(a^{-1}x\partial_x+1)-(c-a-1)ax^{-1} \qquad \text{où} \qquad Q = a(1-x)\partial_x+(c-a-1)ax^{-1}-ab$$

donne l'opérateur de descente après avoir décalé a dans $(c-a-1)^{-1}a^{-1}xQ$ par

$$L_\downarrow = \frac{x(1-x)}{a-c}\partial_x - \frac{bx}{a-c} - 1.$$

Notre objectif est maintenant de calculer une relation de contiguïté pour F. Nous avons obtenu $L_\uparrow(a)\cdot F = \partial_a \cdot F$, où nous avons noté explicitement la dépendance en a du polynôme tordu $L_\uparrow$. Il s'ensuit la relation

$$\partial_a^i \cdot F = L_{\uparrow,i}(a)\cdot F \;=\; L_\uparrow(a)L_\uparrow(a+1)\cdots L_\uparrow(a+i-1)\cdot F,$$

dans laquelle nous pouvons, comme toujours, remplacer un polynôme agissant sur la fonction F par le reste de la division euclidienne de ce polynôme par L, qui annule F. Ainsi, une relation de contiguïté s'obtient en recherchant une combinaison linéaire, à coefficients dans $\mathbb{Q}(a,b,c,x)$ des restes modulo L à droite des $L_{\uparrow,i}(a)$ pour $i = 0,1,2$.

Exercice 5. Terminer ce calcul pour retrouver :

$$(a+1)(1-x)F(a+2,b;c;x) + \big(c - xb + (a+1)(x-2)\big)F(a+1,b;c;x) \\ + (a-c+1)F(a,b;c;x) = 0.$$

6.2. Extension aux séries partiellement hypergéométriques. Nous considérons maintenant des sommes

$$f_n(x) = \sum_{k\geq 0} u_{n,k}x^k$$

dans lesquelles u n'est hypergéométrique qu'en n, mais est seulement P-récursive en k, et satisfait à la relation

$$a_p(n,k)u_{n,k+p} + \cdots + a_0(n,k)u_{n,k} = 0.$$

Comme dans le cas doublement hypergéométrique, cette relation fournit une relation purement différentielle sur f. Comme précédemment, aussi, la relation de récurrence du premier order en n sur u donne une expression de $f_{n+1}(x)$ comme combinaison linéaire de dérivées. On procède donc comme dans la section précédente pour calculer opérateurs de montée, de descente, et relations de contiguïté.

Exercice 6 (Assez calculatoire). Calculer l'opérateur de montée annoncé dans l'introduction de cette section.

Bibliographie

[1] Bronstein (M.) and Petkovšek (M.). – On Ore rings, linear operators and factorisation. *Programmirovanie*, vol. 1, 1994, pp. 27–44. – Also available as Research Report 200, Informatik, ETH Zürich.

[2] Bronstein (Manuel) and Petkovšek (Marko). – An introduction to pseudo-linear algebra. *Theoretical Computer Science*, vol. 157, 1996, pp. 3–33.

[3] Chyzak (Frédéric) and Salvy (Bruno). – Non-commutative elimination in Ore algebras proves multivariate holonomic identities. *Journal of Symbolic Computation*, vol. 26, n° 2, August 1998, pp. 187–227.

[4] Ore (Oystein). – Linear equations in non-commutative fields. *Annals of Mathematics*, vol. 32, 1931, pp. 463–477.

[5] Ore (Oystein). – Theory of non-commutative polynomials. *Annals of Mathematics*, vol. 34, 1933, pp. 480–508.

[6] Takayama (Nobuki). – Gröbner basis and the problem of contiguous relations. *Japan Journal of Applied Mathematics*, vol. 6, n° 1, 1989, pp. 147–160.

CHAPITRE 7

Algorithmes pour les fonctions spéciales dans les algèbres de Ore

1. Algèbres de Ore rationnelles

Une généralisation à plusieurs dérivations et décalages de la notion d'anneau de polynômes tordus du chapitre précédent est donnée par la définition qui suit.

DÉFINITION (Algèbre de Ore). *Étant donnés*
- *un corps $k(x) = k(x_1, \ldots, x_r)$ de fractions rationnelles,*
- *r morphismes σ_i de ce corps commutant deux à deux,*
- *pour chaque i une σ-dérivation δ_i relative à σ_i, c'est-à-dire pour chaque i un endomorphisme linéaire pour lequel $\delta_i(ab) = \sigma_i(a)\delta_i(b) + \delta_i(a)b$ dès que a et b sont dans $k(x)$, toutes ces σ-dérivations commutant deux à deux et δ_i commutant avec σ_j chaque fois que $i \neq j$,*
- *r indéterminées ∂_i,*

l'algèbre de Ore (rationnelle) notée $k(x_1, \ldots, x_r)\langle\partial_1, \ldots, \partial_r; \sigma_1, \ldots, \sigma_r, \delta_1, \ldots, \delta_r\rangle$ ou plus simplement $k(x)\langle\partial; \sigma, \delta\rangle$ est la $k(x)$-algèbre associative engendrée par les ∂_i modulo les relations

$$\partial_i a = \sigma_i(a)\partial_i + \delta_i(a), \qquad \partial_i\partial_j = \partial_j\partial_i,$$

quand a est dans $k(x)$. On note plus simplement $k(x_1, \ldots, x_r)\langle\partial_1, \ldots, \partial_r; \sigma_1, \ldots, \sigma_r\rangle$ ou encore $k(x)\langle\partial; \sigma\rangle$ le cas où tous les δ_i sont nuls.

Donnons un exemple : en notant x pour m_x et n pour m_n, on vérifie l'existence d'une algèbre de Ore $A = \mathbb{C}(n, x)\langle\partial_n, \partial_x; S_n, I, 0, D_x\rangle$ avec $S_n(n) = n + 1$, $S_n(x) = x$, $D_x(n) = 0$, $D_x(x) = 1$, et plus généralement $S_n(a) = a(n + 1, x)$ et $D_x(a) = da/dx$ quand $a = a(n, x) \in \mathbb{C}(n, x)$.

2. Idéal annulateur

Les éléments des algèbres de Ore représentent des opérateurs linéaires, différentiels, de récurrence, ou autres, et agissent donc sur des fonctions, suites, suites de fonctions, etc. Donnons un exemple qui montre que ces objets sont une bonne représentation polynomiale des opérateurs linéaires, l'exemple de la famille des polynômes orthogonaux de Laguerre qui va nous servir pour toute la suite du chapitre.

Pour chaque paramètre strictement positif α, l'intégrale

$$\langle f, g\rangle = \int_0^\infty f(x)g(x)x^\alpha e^{-x}\,dx$$

définit un produit scalaire sur les fonctions polynomiales réelles. Par la théorie des polynômes orthogonaux, on déduit l'existence de bases orthogonales échelonnées en

degré. On a par exemple la base des polynômes orthogonaux de Laguerre, donnée par

$$L_n^{(\alpha)}(x) = \frac{1}{n!}x^{-\alpha}e^x\left(\frac{d}{dx}\right)^n\left(e^{-x}x^{n+\alpha}\right) = \frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{k}(\alpha+k+1)\cdots(\alpha+n)x^k.$$

On vérifie que ces polynômes vérifient les relations (linéaires)

$$\begin{aligned}(n+2)L_{n+2}^{(\alpha)} - (2n+\alpha+3-x)L_{n+1}^{(\alpha)} + (n+\alpha+1)L_n^{(\alpha)} &= 0,\\ xL_n^{(\alpha)\prime} - (n+1)L_{n+1}^{(\alpha)} + (n+\alpha+1-x)L_n^{(\alpha)} &= 0,\\ xL_n^{(\alpha)\prime\prime} + (\alpha+1-x)L_n^{(\alpha)\prime} + nL_n^{(\alpha)} &= 0,\end{aligned}$$

avec les conditions initiales $L_0^{(\alpha)} = 1$ et $L_1^{(\alpha)} = \alpha + 1 - x$. Dans l'algèbre de Ore A ci-dessus, ces équations se recodent en les polynômes tordus suivant, qui annulent la suite de fonctions polynomiales $L^{(\alpha)}$:

$$\begin{aligned}p_1 &= (n+2)\partial_n^2 - (2n+\alpha+3-x)\partial_n + (n+\alpha+1),\\ p_2 &= x\partial_x - (n+1)\partial_n + (n+\alpha+1-x),\\ p_3 &= x\partial_x^2 + (\alpha+1-x)\partial_x + n.\end{aligned}$$

Ces trois polynômes engendrent un idéal à gauche dans A, l'idéal annulateur de $L^{(\alpha)}$ dans A. Pour mémoire, un idéal à gauche I d'un anneau R est un sous-ensemble non vide de R stable par addition et par multiplication à gauche par tout élément de R. Cette stabilité reflète le fait que l'addition terme à terme de deux relations linéaires vérifiées par $L^{(\alpha)}$ est une nouvelle relation linéaire vérifiée par $L^{(\alpha)}$, de même qu'en appliquant un opérateur linéaire sur une relation linéaire vérifiée par $L^{(\alpha)}$, on retrouve une relation linéaire vérifiée par $L^{(\alpha)}$.

