THÈSE DE DOCTORAT

DE

L'UNIVERSITÉ PARIS-SACLAY

PRÉPARÉE À

L'ÉCOLE POLYTECHNIQUE

ÉCOLE DOCTORALE N°580
Sciences et Technologies de l'Information et de la Communication

Spécialités : Mathématiques et Informatique

Algorithmes rapides pour le calcul symbolique de certaines intégrales de contour à paramètre

par

Louis DUMONT

Thèse présentée et soutenue à Palaiseau, le 5 décembre 2016

Composition du jury :

Mme Paola BOITO	Maître de conférences, Université de Limoges	Examinatrice
M. Alin BOSTAN	Chargé de recherche, Inria Saclay	Directeur de thèse
Mme Delphine BOUCHER	Maître de conférences, Université de Rennes 1	Examinatrice
M. Guillaume CHÈZE	Maître de conférences, Université de Toulouse 3	Rapporteur
M. Joris VAN DER HOEVEN	Directeur de recherche, CNRS	Examinateur
Mme Evelyne HUBERT	Chargée de recherche, Inria Sophia Antipolis	Rapporteure
M. Bruno SALVY	Directeur de recherche, Inria Grenoble	Directeur de thèse
M. Jacques-Arthur WEIL	Professeur, Université de Limoges	Examinateur

Table des matières

Introduction

Le fruit du travail du mathématicien prend généralement la forme de traités structurés, épurés et d'une grande généralité sur des objets plus ou moins abstraits. Pour bâtir de tels édifices, le calcul est un outil indispensable. Il émerge au sein du produit fini, bien sûr, car il sert naturellement à l'élaboration de la preuve mathématique. Je pense par exemple aux *Disquisitiones Arithmeticae*, œuvre majeure de Gauss, où certaines preuves font intervenir de longues manipulations formelles sur les équations. En outre, le calcul a une importance fondamentale, bien que moins ostensible, dans la phase de tâtonnement et d'expérimentation qui est à l'origine de la production mathématique. Je pense à Euler qui est connu certes pour son œuvre gigantesque, mais aussi pour ses dons en calcul mental. Je pense aussi à l'œuvre de Jacobi, dans laquelle on trouve quantité de calculs sur des exemples concrets. Par ailleurs, le calcul joue un rôle bien plus direct dans de nombreuses applications : en cryptographie, en combinatoire, en physique, et bien d'autres.

Le calcul formel est l'art de conduire de façon exacte et rapide les calculs sur les objets mathématiques. Pour y parvenir, il faut tout d'abord une bonne façon de représenter l'objet, puis on élabore un algorithme qui effectue l'opération souhaitée à partir de cette représentation. Bien souvent, on dispose de plusieurs représentations possibles pour un même objet, et on peut être amené selon le contexte à jongler entre elles. Il est donc nécessaire de rechercher également des algorithmes efficaces pour les changements de représentation. Par ailleurs, on aimerait bien sûr pouvoir automatiser le calcul. Dès lors que l'on choisit de déléguer le travail à un ordinateur, il devient capital d'avoir des représentations *finies* pour les données que l'on manipule afin de pouvoir les stocker en mémoire.

Ici, je vais traiter de questions liées à l'intégration formelle des fonctions. Dans toute sa généralité, c'est un problème d'une portée trop vaste ; si l'on considère une fonction $f : \mathbb{C} \longrightarrow \mathbb{C}$ trop générale, on sera bien en peine d'en trouver une représentation qui permet de la manipuler algorithmiquement. De même, si f dépend en plus d'un paramètre, discret ou continu, son intégrale sera elle-même une fonction pour laquelle on aura besoin d'une représentation finie. Il est donc nécessaire de se restreindre à des classes de fonctions simples pour lesquelles on dispose d'une représentation finie, à la fois pour l'intégrande et pour l'intégrale.

Le travail qui suit s'articule autour de deux familles d'intégrales de contour à un paramètre, pour lesquelles on disposera effectivement de structures de données finies et que l'on souhaitera calculer. Avant de donner des définitions précises et de dire ce que j'entends par « calculer » ces intégrales, je vais commencer par donner

quelques exemples qui permettront de se faire une idée du type d'objets mis en jeu et du contexte dans lequel ils peuvent apparaître.

0.1 Première série d'exemples avec un paramètre discret

La première famille regroupe des intégrales de contour qui dépendent d'un paramètre *discret*.

Coefficients d'un développement en série de Taylor.
Considérons la fonction

$$f(x) = (1+x)\exp\left(\frac{1}{1-x^2}\right).$$

Elle admet un développement en série de Taylor au voisinage de 0 :

$$f(x) = \sum_{n\geqslant 0} u_n x^n.$$

La suite u_n est alors donnée par les intégrales de Cauchy :

$$u_n = \frac{1}{2\pi i}\oint \frac{f(x)}{x^{n+1}}\mathrm{d}x,$$

l'intégrale étant prise sur un petit cercle autour de 0.

Plus généralement, on saura traiter ce type d'intégrales lorsque l'on remplace f par n'importe quelle fonction hyperexponentielle de x, c'est-à-dire satisfaisant une équation différentielle de la forme

$$f'(x) + r(x)f(x) = 0$$

pour une certaine fraction rationnelle r.

Inverse compositionnel d'un polynôme.
On se donne un polynôme univarié p tel que $p(0) = 0$ et $p'(0) \neq 0$. L'inverse compositionnel de p est l'unique série q de la forme

$$q(x) = \sum_{n\geqslant 1} u_n x^n$$

et telle que

$$p(q(x)) = q(p(x)) = x.$$

Alors les coefficients u_n sont donnés par les intégrales

$$u_n = \frac{1}{2\pi i n}\oint \frac{\mathrm{d}x}{p(x)^n},$$

prises sur un petit cercle autour de 0.

Polynômes de Hermite.

Les polynômes de Hermite forment une famille orthogonale de polynômes. Ils peuvent par exemple être définis de la façon suivante :

$$\mathrm{H}_n(x) = (-1)^n \exp\left(\frac{x^2}{2}\right) \frac{\mathrm{d}^n}{\mathrm{d}x^n} \exp\left(-\frac{x^2}{2}\right).$$

Ces polynômes admettent la représentation intégrale

$$\mathrm{H}_n(x) = \frac{n!}{2\pi i} \oint \frac{\exp\left(tx - \frac{t^2}{2}\right)}{t^{n+1}} \mathrm{d}t.$$

Cadre général.

Dans tous ces exemples, on intègre une suite de fonctions $\Psi(x,n)$ telle que les deux rapports

$$\frac{\Psi(x,n+1)}{\Psi(x,n)} \quad \text{et} \quad \frac{\partial_x \Psi(x,n)}{\Psi(x,n)} \tag{1}$$

sont des fractions rationnelles en n et x. Usuellement, on dit qu'une fonction satisfaisant cette propriété est un *terme mixte hypergéométrique et hyperexponentiel*. Mixte car Ψ dépend à la fois d'une variable continue et d'une variable discrète, hypergéométrique car le premier rapport dans (1) est rationnel, et hyperexponentiel car le deuxième rapport dans (1) est rationnel. On peut se convaincre assez facilement que les deux rapports de (1) caractérisent entièrement Ψ à une constante multiplicative près (indépendante à la fois de x et de n). On peut donc utiliser ces deux fractions rationnelles comme structure de données pour effectuer des opérations qui ne dépendent pas des constantes multiplicatives. Si l'on désire également être capable de déterminer la constante, il faut rajouter une information supplémentaire, comme une évaluation de Ψ par exemple.

0.2 Seconde série d'exemples avec un paramètre continu

Scrutin à deux candidats [1]**.**

On procède au dépouillement d'un vote entre deux candidats, en autorisant les votes blancs. On note b_n la probabilité que les deux candidats soient à égalité après le dépouillement de n bulletins. Comme souvent en combinatoire, la *série génératrice* $\sum_{n\geqslant 0} b_n x^n$ associée à la suite b_n est un outil utile dans son étude. Dans ce cas précis, elle admet la représentation intégrale :

$$\sum_{n\geqslant 0} b_n x^n = \frac{1}{2\pi i} \oint \frac{\mathrm{d}y}{y - \frac{x}{3}(1+y+y^2)}.$$

1. PÓLYA, "Sur les séries entières, dont la somme est une fonction algébrique", §3.

Les dés de Pólya[2]**.**

Imaginons que l'on jette une paire de dés un certain nombre n de fois, et que l'on observe la somme totale obtenue. Alors le score le plus probable est de $7n$. Mais quelle est la probabilité p_n d'obtenir ce score ? Il se trouve que la série génératrice des nombres p_n satisfait :

$$\sum_{n\geqslant 0} p_n x^n = \frac{1}{2\pi i}\oint \frac{y^4}{y^5 - \frac{x}{6^2}(1+y+y^2+y^3+y^4+y^5)^2}\mathrm{d}y.$$

Diagonale d'une fraction rationnelle.

Pour cet exemple, je donne une définition générale car il reviendra de façon importante dans la suite.

Définition 1. Soit $\mathbf{k}$ un corps, et soit $\mathrm{F}\in\mathbf{k}(x,y)$ une fraction rationnelle à deux variables dont le dénominateur ne s'annule pas en $(0,0)$. Alors F admet un développement en série entière :

$$\mathrm{F}(x,y) = \sum_{i,j\geqslant 0} a_{i,j}x^i y^j,$$

avec $a_{i,j}\in\mathbf{k}$ pour tous i et j positifs.

La *diagonale* de F, notée $\Delta\mathrm{F}$ est alors définie comme étant la série univariée

$$\Delta\mathrm{F}(t) = \sum_{n\geqslant 0} a_{n,n}t^n.$$

L'exemple non-trivial le plus simple est celui de la fraction rationnelle

$$\mathrm{F}(x,y) = \frac{1}{1-x-y}.$$

Dans ce cas, on peut calculer le développement explicitement et on obtient

$$\mathrm{F}(x,y) = \sum_{i,j\geqslant 0}\binom{i+j}{i}x^i y^j.$$

On en déduit que sa diagonale vaut par définition :

$$\Delta\mathrm{F}(t) = \sum_{n\geqslant 0}\binom{2n}{n}t^n.$$

Un autre exemple un peu moins évident : on considère la suite d'entiers

$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$

C'est la célèbre suite des nombres de Catalan, intervenant dans le dénombrement de nombreux objets en combinatoire. Il se trouve que leur série génératrice peut

2. PÓLYA, "Sur les séries entières, dont la somme est une fonction algébrique", §4.

être vue comme une diagonale de fraction rationnelle. On pourra en effet vérifier que

$$\sum_{n\geqslant 0} c_n t^n = \Delta\left\{\frac{1-2x}{(1-x)(1-x-y)}\right\}.$$

À ce stade, le lecteur se demandera sûrement ce que vient faire cette notion de diagonale là où avaient été annoncés des exemples d'intégrales. La raison en est que les diagonales admettent toujours des représentations intégrales : si F est une fraction rationnelle, alors

$$\Delta \mathrm{F}(t) = \frac{1}{2\pi i}\oint \frac{1}{y} f\left(\frac{t}{y}, y\right) \mathrm{d}y,$$

où, sans rentrer dans le détail pour l'instant, le contour est un cercle inclus dans une petite couronne autour de 0.

Cadre général.

Dans ce second groupe d'exemples, les intégrales sont toutes de la forme

$$\oint \mathrm{F}(x, y)\mathrm{d}y,$$

où $\mathrm{F}(x, y)$ est une fraction rationnelle bivariée, et où le contour est un petit cercle autour de 0. Je reviendrai de façon plus précise sur les contours d'intégration dans le premier chapitre.

0.3 Structures de données pour représenter les intégrales

Dans les deux familles d'exemples ci-dessus, on a vu que l'on dispose de structures de données pour les intégrandes. Les intégrales quant à elles sont également des fonctions du paramètre. Pour les représenter dans l'ordinateur, une méthode classique consiste à les voir comme des solutions d'équations (algébriques, différentielles, ...). Illustrons cette idée de base dans un cadre plus habituel. Pour manipuler formellement un nombre algébrique, on ne va pas passer par son écriture décimale, car elle peut être infinie. On va plutôt le représenter comme la racine d'un certain polynôme. Ainsi, lorsqu'on écrit $\sqrt{2}$, le plus souvent on entend par là « l'un des deux nombres satisfaisant l'équation $x^2-2=0$ ». Évidemment, en faisant cela on ne fait plus la différence entre $\sqrt{2}$ et $-\sqrt{2}$. Pour lever cette ambiguïté, on pourrait ajouter une information supplémentaire, comme le fait que c'est l'unique solution positive de l'équation. Mais pour beaucoup d'opérations, cette ambiguïté n'est pas gênante. Par exemple, si l'on souhaite simplifier l'expression

$$x^3 - x + 1,$$

avec $x = \sqrt{2}$, alors il suffit de savoir que $x^2 - 2 = 0$ pour faire le calcul

$$x^3 - x + 1 = 2x - x + 1 = x + 1.$$

En utilisant cette structure de données, on peut également effectuer les opérations de base sur les nombres algébriques. Par exemple, en voyant $x = \sqrt{2}$ et $y = \sqrt{3}$ comme des solutions de $x^2 - 2 = 0$ et $y^2 - 3 = 0$ respectivement, on peut facilement obtenir un polynôme annulant $z = x + y = \sqrt{2} + \sqrt{3}$. Il suffit de réécrire les puissances successives de z sur la base $(1, x, y, xy)$:

$$\begin{aligned}(x+y)^2 &= x^2 + 2xy + y^2 = 2xy + 5\ ;\\ (x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 = 11x + 9y\ ;\\ (x+y)^4 &= 20xy + 49.\end{aligned}$$

Et de là on voit facilement que

$$z^4 - 10z^2 + 1 = 0.$$

Ainsi, on adopte la même philosophie lorsque l'on manipule non plus des nombres, mais des fonctions. Reprenons l'exemple déjà rencontré ci-dessus des nombres de Catalan :

$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$

On considère la série génératrice

$$f(x) = \sum_{n \geqslant 0} c_n x^n$$

Alors la fonction f est solution de l'équation polynomiale

$$f(x) = 1 + x f(x)^2$$

(on dit que f est une fonction *algébrique*). À nouveau, cette équation est une représentation finie de la fonction f, qui devient non-ambiguë si l'on rajoute la condition initiale $f(0) = 0$. Par ailleurs, la fonction f vérifie aussi une équation différentielle homogène linéaire à coefficients polynomiaux :

$$x(4x-1)f''(x) + (10x-2)f'(x) + 2f(x) = 0. \tag{2}$$

On peut donc également choisir cette équation pour représenter la fonction f. Elle devient non-ambigüe si l'on précise les valeurs de $f(0)$, $f'(0)$ et $f''(0)$. Lorsqu'une fonction f satisfait une équation différentielle linéaire à coefficients polynomiaux telle que (2), on dira qu'elle est *différentiellement finie*.

