COURS 11

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

DEFINITION 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', \ldots , 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 d suffisamment grand, $A, A', \ldots, A^{(d)}$ sont liées et une relation de liaison entre ces dérivées est une équation différentielle linéaire.

DEFINITION 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

(1)
$$p_d(n)a_{n+d} + p_{d-1}(n)a_{n+d-1} + \dots + p_0(n)a_n = 0, \qquad n \ge 0,$$
 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

(2)
$$q_0(X)A^{(d)}(X) + \dots + q_d(X)A(X) = 0$$

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

(3)
$$[X^n]f'(X) = (n+1)[X^{n+1}]f(X) \quad (n \ge 0),$$

$$[X^n]X^k f(X) = [X^{n-k}]f(X) \quad (n \ge k).$$

Par conséquent, l'extraction du coefficient de X^n de (2) fournit une récurrence linéaire sur les a_n valide dès lors que $n \ge n_0 := \max_{0 \le i \le d} \deg q_i$. Pour obtenir une récurrence valide pour tout $n \ge 0$, 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

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

où A est la série génératrice des coefficients a_n et la notation $(Xd/dX)^k$ signifie que l'opérateur 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

$$q_0(X)A^{(d)}(X) + \dots + q_d(X)A(X) = p(X),$$

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. \Box

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 $\S 1.3$.

1.2. Exemples d'applications.

Exemple 1. Pour calculer le coefficient de X^{1000} dans

$$(1+X)^{1000}(1+X+X^2)^{500}$$
,

une méthode efficace part de l'observation que ce polynôme vérifie l'équation différentielle linéaire du premier ordre

$$\frac{y'}{y} = 1000 \frac{1}{1+X} + 500 \frac{2X+1}{1+X+X^2}.$$

Il s'ensuit que les coefficients de ce polynôme vérifient une récurrence d'ordre 3 à coefficients de degré 1. La méthode de scindage binaire vue au cours 2 permet alors un calcul très rapide.

EXEMPLE 2. Pour calculer une racine du polynôme $P_N(x)$ défini par la série génératrice

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

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.

EXEMPLE 3. 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 rapide ★. Vue l'efficacité obtenue grâce au 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, en mettant en œuvre des techniques abordées dans des cours précédents.
- 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 d/dX, mais comme un polynôme en X et $\theta = Xd/dX$ (θ est parfois appelé l'opérateur d'Euler), alors la conversion en récurrence est assez facile : partant de

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

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 d en θ et m en X se calcule en O(mM(d)) opérations sur les coefficients.

Par rapport au nombre dm de coefficients du résultat, cette complexité est quasi-optimale.

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 d ne requiert que O(M(d)) opérations, par exemple en utilisant la somme composée vue au cours 6.

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+d, il s'agit donc maintenant de calculer des polynômes $b_i(X)$ tels que

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

Récrire le polynôme sous la forme

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

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 P 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

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

ce qui montre que les valeurs de P en $0, \ldots, d$ peuvent être obtenues en O(M(d)) opérations à partir des coefficients a_i , et par suite les coefficients de P en $O(M(d)\log d)$ opérations par interpolation en utilisant les techniques du cours sur l'évaluation-interpolation.

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

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

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+d avec des coefficients de degré au plus d, 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 4. 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 :

$$u_n = F_{n+2}F_n - F_{n+1}^2 = F_{n+1}F_n + F_n^2 - F_{n+1}^2,$$

$$u_{n+1} = F_{n+2}F_{n+1} + F_{n+1}^2 - F_{n+2}^2 = F_{n+1}^2 - F_n^2 - F_nF_{n+1}$$

$$= -u_n.$$

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 $n=0,\ldots,4$ 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

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

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 5. 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 (car la caractéristique est nulle!). En dérivant P(X,Y)=0 et en isolant Y', il vient

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

Par inversion modulaire de P_Y (voir Cours 10), cette identité se récrit via un calcul de pgcd étendu en

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

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 6. 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 scindage binaire. Dans le cas des nombres de Catalan, la récurrence est d'ordre 1, la suite est donc hypergéométrique et s'exprime aisément.

NOTES 121

EXERCICE 4. Trouver une formule explicite des nombre de Catalan. Récrire les fonctions Γ qui pourraient apparaître dans le résultat en termes de factorielles, puis de coefficient binomial.

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 7. 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.

Notes

Les propriétés de clôture des séries D-finies ont été décrites avec leurs applications par Stanley dans [12] ainsi que dans son livre [13], et par Lipshitz dans [8].

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 [6]. Quelques années plus tard, il est encore retrouvé par Tannery [14] 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 [7] et à Singer pour les deux autres [10].

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 [9]. L'algorithme rapide de la section 1.3 provient essentiellement de [3], qui donne une variante légèrement plus efficace (d'un facteur constant). L'exemple 1 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] 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.
- [7] 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.
- [8] Lipshitz (L.). D-finite power series. Journal of Algebra, vol. 122, n° 2, 1989, pp. 353–373.
- [9] 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.
- [10] 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.
- [11] Sloane (N. J. A.). The On-Line Encyclopedia of Integer Sequences. 2006. Published electronically at http://www.research.att.com/~njas/sequences/.
- [12] Stanley (R. P.). Differentiably finite power series. European Journal of Combinatorics, vol. 1, n° 2, 1980, pp. 175–188.
- [13] Stanley (Richard P.). Enumerative combinatorics. Cambridge University Press, 1999, vol. 2, xii+581p.
- [14] 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.