Exemple 1. Partant de la troisième équation donnée pour caractériser les polynômes de Laguerre, un décalage avant de n et une dérivation par rapport à x donnent respectivement

$$xL_{n+1}^{(\alpha)\prime\prime} + (\alpha+1-x)L_{n+1}^{(\alpha)\prime} + (n+1)L_{n+1}^{(\alpha)} = 0$$

et

$$xL_n^{(\alpha)\prime\prime\prime} + (\alpha+2-x)L_n^{(\alpha)\prime\prime} + (n-1)L_n^{(\alpha)\prime} = 0.$$

L'addition de ces deux équations donne l'équation fonctionnelle linéaire

$$xL_n^{(\alpha)\prime\prime\prime} + (\alpha+2-x)L_n^{(\alpha)\prime\prime} + (n-1)L_n^{(\alpha)\prime} + xL_{n+1}^{(\alpha)\prime\prime} + (\alpha+1-x)L_{n+1}^{(\alpha)\prime} + (n+1)L_{n+1}^{(\alpha)} = 0,$$

laquelle correspond au polynôme tordu

$$(\partial_x+\partial_n)p_3 = x\partial^3 + (\alpha+2-x)\partial_x^2 + (n-1)\partial_x + x\partial_x^2\partial_n + (\alpha+1-x)\partial_x\partial_n + (n+1)\partial_n.$$

Toute autre famille de polynômes orthogonaux classique se traiterait de la même manière et aurait pu servir de support au cours. La même nature de système linéaire avec une dérivation sur une variable et un décalage sur une autre permet de traiter de la même façon nombre de familles de fonctions spéciales paramétrées, telles les fonctions de Bessel, de Hankel, etc.

3. Bases de Gröbner pour les idéaux à gauche

La propriété essentielle qui fait fonctionner toute la théorie des bases de Gröbner et l'algorithme de Buchberger dans le cadre de polynômes commutatifs est que le monôme de tête d'un produit de polynômes est le produit des monômes de tête des termes du produit. Cette propriété reste vérifiée sur des polynômes non commutatifs sujets aux relations de définition des algèbres de Ore rationnelles, dès lors qu'on considère des ordres monomiaux sur les ∂_i. En refaisant la théorie en s'efforçant de faire toutes les combinaisons linéaires avec des facteurs à gauche, on obtient le résultat suivant (*cf.* le cours sur les bases de Gröbner classiques) :

THÉORÈME. *Soit A une algèbre de Ore rationnelle.*

(i) *Tout idéal à gauche I de A admet pour chaque ordre monomial (admissible) sur les ∂_i une unique base de Gröbner minimale réduite G, au sens où l'une quelconque des propriétés équivalentes suivantes est vérifiée :*

1. *la partie stable du monoïde des monômes en les ∂_i engendrée par les monômes de tête des éléments de G est égale celle engendrée par ceux de I ;*
2. *tout f non nul de I est réductible par G ;*
3. *pour tout f dans A, il existe un unique r dans A dont aucun monôme ne soit divisible par un monôme de tête d'un élément de G et tel que $f-r$ soit dans l'idéal I ;*
4. *pour tout f dans I, le reste de la division (à droite) de f par G est nul.*

(ii) *Soit $P = \{p_k\}_{1\leq k\leq r}$ un système de générateurs non nuls d'un idéal à gauche I de A. Tous les S-polynômes* $\mathrm{Spoly}(p_i, p_j)$ *(définis par des combinaisons linéaires à gauche) se réduisent à 0 par P si et seulement si P est une base de Gröbner de l'idéal.*

(iii) *Une variante de l'algorithme de Buchberger termine et renvoie une base de Gröbner de tout idéal à gauche I de A.*

Une différence du cas non commutatif réside dans le calcul des S-polynômes. Dans le cas commutatif, le S-polynôme de deux polynômes non nuls f_1 et f_2 se définit théoriquement par

$$\mathrm{Spoly}(f_1, f_2) = \frac{c_2}{c_1 \wedge c_2}\frac{m_2}{m_1 \wedge m_2} f_1 - \frac{c_1}{c_1 \wedge c_2}\frac{m_1}{m_1 \wedge m_2} f_2,$$

où c_i dénote le coefficient dominant de f_i et m_i son monôme dominant, pour $i = 1, 2$. Cette dernière formule doit être adaptée dans le cas de polynômes tordus : chacun des c_i dénote maintenant le coefficient dominant de

$$\frac{m_{3-i}}{m_1 \wedge m_2} f_i.$$

Plutôt que de poursuivre la théorie dans le détail, montrons le calcul sur un exemple.

En repartant des polynômes p_1 et p_2 qui annulent la suite des polynômes orthogonaux de Laguerre, montrons que le polynôme p_3 s'obtient par élimination de S par un calcul pour l'ordre $\mathsf{lex}(\partial_n, \partial_x)$. Pour cet ordre, le terme de tête de p_1 est $(n+2)\times\partial_n^2$, celui de p_2 est $-(n+1)\times\partial_n$. On calcule donc d'abord le S-polynôme de p_1 et de p_2, sous la forme

$$\mathrm{Spoly}(p_1, p_2) = p_1 + \partial_n p_2 = x\partial_x\partial_n - (n+1)\partial_n + (n+\alpha+1).$$

Remarquons que ce S-polynôme n'est pas $(n+1)p_1 + (n+2)\partial_n p_2$, lequel aurait $(n+2)\partial_n^2$ comme terme dominant, et non pas $\partial_x\partial_n$ pour monôme de tête. Il est réductible par p_2 ; après multiplication par $(n+1)$ et ajout de $x\partial_x p_2$, on obtient

$$x^2\partial_x^2 + (n+\alpha+2-x)x\partial_x - (n+1)^2\partial_n + (n+1)(n+\alpha+1) - x.$$

Ce polynôme a ∂_n pour monôme de tête et est réductible par p_2 ; après retranchement de $(n+1)p_2$, on aboutit à

$$x^2\partial_x^2 + (\alpha+1-x)x\partial_x + nx,$$

qui n'est autre que xp_3. En poursuivant, on montre que les S-polynômes de p_1 et p_2 avec p_3 se réduisent à 0 ; puisque le monôme de tête de p_2, ∂_n, divise celui de p_1, ∂_n^2, une base de Gröbner minimale pour l'ordre $\mathsf{lex}(\partial_n, \partial_x)$ est $\{p_2, p_3\}$.

De façon analogue, une base de Gröbner pour l'ordre $\mathsf{lex}(\partial_x, \partial_n)$ de l'idéal engendré par p_2 et p_3 est $\{p_1, p_2\}$. Les bases de Gröbner permettent de déterminer la redondance du système $\{p_1, p_2, p_3\}$.

Exercice 1. Calculer une base de Gröbner pour l'ordre $\mathsf{lex}(\partial_x, \partial_n)$ de l'idéal engendré par p_2 et p_3 et vérifier le point ci-dessus.

Les polynômes p_1, p_2, p_3 qui annulent la suite des polynômes orthogonaux de Laguerre sont encore plus contraints qu'il n'y paraît jusqu'à présent : p_2 se déduit en fait de p_1. En effet, ne connaissant que p_1, on peut rechercher le polynôme p_2 sous la forme indéterminée

$$p_2 = \partial_x - u(n,x)\partial_n - v(n,x),$$

pour des fractions rationnelles à déterminer u et v, et faire l'hypothèse heuristique que $\{p_1, p_2\}$ est une base de Gröbner pour l'ordre $\mathsf{lex}(\partial_x, \partial_n)$. (Cette hypothèse heuristique est en fait naturelle dès qu'on sait qu'on a affaire à une famille de polynômes orthogonaux.)

Exercice 2 (Presque un problème). Utiliser la théorie des bases de Gröbner pour donner un système de récurrence linéaires sur u et v qui, après résolution, redonne le polynôme p_2. (Pour la résolution, on se souviendra des conditions initiales $L_0^{(\alpha)} = 1$ et $L_1^{(\alpha)} = \alpha + 1 - x$.)

4. Module quotient et dimension de l'espace des solutions

Dans le cas commutatif, le quotient l'une algèbre A de polynômes par l'un de ses idéaux (bilatères) I reste munie d'un produit canonique et est donc une algèbre. Cette propriété n'est plus réalisée dans le cas d'une algèbre de Ore $A = k(x)\langle\partial; \sigma, \delta\rangle$. Mais, en voyant A comme un idéal à gauche trivial de lui-même, le quotient A/I conserve une addition canonique, ainsi que la stabilité par multiplication à gauche par tout élément de A, ce qui fait de ce quotient un module à gauche sur A. Ce module est en particulier un espace vectoriel sur $k(x)$.