La même idée s'applique lorsque f est une fonction d'une variable discrète, c'est-à-dire une suite. On pourra la représenter à l'aide d'une récurrence. Par exemple, si l'on considère la suite

$$u_n = n!,$$

on peut la représenter comme étant une solution de

$$u_{n+1} - (n+1)u_n = 0. \tag{3}$$

Lorsqu'une suite (u_n) vérifie une récurrence linéaire à coefficients polynomiaux telle que (3), on dira qu'elle est *polynomialement récursive*.

Parmi les exemples ci-dessus, on verra par la suite que toutes les intégrales dépendant d'un paramètre continu sont des fonctions algébriques. En particulier cela implique qu'elles sont également différentiellement finies (c'est un vieux théorème remontant à Abel, voir le théorème 117 en annexe). Quand aux intégrales dépendant d'un paramètre discret, ce sont des suites polynomialement récursives. De là, une façon naturelle de formuler le problème du calcul de ces intégrales est la suivante : une fonction dépendant d'un paramètre étant donnée, trouver une équation, algébrique ou différentielle, ou une récurrence satisfaite par son intégrale.

0.4 La méthode du télescopage créatif pour calculer les intégrales

Une méthode aujourd'hui très classique pour s'attaquer à ce genre de problème est le télescopage créatif. Illustrons-la sur l'exemple de l'intégrale

$$\oint \frac{\mathrm{d}y}{y-x-y^2}.$$

On peut vérifier que l'intégrande vérifie :

$$(1-4x)\cdot\partial_x\left(\frac{1}{y-x-y^2}\right)-2\cdot\frac{1}{y-x-y^2}=\partial_y\left(\frac{2y-1}{y-x-y^2}\right). \tag{4}$$

Nous verrons bien sûr par la suite d'où vient ce type de résultat, mais contentons nous pour le moment de constater que cette relation est suffisante pour calculer l'intégrale qui nous intéresse. En effet, en intégrant de chaque côté de l'égalité, le membre de droite devient nul, tandis que dans le membre de gauche l'intégration par rapport à y et la dérivation par rapport à x commutent. On en tire donc :

$$(1-4x)\cdot\partial_x\left(\oint\frac{\mathrm{d}y}{y-x-y^2}\right)-2\oint\cdot\frac{\mathrm{d}y}{y-x-y^2}=0.$$

Dans ce cas simple, on peut même résoudre cette équation différentielle explicitement et obtenir l'expression

$$\oint\frac{\mathrm{d}y}{y-x-y^2}=\frac{c}{\sqrt{1-4x}},$$

pour une certaine constante c.

Le point clé de la méthode est donc d'établir une relation telle que (4). C'est ce procédé que l'on appelle le *télescopage créatif*.

Le même principe s'applique dans le cas d'un paramètre discret. Prenons par exemple l'intégrale

$$u_n=\oint\frac{\exp(x)}{x^{n+1}}\mathrm{d}x.$$

Ici une simple intégration par parties montre que l'intégrande satisfait la relation

$$\frac{\exp(x)}{x^{n+1}} - (n+1)\frac{\exp(x)}{x^{n+2}} = \partial_x\left(\frac{\exp(x)}{x^{n+1}}\right)$$

Et à nouveau en intégrant cette égalité le membre de droite s'annule et on obtient sans surprise la récurrence

$$u_n - (n+1)\,u_{n+1} = 0.$$

Plus généralement, il est pratique d'utiliser la notation d'opérateur. Si ∂ est la dérivation par rapport à x ($\partial f(x,y) = \partial_x f(x,y)$, cas continu) ou le décalage par rapport à x ($\partial f(x,y) = f(x+1,y)$, cas discret), on notera

$$\left(\sum_{i=0}^{r} a_i(x)\partial^i\right)\cdot f = \sum_{i=0}^{r} a_i(x)\partial^i f(x,y).$$

Si une fonction $f(x,y)$ satisfait une équation du type

$$\left(\sum_{i=0}^{r} a_i(x)\partial^i\right)\cdot f(x,y) = \partial_y g(x,y),$$

pour une certaine fonction g et des fractions rationnelles a_i, on dira que $\mathrm{L} = \sum_{i=0}^{r} a_i(x)\partial^i$ est un *télescopeur* pour f. L'entier r est alors appelé l'*ordre* de L, et le *degré* de L est défini comme le maximum des degrés des a_i.

Ici, nous n'appliquerons la méthode du télescopage créatif qu'à des exemples similaires à ceux-ci. C'est-à-dire dans des situations où l'on cherche à calculer l'intégrale d'une fonction par rapport à l'une de ses variables. La méthode s'applique par ailleurs à des exemples bien plus généraux. Notamment, on peut calculer ainsi non seulement des intégrales, mais aussi des sommes, simples ou multiples.

0.5 Résultats existants

0.5.1 Télescopage créatif

Les premiers embryons d'idées ayant mené au télescopage créatif remontent à des calculs de Fasenmyer[3] sur des suites hypergéométriques. C'est à Zeilberger[4] que l'on doit le premier algorithme général, qui repose sur des méthodes d'élimination. C'était alors plutôt un algorithme théorique, très peu efficace en pratique. De plus, cette approche fournit un télescopeur qui a priori n'est pas d'ordre minimal.

Une deuxième génération d'algorithmes vise à améliorer l'efficacité de l'algorithme de Zeilberger. En utilisant l'algorithme de Gosper[5], Zeilberger[6] met au

3. FASENMYER, "Some generalized hypergeometric polynomials" ; FASENMYER, "A Note on Pure Recurrence Relations".
4. ZEILBERGER, "A holonomic systems approach to special functions identities".
5. GOSPER, "Decision Procedure for Indefinite Hypergeometric Summation".
6. ZEILBERGER, "A fast algorithm for proving terminating hypergeometric identities".

point un algorithme rapide dans le cas de la sommation simple d'une suite hypergéométrique. Cette méthode est raffinée et généralisée au cas hypergéométrique multivarié dans la thèse de Yen [7], ainsi que par Wilf et Zeilberger [8]. Une variante de cette approche s'appliquant au cas de l'intégration simple d'une fonction hyperexponentielle est décrite par Almkvist et Zeilberger [9]. Vient ensuite l'algorithme de Chyzak [10] qui traite le cas d'une fonction différentiellement finie ou polynomialement récursive quelconque, et pour lequel Koutschan [11] a proposé des variantes visant à améliorer son efficacité en pratique. Cette deuxième génération a l'avantage d'être plus efficace en pratique et de permettre le calcul du télescopeur d'ordre minimal. Cependant, elle ne permet pas d'obtenir de bonnes bornes sur l'ordre et le degré du télescopeur calculé.

La troisième génération d'algorithmes permet de mieux maîtriser la taille du télescopeur calculé. Elle commence avec un article d'Apagodu et Zeilberger [12] qui proposent, dans le cas d'une suite hypergéométrique, un *ansatz* menant au calcul d'un télescopeur dont on maîtrise à la fois l'ordre et le degré. Cependant, on n'a aucune garantie quant à sa minimalité. Cette approche a été utilisée par Chen et Kauers [13], puis plus tard par Kauers et Yen [14] pour trouver des compromis de taille entre l'ordre et le degré de télescopeurs non-minimaux.

Enfin, plus récemment, de nombreux travaux ont été effectués sur une quatrième génération d'algorithmes qui reposent sur des réductions semblables à celle de Hermite pour l'intégration des fractions rationnelles [15]. L'avantage des approches par réductions est qu'elles produisent des algorithmes qui fournissent efficacement un télescopeur d'ordre minimal dont on maîtrise l'ordre et le degré. Les travaux dans cette lignée commencent avec Bostan, Chen, *et al.* [16] pour le cas de l'intégration des fractions rationnelles bivariées, étendu ensuite aux fonctions hyperexponentielles [17]. Plus récemment, en utilisant la réduction de Trager [18], le cas des fonctions algébriques bivariées a été traité par Chen, Kauers et Koutschan [19]. La généralisation à des fractions rationnelles dépendant d'un plus grand nombre de variables fait l'objet des travaux de Lairez avec Bostan et Salvy et dans sa thèse [20].

---

7. YEN, "Contributions to the proof theory of hypergeometric identities".
8. WILF et ZEILBERGER, "An alorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities".
9. ALMKVIST et ZEILBERGER, "The method of differentiating under the integral sign".
10. CHYZAK, "An extension of Zeilberger's fast algorithm to general holonomic functions".
11. KOUTSCHAN, "A Fast Approach to Creative Telescoping".
12. APAGODU et ZEILBERGER, "Multi-variable Zeilberger and Almkvist-Zeilberger algorithms and the sharpening of Wilf-Zeilberger theory".
13. CHEN et KAUERS, "Trading order for degree in creative telescoping" ; CHEN et KAUERS, "Order-degree curves for hypergeometric creative telescoping".
14. KAUERS et YEN, "On the length of integers in telescopers for proper hypergeometric terms".
15. HERMITE, "Sur l'intégration des fractions rationnelles".
16. BOSTAN, CHEN, CHYZAK et LI, "Complexity of creative telescoping for bivariate rational functions".
17. BOSTAN, CHEN, CHYZAK, LI et XIN, "Hermite reduction and creative telescoping for hyperexponential functions".
18. TRAGER, "Algebraic Factoring and Rational Function Integration".
19. CHEN, KAUERS et KOUTSCHAN, "Reduction-Based Creative Telescoping for Algebraic Functions".
20. BOSTAN, LAIREZ et SALVY, "Creative telescoping for rational functions using the Griffiths-Dwork method" ; LAIREZ, "Computing periods of rational integrals" ; LAIREZ, "Periods of rational integrals :

Enfin, on pourra également trouver un historique plus détaillé de la création télescopique dans le mémoire d'habilitation à diriger des recherches de Chyzak[21].

0.5.2 Diagonales de fractions rationnelles

Les diagonales de fractions rationnelles peuvent s'écrire comme des intégrales de fractions rationnelles. Ce fait était déjà constaté par Pólya[22], puis par Furstenberg[23] afin de montrer que les diagonales de fractions rationnelles bivariées sont algébriques. Il existe trois autres démonstrations purement algébriques de ce résultat. La première, due à Fliess[24] utilise des séries non-commutatives. La deuxième, due à Gessel[25], repose sur des manipulations formelles de séries de Laurent. La troisième, due à Bousquet-Mélou[26], repose sur des arguments de combinatoire.

La notion de diagonale se généralise à des séries en un plus grand nombre de variables : la diagonale d'une série multivariée ayant pour coefficients $a_{i_1,i_2,\ldots,i_k}$ est la série univariée ayant pour coefficients $a_{i,i,\ldots,i}$. C'est une notion très riche qui fait encore aujourd'hui l'objet de nombreuses recherches. Il est encore vrai en caractéristique non-nulle que la diagonale d'une fraction rationnelle multivariée est algébrique[27]. En caractéristique nulle, ce n'est plus vrai en général, mais Christol[28] et Lipshitz[29] ont montré que les diagonales sont toujours différentiellement finies.

0.6 Plan de la thèse et contributions

0.6.1 Survol

Le premier chapitre aborde quelques points techniques qui sont nécessaires dans la suite de l'exposé, et ne contient pas de nouveaux résultats. La majeure partie des contributions est regroupée dans les deuxième et troisième chapitre, où sont attaqués de façon indépendante deux problèmes d'intégration. Le quatrième chapitre est une application directe du chapitre trois au calcul de polynômes annulateurs pour les diagonales de fractions rationnelles. Le dernier chapitre est une application en combinatoire, pour le calcul des séries génératrices de marches unidimensionnelles.

Je développe maintenant avec un peu plus de précision la structure et les résultats des différents chapitres. Certaines notations standard ne seront rappelées que dans la section 0.7 ci-après, on pourra s'y référer en cas de doute. Précisons également que les résultats de complexité seront énoncés dans le modèle de la

algorithms and applications".

21. CHYZAK, "The ABC of Creative Telescoping — Algorithms, Bounds, Complexity".
22. PÓLYA, "Sur les séries entières, dont la somme est une fonction algébrique".
23. FURSTENBERG, "Algebraic Functions over Finite Fields".
24. FLIESS, "Sur divers produits de séries formelles".
25. GESSEL, "A factorization for formal Laurent series and lattice path enumeration".
26. BOUSQUET-MÉLOU, "Rational and algebraic series in combinatorial enumeration", §3.4.1.
27. FURSTENBERG, "Algebraic Functions over Finite Fields", Th. 1.
28. CHRISTOL, "Diagonales de fractions rationnelles et équations différentielles" ; CHRISTOL, "Diagonales de fractions rationnelles et équations de Picard-Fuchs".
29. LIPSHITZ, "The diagonal of a D-finite power series is D-finite".

complexité *arithmétique* dans le pire des cas. On compte donc le nombre d'opérations élémentaires effectuée dans le corps de base par les algorithmes. On utilisera la notation $\tilde{O}$ pour signifier que l'on néglige des facteurs polylogarithmiques.

0.6.2 Deuxième chapitre

Le deuxième chapitre est consacré au calcul d'intégrales de termes mixtes hypergéométriques et hyperexponentiels par télescopage créatif. Il s'agit de résultats obtenus avec Bostan et Salvy en 2016[30]. L'objectif est la mise au point de l'algorithme TCMixte (algorithme 5). C'est un algorithme de création télescopique qui repose sur une réduction semblable à la réduction de Hermite des fractions rationnelles (proposition 43). La réduction est réalisée en pratique par l'algorithme Réduction (algorithme 4). L'analyse de l'algorithme TCMixte donne lieu au théorème suivant, qui résume les théorèmes 45, 46 et 60.