Dans le cas commutatif, un cadre particulier important est celui d'un quotient de dimension finie comme espace vectoriel, car il représente une famille finie de points solutions. Le cas d'un quotient d'une algèbre de Ore qui est un espace vectoriel sur $k(x)$ de dimension finie est lui-aussi important ; dans l'interprétation en opérateurs linéaires, il correspond en règle générale à un espace vectoriel de solutions de dimension finie sur k.

Dans la fin de cette section, nous allons quelque peu détailler ce lien dans le cas d'opérateurs différentiels ; d'autres cadres fournissent le même genre de résultats. Nous irons plus loin sur le sujet dans la section sur les fonctions ∂-finies.

4.1. Séries formelles solutions en un point régulier dans le cas différentiel. Considérons une algèbre de Ore

$$A = \mathbb{C}(x_1, \ldots, x_r)\langle \partial_1, \ldots, \partial_r; I, \ldots, I, D_{x_1}, \ldots, D_{x_r}\rangle,$$

un idéal à gauche I de cette algèbre, donné par un système différentiel linéaire. Nous voulons décrire les solutions séries annulées par tous les éléments de I, où une série est ici un élément de $\mathbb{C}[[x_1, \ldots, x_r]]$, c'est-à-dire une combinaison linéaire formelle éventuellement infinie de monômes à exposants entiers positifs. Dans cette objectif, cette section ébauche un analogue en plusieurs variables de la conversion entre équation différentielle décrivant une fonction D-finie d'une variable et équation de récurrence vérifiée par la suite P-récursive des coefficients.

Fixons un ordre monomial sur les monômes en les ∂_i, puis, pour cet ordre, une base de Gröbner B de I, donnée par des éléments de A sans fractions, c'est-à-dire avec des coefficients polynomiaux. Cette base de Gröbner B fournit un escalier ; notons S l'ensemble des multi-exposants $s = (s_1, \ldots, s_r)$ des monômes $\partial^s = \partial_1^{s_1} \cdots \partial_r^{s_r}$ sous l'escalier, c'est-à-dire des monômes qui ne sont pas réductibles par B. Le module quotient A/I a alors une base d'espace vectoriel sur $\mathbb{C}(x)$ constituée des $\partial^s + I$, les classes des ∂_s modulo I, pour s décrivant S. Soit u le polynôme produit des coefficients de tête des éléments de B et faisons l'hypothèse que u ne s'annule pas pour $x_1 = \cdots = x_r = 0$. Nous affirmons qu'alors, l'idéal I admet un espace vectoriel de solutions séries dans $\mathbb{C}[[x_1, \ldots, x_r]]$ de dimension le cardinal de S, c'est-à-dire la dimension sur $\mathbb{C}(x)$ de A/I vu comme espace vectoriel. On dit dans ce cas que le point $(0, \ldots, 0)$ est régulier pour le système différentiel linéaire définissant l'idéal I.

En effet, pour tout multi-exposant $n = (n_1, \ldots, n_r)$, la réduction du monôme ∂^n par B fournit une combinaison linéaire $\sum_{s\in S} v_{n,s}\partial^s$ congrue à ∂^n modulo I. Notons que par construction, les coefficients $v_{n,s}$ sont éléments de $\mathbb{C}[x_1, \ldots, x_r, u^{-1}]$ et ont ainsi une évaluation bien définie en $x_1 = \cdots = x_r = 0$. Maintenant, puisque chaque élément de I s'annule sur toute solution série

$$\phi = \sum_{n_1\in\mathbb{N},\ldots,n_r\in\mathbb{N}} c_{n_1,\ldots,n_r} x_1^{n_1} \cdots x_r^{n_r}$$

de I, le monôme ∂^n et la somme $\sum_{s\in S} v_{n,s}\partial^s$ ont la même action sur ϕ :

$$\partial^n \cdot \phi = \sum_{s\in S} v_{n,s}\partial^s \cdot \phi.$$

Une évaluation en $x_1 = \cdots = x_r = 0$ donne la relation

$$n_1! \ldots n_r!\, c_{n_1,\ldots,n_r} = \sum_{s\in S} v_{n,s}(0, \ldots, 0) s_1! \ldots s_r!\, c_{s_1,\ldots,s_r}.$$

Autrement dit, la série ϕ est totalement déterminée par ses quelques premiers coefficients c_s pour $s \in S$, en nombre donné par la dimension de A/I.

Illustrons cette idée en reprenant l'exemple des polynômes orthogonaux de Laguerre, qui étendent déjà légèrement le cadre purement différentiel qui précède. Posons

$$L_n^{(\alpha)}(x) = \sum_{k=0}^{n} \ell_{n,k} x^k.$$

En multipliant chaque p_i pour $i = 1, 2, 3$ par ∂_x^k, il vient

$$\partial_x^k p_1 = (n+2)\partial_n^2\partial_x^k - (2n+\alpha+3-x)\partial_n\partial_x^k + k\partial_n\partial_x^{k-1} + (n+\alpha+1)\partial_x^k,$$
$$\partial_x^k p_2 = x\partial_x^{k+1} - (n+1)\partial_n\partial_x^k + (n+\alpha+k+1-x)\partial_x^k - k\partial_x^{k-1},$$
$$\partial_x^k p_3 = x\partial_x^{k+2} + (\alpha+k+1-x)\partial_x^{k+1} + (n-k)\partial_x^k.$$

Après application sur $L^{(\alpha)}$, évaluation en $x = 0$ et division par $k!$, on trouve les relations de récurrence sur la famille doublement indexée des $\ell_{n,k}$

$$(n+2)\ell_{n+2,k} - (2n+\alpha+3)\ell_{n+1,k} + \ell_{n+1,k-1} + (n+\alpha+1)\ell_{n,k} = 0,$$
$$-(n+1)\ell_{n+1,k} + (n+\alpha+k+1)\ell_{n,k} - \ell_{n,k-1} = 0,$$
$$(k+1)(\alpha+k+1)\ell_{n,k+1} + (n-k)\ell_{n,k} = 0.$$

En décalant la dernière vers l'arrière en k puis éliminant $\ell_{n,k-1}$ entre la relation obtenue et la deuxième récurrence ci-dessus, on obtient la récurrence

$$(n+1-k)\ell_{n+1,k} - (n+\alpha+1)\ell_{n,k} = 0.$$

Ce jeu de récurrences fournit tous les $\ell_{n,k}$.

4.2. Solutions en séries des systèmes hypergéométriques de Gel'fand, Kapranov et Zelevinsky. Prenons un exemple concret, celui des systèmes hypergéométriques dans la formulation de Gel'fand, Kapranov et Zelevinsky. L'algèbre de Ore qui intervient dans cet exemple est l'algèbre A engendrée par quatre indéterminées $\partial_1, \ldots, \partial_4$ sur le corps $\mathbb{C}(x_1, \ldots, x_4)$, chaque ∂_i représentant l'opérateur de dérivation par rapport à x_i. Le système GKZ est le système

$$p_1 = \partial_2\partial_3 - \partial_1\partial_4,$$
$$p_2 = x_1\partial_1 - x_4\partial_4 + (1-c),$$
$$p_3 = x_2\partial_2 + x_4\partial_4 + a,$$
$$p_4 = x_3\partial_3 + x_4\partial_4 + b,$$

pour des paramètres complexes a, b et c. L'objectif de l'exemple est de montrer que ce système admet un espace vectoriel de solutions formelles de dimension exactement 2, où par solution formelle nous entendons plus maintenant généralement une série de la forme

$$x_1^{a_1}\ldots x_4^{a_4} \sum_{n_1\in\mathbb{Z},\ldots,n_4\in\mathbb{Z}} c_{n_1,\ldots,n_4} x_1^{n_1}\cdots x_4^{n_4},$$

pour des a_i et des coefficients complexes, ou une combinaison linéaire de telles séries. (Il y a bien un espace vectoriel sur $\mathbb{C}$ où vivent ces séries, mais pas de produit sur ces séries. En revanche, toute série peut être multipliée par un polynôme en les x_i et leurs inverses x_i^{-1}, ainsi que dérivée formellement par rapport à chacune des indéterminées, tout en restant dans l'espace vectoriel.)