Théorème 2. *Soit* $\mathbf{k}$ *un corps de caractéristique* 0. *Soit* $\Psi(n,x)$ *un terme mixte hypergéométrique et hyperexponentiel de la forme*

$$\Psi(n,x) = \mathscr{P}(n,x)\Phi(n,x),$$

avec

$$\Phi(n,x) = \mathfrak{h}(x)^n \exp\left(\int \frac{\mathfrak{v}(x)}{\mathfrak{w}(x)}\right), \tag{5}$$

où $\mathfrak{h} \in \mathbf{k}(x)$ *est une fraction rationnelle,* $\mathscr{P} \in \mathbf{k}(n)[x]$ *et* $\mathfrak{v}, \mathfrak{w} \in \mathbf{k}[x]$ *sont des polynômes. Soit* d *un majorant des degrés en toutes les variables de tous les polynômes ci-dessus et des numérateurs et dénominateurs de* $\mathfrak{h}$ *et* $\partial_x\Phi/\Phi$.

Alors Ψ *admet un télescopeur d'ordre* $r \leqslant d$ *et de degré majoré par*

$$d(2r+1).$$

Un télescopeur possédant les propriétés ci-dessus est produit par l'algorithme TCMixte (algorithme 5 p. 52).

Si on suppose de plus que tous les polynômes sont sans carré, alors le télescopeur a une taille arithmétique $O(d^3)$*, et est calculé par l'algorithme TCMixte en au plus* $\tilde{O}(d^5)$ *opérations arithmétiques dans* $\mathbf{k}$.

0.6.3 Troisième chapitre

Dans le troisième chapitre, je m'intéresse aux intégrales de fractions rationnelles bivariées et présente les principaux résultats obtenus avec Bostan et Salvy en 2015[31]. Comme on l'a vu dans l'introduction, on dispose de deux structures de données pour les représenter : on peut les voir comme des fonctions algébriques et chercher à calculer un polynôme annulateur, ou bien comme des fonctions différentiellement finies et chercher à calculer un télescopeur pour la fraction rationnelle. C'est le premier point de vue qui va nous intéresser dans ce chapitre dont le but est d'établir le résultat suivant.

30. BOSTAN, DUMONT et SALVY, "Efficient Algorithms for Mixed Creative Telscoping".
31. BOSTAN, DUMONT et SALVY, "Algebraic Diagonals and Walks".

Théorème 3. *Soit* $\mathbf{k}$ *un corps de caractéristique* 0, *et* $A, B \in \mathbf{k}[x][y]$ *deux polynômes premiers entre eux. On note* $d_x = \max(\deg_x A, \deg_x B)$, $d_y = \max(\deg_y A, \deg_y B)$, *et* c *le nombre de racines distinctes de* B *qui s'annulent en* $x = 0$. *Alors il existe un polynôme* $\Phi \in \mathbf{k}[x, y]$ *tel que*

$$\Phi\left(x, [y^{-1}]\frac{A(x,y)}{B(x,y)}\right) = 0,$$

et tel que

$$\deg_x \Phi \leqslant 2d_x d_y \binom{d_y - 1}{c}, \quad \deg_y \phi = \binom{d_y}{c},$$

De plus, un tel polynôme est calculé par l'algorithme PolIntFRat (algorithme 8 p. 75) en

$$\tilde{O}\left(c d_x d_y \binom{d_y}{c}^2 + d_x d_y^5\right)$$

opérations arithmétiques dans $\mathbf{k}$.

Une définition précise de ce que veut dire la notation $[y^{-1}]$ dans ce cas sera donnée dans la définition 7. Ce théorème résume les théorèmes 79 et 80, dans lesquels seront prouvées de meilleures bornes faisant intervenir les degrés de la partie sans carré du dénominateur.

Un fait essentiel à retirer de ce théorème est que le degré du polynôme annulateur peut être exponentiel en le degré de la fraction rationnelle intégrée. C'est un résultat important à mettre en contraste avec le fait que le télescopeur minimal d'une fraction rationnelle a quant à lui une taille polynomiale [32].

Cet algorithme repose sur deux nouveaux algorithmes, présentés au début du chapitre, qui effectuent des opérations auxiliaires. Le premier calcule un polynôme qui annule tous les résidus d'une fraction rationnelle donnée. C'est une généralisation du résultant de Rothstein et Trager, ainsi que des résultants de Bronstein.

Le second est l'algorithme 7 qui, étant donné un polynôme $P(y) = \prod_{i=1}^{n}(y - \alpha_i)$ et un entier $c > 0$, calcule le polynôme

$$\prod_{i_1 < i_2 < \cdots < i_c} (y - (\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_c})).$$

C'est une variante additive de l'algorithme Platypus de Banderier et Flajolet [33]. L'élément clé de l'algorithme est la proposition 76, et il est analysé dans les théorèmes 77 et 78.

0.6.4 Quatrième chapitre

Le quatrième chapitre traite des diagonales de fractions rationnelles bivariées. Il est connu depuis Pólya [34] que ce sont des fonctions algébriques, et l'objectif du

32. Bostan, Chen, Chyzak et Li, "Complexity of creative telescoping for bivariate rational functions", Corollaire 27.
33. Banderier et Flajolet, "Basic Analytic Combinatorics of Directed Lattice Paths".
34. Pólya, "Sur les séries entières, dont la somme est une fonction algébrique".

chapitre est de rendre ce résultat effectif. En utilisant la représentation intégrale des diagonales, cela devient une application directe du chapitre précédent. Ceci mène à l'algorithme PolynômeDiagonale (algorithme 9) qui, étant donnée une fraction rationnelle bivariée, calcule un polynôme annulateur pour sa diagonale.

La fin du chapitre est consacrée à l'étude du degré du polynôme minimal de ces diagonales dans le cas générique. La proposition 100 met en évidence que le polynôme calculé par l'algorithme 9 est minimal dans le cas générique.

Les résultats de ce chapitre sont résumés dans le théorème suivant.

Théorème 4. *Soient* $A, B \in \mathbf{k}[x, y]$ *des polynômes premiers entre eux. On note* $d_x = \max(\deg_x A, \deg_x B)$, $d_y = \max(\deg_y A, \deg_y B)$. *Alors il existe un polynôme* $\Phi \in \mathbf{k}[t][y]$ *annulant la diagonale de la fraction* A/B, *et tel que*

$$\deg_t \Phi \leqslant 2d_x(d_x + d_y + 1)\binom{d_x + d_y}{c}, \quad \deg_y \Phi = \binom{d_x + d_y}{c},$$

où c *est le nombre de racines du numérateur de* $B(\frac{t}{y}, y)$ *qui sont nulles en* $t = 0$.

Un polynôme Φ *ayant ces propriétés peut être calculé par l'algorithme PolynômeDiagonale (algorithme 9 p. 86) en*

$$\tilde{O}\left(cd_x(d_x + d_y)\binom{d_x + d_y}{c}^2 + (d_x + d_y)^6\right)$$

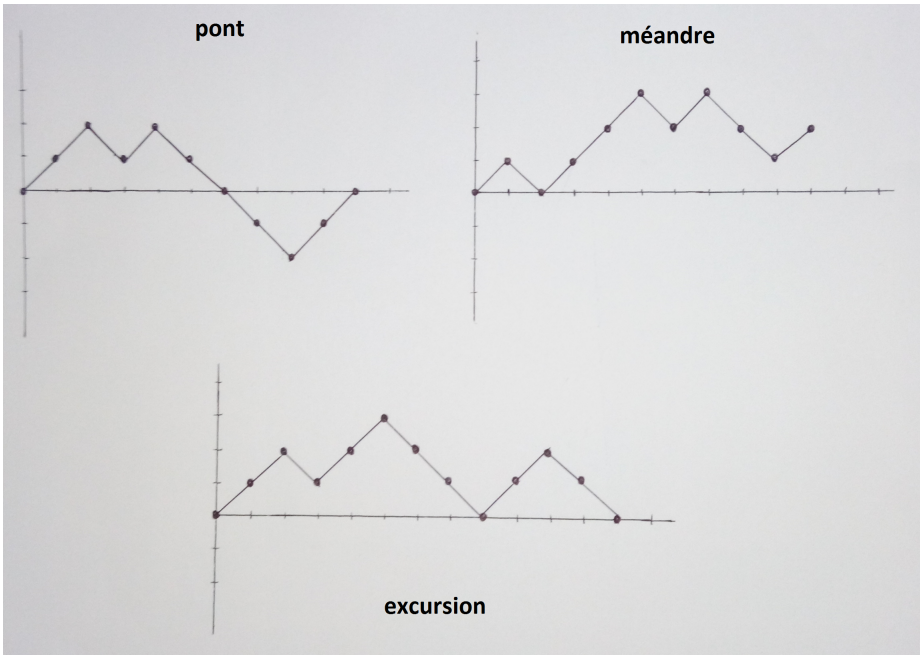
opérations arithmétiques dans $\mathbf{k}$.

De plus, la borne sur le degré en y *de* Φ *est génériquement atteinte.*

0.6.5 Cinquième chapitre

Le cinquième chapitre est une application à la combinatoire des résultats des premier et troisième chapitre sur l'intégration des fractions rationnelles bivariées. Le but du chapitre est d'établir une méthode efficace pour dénombrer certaines familles de marches unidimensionnelles sur $\mathbb{Z}$. On s'autorise un ensemble de pas $S \subset \mathbb{Z}$, et une marche est une suite finie d'entiers telle que chaque saut appartient à S. La *longueur* de la marche est le nombre d'éléments de la suite.

— les ponts : marches revenant à l'origine ;
— les méandres : marches confinées aux entiers positifs ;
— les excursions : marches confinées aux entiers positifs et revenant à l'origine.



Les trois familles de marches ($\mathrm{S} = \{-1, 1\}$)

Des définitions plus précises seront données au début du chapitre.

Parmi les méthodes connues jusqu'à présent pour effectuer ce calcul, la plus efficace reposait sur l'algébricité des séries génératrices des marches concernées. Je commence par constater que, dans le pire des cas, cette méthode nécessite un pré-calcul de complexité exponentielle en l'amplitude de l'ensemble de sauts autorisés.

Fort de ce constat, je présente une nouvelle méthode qui repose sur le fait que la série génératrice des ponts est une intégrale de fraction rationnelle bivariée, ce qui permet de la calculer par télescopage créatif. Les excursions et les méandres peuvent ensuite être dénombrées par évaluation de formules sur les séries génératrices. Cette méthode permet de réduire à une complexité polynomiale le pré-calcul, au prix de perdre des facteurs logarithmiques sur le calcul qui s'ensuit.

L'objectif est d'arriver au théorème suivant :

Théorème 5. *Soit* S *un ensemble fini de pas. Soit* d *la différence entre son plus grand élément et son plus petit élément. Soit* u_n *le nombre de ponts (resp. excursions, méandres) de longueur* n*, constitués de pas appartenant à* S*. Alors l'algorithme* Marches *(algorithme 10 p. 101) permet de calculer* $u_0, u_1, \ldots, u_\mathrm{N}$ *en* $\mathrm{O}(d^2\mathrm{N})$ *(resp.* $\tilde{\mathrm{O}}(d^2\mathrm{N})$*) opérations arithmétiques dans* $\mathbb{Q}$*, après un pré-calcul en* $\tilde{\mathrm{O}}(d^5)$ *opérations arithmétiques dans* $\mathbb{Q}$*.*

0.7 Conventions et notations

0.7.1 Ensembles

On note respectivement $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{C}$ les ensembles des nombres entiers positifs ou nuls, des nombres entiers relatifs, des nombres rationnels et des nombres complexes.

On fixe un corps $\mathbf{k}$ de caractéristique nulle. Pour la plupart des énoncés, on travaillera sur le corps $\mathbf{k}$. Lorsqu'une définition ou un résultat est valable pour tout corps de caractéristique nulle, mais voué à être utilisé pour un corps spécifique, le corps sera noté $\mathbb{K}$ avec l'idée que $\mathbb{K}$ sera plus tard instancié en $\mathbb{K} = \mathbf{k}(x)$ par exemple.

La notation $\overline{\mathbb{K}}$ signifiera une clôture algébrique de $\mathbb{K}$ fixée.

0.7.2 Polynômes

Pour tout corps $\mathbb{K}$, on note $\mathbb{K}[x]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$.

Le degré d'un polynôme $p \in \mathbb{K}[x]$ sera noté $\deg_x p$. Si $d \in \mathbb{N}$, on note également $\mathbb{K}[x]_d$ l'anneau des polynômes de degré inférieur ou égal à d. On note également $\mathbb{K}[x,y] = \mathbb{K}[x][y]$ et $\mathbb{K}[x,y]_{d_x,d_y} = \mathbb{K}[x]_{d_x}[y]_{d_y}$, et de même pour un nombre de variable plus élevé. Pour un polynôme bivarié $\mathrm{P} \in \mathbb{K}[x,y]$, on définit son *degré total* par $\deg\mathrm{t}_{x,y}\,\mathrm{P} = \deg_x \mathrm{P} + \deg_y \mathrm{P}$.

Si $p \in \mathbb{K}[x]$, on note $\mathrm{lc}_x\, p$ le coefficient dominant de p, c'est-à-dire le coefficient de $x^{\deg_x p}$ dans p. On dira que p est *unitaire* si $\mathrm{lc}_x(p) = 1$.

Si $p \in \mathbb{K}[x]$, on note $\mathrm{rec}_x\, p$ le polynôme réciproque de p, défini par

$$\mathrm{rec}_x\, p(x) = x^{\deg_x p}\, p\left(\frac{1}{x}\right).$$

Si $p, q \in \mathbb{K}[x]$ sont deux polynômes, on note $\mathrm{Résultant}_x(p,q)$ leur résultant (voir la définition 127 en annexe).

Pour un polynôme $p \in \mathbb{A}[x]$ où $\mathbb{A}$ est un anneau factoriel, on dit que p est *primitif* lorsque ses coefficients sont premiers entre eux dans leur ensemble.