Soit I l'idéal engendré par le système $\{p_1, \ldots, p_4\}$ et calculons à partir de ce système une base de Gröbner de I pour l'ordre $\mathsf{lex}(\partial_1, \ldots, \partial_4)$. Les monômes de tête respectifs de p_1 et p_2 sont $\partial_1\partial_4$ et ∂_1. Le S-polynôme de p_1 et de p_2 est donc

$$\mathrm{Spoly}(p_1, p_2) = x_1p_1 + \partial_4 p_2 = x_1\partial_2\partial_3 - x_4\partial_4^2 - c\partial_4,$$

dont le monôme de tête est $\partial_2\partial_3$; il est donc réductible par p_3. Après multiplication par $-x_2$ et ajout de $x_1\partial_3 p_3$, on obtient

$$x_1x_4\partial_3\partial_4 + ax_1\partial_3 + x_2x_4\partial_4^2 + cx_2\partial_4.$$

Ce polynôme a $\partial_3\partial_4$ pour monôme de tête et est donc réductible par p_4. Après multiplication par x_3 et retranchement de $x_1x_4\partial_4 p_4$, on aboutit à

$$ax_1x_3\partial_3 + (x_2x_3 - x_1x_4)x_4\partial_4^2 + \big(cx_2x_3 - (b+1)x_1x_4\big)\partial_4,$$

qui est encore réductible par p_4. Après retranchement de ax_1p_4, on a finalement un polynôme qui n'est pas réductible par $\{p_1, \dots, p_4\}$, à savoir

$$p_5 = (x_2x_3 - x_1x_4)x_4\partial_4^2 + \big(cx_2x_3 - (a+b+1)x_1x_4\big)\partial_4 - abx_1.$$

Par ailleurs, les S-polynômes entre les polynômes p_2, p_3 et p_4 pris deux à deux sont tous nuls, comme on le vérifie en observant que les $x_i\partial_i$ commutent deux à deux. En poursuivant les calculs sur les S-polynômes $\mathrm{Spoly}(p_i, p_5)$, on montre que tous ces derniers se réduisent à 0 par $\{p_1, \dots, p_5\}$. On obtient ainsi qu'un base de Gröbner minimale est $\{p_2, p_3, p_4, p_5\}$, avec les monômes dominants respectifs ∂_1, ∂_2, ∂_3 et ∂_4^2.

Le module quotient A/I a donc une base d'espace vectoriel sur $\mathbb{C}(x_1, \dots, x_4)$ constituée de $1+I$ et ∂_4+I, les classes respectives de 1 et ∂_4 modulo I. La structure de module est donnée explicitement par l'action des ∂_i sur ces deux éléments de base.

Exercice 3. Donner l'expression explicite de cette action en récrivant chaque $\partial_i \cdot (1+I)$ et chaque $\partial_i \cdot (\partial_4 + I)$ sur la base $(1+I, \partial_4 + I)$.

Revenons sur les solutions séries du système GKZ. Le polynôme p_2 agit sur un monôme par

$$p_2 \cdot (x_1^{\lambda_1} \cdots x_4^{\lambda_4}) = (\lambda_1 - \lambda_4 + 1 - c)x_1^{\lambda_1} \cdots x_4^{\lambda_4}.$$

(Notons la distinction entre le produit dans A noté $p_2x_1^{\lambda_1} \cdots x_4^{\lambda_4}$ et l'opération de p_2, ici sur une serie h en x, notée $p_2 \cdot h$; on comparera par exemple $\partial_1 x_1^5 = x_1^5\partial_1 + 5x_1^4$ et $\partial_1 \cdot x_1^5 = 5x_1^4$.) Ainsi, un monôme $x_1^{\lambda_1} \cdots x_4^{\lambda_4}$ ne peut apparaître avec un coefficient non nul dans une série ϕ solution du système GKZ que si $\lambda_1 - \lambda_4 + 1 - c$ est nul. En poursuivant ce type de raisonnement avec p_3 et p_4, on obtient de même les contraintes $\lambda_2 + \lambda_4 + a = 0$ et $\lambda_3 + \lambda_4 + a = 0$ et on aboutit à ce que les seuls monômes pouvant apparaître avec un coefficient non nul sont de la forme

$$x_1^{\lambda_4+c-1}x_2^{-\lambda_4-a}x_3^{-\lambda_4-b}x_4^{\lambda_4} = \frac{x_1^{c-1}}{x_2^a x_3^b}\left(\frac{x_1x_4}{x_2x_3}\right)^{\lambda_4},$$

et une solution ϕ est nécessairement de la forme

$$\phi = \frac{x_1^{c-1}}{x_2^a x_3^b} f\left(\frac{x_1x_4}{x_2x_3}\right),$$

pour une série formelle f en y à exposants entiers relatifs. Reste à exploiter que ϕ est solution de p_1, ou de manière équivalente puisque sous la forme ci-dessus ϕ est déjà solution de p_2, p_3 et p_4, de p_5. Après avoir évalué en $y = x_1x_4/x_2x_3$, on a

$$0 = \frac{x_2^a x_3^b}{x_1^{c-2}} p_5 \cdot \phi = (1-y)yf''(y) + \big(c - (a+b+1)y\big)f'(y) - abf(y).$$

On reconnaît là l'équation hypergéométrique de Gauss, annulée par la série de Gauss

$$f_1 = {}_2\mathrm{F}_1(a, b; c; y) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n}\frac{y^n}{n!}$$

où $(x)_n$ représente le symbole de Pochhammer, $x(x+1)\cdots(x+n-1)$. On vérifie qu'une solution formelle linéairement indépendante avec f_1 est $f_2 = y^{1-c}\,{}_2\mathrm{F}_1(a-c+1, b-c+1; 2-c; y)$. On a ainsi obtenu deux solutions formelles linéairement indépendantes du système GKZ, $\phi_i = x_1^{c-1}/x_2^a x_3^b \times f_i(x_1x_4/x_2x_3)$ pour $i = 1$ et $i = 2$.

Pour tout système différentiel représenté par un idéal I de A, un résultat d'analyse, le théorème de Cauchy–Kovalevskaya, affirme l'existence, au voisinage de tout point en dehors d'une certaine variété singulière, d'un $\mathbb{C}$-espace vectoriel de solutions analytiques de dimension celle sur $\mathbb{C}(x)$ de l'espace vectoriel A/I. Or, on montre que cette variété singulière est incluse dans le lieu des zéros du produit des coefficients polynomiaux de tête d'une base de Gröbner de I écrite sans fractions.

Dans le cas de notre exemple, la dimension de A/I est 2 et la variété singulière est incluse dans le lieu des zéros de $x_1\cdots x_4(x_2x_3 - x_1x_4)$. Hors de ce lieu, y n'est ni nul, ni infini, ni égal à 1, et les fonctions ϕ_1 et ϕ_2 sont donc analytiques puisque, moyennant quelques hypothèses sur les paramètres a, b et c, les deux séries solutions de l'équation de Gauss, f_1 et f_2, représentent des fonctions analytiques sur $\mathbb{C} \setminus \{0, 1\}$. On a donc trouvé un espace de solutions analytiques de dimension 2, et par le théorème de Cauchy–Kovalevskaya, toutes les solutions analytiques du système GKZ en dehors de sa variété singulière.

5. Les fonctions ∂-finies et leurs clôtures

Nous poursuivons maintenant avec le cas particulier important des système fonctionnels linéaires correspondant à des modules A/I de dimension finie sur $\mathbb{C}(x)$. L'objectif est ici de montrer que pour une algèbre A donnée, leurs solutions, que nous appellerons « fonctions ∂-finies », forment une algèbre sur $\mathbb{C}$. Nous allons donner un algorithme pour calculer les clôtures correspondantes. Voici tout de suite la définition, déjà motivée par les sections et chapitres précédents sur les fonctions D-finies et les suites P-récursives.

Définition (Fonction ∂-finie). *Étant donnée une algèbre de Ore (rationnelle)*

$$A = \mathbb{C}(x_1, \ldots, x_r)\langle \partial_1, \ldots, \partial_r; \sigma_1, \ldots, \sigma_r, \delta_1, \ldots, \delta_r\rangle$$

agissant sur un $\mathbb{C}(x_1, \ldots, x_r)$-espace vectoriel V, un élément f de V est dit ∂-fini lorsque l'une des conditions équivalentes suivantes est vérifiée :

1. *pour chaque i entre 1 et r, il existe un polynôme $P_i = P_i(x_1, \ldots, x_r, \partial_i)$ dont l'action annule f ;*
2. *la famille des $\partial^a \cdot f$, où ∂^a décrit les monômes de A, engendre un espace vectoriel de dimension finie sur $\mathbb{C}(x)$;*
3. *le module quotient A/I où I note l'idéal annulateur de f pour l'action de A est un espace vectoriel de dimension finie sur $\mathbb{C}(x)$.*

Par commodité, nous appellerons « fonctions » les éléments de l'espace vectoriel V, ce quand bien même il ne s'agirait pas de fonctions de l'analyse, mais afin d'éviter la terminologie plus lourde et moins imagée d'« éléments ∂-finis d'un module sur A ».

Exercice 4. Vérifier l'équivalence entre les trois points de la définition ci-dessus.

5.1. Méthode du vecteur cyclique. L'algorithme envisagé pour les clôtures des fonctions ∂-finies s'appuie le calcul de vecteur cyclique. Rappelons-en l'idée. Classiquement, étant donné un espace vectoriel V sur un corps k, sur lequel on suppose donnée une action de $k[X]$, un vecteur $v \in V$ est dit *cyclique* si la famille $\{X^i \cdot v\}$ engendre V comme k-espace vectoriel. Alors, v engendre V comme $k[X]$-module. Pour calculer, on suppose que V est de dimension finie d et que l'action de X est donnée sur une base $B = (b_1, \ldots, b_d)$ de V par une matrice M telle que $X \cdot v = (a_1, \ldots, a_d)M\,{}^tB$ pour tout vecteur $v = a_1b_1 + \cdots + a_db_d$. Pour tester si v est cyclique et le cas échéant rendre explicite la structure de module de V, on range dans une matrice les lignes $(a_1, \ldots, a_d)M^i$ pour $0 \leq i \leq m$ avec m à déterminer et on cherche par l'algorithme de Gauss une dépendance linéaire entre les lignes de la matrice obtenue. En procédant avec des $m \geq 0$ successifs, la première dépendance linéaire fournit le polynôme minimal de v sous l'action de X sur V ; son degré m vérifie $m \leq d$.

Ce calcul s'étend d'abord au cadre commutatif de l'action d'une algèbre $k[X] = k[X_1, \ldots, X_r]$ de polynômes en plusieurs indéterminées. Chaque X_i correspond alors à une matrice M_i et la commutativité des X_i dans $k[X]$ induit la commutativité entre les matrices M_i. Au lieu d'itérer sur les monômes X^i par ordre croissant de i, on itère maintenant sur les monômes $X^a = X_1^{a_1} \cdots X_r^{a_r}$ selon tout ordre qui assure qu'un monôme n'est considéré qu'après tous ses diviseurs. Soit $a(0)$, $a(1)$, etc, l'ordre dans lequel les multi-exposants des monômes sont énumérés. À chaque étape, on recherche une dépendance linéaire entre des vecteurs

$$X^{a(0)} \cdot v, \ldots, X^{a(m)} \cdot v.$$

En cas d'échec, on conserve ces $m + 1$ vecteurs et on reprend la recherche après avoir ajouté le nouveau vecteur $X^{a(m+1)} \cdot v$; en cas de succès, on retire le dernier vecteur introduit, $X^{a(m)} \cdot v$, on évite par la suite tous les multiples de ce monôme, et on introduit le nouveau vecteur $X^{a(m+1)} \cdot v$ pour reprendre la recherche sur la famille

$$X^{a(0)} \cdot v, \ldots, X^{a(m-1)} \cdot v, X^{a(m+1)} \cdot v.$$

Ce calcul termine si et seulement si le quotient $k[X]/I$, vu comme k-espace vectoriel, est de dimension finie. Chaque dépendance linéaire calculée fournit un polynôme P tel que $P(X_1, \ldots, X_r) \cdot v = 0$. Lorque l'itération sur les monômes X^a suit l'ordre croissant selon un ordre monomial (admissible), l'ensemble des polynômes annulateurs obtenus constitue une base de Gröbner de I pour l'ordre choisi.

5.2. Algorithmes de clôture des fonctions ∂-finies. Le procédé du vecteur cyclique s'étend au cas de l'action d'une algèbre de Ore (rationnelle) en présence de fonctions ∂-finies. Pour une algèbre de Ore

$$A = \mathbb{C}(x)\langle \partial_1, \ldots, \partial_r; \sigma_1, \ldots, \sigma_r, \delta_1, \ldots, \delta_r \rangle,$$

l'espace vectoriel utilisé est un module du type A/I, vu comme espace vectoriel sur $\mathbb{C}(x)$, ou plutôt un module obtenu à partir de quelques constructions de base sur des modules de la forme A/I, comme on va le voir sur l'exemple plus bas. L'espace V étant d'une certaine dimension finie d et une base $B = (b_1, \ldots, b_d)$ de V étant fixée, l'action de chaque ∂_i sur un vecteur $v = a_1b_1 + \cdots + a_db_d$ est donnée par une matrice M_i sous la forme

$$\partial_i \cdot v = \big(\sigma_i(a_1, \ldots, a_d)M_i + \delta_i(a_1, \ldots, a_d)\big)\,{}^tB,$$

en adoptant une notation selon laquelle les σ_i et δ_i agissent distributivement sur les entrées de vecteurs ou de matrices. Pour le choix particulier $v = b_\ell$, on observe que la ℓ-ième ligne de M_i n'est autre que le vecteur ligne des composantes de $\partial_i \cdot b_\ell$ sur la base B.

En faisant maintenant agir ∂_j et en posant $a = (a_1, \dots, a_d)$, on a

$$\partial_j\partial_i \cdot v = \big(\sigma_j\sigma_i(a)\sigma_j(M_i)M_j + \sigma_j\delta_i(a)M_j + \sigma_j\sigma_i(a)\delta_j(M_i) + \delta_j\sigma_i(a)M_i + \delta_j\delta_i(a)\big)\,{}^tB.$$

En tenant compte, pour $i \neq j$ de la commutation $\partial_i\partial_j = \partial_j\partial_i$ et des commutations entre morphismes de corps et σ-dérivations données par la définition des algèbres de Ore, on déduit la relation suivante, qui remplace la commutation entre les matrices du cas commutatif,

$$\sigma_j(M_i)M_j + \delta_j(M_i) = \sigma_i(M_j)M_i + \delta_i(M_j).$$

Lorsque de telles relations sont assurées, la même méthode de recherche de dépendances linéaires par la méthode de Gauss que dans le cas commutatif s'applique et fournit un calcul de l'addition et du produit de fonctions ∂-finies, ou même d'une expression polynomiale en des fonctions ∂-finies. Plutôt que de faire une présentation formelle de ces algorithmes, nous en donnons l'idée sur un exemple.

Prenons celui du calcul du produit des deux fonctions f et g en deux variables x et y, données par $f(x, y) = \exp(xy)$ et $g(x, y) = J_\mu(x+y)$, où, pour un paramètre μ complexe, J_μ est la fonction de Bessel de première espèce, solution de l'équation différentielle

$$z^2 J''_\mu(z) + zJ'_\mu(z) + (z^2 - \mu^2)J_\mu(z) = 0$$

qui admet à l'origine le développement asymptotique

$$J_\mu(z) \sim \frac{1}{2^\mu} \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{n!\,\Gamma(n + \mu + 1)}.$$

Considérons l'algèbre de Ore $A = \mathbb{C}(\mu, x, y)\langle\partial_x, \partial_y; I, I, D_x, D_y\rangle$, où μ est maintenant un paramètre formel. Des bases de Gröbner des annulateurs I et J dans A de f et g pour l'ordre $\mathsf{lex}(\partial_y, \partial_x)$ sont respectivement

$$\{\partial_x - y, \partial_y - x\} \qquad \text{et} \qquad \{(x+y)^2\partial_x^2 + (x+y)\partial_x + (x+y)^2 - \mu^2, \partial_y - \partial_x\}.$$

En désignant maintenant par f et g les vecteurs cycliques générateurs des modules A/I et A/J, avec un petit abus de notation, on introduit donc l'espace vectoriel sur $\mathbb{C}(\mu)$ de base $B = \big(f \otimes g, f \otimes (\partial_x \cdot g)\big)$, où l'on voit le produit $h = f \otimes g$ donné par ses coordonnées $(1, 0)$. Puisque

$$\partial_x \cdot (f \otimes g) = (\partial_x \cdot f) \otimes g + f \otimes (\partial_x \cdot g) = yf \otimes g + f \otimes (\partial_x \cdot g)$$

et

$$\begin{aligned}\partial_x \cdot \big(f \otimes (\partial_x \cdot g)\big) &= yf \otimes (\partial_x \cdot g) + f \otimes (\partial_x^2 \cdot g) \\ &= yf \otimes (\partial_x \cdot g) + \big((x+y)^{-2}\mu^2 - 1\big)f \otimes g - (x+y)^{-1} f \otimes (\partial_x \cdot g),\end{aligned}$$

et des relations similaires pour l'action de ∂_y, on trouve les matrices

$$M_x = \begin{pmatrix} y & 1 \\ (x+y)^{-2}\mu^2 - 1 & y - (x+y)^{-1} \end{pmatrix}$$

et

$$M_y = \begin{pmatrix} x & 1 \\ (x+y)^{-2}\mu^2 - 1 & x - (x+y)^{-1} \end{pmatrix}.$$