On dira qu'un polynôme est *sans carré* lorsqu'il est premier avec sa dérivée. La *décomposition sans carré* d'un polynôme $p \in \mathbb{A}[x]$, où $\mathbb{A} = \mathbb{K}$ ou $\mathbb{A} = \mathbb{K}[x]$, est une factorisation $p = p_1^1 p_2^2 \dots p_m^m$, où les $p_i \in \mathbb{A}[x]$ sont tous primitifs sauf p_1, sans carré, premiers entre eux deux à deux, et $\deg_x p_m > 0$. La *partie sans carré* de p, notée $p^\star$, est le polynôme $p^\star = p_1 p_2 \dots p_m$. Remarquons que si p est un polynôme sans carré, alors on a $p = p^\star$.

0.7.3 Fractions rationnelles

Pour tout corps $\mathbb{K}$, on note $\mathbb{K}(x)$ le corps des fractions rationnelles à coefficients dans $\mathbb{K}$. Si $f \in \mathbb{K}(x)$, on définit son *numérateur* et son *dénominateur*, notés respectivement $\mathrm{numer}(f)$ et $\mathrm{denom}(f)$, comme étant l'unique paire de polynômes $a, b \in \mathbb{K}[x]$ premiers entre eux, avec b unitaire, tels que $f = a/b$. L'écriture a/b est alors appelée la forme *réduite* de la fraction f.

Si $b \in \mathbb{K}[x]$ est un polynôme, on note $\mathbb{K}[x][\frac{1}{b}]$ le localisé de $\mathbb{K}[x]$ en b, c'est à dire le sous anneau de $\mathbb{K}(x)$ constitué des fractions dont le dénominateur est une puissance de b.

On sera amenés à manipuler plusieurs notions de degré pour les fractions rationnelles. Si $f \in \mathbb{K}(x)$, on définit son *degré* par

$$\deg_x f = \max(\deg_x \operatorname{numer}(f), \deg_x \operatorname{denom}(f)).$$

Avec cette notion de degré, on définit $\mathbb{K}(x)_d$ et $\mathbb{K}(x_1, x_2, \ldots, x_n)_{d_1,d_2,\ldots,d_n}$ de même que pour les polynômes. On définit également le *degré à l'infini* de f par

$$\deg_x^\infty f = \deg_x \operatorname{numer}(f) - \deg_x \operatorname{denom}(f).$$

Enfin, on définit le *degré rationnel* de f, noté $\operatorname{Rdeg}_n f$ comme étant le couple formé des degrés de son numérateur et son dénominateur. On écrira :

$$\operatorname{Rdeg}_x f = \left[\frac{\deg_x \operatorname{numer}(f)}{\deg_x \operatorname{denom}(f)} \right].$$

On utilisera également les notations évidentes pour comparer les degrés rationnels, par exemple :

$$\operatorname{Rdeg}_x f \leqslant \left[\frac{d}{e} \right] \iff \deg_x \operatorname{numer}(f) \leqslant d \text{ et } \deg_x \operatorname{denom}(f) \leqslant e.$$

On dira d'une fraction $F \in \mathbb{K}(x_1, x_2, \ldots, x_n)$ qu'elle est *régulière* en $(0, 0, \ldots, 0)$ lorsque son dénominateur ne s'annule pas en $(0, 0, \ldots, 0)$. Dans le cas contraire, on dira qu'elle est *singulière*.

Pour une fraction $f \in \mathbb{K}(x)$ et un pôle α de f, on note $\operatorname{Res}(f, \alpha)$ le *résidu* de f en α. Rappelons sa définition : si m est la multiplicité du pôle α, on peut toujours écrire de façon unique

$$f(x) = \sum_{i=1}^{m} \frac{a_i}{(x-\alpha)^i} + g(x),$$

où g est une fraction rationnelle qui n'admet pas de pôle en α. On a par définition $a_1 = \operatorname{Res}(f, \alpha)$.

0.7.4 Séries

Pour tout corps $\mathbb{K}$, on note $\mathbb{K}[[x]]$ l'anneau des séries entières formelles à coefficients dans $\mathbb{K}$. Si $f(x) = \sum_{n \geqslant 0} a_n x^n \in \mathbb{K}[[x]]$, on notera $[x^n]f = a_n$. On note également

$$f \bmod x^n = \sum_{i=0}^{n-1} a_n x^n.$$

La valuation de f sera notée $\operatorname{val}_x f$. Rappelons sa définition :

$$\operatorname{val}_x f = \inf\{n \in \mathbb{N} \mid a_n \neq 0\}.$$

Si $f, g \in \mathbb{K}[[x]]$ sont deux séries entières, on écrira $f(x) = g(x) + \mathrm{O}(x^n)$ pour signifier que $\mathrm{val}_x(f-g) \geqslant n$.

On sera amené à utiliser les séries exponentielle et logarithme, définies respectivement par

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \text{et } \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}.$$

On définit l'intégrale indéfinie d'une série par

$$\int \left(\sum_{n \geqslant 0} u_n x^n \right) \mathrm{d}x = \sum_{n \geqslant 0} u_n \frac{x^{n+1}}{n+1}.$$

On note également $\mathbb{K}((x))$ le corps des séries de Laurent à coefficients dans $\mathbb{K}$, c'est-à-dire le corps de fractions de $\mathbb{K}[[x]]$, ou encore l'ensemble des séries de la forme $\sum_{n \geqslant \mathrm{K}} a_n x^n$ avec $a_n \in \mathbb{K}$ et $\mathrm{K} \in \mathbb{Z}$.

Enfin, lorsque $\mathbb{K}$ est algébriquement clos, on note $\mathbb{K}\langle\langle x \rangle\rangle$ le corps des séries de Puiseux à coefficients dans $\mathbb{K}$. Sa définition est rappelée dans l'annexe A.3.

0.7.5 Complexité

Pour analyser l'efficacité des algorithmes, il existe diverses façons de mesurer la complexité. Ici, on évaluera la complexité arithmétique dans le pire des cas des algorithmes, c'est-à-dire le nombre d'opérations dans le corps de base effectuées dans le pire des cas par un appel. Ce modèle a l'avantage et en même temps le désavantage de ne pas dépendre du matériel ou de l'implémentation utilisés pour effectuer les calculs. Il est donc utile pour comparer les algorithmes d'un point de vue théorique. À partir de maintenant et jusqu'à la fin du texte, on comprendra « opérations arithmétiques dans **k** » (addition, multiplication et division) chaque fois que l'on parlera d'opérations pour évaluer une complexité.

Si la complexité est une fonction $c(x_1, x_2, \ldots, x_n)$ d'un certain nombre de paramètres, on utilisera la notation

$$c(x_1, x_2, \ldots, x_n) = \mathrm{O}(f(x_1, x_2, \ldots, x_n))$$

pour signifier l'existence d'un entier N indépendant des x_i et d'une constante $\mathrm{C} > 0$ telle que

$$c(x_1, x_2, \ldots, x_n) \leqslant \mathrm{C} f(x_1, x_2, \ldots, x_n)$$

dès lors que $x_1, x_2, \ldots, x_n$ sont plus grands que N.

On utilisera également la notation $\tilde{\mathrm{O}}$ pour signifier que l'on omet des facteurs polylogarithmiques. Par exemple, $n \log n \log\log n = \tilde{\mathrm{O}}(n)$, ou encore $nm \log n \log m = \tilde{\mathrm{O}}(nm)$.

On dira qu'un algorithme a une complexité *optimale* (resp. quasi-optimale) lorsque sa complexité est linéaire (resp. linéaire à des facteurs logarithmiques près) en la taille de sa sortie.

L'algèbre linéaire est un ingrédient important pour de nombreux algorithmes. La plupart des opérations de base (inversion, polynôme caractéristique, déterminant, ...) se ramènent à la multiplication matricielle, qui est un problème réputé

difficile. On introduit donc un exposant faisable ω pour la multiplication de matrices sur $\mathbf{k}$, c'est-à-dire tel qu'il existe un algorithme qui effectue la multiplication de deux matrices carrées de taille n en $O(n^\omega)$ opérations dans $\mathbf{k}$. On sait depuis Strassen [35] que l'on peut avoir $\omega < 3$, et on ne sait pas encore à l'heure actuelle s'il est possible d'atteindre l'optimalité ($\omega = 2$) ou même la quasi-optimalité.

L'annexe B rassemble des résultats de complexité pour diverses opérations qui serviront de briques de base pour les analyses de complexité à venir.

0.7.6 Miscellanées

On utilisera les notations classiques pgcd et ppcm pour le plus grand commun diviseur et le plus petit commun multiple.

Si f est une fonction, un polynôme, une série, ..., dépendant entre autre de la variable x, on notera

$$\partial_x f$$

sa dérivée par rapport à x. On notera également la dérivée f' lorsque f ne dépend que d'une seule variable.

Le coefficient binomial $\binom{n}{k}$ est défini par

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

lorsque $n \geqslant 0$ et $0 \leqslant k \leqslant n$, et vaut 0 dans tous les autres cas.

Enfin, j'ai pris le parti d'utiliser des lettres minuscules pour nommer les fonctions d'une variable, et des lettres majuscules pour les fonctions de plusieurs variables.

35. STRASSEN, "Gaussian Elimination is Not Optimal".

Chapitre 1

Résultats préliminaires

1.1 Point de vue algébrique sur l'intégration des fractions rationnelles

Pour le problème du calcul symbolique des intégrales de contour de fractions rationnelles que l'on va considérer par la suite, les algorithmes sont fondés sur des idées analytiques mais n'effectuent que des manipulations algébriques en pratique. Pour fixer les idées sur ce sujet, commençons par l'exemple du cas univarié. Soit une fraction rationnelle $f \in \mathbf{k}(y)$ et supposons que l'on s'intéresse à l'intégrale

$$\oint f(y)\mathrm{d}y$$

sur un cercle autour de 0 qui est assez petit pour ne contenir aucun pôle non-nul de f. L'analyse complexe crée alors un pont entre l'analyse et l'algèbre : cette intégrale peut être obtenue, à un facteur $2\pi i$ près, comme le coefficient de y^{-1} dans le développement de f en série de Laurent au voisinage de 0. Ou, en d'autres termes, comme le résidu de f en 0.

Dans le cas d'une fraction rationnelle $\mathrm{F}(x,y)$ bivariée que l'on souhaite intégrer par rapport à y, le contour d'intégration est maintenant paramétré par x. Pour justifier le type d'intégrales que l'on va calculer et leur interprétation algébrique, intéressons-nous à l'exemple des diagonales de fractions rationnelles.

Soit $\mathrm{F} \in \mathbb{C}(x,y)$ une fraction rationnelle régulière en $(0,0)$, alors F admet un développement dans $\mathbb{C}[[x,y]]$:

$$\mathrm{F}(x,y) = \sum_{i,j\geqslant 0} a_{i,j} x^i y^j.$$

De plus, il existe $\epsilon > 0$ tel que cette égalité est vraie pour toutes valeurs $x, y \in \mathbb{C}$ telles que $|x|, |y| < \epsilon$. Maintenant, si l'on fixe $t \in \mathbb{C}$ tel que $|t| < \epsilon^2$, alors pour tout $y \in \mathbb{C}$ tel que $\frac{|t|}{\epsilon} < |y| < \epsilon$, on a en particulier $|t/y| < \epsilon$, et donc

$$\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right) = \sum_{i,j\geqslant 0} a_{i,j} t^i y^{j-i-1}.$$

Choisissons un contour γ_t qui est un petit cercle de rayon δ avec $|t|/\epsilon < \delta < \epsilon$, et intégrons cette égalité :

$$\oint_{\gamma_t} \frac{1}{y} \mathrm{F}\left(\frac{t}{y}, y\right) = [y^{-1}] \sum_{i,j \geqslant 0} a_{i,j}\, t^i\, y^{j-i-1} = \sum_{i \geqslant 0} a_{i,i}\, t^i = \Delta\mathrm{F}(t).$$

On retrouve la formule intégrale pour la diagonale de F. Mais allons plus loin, et tentons d'évaluer cette intégrale. Par la formule des résidus, elle est égale à la somme des résidus de F à l'intérieur du contour d'intégration. Mais lorsque t tend vers 0, on peut choisir le rayon de γ_t de plus en plus petit, de sorte qu'il ne contient plus que les pôles de l'intégrande qui tendent vers 0 avec t. Ceci motive la définition suivante :

Définition 6. Soit $\mathrm{P} \in \mathbf{k}(x)[y]$ un polynôme. On appelle *petite branche* de P toute racine de P qui tend vers 0 lorsque x tend vers 0. En termes de séries de Puiseux, ce sont celles qui ont une valuation strictement positive.

De même, si $\mathrm{G} \in \mathbf{k}(x)(y)$ est une fraction rationnelle, on appelle *petits pôles* de G les petites branches de son dénominateur.

Dans la suite, on notera Nsmall(P) le nombre de petites branches d'un polynôme P.

Avec ce vocabulaire, on a montré que, pour t assez petit, $\Delta\mathrm{F}(t)$ est la somme des résidus à ses petits pôles de la fraction $\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right)$.

Essayons maintenant d'avoir un point de vue plus algébrique sur ce résultat. Ceci permettra d'une part d'élaborer et analyser les algorithmes plus aisément, et d'autre part de rendre les arguments valables sur un corps de caractéristique 0 quelconque. On peut voir le développement en série

$$\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right) = \sum_{i,j \geqslant 0} a_{i,j}\, t^i\, y^{j-i-1}$$

comme une égalité formelle entre séries de Laurent dans $\mathbb{C}((y))((t))$. Le fait que l'égalité vive dans ce corps traduit la condition analytique « t est petit devant y ». Dans ce contexte formel, le pendant algébrique de l'intégration devient simplement l'extraction du coefficient de y^{-1}. Je vais généraliser cette idée et montrer que la formule des résidus admet également un analogue algébrique dans ce cadre.

Définition 7. Soit $\mathrm{F} \in \mathbf{k}(x, y)$ une fraction rationnelle. On écrit le développement en série de Laurent de F dans $\mathbf{k}((y))((x))$:

$$\mathrm{F}(x, y) = \sum_{i \geqslant \mathrm{K}} a_i(y)\, x^i,$$

avec, pour tout $i \geqslant \mathrm{K}$, $a_i(y) \in \mathbf{k}((y))$.

On définit alors la série $[y^{-1}]\mathrm{F}(x, y) \in \mathbf{k}((x))$ par

$$[y^{-1}]\mathrm{F}(x, y) = \sum_{i \geqslant \mathrm{K}} \left([y^{-1}]\, a_i(y)\right) x^i.$$

Proposition 8. *Soit* $\mathrm{F} \in \mathbf{k}(x,y)$ *une fraction rationnelle bivariée. Soient* $y_1, y_2, \dots, y_s \in \overline{\mathbf{k}(x)}$ *les petits pôles de* F *vue comme élément de* $\mathbf{k}(x)(y)$.

Alors

$$[y^{-1}]\mathrm{F}(x,y) = \sum_{i=1}^{s} \mathrm{Res}(\mathrm{F}, y_i).$$

La preuve est inspirée de la preuve de Gessel[1] que les diagonales de fractions rationnelles à deux variables sont algébriques. (On en trouvera d'ailleurs une présentation très claire chez Stanley[2])

Démonstration. Commençons par décomposer en éléments simples la fraction F vue comme un élément de $\mathbf{k}(x)(y)$. Si l'on note $y_{s+1}, y_{s+2}, \dots, y_n \in \overline{\mathbf{k}(x)}$ les grands pôles et m_i la multiplicité de y_i dans F, il existe des éléments $r_{i,j} \in \overline{\mathbf{k}(x)}$ pour $i \in \{1,2,\dots,n\}$ et $j \in \{1,2,\dots,m_i\}$ tels que

$$\mathrm{F}(x,y) = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \mathrm{F}_{i,j}(x,y), \tag{1.1}$$

où

$$\mathrm{F}_{i,j}(x,y) = \frac{r_{i,j}(x)}{(y - y_i(x))^j}, \qquad 1 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant m_i.$$

En particulier, $r_{i,1}(x)$ est le résidu de F en $y_i(x)$ pour tout $i \in \{1,2,\dots,n\}$. Par le théorème de Puiseux (théorème 120 de l'annexe A), il existe $\mathrm{N} \in \mathbb{N}^\star$ tel que les y_i et $r_{i,j}$ appartiennent tous à $\overline{\mathbf{k}}((x^{1/\mathrm{N}}))$. Pour appliquer l'opérateur $[y^{-1}]$ aux deux côtés de l'équation (1.1), il faut trouver un anneau dans lequel à la fois l'égalité et l'opérateur $[y^{-1}]$ ont un sens. Nous allons vérifier que $\mathbb{A} = \overline{\mathbf{k}}((y))((x^{1/\mathrm{N}}))$ avec $[y^{-1}]$ calculé coefficient par coefficient conviennent.

Tout d'abord, $\mathrm{F}(x,y)$ appartient à $\mathbb{A}$ puisque c'est une fraction rationnelle. Pour développer le membre droit, on considère chaque terme séparément en distinguant les cas $\mathrm{val}_x(y_i) \leqslant 0$ et $\mathrm{val}_x(y_i) > 0$. Si $\mathrm{val}_x(y_i) \leqslant 0$, $\mathrm{F}_{i,j}$ peut s'écrire :

$$\mathrm{F}_{i,j} = \frac{r_{i,j}}{(-y_i)^j} \cdot \frac{1}{\left(1 - y/y_i\right)^j} = \frac{r_{i,j}}{(-y_i)^j} \sum_{k \geqslant 0} \binom{-j}{k} \frac{y^k}{y_i^k} \in \overline{\mathbf{k}}((x^{1/\mathrm{N}}))[[y]].$$

Comme $\mathrm{val}_x(1/y_i) \geqslant 0$, la série $\mathrm{F}_{i,j}/r_{i,j}$ appartient à $\overline{\mathbf{k}}[[x^{1/\mathrm{N}}]][[y]] \cong \overline{\mathbf{k}}[[y]][[x^{1/\mathrm{N}}]]$. Donc $\mathrm{F}_{i,j} \in \overline{\mathbf{k}}[[y]]((x^{1/\mathrm{N}})) \subset \mathbb{A}$, et en particulier $[y^{-1}]\mathrm{F}_{i,j} = 0$.

Si à l'inverse $\mathrm{val}_x(y_i) > 0$, alors $\mathrm{F}_{i,j}$ se développe directement dans $\mathbb{A}$:

$$\mathrm{F}_{i,j} = \frac{r_{i,j}}{y^j} \cdot \frac{1}{\left(1 - y_i/y\right)^j} = \frac{r_{i,j}}{y^j} \sum_{k \geqslant 0} \binom{-j}{k} \frac{y_i^k}{y^k}.$$

Comme $y_i/y \in \mathbb{A}$ et $\mathrm{val}_x(y_i/y) > 0$, le membre droit de cette chaîne d'égalités est la somme d'une série convergente (au sens des séries formelles de Laurent) de $\mathbb{A}$, et donc appartient à $\mathbb{A}$. Dans ce cas, on obtient $[y^{-1}]\mathrm{F}_{i,j} = r_{i,1}$.

Tous les éléments sont maintenant réunis pour que l'on puisse appliquer $[y^{-1}]$ aux deux côtés de l'équation (1.1), ce qui donne le résultat attendu. □

1. GESSEL, "A factorization for formal Laurent series and lattice path enumeration".
2. STANLEY, *Enumerative combinatorics*, Th. 6.3.3.

Corollaire 9. *Soit* $\mathrm{F} \in \mathbf{k}(x,y)$ *une fraction rationnelle. Alors* $[y^{-1}]\mathrm{F}(x,y)$ *est une série algébrique.*

Démonstration. Reprenons les notations de la proposition, et notons de plus $y_s, y_{s+1}, \ldots, y_n$ les grands pôles de F. Alors $\mathrm{Res}(\mathrm{F}, y_i) \in \mathbf{k}(x)(y_1, y_2, \ldots, y_n)$ pour tout $i \in \{1,2,\ldots,s\}$. On en déduit que

$$[y^{-1}]\mathrm{F}(x,y) \in \mathbf{k}(x)(y_1, y_2, \ldots, y_n),$$

ce qui en fait une série algébrique. □

1.2 Télescopage créatif bivarié

1.2.1 Généralités sur les algorithmes de télescopage créatif par réductions

La méthode du télescopage créatif s'applique dans divers contextes. Elle peut servir à l'intégration comme à la sommation, et elle peut servir à calculer des opérateurs différentiels, de récurrence, aux q-différences,... Le formalisme des algèbres d'opérateurs apporte un vocabulaire permettant d'énoncer des résultats généraux et de les prouver dans tous ces contextes à la fois. Malheureusement, ceci vient au prix d'une perte importante en clarté et des notations parfois difficiles à décrypter lorsque l'on souhaite appliquer un résultat en pratique.

J'ai donc décidé d'adopter une position intermédiaire : je ne vais traiter que le cas de l'intégration, et je vais utiliser de façon légèrement informelle le vocabulaire des algèbres d'opérateurs et des extensions de corps différentiels sans rentrer dans le détail de la construction. Les définitions et les résultats qui suivent se généralisent sans problème si l'on remplace dérivée par différence finie et intégration par sommation.

On se donne un corps $\mathbb{K}$ de caractéristique 0, et on suppose que l'on dispose d'une extension différentielle $\mathbb{A}$ de $\mathbb{K}(x)$, c'est-à-dire un anneau contenant $\mathbb{K}(x)$ muni d'une dérivation qui agit sur $\mathbb{K}(x)$ comme la dérivation usuelle. On suppose qu'on dispose également d'un opérateur, noté ∂, qui agit sur $\mathbb{A}$ et est compatible avec la dérivation de $\mathbb{A}$, c'est-à-dire

$$\forall f \in \mathbb{A}\ (\partial f)' = \partial(f').$$

Les exemples les plus importants pour ∂ sont l'opérateur de décalage $n \mapsto n+1$ lorsque $\mathbb{K} = \mathbf{k}(n)$ ou la dérivation usuelle lorsque $\mathbb{K} = \mathbf{k}(t)$.

Dans la suite, on va s'intéresser plus particulièrement à deux exemples. Le premier lorsque $\mathbb{K} = \mathbf{k}(t)$, $\mathbb{A} = \mathbf{k}(t,x)$ et $\partial = \partial_t$ est la dérivation par rapport à t. Le second lorsque $\mathbb{K} = \mathbf{k}(n)$ et $\mathbb{A} = \mathbf{k}(n)(x)[\Psi]$ où Ψ est un terme mixte hypergéométrique et hyperexponentiel. Dans ce second cas, $\partial = \mathrm{S}_n$ est le décalage par rapport à n.

On note $\mathbb{K}\langle\partial\rangle = \left\{c_0 + c_1\partial + \cdots + c_r\partial^r \mid c_0, c_1, \ldots, c_r \in \mathbb{K}\right\}$. Les chevrons $\langle\rangle$ servent à signifier que ∂ ne commute pas avec les éléments $\mathbb{K}$. En ajoutant une règle de

commutation, on sait additionner et multiplier les éléments de $\mathbb{K}\langle\partial\rangle$. Par exemple si $\mathbb{K}=\mathbf{k}(t)$ et $\partial=\partial_t$ représente la dérivation, la règle de Leibniz se traduit par

$$\partial_t t = t\partial_t + 1.$$

Si $\mathbb{K}=\mathbf{k}(n)$ et $\partial=\mathrm{S}_n$ représente le décalage par rapport à n, on utilise la règle

$$\mathrm{S}_n n = (n+1)\mathrm{S}_n.$$

Si $\mathrm{L}=\sum_{i=0}^{r} c_i\partial^i$ avec $c_r\neq 0$, on dit que r est l'*ordre* de L, noté ord L, et on définit le *degré* de L par

$$\deg \mathrm{L} = \max_{0\leqslant i\leqslant r} \deg_n c_i.$$

Si de plus $f\in\mathbb{A}$, on note

$$\mathrm{L}\cdot f = \sum_{i=0}^{r} c_i\partial^i f.$$

Le lecteur souhaitant une construction précise de l'algèbre d'opérateurs $\mathbb{K}\langle\partial\rangle$ pourra se référer aux travaux de Chyzak avec Salvy[3] et dans sa thèse[4]. Pour ce qui est des extensions de corps différentiels et de corps aux différences, on trouvera une bonne présentation dans les livres de Singer et van der Put[5].

Définition 10. Soit $f\in\mathbb{A}$ on appelle *télescopeur* pour f tout opérateur $\mathrm{L}\in\mathbb{K}\langle\partial\rangle$ tel qu'on ait, pour un certain $g\in\mathbb{A}$,

$$\mathrm{L}\cdot f = g'.$$

Exemple 11. Voici un exemple dans chacun des deux contextes mentionnés ci-dessus.

(1) $\mathbb{K}=\mathbf{k}(t)$ et $\partial=\partial_t$. La fraction rationnelle $\mathrm{F}(t,x)=\frac{1}{x-t-x^2}$ vérifie

$$(1-4t)\cdot\partial_t\mathrm{F}(t,x) - 2\cdot\mathrm{F}(t,x) = \partial_x\left((2x-1)\cdot\mathrm{F}(t,x)\right).$$

F admet donc

$$(1-4t)\cdot\partial_t - 2$$

comme télescopeur.

(2) $\mathbb{K}=\mathbf{k}(n)$ et $\partial=\mathrm{S}_n$. Le terme mixte hypergéométrique et hyperexponentiel

$$\Psi(n,x) = \frac{(1+x)\exp(x)}{x^{n+1}}$$

vérifie l'équation

$$(n+1)^2\cdot\Psi(n+1,x) - (n+2)\cdot\Psi(x) = \partial_x\left(-\frac{((n+2)x+n+1)\exp(x)}{x^{n+1}}\right).$$

Ψ admet donc

$$(n+1)^2\cdot\mathrm{S}_n - (n+2)$$

comme télescopeur.

3. Chyzak et Salvy, "Non-commutative elimination in Ore algebras proves multivariate identities".
4. Chyzak, "Fonctions holonomes en calcul formel".
5. Put et Singer, *Galois Theory of Difference Equations*; Put et Singer, *Galois Theory of Linear Differential Equations*.

Pré-algorithme Télescopage(f)

Entrée Un élément $f \in \mathbb{A}$

Sortie $(c_0, \ldots, c_{r-1})$ tel que $\partial^r f - \sum_{i=0}^{r-1} c_i \partial^i f = g'$ pour un certain $g \in \mathbb{A}$

pour $k \leftarrow 0, \ldots$ **faire**
  si $\operatorname{rang}_{\mathbb{K}}([f], [\partial f], \ldots, [\partial^k f]) < k+1$ **alors**
    Résoudre $[\partial^k f] = \sum_{i=0}^{k-1} c_i [\partial^i f]$ en $c_0, \ldots, c_{k-1} \in \mathbb{K}$;
    renvoyer $(c_0, \ldots, c_{k-1})$

Algorithme 1: Télescopage créatif par réductions

Définition 12. Une *réduction* dans $\mathbb{A}$ au-dessus de $\mathbb{K}$, est une application

$$[\cdot] \; : \; \mathbb{A} \longrightarrow \mathbb{A}$$

vérifiant :

1. pour tout $f \in \mathbb{A}$, il existe $g \in \mathbb{A}$ tel que $f - [f] = g'$;
2. $[\cdot]$ est une application $\mathbb{K}$-linéaire.

On suppose à partir de maintenant que l'on dispose d'une réduction $[\cdot] : \mathbb{A} \to \mathbb{A}$. La définition implique de façon immédiate la proposition suivante.

Proposition 13. *Soit $f \in \mathbb{A}$.*
Si $[f] = 0$, alors il existe $g \in \mathbb{A}$ tel que $f = g'$.

Démonstration. C'est évident par la propriété (1) dans la définition précédente. □

Ce fait très simple est la base du pré-algorithme Télescopage pour la recherche de télescopeurs. C'est un pré-algorithme dans le sens où il est a priori possible qu'il ne termine pas (par exemple si on l'applique à un élément qui n'admet pas de télescopeur). Montrons immédiatement sa correction.