Choisissons d'itérer selon un ordre raffinant le degré total en ∂_x et ∂_y. On fait d'abord agir ∂_y pour trouver $\partial_y \cdot h = \big((1,0)M_y + d(1,0)/dy\big)\,{}^tB = (x,1)\,{}^tB$, qui n'est pas lié avec $(1,0)$. De même, on trouve $\partial_x \cdot h = (y,1)\,{}^tB$, qui fournit la liaison $p_1 \cdot h = 0$ pour $p_1 = \partial_x - \partial_y + (x-y)$. Pour la suite du calcul, on exclut alors tous les monômes divisibles par ∂_x ; le monôme considéré suivant est ∂_y^2. Son action sur h donne

$$\partial_y^2 \cdot h = \big((x,1)M_y + d(x,1)/dy\big)\,{}^tB = \big((x+y)^{-2}\mu^2 + x^2 - 1, 2x - (x+y)^{-1}\big)\,{}^tB,$$

et l'on obtient un second annulateur de h,

$$p_2 = (x+y)^2\partial_y^2 - (x+y)(2x^2+2xy-1)\partial_y + (x+y)(x^3+x^2y+y) - \mu^2.$$

Pour la suite du calcul, on exclut donc tous les monômes divisibles par ∂_y^2, si bien qu'il ne reste plus aucun monôme à considérer. L'idéal annulateur de h est l'idéal $Ap_1 + Ap_2$, dont $\{p_1, p_2\}$ est une base de Gröbner pour l'ordre $\mathsf{lex}(\partial_y, \partial_x)$, de monômes de tête respectifs ∂_x et ∂_y^2 ; le module A/I est donné comme $\mathbb{C}(x,y)$-espace vectoriel par sa base $(1+I, \partial_x + I)$.

Le calcul qui précède se revisite en abandonnant l'écriture matricielle et en faisant apparaître plus explicitement les calculs de restes modulo une base de Gröbner. On récrit d'abord $\partial_y \cdot h$ sous la forme

$$\partial_y \cdot h = (\partial_y \cdot f) \otimes g + f \otimes (\partial_y \cdot g) = xf \otimes g + f \otimes (\partial_x \cdot g),$$

après réductions par les bases de Gröbner pour I et J ; ce vecteur est donc linéairement indépendant de h. On procède ensuite de même pour $\partial_x \cdot h$, de façon à avoir

$$\partial_x \cdot h = (\partial_x \cdot f) \otimes g + f \otimes (\partial_x \cdot g) = yf \otimes g + f \otimes (\partial_x \cdot g);$$

on retrouve ainsi l'annulateur p_1. Le monôme considéré suivant est ∂_y^2, d'action sur h

$$\partial_y^2 \cdot h = x^2 f \otimes g + 2xf \otimes (\partial_x \cdot g) - (x+y)^{-2} f \otimes \big((x+y)\partial_x + (x+y)^2 - \mu^2\big)g;$$

ce vecteur est donc linéairement lié à h et $\partial_y \cdot h$ et l'on retrouve le second annulateur p_2. Le calcul se termine de la même manière.

Pour l'algorithme d'addition, les mêmes idées algorithmiques fonctionnent en calculant dans la somme directe $A/I \oplus A/J$.

Bibliographie

[1] Chyzak (Frédéric) and Salvy (Bruno). – Non-commutative elimination in Ore algebras proves multivariate holonomic identities. *Journal of Symbolic Computation*, vol. 26, n° 2, August 1998, pp. 187–227.

[2] Saito (Mutsumi), Sturmfels (Bernd), and Takayama (Nobuki). – *Gröbner deformations of hypergeometric differential equations*. – Springer-Verlag, Berlin, 2000, viii+254p.

CHAPITRE 8

Sommation et intégration symboliques des fonctions spéciales

Résumé

Dans ce chapitre, nous décrivons un algorithme qui peut se voir comme une extension de l'algorithme de Zeilberger pour des sommants ∂-finis, et qui traite dans le même formalisme sommation et intégration. Les quelques sommes et intégrales suivantes, que nous envisageons de traiter avec cet algorithme, montrent une variété d'applications qui vont de la combinatoire à la physique mathématique en passant par la théorie des fonctions spéciales :

$$\sum_{k=0}^{n}\left(\sum_{j=0}^{k}\binom{n}{j}\right)^3 = n2^{3n-1} + 2^{3n} - 3n2^{n-2}\binom{2n}{n},$$

$$\sum_{n=0}^{\infty} H_n(x)H_n(y)\frac{u^n}{n!} = \frac{\exp\left(\frac{4u(xy-u(x^2+y^2))}{1-4u^2}\right)}{\sqrt{1-u^2}},$$

$$\frac{1}{2}J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \cdots = \frac{1}{2},$$

$$\int_{-1}^{+1} \frac{e^{-px}T_n(x)}{\sqrt{1-x^2}}\,dx = (-1)^n\pi I_n(p),$$

$$\int_0^{+\infty} xe^{-px^2} J_n(bx)I_n(cx)\,dx = \frac{1}{2p}\exp\left(\frac{c^2-b^2}{4p}\right)J_n\left(\frac{bc}{2p}\right),$$

$$\int_0^{+\infty} xJ_1(ax)I_1(ax)Y_0(x)K_0(x)\,dx = -\frac{\ln(1-a^4)}{2\pi a^2},$$

$$\sum_{k=0}^{n}\frac{q^{k^2}}{(q;q)_k(q;q)_{n-k}} = \sum_{k=-n}^{n}\frac{(-1)^k q^{(5k^2-k)/2}}{(q;q)_{n-k}(q;q)_{n+k}}.$$

Ici, J, Y, I et K sont des variantes de fonctions de Bessel, qui apparaissent fréquemment pour décrire des modèles physiques à symétrie cylindrique ou sphérique ; H et T sont des familles de polynômes orthogonaux de Hermite et Tchébichev ; $(q;q)_n$ représente le produit $(1-q)\cdots(1-q^m)$. La première identité intervient dans une discrétisation d'une question de probabilités sur la position du maximum de trois variables aléatoires gaussiennes ; la dernière est une variante finie d'une des identités de Rogers–Ramanujan, en théorie des partitions.

1. Expression de la création télescopique en termes d'algèbres de Ore rationnelles

On a déjà exposé dans ce cours la méthode de la création télescopique, en l'appliquant à la sommation hypergéométrique définie par une combinaison de l'algorithme de Gosper et d'une idée due à Zeilberger. Cette approche se généralise en des algorithmes de sommation et intégration pour les suites et fonctions ∂-finies.

Rappelons le principe de la méthode. Soit à évaluer une somme paramétrée

$$F_n = \sum_{k=a}^{b} f_{n,k}.$$

En toute généralité, le principe de la création télescopique est de déterminer une suite auxiliaire $g = (g_{n,k})$ ainsi que des coefficients η_0, …, η_r, fonctions de la variable n, tels que se trouve vérifiée la relation

$$\eta_r(n) f_{n+r,k} + \cdots + \eta_0(n) f_{n,k} = g_{n,k+1} - g_{n,k}.$$

Ici, nous ne faisons pas plus d'hypothèses sur les η_i et g que celle de pouvoir évaluer la relation ci-dessus pour tout n quand k décrit les entiers de a à b. Dans ce cas, une sommation sur k fournit l'égalité

$$\eta_r(n) F_{n+r} + \cdots + \eta_0(n) F_n = g_{n,b+1} - g_{n,a}.$$

Si le membre de droite n'est pas déjà nul, on recherche un opérateur annulateur de ce second membre ; par composition, on obtient une récurrence homogène sur F. Dans bien des cas, on sait prédire à partir de conditions analytiques sur f la nullité du terme $g_{n,b+1} - g_{n,a}$.

Des algorithmes d'efficacités différentes ont été donnés selon le domaine de recherche des η_i et de g, et selon le compromis choisi entre efficacité et richesse de la classe de suites f en entrée. En particulier, l'algorithme de Zeilberger, optimisé pour une suite f hypergéométrique, revient à rechercher des η_i polynomiaux et une suite g similaire à f, c'est-à-dire un multiple ϕf pour une fraction rationnelle ϕ en n et k. La suite $g = \phi f$ devant être une somme indéfinie, la recherche de ϕ et des η_i se fait par une variante paramétrée de l'algorithme de Gosper. Notons que le domaine de recherche de g est l'espace vectoriel $\mathbb{C}(n,k)f$, qui n'est autre, dans le cas hypergéométrique, que le module engendré par f sur l'algèbre de Ore $A = \mathbb{C}(n,k)\langle \partial_n, \partial_k; S_n, S_k\rangle$. Nous considérons ici la généralisation au cas où f est une fonction ∂-finie et où le module $A \cdot f$ est un espace vectoriel de dimension finie sur $\mathbb{C}(n,k)$, mais pas forcément de dimension 1. Soit v_1, …, v_d les éléments d'une base vectorielle de $A \cdot f$; l'algorithme de Zeilberger étendu recherche g sous la forme indéterminée $\phi_1 v_1 + \cdots + \phi_d v_d$, pour des fractions rationnelles ϕ_i en n et k. Cette recherche se fait par une extension ∂-finie de la variante paramétrée de l'algorithme de Gosper.