Proposition 14. *Soit $f \in \mathbb{A}$.*
Si l'appel Télescopage(f) *termine, alors il retourne les coefficients d'un télescopeur pour f.*

Démonstration. Si l'appel termine, sa sortie est un $r-1$-uplet $(c_0, c_1, \ldots, c_{r-1})$ tel que

$$[\partial^r f] - \sum_{i=0}^{r-1} c_i [\partial^i f] = 0.$$

En utilisant la $\mathbb{K}$-linéarité de $[\cdot]$, cela implique que

$$\left[\partial^r f - \sum_{i=0}^{r-1} c_i \partial^i f \right] = 0.$$

Et donc, par la proposition précédente, il existe $g \in \mathbb{A}$ tel que

$$\partial^r f - \sum_{i=0}^{r-1} c_i \partial^i f = g',$$

ce qui est exactement la définition d'un télescopeur pour f. □

Ainsi, toute réduction dans $\mathbb{A}$ fournit un pré-algorithme de calcul de télescopeur, à condition d'être capable de garantir sa terminaison. Nous allons maintenant voir deux propriétés qui, lorsqu'elles sont satisfaites par la réduction, assurent la terminaison de l'algorithme 1 quelle que soit son entrée $f \in \mathbb{A}$.

Définition 15.

1. On dit que $[\cdot]$ est *confinée* s'il existe un $\mathbb{K}$-espace vectoriel de dimension finie $\mathrm{V} \subset \mathbb{A}$ tel que $\forall f \in \mathbb{A}\ [f] \in \mathrm{V}$.
2. On dit que $[\cdot]$ est *normale* si $\forall g \in \mathbb{A}\ [g'] = 0$.

Proposition 16. *Soit $f \in \mathbb{A}$.*

1. *Si $[\cdot]$ est confinée, alors l'appel* Télescopage(f) *termine.*
2. *Si $[\cdot]$ est normale et f admet un télescopeur sur $\mathbb{K}$, alors l'appel* Télescopage(f) *termine et calcule un télescopeur d'ordre minimal pour f.*

Démonstration. (1) Par définition, il existe un $\mathbb{K}$-espace vectoriel de dimension finie V tel que $\forall f \in \mathbb{A}\ [f] \in \mathrm{V}$. Notons r la dimension de V. Alors les $r+1$ éléments de V

$$[f], [\partial f], \ldots, [\partial^r f]$$

sont linéairement dépendants sur $\mathbb{K}$, ce qui provoque la terminaison de l'algorithme si elle n'a pas eu lieu avant.

(2) On a fait l'hypothèse qu'il existe $c_0, c_1, \ldots, c_{r-1}$ et $g \in \mathbb{A}$ tels que

$$\partial^r - \sum_{i=0}^{r-1} c_i \partial^i f = g'.$$

On peut supposer sans perte de généralité que r est minimal. Alors, en utilisant la linéarité et la normalité de $[\cdot]$, on obtient

$$[\partial^r f] - \sum_{i=0}^{r-1} c_i [\partial^i f] = 0. \tag{1.2}$$

De plus, une telle relation de liaison ne peut exister pour un r plus petit, sinon par le même raisonnement que ci-dessus elle donnerait un télescopeur d'ordre plus petit, contredisant la minimalité de r. On en déduit que l'algorithme ne termine que lorsqu'il détecte la relation (1.2), et donc sa sortie est bien le télescopeur minimal de f. □

Corollaire 17. *Si la réduction $[\cdot]$ est à la fois normale et confinée, alors tout élément $f \in \mathbb{A}$ admet un télescopeur sur $\mathbb{K}$. De plus, pour tout $f \in \mathbb{A}$ l'appel* Télescopage(f) *termine et calcule un télescopeur d'ordre minimal pour f.*

Remarque 18. *La preuve du point (1) de la proposition 16 montre également que si la réduction* $[\cdot]$ *est confinée, alors la dimension de l'espace* V *fournit une borne sur l'ordre des télescopeurs calculés par* Télescopage(f).

Enfin, concluons ces généralités avec une optimisation importante du pré-algorithme Télescopage. Lors de l'exécution de l'algorithme sur $f \in \mathbb{A}$, on calcule successivement les réductions des $\partial^i f$. Faire cette opération trop brutalement peut être coûteux en pratique, car les applications répétées de ∂ peuvent faire exploser la taille des fonctions que l'on réduit. Par exemple, si f est une fraction rationnelle et ∂ est la dérivation, le degré du dénominateur de f augmente à chaque dérivation.

Si la réduction est confinée, on peut espérer contourner ce problème en reliant $[\partial^i f]$ à $[\partial[\partial^{i-1} f]]$. En effet, $[\partial^{i-1} f]$ aura été calculée à l'étape précédente de l'algorithme et aura une taille raisonnable grâce à la propriété de confinement.

Proposition 19. *Si la réduction* $[\cdot]$ *est normale, alors pour tout* $f \in \mathbb{A}$ *et tout* $i > 0$ *:*

$$[\partial^i f] = [\partial[\partial^{i-1} f]].$$

Démonstration. Par définition, il existe $g \in \mathbb{A}$ tel que

$$\partial^{i-1} f = [\partial^{i-1} f] + g'.$$

En appliquant ∂ des deux côtés de l'égalité et en utilisant le fait que ∂ commute avec la dérivation, on obtient

$$\partial^i f = \partial[\partial^{i-1} f] + (\partial g)'.$$

La conclusion suit alors en réduisant cette égalité car $[(\partial g)'] = 0$ par normalité. □

1.2.2 Rappel sur le cas différentiel-différentiel

En guise d'exemple, je vais présenter en détail la réduction de Hermite[6]. C'est l'occasion d'illustrer les concepts introduits dans le paragraphe précédent, mais également de préparer le chapitre 2 dans lequel je vais construire une réduction qui repose exactement sur le même principe.

On cherche à répondre au problème de la création télescopique pour une fraction rationnelle $F \in \mathbf{k}(x, y)$, c'est-à-dire trouver une équation du type

$$\partial_x^r F(x, y) - \sum_{i=0}^{r-1} c_i(x) \partial_x^i F(x, y) = \partial_y G(x, y)$$

pour une certaine fraction rationnelle $G \in \mathbf{k}(x, y)$. Si l'on note $B^\star \in \mathbf{k}(x, y)$ la partie sans carré du dénominateur de F, on constate immédiatement que le membre de gauche appartient à $\mathbf{k}(x)[y]\left[\frac{1}{B}\right]$, et il doit donc en être de même pour G. Avec les notations du paragraphe précédent, on s'intéresse donc au cas $\mathbb{A} = \mathbf{k}(x)[y]\left[\frac{1}{B}\right]$ et $\mathbb{K} = \mathbf{k}(x)$.

L'idée de base de la réduction de Hermite est que l'on sait diminuer la multiplicité des pôles d'une fraction rationnelle en lui ajoutant des dérivées bien choisies.

6. HERMITE, "Sur l'intégration des fractions rationnelles".

Lemme 20. *Soient $a, p, q \in \mathbb{K}[y]$ trois polynômes premiers entre eux deux à deux avec p sans carré, et un entier $k \geqslant 2$. Notons $q^\star$ la partie sans carré de q.*

Alors il existe des polynômes $b, c \in \mathbb{K}[y]$ tels que

$$\frac{a}{p^k q} = \frac{b}{p^{k-1} q} + \left(\frac{c q^\star}{p^{k-1} q}\right)'.$$

Démonstration. p étant sans carré et premier avec q, on a $\gcd(p, p' q^\star) = 1$, donc il existe $u, v \in \mathbb{K}[y]$ tels que $a = up + vp'q^\star$. On calcule alors

$$\frac{a}{p^k q} = \frac{u}{p^{k-1} q} + \frac{v q^\star}{q} \cdot \frac{p'}{p^k}.$$

Or, on a

$$\frac{v q^\star}{q} \cdot \frac{p'}{p^k} = -\frac{1}{k-1}\left(\left(\frac{v q^\star}{p^{k-1} q}\right)' - \frac{(v q^\star)'}{p^{k-1} q} + \frac{v q^\star q'}{p^{k-1} q^2}\right).$$

(Cette dernière égalité n'est autre que la formule d'intégration par parties.) On en déduit qu'on a l'égalité annoncée dans le lemme en posant

$$b = u + \frac{(v q^\star)'}{k-1} - \frac{v}{k-1} \cdot \frac{q^\star q'}{q}, \quad c = -\frac{v}{k-1}.$$

Et b est bien un polynôme car q divise $q^\star q'$. □

Insistons sur le point central de la preuve précédente qui est la relation de Bézout entre p et $p' q^\star$. Elle recèle deux idées importantes : la première est que la présence de p' permet de faire apparaître une dérivée, provoquant la chute de l'ordre du pôle avec l'intégration par partie ; la seconde est que la présence de $q^\star$ empêche l'augmentation de la multiplicité de q dans le dénominateur lors de l'intégration par parties.

En répétant la réduction élémentaire du lemme 20, on peut réduire la multiplicité de tous les pôles jusqu'à ce que le dénominateur devienne sans carré : c'est la réduction de Hermite.

Proposition 21. *Soit $f \in \mathbb{K}(y)$ une fraction rationnelle dont on note $a, b \in \mathbb{K}[y]$ le numérateur et le dénominateur (a et b sont premiers entre eux). On note $b^\star$ la partie sans carré de b.*

Alors il existe un unique couple de polynômes $q, r \in \mathbb{K}[y]$ tels que $\deg_y r < \deg_y b^\star$ *et*

$$\frac{a}{b} = \frac{r}{b^\star} + \left(\frac{q b^\star}{b}\right)'. \tag{1.3}$$

On définit alors la réduction de Hermite *de f par*

$$[f] = \frac{r}{b^\star}.$$

Démonstration. Pour prouver l'existence de r et q, on utilise le lemme précédent. Écrivons la décomposition sans carré de b :

$$b = b_1 b_2^2 \dots b_m^m.$$

On applique le lemme 20 avec $p = b_2$, puis deux fois avec $p = b_3$, *etc.*, ce qui produit une égalité de la forme annoncée. Il suffit ensuite de faire une division euclidienne par $b^\star$ pour assurer la condition sur le degré de r.

Pour l'unicité, supposons que l'on a deux écritures de la forme (1.3) avec deux polynômes $r_1, r_2 \in \mathbb{K}[y]$ de degrés strictement inférieurs à celui de $b^\star$. Alors la fraction rationnelle

$$\frac{r_1 - r_2}{b^\star}$$

est une dérivée, ce qui implique que tous ses résidus sont nuls. Mais comme elle a un degré à l'infini négatif et tous ses pôles sont simples, une décomposition en éléments simples montre qu'elle doit être nulle, soit $r_1 = r_2$. L'égalité des polynômes q_1 et q_2 correspondants suit facilement. □

Remarquons que la proposition 21 peut également être obtenue en faisant de l'algèbre linéaire. C'est l'approche adoptée par Horowitz [7] et Ostrogradsky [8].

Corollaire 22. *La réduction de Hermite est une réduction au sens de la définition 12, qui est normale et confinée.*

Démonstration. C'est immédiat à partir de la proposition. La linéarité, et la normalité sont des conséquences de l'unicité de la réduction, et le confinement provient de la condition de degré sur la réduction. □

En appliquant l'algorithme 1 avec la réduction de Hermite et en analysant de plus près les degrés des objets mis en jeu ainsi que la complexité de l'algorithme, Bostan, Chen, *et al.* [9] ont montré :

Théorème 23. *Soient* $A, B \in \mathbf{k}[x, y]$ *deux polynômes non-nuls premiers entre eux. On note respectivement* $d_x, d_y, d_x^\star, d_y^\star$ *les degrés en* x *et* y *de* B *et de sa partie sans carré. On suppose également que* $\deg_y A < d_y$ *et* $\deg_x A < d_x$*, et que* B *est primitif par rapport à* y.

Alors la fraction rationnelle A/B *admet un télescopeur minimal* L *tel que*

$$\operatorname{ord} L \leqslant d_y^\star, \quad \deg L = O(d_x d_y d_y^\star).$$

De plus, un tel télescopeur peut être calculé par l'algorithme HermiteTelescoping [10] *en*

$$\tilde{O}(d_x d_y^{\omega+3})$$

opérations arithmétiques dans $\mathbf{k}$.

7. HOROWITZ, "Algorithms for Partial Fraction Decomposition and Rational Function Integration".
8. OSTROGRADSKY, "De l'intégration des fractions rationnelles".
9. BOSTAN, CHEN, CHYZAK et LI, "Complexity of creative telescoping for bivariate rational functions".
10. Ibid., Fig. 3.

Exemple 24. Reprenons l'exemple du scrutin à deux candidats présenté dans l'introduction. On avait une suite de probabilités b_n qui vérifie

$$\sum_{n\geqslant 0} b_n x^n = \frac{1}{2\pi i}\oint \frac{\mathrm{d}y}{y-\frac{x}{3}(1+y+y^2)}.$$

Nommons $f(x)$ cette série, et posons

$$\mathrm{F}(x,y) = \frac{1}{y-x(1+y+y^2)}$$

(on omet le facteur 1/3 pour alléger un peu les calculs). Nous allons calculer un télescopeur pour $\mathrm{F}(x,y)$ en utilisant la réduction de Hermite. Dans les notations du paragraphe précédent, on prend donc $\mathbb{K} = \mathbf{k}(x)$ et $\partial = \partial_x$. La fraction F elle-même est déjà réduite, on passe donc à sa dérivée :

$$\partial_x \mathrm{F}(x,y) = \frac{1+y+y^2}{(y-x(1+y+y^2))^2}.$$

Pour réduire la multiplicité de $\mathrm{P}(x,y) = y-x(1+y+y^2)$ dans le dénominateur, on procède de même que dans la preuve du lemme 20. On commence par calculer la relation de Bézout

$$1 = \frac{4x}{1-2x-3x^2}\cdot \mathrm{P}(x,y) + \frac{1-x-2xy}{1-2x-3x^2}\cdot \partial_y \mathrm{P}(x,y).$$

En refaisant le calcul de la preuve, il vient :

$$\partial_x \mathrm{F}(x,y) = \frac{2xy^2+(2x-2)y-(1+x)}{3x^2-2x-1}\cdot \mathrm{F}(x,y) + \partial_y\left(\frac{(2xy+x-1)(1+y+y^2)}{1-2x-3x^2}\cdot \mathrm{F}(x,y)\right).$$

Et en utilisant la division euclidienne

$$\frac{2xy^2+(2x-2)y-(1+x)}{3x^2-2x-1} = \frac{2}{1-2x-3x^2}\mathrm{P}(x,y) + \frac{3x+1}{1-2x-3x^2},$$

on obtient

$$\partial_x \mathrm{F}(x,y) = \frac{3x+1}{1-2x-3x^2}\cdot \mathrm{F}(x,y) + \partial_y\left(\frac{(x+1)y^2+(x-1)(y+1)}{1-2x-3x^2}\cdot \mathrm{F}(x,y)\right).$$

Ceci est un télescopeur pour F, et en intégrant l'égalité par rapport à y on en déduit l'équation différentielle

$$(1-2x-3x^2)\partial_x f - (3x+1) f = 0. \tag{1.4}$$

En résolvant cette équation, on trouve

$$f(x) = \frac{1}{\sqrt{1-2x-3x^2}}.$$

Après un changement de variable $x \mapsto x/3$, ceci permet de calculer les nombres b_n :

$$\sum_{n\geqslant 0} b_n x^n = 1 + \frac{1}{3}x + \frac{1}{3}x^2 + \frac{7}{27}x^3 + \frac{19}{81}x^4 + \frac{17}{81}x^5 + \frac{47}{243}x^6 + \dots$$

1.3 Calcul des premiers termes des suites polynomialement récursives

1.3.1 Dérouler une récurrence

Dans la suite du texte, les suites polynomialement récursives et les fonctions différentiellement finies seront omniprésentes, et constitueront des structures de données pour toutes les fonctions manipulées. Ces deux notions sont intimement liées par la propriété élémentaire suivante :

Proposition 25. *Soit $f(x) = \sum_{n\geqslant 0} u_n x^n \in \mathbf{k}[[x]]$. Alors*

$$f \text{ est différentiellement finie} \iff (u_n)_{n\in\mathbb{N}} \text{ est polynomialement récursive.}$$

De plus, dans cette correspondance, à partir d'une équation différentielle d'ordre r et de degré d, on obtient une récurrence d'ordre au plus $d+r$ et de degré r.

Démonstration. Pour faire court, on obtient une récurrence à partir d'une équation différentielle par extraction du coefficient de x^n pour tout n, et on passe d'une récurrence à une équation différentielle par sommation. On a ainsi une correspondance

$$x \longleftrightarrow u_{n-1}, \qquad \partial_x \longleftrightarrow (n+1)u_{n+1}$$

Pour ce qui est de l'ordre et du degré de la récurrence, on les voit en regardant le degré et le décalage pour chaque monôme individuellement grâce à la correspondance ci-dessus. □

L'algorithme suggéré dans cette preuve pour faire cette correspondance en pratique n'est pas efficace, mais une méthode par évaluation et interpolation de Bostan et Schost[11] permet de le faire en complexité quasi-optimale. La preuve est très sommaire, mais il est bien plus facile de se convaincre du résultat à l'aide d'un exemple.

Exemple 26. Considérons la fonction

$$f(x) = \frac{\exp(x)}{1-x}.$$

On a $f(x) = \sum_{n\geqslant 0} u_n x^n$, où

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

En dérivant f, on se rend très vite compte qu'elle satisfait l'équation différentielle

$$(1-x)f'(x) + (x-2)f(x) = 0.$$

En remplaçant f par son développement en série, il vient

$$\sum_{n\geqslant 1} n u_n x^{n-1} - \sum_{n\geqslant 1} n u_n x^n + \sum_{n\geqslant 0} u_n x^{n+1} - 2\sum_{n\geqslant 0} u_n x^n = 0.$$

11. BOSTAN et SCHOST, "Polynomial evaluation and interpolation on special sets of points", sous Cor. 2.

On uniformise alors les exposants de x en faisant des changements d'indices, ce qui donne

$$\sum_{n\geqslant 0}(n+1)u_{n+1}x^n - \sum_{n\geqslant 1} nu_n x^n + \sum_{n\geqslant 1} u_{n-1}x^n - 2\sum_{n\geqslant 0} u_n x^n = 0.$$

Enfin, en identifiant terme à terme les deux membres de cette égalité et en faisant le changement de variable $n \mapsto n+1$, on en déduit que

$$\forall n \geqslant 0 \quad (n+2)u_{n+2} - (n+3)u_{n+1} + u_n = 0.$$

Et on pourra se convaincre par un calcul direct que les nombres $\sum_{k=0}^{n} 1/k!$ satisfont bien cette récurrence.

Dans de nombreuses applications, on désirera calculer le développement d'une série f différentiellement finie jusqu'à un certain ordre. À la lumière de la proposition 25, cela revient de façon équivalente à calculer les premiers termes d'une suite polynomialement récursive. L'algorithme naïf consiste alors à calculer assez de conditions initiales par un autre moyen, puis à calculer chaque terme de la suite en fonction des précédents à l'aide de la récurrence. La complexité arithmétique de cette méthode est optimale en N :

Proposition 27. *Soit (u_n) une suite d'éléments de* **k** *polynomialement récursive satisfaisant une récurrence d'ordre r et de degré d. Alors l'algorithme naïf permet de calculer les* N *premiers termes de la suite (u_n) en*

$$\mathrm{O}(drN)$$

opérations arithmétiques dans **k**.

Exemple 28. Considérons un exemple classique en combinatoire : le nombre u_n de mots bien parenthésés de longueur $2n$ sur l'alphabet $\{(,)\}$. u_n n'est autre que le n-ième nombre de Catalan, qui a déjà fait une apparition dans l'introduction. En coupant un mot bien parenthésé w de longueur $2n$ après la parenthèse qui ferme la première parenthèse ouvrante, c'est-à-dire en écrivant $w = (w_1)w_2$, avec w_1 et w_2 des mots bien parenthésés, on se convainc assez vite que les nombres u_n vérifient la récurrence

$$u_0 = 1, \qquad \forall n \geqslant 0 \quad u_{n+1} = \sum_{k=0}^{n} u_k u_{n-k}.$$

Si l'on utilise cette récurrence pour calculer $u_0, u_1, \ldots, u_N$, chaque terme u_n est obtenu comme la somme de n produits de deux entiers. On effectue donc au total $\mathrm{O}(N^2)$ opérations arithmétiques dans $\mathbb{Q}$.

Si au lieu d'utiliser cette récurrence on part de l'équation différentielle satisfaite par la série génératrice $f(x)$ des nombres de Catalan,

$$x(4x-1)f''(x) + (10x-2)f'(x) + 2f(x) = 0,$$

la correspondance de la proposition 25 donne la récurrence :

$$u_0 = 1, \qquad \forall n \geqslant 0 \quad (n+2)u_{n+1} - (4n+2)u_n = 0.$$

En utilisant cette récurrence-ci, le calcul du n-ième terme à partir du précédent ne requiert qu'un nombre constant d'opérations arithmétiques, et on obtient donc $u_0, u_1, \ldots, u_N$ en O(N) opérations dans $\mathbb{Q}$.

En général, tout ne se passe pas forcément aussi bien que dans cet exemple. En effet, il n'y avait pas de problème pour appliquer la récurrence pour toute valeur positive de n car le coefficient $n+2$ ne s'annule pas, et on peut donc diviser. Si jamais le coefficient de tête de la récurrence s'annulait pour une certaine valeur de n, alors il faudrait calculer le coefficient correspondant par un autre moyen. Ceci motive la définition suivante :

Définition 29. Soit $L \in \mathbf{k}(x)\langle \partial_x \rangle$ un opérateur différentiel linéaire à coefficients polynomiaux.

On appelle *polynôme indiciel* de L le coefficient de tête de la récurrence linéaire à coefficients polynomiaux associée à L.

L'*exposant* de L est défini comme étant la plus grande racine entière de son polynôme indiciel.

Ainsi, pour développer une série $\sum_{n\geqslant 0} u_n x^n$ solution d'un opérateur différentiel d'exposant α et d'ordre r, il est suffisant de calculer $\max(r, \alpha+1)$ conditions initiales.

Ceci amène potentiellement à calculer un grand nombre de conditions initiales, comme le montre l'exemple ci-dessous, ce qui peut être prohibitif puisqu'on les calcule en général par l'intermédiaire d'un autre algorithme plus coûteux.

Exemple 30. Considérons la fonction $f(x) = x^c \exp(x)$ avec $c \in \mathbb{N}$, dont on écrit le développement en série

$$f(x) = \sum_{n\geqslant 0} u_n x^n.$$

Alors f satisfait l'équation différentielle du premier ordre

$$x f'(x) - (x+c) f(x) = 0,$$

qui se traduit en la récurrence

$$(n-c)u_n - u_{n-1} = 0.$$

Cette récurrence est d'ordre 1 et de degré 1 quelle que soit la valeur de c, mais à cause de la singularité en $n = c$, il est suffisant de connaître les $c+1$ termes $u_0, u_1, \ldots, u_c$ afin de la dérouler.

1.3.2 Développement d'une série algébrique

Nous allons maintenant montrer que dans le cas où une fonction f est algébrique, l'exposant de l'équation différentielle minimale dont elle est solution ne peut être trop grand. Plus précisément, il est toujours polynomial en le bidegré de l'équation algébrique satisfaite par f.

Dans ce paragraphe, on considère une fonction algébrique $f(x)$ solution d'un polynôme sans carré $P \in \mathbf{k}[x][y]$ dont on note d_x et d_y les degrés respectifs en x et

y. Par le théorème d'Abel, dont l'énoncé précis ainsi que des références pour les preuves sont donnés dans l'annexe A (cf. Théorème 117), f est différentiellement finie et solution de la résolvante différentielle $\mathrm{L_P}$ de P (voir la définition 118). De plus, on peut choisir des racines $y_1 = f, y_2, \ldots, y_n$ de P telles que $(y_1, y_2, \ldots, y_n)$ soit une base de l'espace des solutions de $\mathrm{L_P}$. En particulier, on a $n \leqslant d_y$.

L'obtention de cette borne repose principalement sur deux ingrédients. Le premier est que les zéros du polynôme indiciel de $\mathrm{L_P}$ sont intimement liés aux valuations des solutions de $\mathrm{L_P}$ (lemme 32). Le second est la notion de Wronskien, qui va nous permettre de majorer les valuations des solutions de $\mathrm{L_P}$ (lemme 33). Rappelons sa définition :

Définition 31. Soient $f_1, f_2, \ldots, f_n \in \overline{\mathbf{k}}\langle\langle x\rangle\rangle$ des séries de Puiseux. Leur *Wronskien*, noté $\mathrm{Wr}(f_1, f_2, \ldots, f_n)$ est défini par

$$\mathrm{Wr}(f_1, f_2, \ldots, f_n) = \begin{vmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_n' \\ \vdots & \vdots & \vdots & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & \cdots & f_n^{(n-1)} \end{vmatrix}.$$

Lemme 32. *Soit* α *l'exposant de* $\mathrm{L_P}$. *Alors il existe une série de Laurent* $f \in \mathbf{k}((x))$, *solution de* $\mathrm{L_P}$, *et telle que*

$$\mathrm{val}_x f = \alpha.$$

Démonstration. On trouvera la preuve dans le livre d'Ince [12]. □

Lemme 33. *Soit* $y \in \mathbf{k}((x))$ *une série de Laurent non-nulle solution de* $\mathrm{L_P}$. *Alors*

$$\mathrm{val}(y) \leqslant \mathrm{val}(\mathrm{Wr}(y_1, y_2, \ldots, y_n)) + \mathrm{O}(d_x d_y + d_y^2).$$

Démonstration. On décompose y sur la base $(y_1, y_2, \ldots, y_n)$:

$$y(x) = \sum_{i=1}^{n} \lambda_i y_i,$$

avec $\lambda_i \in \mathbf{k}$ pour tout i. On peut de plus supposer sans perte de généralité que $\lambda_1 \neq 0$. Le fait que $\mathrm{val}(f') \geqslant \mathrm{val}(f) - 1$ pour tout $f \in \mathbf{k}((x))$ implique que

$$\mathrm{val}(\mathrm{Wr}(y, y_2, \ldots, y_n)) \geqslant \mathrm{val}(y) + \sum_{i=2}^{n} \mathrm{val}(y_i) - \binom{n}{2}.$$

Par multilinéarité du Wronskien, le membre gauche de l'inégalité n'est autre que $\mathrm{val}(\mathrm{Wr}(y_1, y_2, \ldots, y_n))$. Par ailleurs, les valuations des y_i sont en valeur absolue des pentes du polygone de Newton de P (voir proposition 122). On obtient ainsi la majoration :

$$\mathrm{val}(y) \leqslant \mathrm{val}(\mathrm{Wr}(y_1, y_2, \ldots, y_n)) + (d_y - 1)\max(d_x, d_y) + \frac{d_y(d_y-1)}{2},$$

ce qui permet de conclure. □

12. INCE, *Ordinary differential equations*, §15.31.

Proposition 34. *Soit* $P \in \mathbf{k}[x][y]$ *un polynôme tel que* $\operatorname{bideg} P \leqslant (d_x, d_y)$*, et soit* L_P *la résolvante différentielle de* P.

Alors toutes les séries de Laurent $y(x)$ *solutions de* L_P *vérifient uniformément :*

$$\operatorname{val}_x(y(x)) = O(d_x d_y^2).$$

Démonstration. D'après le lemme 33, il suffit de prouver que

$$\operatorname{val}(\operatorname{Wr}(y_1, y_2, \dots, y_n)) = O(d_x d_y^2).$$

L'argument qui suit est inspiré d'un calcul similaire dans un article de Bostan, Chyzak *et al.*[13], dont on va commencer par rappeler quelques résultats.