Tout ce qui a été dit s'étend au monde différentiel pour l'évaluation d'une intégrale paramétrée

$$F(x) = \int_a^b f(x,y)\, dy.$$

On cherche alors une relation

$$\eta_r(x) \frac{\partial^r f}{dx^r}(x,y) + \cdots + \eta_0(x) f(x,y) = \frac{\partial g}{dy}(x,y),$$

qui après intégration fournit l'égalité

$$\eta_r(x)F^{(r)}(x) + \cdots + \eta_0(x)F(x) = \int_a^b g(x,y)\,dy.$$

La même méthode permet aussi de traiter des sommations paramétrées continûment,

$$F(x) = \sum_{k=a}^{b} f_k(x),$$

et des suites d'intégrales de la forme

$$F_n = \int_a^b f_n(y)\,dy.$$

EXERCICE 1. Formuler la relation entre f et g à rechercher dans ces deux derniers cas.

2. L'algorithme sur l'exemple $\frac{1}{2}J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \cdots = \frac{1}{2}$

Nous allons montrer que la famille paramétrée des fonctions de Bessel de première espèce, J_ν, où chaque J_ν est une solution que nous allons préciser de l'équation de Bessel

$$x^2y''(x) + xy'(x) + (x^2 - \nu^2)y(x) = 0,$$

a une somme $\frac{1}{2}J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \cdots$ qui s'évalue à $\frac{1}{2}$.

L'équation de Bessel et les fonctions de Bessel peuvent être considérées pour des valeurs complexes du paramètre ν, mais vu la nature de la somme à étudier, nous nous limiterons dorénavant à des valeurs entières $\nu \in \mathbb{N}$. En étudiant l'équation indicielle de l'équation de Bessel, on s'aperçoit qu'il existe pour chaque ν des solutions dans les séries formelles $\mathbb{C}[[x]]$ et que ces solutions constituent un espace vectoriel de dimension 1 sur $\mathbb{C}$ de séries. Une base de ces solutions formelles est donnée par la série de Bessel

$$J_\nu(x) = (x/2)^\nu \sum_{n=0}^{\infty} \frac{(-1)^n (x/2)^{2n}}{n!\,(n+\nu)!},$$

de valuation ν, qui vu la décroissance de ses coefficients est pour chaque entier ν une série définissant une fonction entière (de rayon de convergence $+\infty$.)

EXERCICE 2. Vérifier ces résultats.

On vérifie par simple substitution et évaluation que ces fonctions J_ν satisfont aussi aux relations

$$xJ'_\nu(x) + xJ_{\nu+1}(x) - \nu J_\nu(x) = 0 \qquad \text{et} \qquad xJ_{\nu+2}(x) - 2(\nu+1)J_{\nu+1}(x) + xJ_\nu(x) = 0.$$

En introduisant l'algèbre de Ore $A = \mathbb{C}(\nu, x)\langle \partial_\nu, \partial_x; S_\nu, I, 0, D_x\rangle$ où S_ν est le décalage avant sur ν et D_x est la dérivation par rapport à x, on a donc un système d'annulateurs pour J,

$$\begin{aligned} p_1 &= x^2\partial_x^2 + x\partial_x + x^2 - \nu^2, \\ p_2 &= x\partial_x + x\partial_\nu - \nu, \\ p_3 &= x\partial_\nu^2 - 2(\nu+1)\partial_\nu + x. \end{aligned}$$

Les deux premiers forment une base de Gröbner de l'idéal engendré pour l'ordre $\mathsf{lex}(\partial_\nu, \partial_x)$; les deux derniers pour l'ordre $\mathsf{lex}(\partial_x, \partial_\nu)$.

EXERCICE 3. Pour chacun des idéaux $Ap_1 + Ap_2$ et $Ap_2 + Ap_3$, calculer la base de Gröbner minimale réduite pour chacun des deux ordres $\mathsf{lex}(\partial_\nu, \partial_x)$ et $\mathsf{lex}(\partial_x, \partial_\nu)$.

Bien évidemment, J est une fonction ∂-finie. Le module $A \cdot J$ est donné, par exemple, comme l'espace vectoriel sur $\mathbb{C}(\nu, x)$ de base $(J, \partial_\nu \cdot J)$. Pour représenter le carré de J en vue d'une sommation, on peut observer que, en tant qu'espace vectoriel, le module $A \cdot J^2$ admet la base $\big(J^2, J \times (\partial_\nu \cdot J), (\partial_\nu \cdot J)^2\big)$ et utiliser l'algorithme de clôture par produit pour obtenir une base de Gröbner. En fait, le calcul qui suit n'a même pas besoin d'une représentation aussi explicite de $f = J^2$: pour calculer la somme $\frac{1}{2}J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \cdots$ comme fonction de x, on recherche une fonction η de x, indépendante de ν, telle que $f' + \eta f$ soit la différence finie en ν d'un élément g de $A \cdot J^2$. Pour la suite du calcul, nous fixons cet élément sous la forme indéterminée donnée par

$$g(\nu) = \phi_0(\nu)J_\nu^2 + \phi_1(\nu)J_{\nu+1}^2 + \phi_2(\nu)J_\nu J_{\nu+1},$$

où nous avons omis de faire référence à la variable x dans les évaluations de g, des ϕ_i et de J, car cette variable ne va intervenir que comme paramètre dans le calcul des fractions rationnelles ϕ_i. (On peut penser qu'on travaille temporairement dans l'algèbre de Ore $A' = \mathbb{C}(\nu, x)\langle \partial_\nu; S_\nu \rangle$.)

En supposant le problème résolu, on a alors par construction la relation $f' + \eta f = (\partial_\nu - 1) \cdot g$, puis, après réduction de chaque occurence des dérivées et décalées de J par la base de Gröbner $\{p_2, p_3\}$,

$$\begin{aligned}
&2J_\nu J'_\nu + \eta J_\nu^2 = (\partial_\nu - 1) \cdot \big(\phi_0(\nu)J_\nu^2 + \phi_1(\nu)J_{\nu+1}^2 + \phi_2(\nu)J_\nu J_{\nu+1}\big) \\
&= \phi_0(\nu+1)J_{\nu+1}^2 - \phi_0(\nu)J_\nu^2 + \phi_1(\nu+1)x^{-2}\big(2(\nu+1)J_{\nu+1} - xJ_\nu\big)^2 - \phi_1(\nu)J_{\nu+1}^2 \\
&\qquad + \phi_2(\nu+1)x^{-1}J_{\nu+1}\big(2(\nu+1)J_{\nu+1} - xJ_\nu\big) - \phi_2(\nu)J_\nu J_{\nu+1},
\end{aligned}$$

laquelle se récrit

$$\begin{aligned}
&\big(2\nu x^{-1} + \eta\big)J_\nu^2 - 2J_\nu J_{\nu+1} \\
&= \big(\phi_1(\nu+1) - \phi_0(\nu)\big)J_\nu^2 - \big(4(\nu+1)x^{-1}\phi_1(\nu+1) + \phi_2(\nu+1) + \phi_2(\nu)\big)J_\nu J_{\nu+1} \\
&\quad + \big(\phi_0(\nu+1) + 4(\nu+1)^2x^{-2}\phi_1(\nu+1) - \phi_1(\nu) + 2(\nu+1)x^{-1}\phi_2(\nu+1)\big)J_{\nu+1}^2.
\end{aligned}$$

De l'indépendance linéaire des fonctions J_ν^2, $J_{\nu+1}^2$ et $J_\nu J_{\nu+1}$ sur $\mathbb{C}(\nu, x)$, on déduit les relations nécessaires

$$\begin{aligned}
-\phi_0(\nu) + \phi_1(\nu+1) &= 2\nu x^{-1} + \eta, \\
4(\nu+1)x^{-1}\phi_1(\nu+1) + \phi_2(\nu) + \phi_2(\nu+1) &= 2, \\
\phi_0(\nu+1) - \phi_1(\nu) + 4(\nu+1)^2x^{-2}\phi_1(\nu+1) + 2(\nu+1)x^{-1}\phi_2(\nu+1) &= 0.
\end{aligned}$$

En résolvant les deux premières respectivement en ϕ_0 et en ϕ_1, puis en substituant dans la dernière, on trouve la récurrence

$$\begin{aligned}
&x^2(\nu+1)\phi_2(\nu+3) - (\nu+1)(4\nu^2 + 20\nu + 24 - x^2)\phi_2(\nu+2) \\
&+(\nu+3)(4\nu^2+12\nu+8-x^2)\phi_2(\nu+1) - x^2(\nu+3)\phi_2(\nu) = -4x(\eta\nu^2 + 4\eta\nu + 3\eta + x).
\end{aligned}$$

Nous résolvons maintenant celle-ci en ses solutions rationnelles par l'algorithme d'Abramov, dans sa variante paramétrée qui résoud en $\phi_2 \in \mathbb{C}(n, \nu)$ et simultanément en $\eta \in \mathbb{C}$. Les coefficients extrêmes de la partie homogène indiquent que toute solution rationnelle doit être polynomiale, puisque le p. g. c. d. entre $(\nu-3)+1$

et $x+3$ vaut 1. La mise sous forme de différences finies de la partie homogène indique que l'opérateur associé accroît de 2 le degré d'un polynôme. Le degré de la partie inhomogène étant 2, toute solution rationnelle ne peut être qu'une constante. On trouve $\phi_2 = 1$ et $\eta = 0$, d'où après report $\phi_1 = 0$ et $\phi_0 = -2\nu/x$. Autrement dit, on a

$$\partial_x \cdot J_\nu^2 = (\partial_\nu - 1) \cdot \left(J_\nu J_{\nu+1} - 2\nu x^{-1} J_\nu^2 \right),$$

qui par sommation fournit

$$\partial_x \cdot \sum_{\nu=0}^{N} J_\nu^2 = J_{N+1}\big(J_{N+2} - 2(N+1)x^{-1} J_{N+1}\big) - J_0 J_1.$$

Comme la série $J_N \in \mathbb{C}[[x]]$ a valuation N, le membre droit tend vers $-J_0 J_1 = \frac{1}{2}\partial_x \cdot J_0^2$ quand N tend vers ∞ pour la topologie usuelle donnée par la métrique $|s| = 2^{-v}$ pour toute série non nulle s de valuation v. On a donc

$$\partial_x \cdot \left(\tfrac{1}{2} J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \cdots \right) = 0$$

qui caractérise la somme par une condition initiale. Une simple évaluation en 0 montre que la somme vaut $\frac{1}{2}$, ce qui achève la preuve de l'identité annoncée.

3. Bases de Gröbner de modules et découplage de systèmes

Dans l'exemple qui précède, on a pour le moment effectué le découplage « à la main », mais un procédé systématique et automatique est disponible, par le biais des bases de Gröbner de modules, qui généralisent la notion de base de Gröbner pour les idéaux. Cette notion existe tant dans le domaine des polynômes commutatifs que dans le cadre non commutatif des algèbres de Ore ; nous la présentons directement dans ce second cas.

Dans le cas d'un idéal I d'une algèbre de Ore A, les éléments de I s'interprètent comme autant d'équations vérifiées par une fonction inconnue ϕ. Dans une perspective algorithmique, chaque idéal est engendré par un nombre fini de générateurs. Une question naturelle est celle de systèmes linéaires sur un vecteur de fonctions inconnues $(\phi_1, \ldots, \phi_d)$, à coefficients dans A. On considère des systèmes d'un nombre fini d'équations de la forme $g_i = g_{i,1} \cdot \phi_1 + \cdots + g_{i,d} \cdot \phi_d$ pour des polynômes tordus $g_{i,j}$ de A. Un tel système se représente de façon compacte par une matrice $(g_{i,j})$ à entrées dans A. Les questions qui sont alors naturelles sont celle de l'algèbre linéaire pour ces matrices, dont en particulier celle de donner un algorithme du pivot de Gauss pour des coefficients dans A, c'est-à-dire non plus dans un corps, mais dans un anneau, et non commutatif de surcroît.

Pour ce faire, au lieu de considérer simplement un ordre monomial sur les monômes ∂^a d'une algèbre de Ore $A = k(x)\langle \partial; \sigma, \delta \rangle$, pour lequel tout idéal à gauche admet une base de Gröbner, on s'intéresse plus généralement à un module libre de rang fini sur A, donné par une base sous la forme $A^d = Ae_1 + \cdots + Ae_d$ et muni d'un ordre sur les $\partial^a e_i$, dans lequel on va étendre la notion de base de Gröbner pour des sous-modules à gauche de A^d. La notion d'ordre monomial conserve formellement la même définition, si ce n'est que les e_i ne peuvent apparaître que linéairement dans les monômes $\partial^a e_i$ et qu'ils ne peuvent servir pour des multiplications à gauche. La notion de S-polynôme s'étend aussi mot pour mot, à ceci près que deux polynômes de monômes de tête $\partial^a e_i$ et $\partial^b e_j$ ont un S-polynôme nul dès lors que i et j sont différents. Les définitions et caractérisations équivalentes des bases de Gröbner d'idéaux restent alors valables pour les sous-modules du module libre A^d.

L'algorithme de Buchberger, modifié pour suivre ces nouvelles définitions, termine sur tout sous-module en fournissant une base de Gröbner. Pour certains ordres, ce calcul correspond à l'algorithme de Gauss.

Un point de vue presque équivalent, mais qui donne une variante des calculs avec un peu plus de réductions, est que le calcul est celui d'une base de Gröbner dans l'anneau $A[e_1, \ldots, e_d]$ des polynômes en les indéterminées commutatives e_i à coefficients dans l'anneau A pour l'idéal à gauche engendré par les g_i initiaux et tous les produits $e_i e_j = 0$.

Reprenons l'exemple du découplage des relations entre les coordonnées ϕ_i donnant g dans la section précédente sur la somme des carrés fonctions de Bessel. Ces relations se recodent par les éléments

$$\begin{aligned}
g_1 &:= -e_0 + \partial_\nu e_1 - (2\nu x^{-1} + \eta)e_3,\\
g_2 &:= 4(\nu+1)x^{-1}\partial_\nu e_1 + (\partial_\nu + 1)e_2 - 2e_3,\\
g_3 &:= \partial_\nu e_0 + \big(4(\nu+1)^2 x^{-2}\partial_\nu - 1\big)e_1 + 2(\nu+1)x^{-1}\partial_\nu e_2,\\
g_4 &:= (\partial_\nu - 1)e_3,
\end{aligned}$$

du module libre A^4 pour l'algèbre de Ore $A = \mathbb{C}(n,k)\langle \partial_n, \partial_k; S_n, S_k\rangle$. Ici, chaque e_i représente la fonction rationnelle inconnue ϕ_i, et l'on a astucieusement représenté les second membres de équations inhomogènes d'origine comme multiple d'une nouvelle inconnue représentée par e_3 et contrainte par g_4 à être constante.

Le découplage effectué dans la section précédente revient au calcul d'une base de Gröbner pour l'ordre $\mathsf{lex}(e_0, e_1, e_2, e_3, \partial_\nu)$. Les monômes de tête respectifs des g_i sont e_0, $\partial_\nu e_1$, $\partial_\nu e_0$ et $\partial_\nu e_3$, si bien que le seul S-polynôme non nul est $\mathrm{Spoly}(g_1, g_3)$. Il est donné par

$$\begin{aligned}
&\mathrm{Spoly}(g_1, g_3) = \partial_\nu g_1 + g_3\\
&\quad = \big(\partial_\nu^2 + 4(\nu+1)^2 x^{-2}\partial_\nu - 1\big)e_1 + 2(\nu+1)x^{-1}\partial_\nu e_2 - \big(2(\nu+1)x^{-1} + \eta\big)\partial_\nu e_3.
\end{aligned}$$

Après réductions par g_2 et g_3, ce polynôme devient

$$g_5 = -e_1 - \left(\frac{x}{4(\nu+2)}\partial_\nu^2 + \frac{x^2 - 4\nu^2 - 12\nu - 8}{4x(\nu+2)}\partial_\nu + \frac{\nu+1}{x}\right)e_2 + \left(\frac{x}{2(\nu+2)} - \eta\right)e_3,$$

qui est adjoint à la base de Gröbner en cours de calcul. L'unique nouvel S-polynôme à considérer est celui entre ce g_5 et g_2, qui est $\mathrm{Spoly}(g_2, g_4) = g_2 + 4(\nu+1)x^{-1}\partial_\nu g_5$ et a pour monôme de tête $\partial_\nu^3 e_2$. Après réduction par e_3 et renormalisation, le dernier polynôme introduit dans la base de Gröbner est

$$\begin{aligned}
\big((\nu+1)x^2\partial_\nu^3 + (\nu+1)(x^2 - 4\nu^2 - 20\nu - 24)\partial_\nu^2 \\
- (\nu+3)(x^2 - 4\nu^2 - 12\nu - 8)\partial_\nu - (\nu+3)x^2\big)e_2 \\
+ 4\big((\nu^2 + 4\nu + 3)\eta + x\big)x e_3.
\end{aligned}$$

Ce polynôme n'est autre qu'un recodage de l'équation inhomogène du troisième ordre qui a permis de déterminer ϕ_2 dans la section précédente.

Bibliographie

[1] Chyzak (Frédéric). – An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Mathematics*, vol. 217, n° 1-3, 2000, pp. 115–134.