Il existe des polynômes $W_k \in \mathbf{k}[x, y]$ tels que, pour tout $i \in \{1, 2, \dots, n\}$ et tout $k \geqslant 1$, la dérivée $y_i^{(k)}$ peut s'écrire sous la forme

$$y_i^{(k)} = \frac{W_k(x, y_i)}{P_y(x, y_i)^{2k-1}}.$$

De plus, les polynômes W_k satisfont

$$\deg_x W_k \leqslant (2d_x - 1)k - d_x, \quad \deg_y W_k \leqslant 2(d_y - 1)k - d_y + 2. \tag{1.5}$$

On en déduit que $D = \prod_{i=1}^{n} P_y(x, y_i)^{2n-3} \in \mathbf{k}[x, y_1, y_2, \dots, y_n]$ est un polynôme tel que $\operatorname{Wr}(y_1, y_2, \dots, y_n) \cdot D \in \mathbf{k}[x, y_1, y_2, \dots, y_n]$. On notera R ce dernier polynôme. R est le déterminant de la matrice

$$\mathscr{N} = \begin{pmatrix} y_1 P_y(x, y_1)^{2n-3} & \cdots & y_n P_y(x, y_n)^{2n-3} \\ W_1(x, y_1) P_y(x, y_1)^{2n-4} & \cdots & W_1(x, y_n) P_y(x, y_n)^{2n-4} \\ W_2(x, y_1) P_y(x, y_1)^{2n-6} & \cdots & W_2(x, y_n) P_y(x, y_n)^{2n-6} \\ \vdots & \vdots & \vdots \\ W_{n-1}(x, y_1) & \cdots & W_{n-1}(x, y_n) \end{pmatrix}.$$

R est un polynôme antisymétrique en $y_1, y_2, \dots, y_n$ et donc R^2 quant à lui est symétrique, de même que D. La proposition 126 montre donc que D et R^2 sont des fractions rationnelles en x. Or, on a

$$\operatorname{Wr}(y_1, y_2, \dots, y_n) = \frac{R}{D}.$$

Donc ce Wronskien est la racine carrée d'une fraction rationnelle en x. Ce résultat de structure et les bornes de la proposition 126 vont fournir la majoration attendue.

Si $\det(\mathscr{N})$ est vu comme un élément de $\mathbf{k}[x, y_1, y_2, \dots, y_n]$, alors

$$\begin{aligned} \deg_x \det(\mathscr{N})^2 &\leqslant 2 \sum_{k=0}^{n-1} ((2n-3)d_x - k) \\ &\leqslant 2n(2n-3)d_x + n(n-1), \end{aligned}$$

13. BOSTAN, CHYZAK et al., "Differential equations for algebraic functions", §2.2.

et pour tout $i \in \{1,2,\dots,n\}$,

$$\deg_{y_i} \det(\mathcal{N})^2 \leqslant 2(2n-3)d_y - 2(2n-4).$$

De même, en voyant D comme un élément de $\mathbf{k}[x, y_2, y_2, \dots, y_n]$, on calcule

$$\deg_x \mathrm{D} = n(2n-3)d_x, \quad \deg_{y_i} \mathrm{D} = (2n-3)(d_y-1).$$

Maintenant, on note $p(x)$ le coefficient dominant de $\mathrm{P}(x,y)$, et on en déduit que

$$\mathrm{Wr}(y_1, y_2, \dots, y_n) = \frac{\mathrm{U}(x)}{p(x)\mathrm{V}(x)},$$

où

$$\deg_x \mathrm{U}^2 \leqslant 2n(2n-3)d_x + n(n-1) + 2(2n-3)d_x d_y - 2(2n-4)d_x.$$

Finalement, les inégalités $\mathrm{val}(\mathrm{Wr}(y_1, y_2, \dots, y_n)) \leqslant \frac{1}{2}\mathrm{val}(\mathrm{U}^2) \leqslant \frac{1}{2}\deg_x(\mathrm{U}^2)$ et $n \leqslant d_y$ donnent

$$\mathrm{val}(\mathrm{Wr}(y_1, y_2, \dots, y_n)) = \mathrm{O}(d_x d_y^2),$$

ce qui termine la preuve. □

Corollaire 35. *Soit* $\mathrm{P} \in \mathbf{k}[x][y]$ *un polynôme tel que* $\mathrm{bideg}\,\mathrm{P} \leqslant (d_x, d_y)$*, et soit* L_P *la résolvante différentielle de* P*. Soit* α *l'exposant de* L_P*.*

Alors

$$\alpha = \mathrm{O}(d_x d_y^2).$$

Démonstration. Ceci découle de la proposition et du lemme 32. □

Chapitre 2

Intégrales de termes mixtes

J'ai présenté dans le chapitre précédent la méthode du télescopage créatif par réduction. Maintenant, je vais construire une réduction pour une instance du problème, à savoir le télescopage créatif pour les termes mixtes hypergéométriques et hyperexponentiels de la forme

$$\Psi(n,x) = \Upsilon(n)\cdot\mathscr{P}(n,x)\cdot\mathfrak{h}(x)^n\cdot\exp\left(\int\mathfrak{g}(x)\mathrm{d}x\right), \tag{2.1}$$

où $\mathscr{P}\in\mathbf{k}(n)[x]$ est un polynôme, $\mathfrak{h}$ et $\mathfrak{g}$ sont des fractions rationnelles, et Υ est une suite hypergéométrique. On en a vu plusieurs exemples dans l'introduction. Si l'on s'intéresse à cette forme-ci en particulier, c'est parce que Chen, Chyzak, *et al.*[1] ont prouvé que parmi les termes mixtes hypergéométriques et hyperexponentiels, ce sont exactement ceux de cette forme pour lesquels il existe des télescopeurs.

On souhaite donc trouver des relations du type

$$\sum_{i=0}^{r} c_i(n)\mathrm{S}_n^i\cdot\Psi = (\mathrm{K}\Psi)',$$

avec $\mathrm{K}\in\mathbf{k}(n,x)$. (Pour ce chapitre, on notera $f'(n,x)=\partial_x f(n,x)$, ce qui ne sera pas ambigu car on ne dérivera jamais par rapport à n.) La première chose à remarquer est qu'il suffit de traiter le cas $\Upsilon(n)=1$. En effet, si $\Psi(n,x)=\Upsilon(n)\cdot\mathrm{F}(n,x)$ et si l'on a trouvé un télescopeur $\sum_{i=0}^{r}c_i(n)\mathrm{S}_n^i$ pour F, alors l'opérateur

$$\sum_{i=0}^{r} c_i(n)\frac{\Upsilon(n)}{\Upsilon(n+i)}\mathrm{S}_n^i$$

est un télescopeur pour Ψ puisque $\Upsilon(n)/\Upsilon(n+i)$ est une fraction rationnelle.

Une fois de plus, c'est un problème d'une nature purement algébrique. En effet, lorsque $\mathbf{k}=\mathbb{C}$, une fonction Ψ du type (2.1) est méromorphe sur $\mathbb{C}$. On peut donc rechercher un télescopeur pour Ψ en tant qu'objet formel, et le principe de

1. Chen, Chyzak et al., "On the existence of telescopers for mixed hypergeometric terms".

continuation analytique montre que tout télescopeur obtenu par ce biais en sera également un pour Ψ vu comme une fonction de la variable complexe.

On continue donc à raisonner sur un corps $\mathbf{k}$ de caractéristique 0 et pour des raisons qui seront apparentes par la suite, il convient de poser $\Psi = \mathscr{P}\cdot\Phi$ car le polynôme $\mathscr{P}$ jouera un rôle spécial. On voit désormais Φ comme une indéterminée, et on travaille dans l'anneau $\mathbb{A} = \mathbf{k}(n,x)[\Phi]$ auquel on étend les opérateurs de décalage et de dérivation en imposant

$$\mathrm{S}_n\Phi = \mathrm{F}_1\Phi, \quad \Phi' = \mathrm{F}_2\Phi,$$

où $\mathrm{F}_1, \mathrm{F}_2 \in \mathbf{k}(n,x)$. De plus, pour que Ψ représente bien un terme du type (2.1), on fixe la forme de F_1 et F_2 :

Notations 36. Dans tout ce chapitre, on s'intéresse à un terme mixte $\Psi(n,x)$ de la forme

$$\Psi(n,x) = \mathscr{P}(n,x)\Phi(n,x),$$

où $\mathscr{P} \in \mathbf{k}(n)[x]$ et il existe $\mathfrak{h} \in \mathbf{k}(x)$ et $\mathfrak{v}, \mathfrak{w} \in \mathbf{k}[x]$ tels que

$$\frac{\Phi'}{\Phi} = n\frac{\mathfrak{h}'}{\mathfrak{h}} + \frac{\mathfrak{v}}{\mathfrak{w}}.$$

On note respectivement $\mathrm{A} \in \mathbf{k}[n,x]$ et $b \in \mathbf{k}[x]$ le numérateur et le dénominateur de la forme réduite de Φ'/Φ.

La réduction que je vais construire repose sur la même idée que la réduction de Hermite présentée dans le chapitre précédent. Par définition, on a $\mathrm{S}_n\Phi = \mathfrak{h}\Phi$, donc le décalage augmente la multiplicité des pôles de $\mathfrak{h}$. La réduction va consister à ajouter des dérivées de façon à réduire ces multiplicités, et récrire ainsi les décalages sous la forme $\mathrm{R}\Phi$, où $\mathrm{R} \in \mathbf{k}(n)[x]$.

La construction est faite dans la deuxième section. La première section quant à elle met en place des propriétés qui se traduiront par le confinement et la normalité de la réduction. Dans la troisième section, j'analyserai quantitativement l'algorithme de télescopage créatif qui en découle pour évaluer la taille des télescopeurs calculés. Les deux dernières sections contiennent des exemples et l'analyse de complexité des algorithmes.

Les algorithmes des deux premières sections sont fondamentalement univariés et pourraient être adaptés à des termes hyperexponentiels ne dépendant pas de n. On notera alors $\mathbb{K} = \mathbf{k}(n)$ et on travaillera dans $\mathbb{K}$.

2.1 Confinement

Lemme 37. *Avec les notations 36, notons de plus*

$$\delta = \max(\deg_x \mathrm{A}, \deg_x b - 1).$$

Alors, pour tout polynôme $\mathrm{P} \in \mathbb{K}[x]$*, il existe une unique paire de polynômes* $\mathrm{R}, \mathrm{Q} \in \mathbb{K}[x]$*, avec*

$$\deg_x \mathrm{R} < \delta, \quad \deg_x \mathrm{Q} \leqslant \deg_x \mathrm{P} - \delta,$$

et tels que

$$\mathrm{P}\Phi = \mathrm{R}\Phi + (\mathrm{Q}b\Phi)'. \tag{2.2}$$

Démonstration. L'équation (2.2) se récrit :

$$\mathrm{QA} + (\mathrm{Q}b)' = \mathrm{P} - \mathrm{R}. \tag{2.3}$$

Notons $d = \deg_x \mathrm{P} - \delta$, et considérons l'application linéaire

$$\phi : \mathbb{K}[x]_d \to \mathbb{K}[x]_d \quad \mathrm{Q} \mapsto (\mathrm{QA} + (\mathrm{Q}b)') \operatorname{div} x^\delta,$$

où $u \operatorname{div} v$ est le quotient de la division euclidienne de u par v. Alors, pour tout $k \in \{0, 1, \ldots, d\}$, $\phi(x^k)$ est de degré au plus k. Son coefficient de degré k vaut

$$\begin{cases} \mathrm{lc}(\mathrm{A}) & \text{si } \deg_x \mathrm{A} > \deg_x b - 1, \\ k + \delta + 1 & \text{si } \deg_x b - 1 > \deg_x \mathrm{A}, \\ \mathrm{lc}(\mathrm{A}) + k + \delta + 1 & \text{si } \deg_x \mathrm{A} = \deg_x b - 1. \end{cases}$$

Dans les deux premiers cas, on a clairement $\mathrm{lc}(\phi(x^k)) \neq 0$. Par ailleurs, si l'on est dans le troisième cas, alors comme $\deg_x^\infty(\mathfrak{h}'/\mathfrak{h}) = -1$ on doit également avoir $\deg_x^\infty(\mathfrak{v}/\mathfrak{w}) < 0$. Mais dans ce cas, si l'on pose $\mathfrak{h}'/\mathfrak{h} = p/q$ où $p, q \in \mathbf{k}[x]$ vérifient $\deg_x p = \deg_x q - 1$, on obtient que $\mathrm{A}/b = (np\mathfrak{w} + q\mathfrak{v})/(q\mathfrak{w})$. Or,

$$\deg_x(q\mathfrak{v}) \leqslant \deg_x q + \deg_x \mathfrak{w} - 1 = \deg_x(p\mathfrak{w}).$$

Donc $\mathrm{lc}(\mathrm{A})$ dépend de n et ne peut être nul. Ainsi, dans tous les cas $\phi(x^k)$ est un polynôme de degré exactement k. On en déduit que ϕ est un isomorphisme. Ceci conclut quant à l'existence et l'unicité de Q et R, vu que l'équation (2.3) est équivalente à $\phi(\mathrm{Q}) = \mathrm{P} \operatorname{div} x^\delta$ et $\mathrm{R} = \mathrm{P} - \mathrm{QA} - (\mathrm{Q}b)'$.

La construction montre très clairement que les degrés de R et Q sont tels qu'annoncés. □

La quantité δ de ce lemme va intervenir de façon capitale tout au long de chapitre. Fixons donc une bonne fois pour toutes cette notation.

Notation 38. Les polynômes A et b étant ceux définis dans les notations 36, on note $\delta = \max(\deg_x \mathrm{A}, \deg_x b - 1)$.

La preuve du lemme 37 est complètement effective, et conduit à l'algorithme Confinement (algorithme 2). Ainsi dans une expression $\mathrm{P}\Phi$, où $\mathrm{P} \in \mathbb{K}[x]$ est un polynôme, on peut toujours réduire le degré de P en ajoutant des dérivées. Cette propriété servira à confiner la réduction que nous allons construire dans la section suivante.

On termine cette section par une proposition qui permettra d'obtenir l'autre propriété importante pour notre réduction : la normalité.

Proposition 39. *On reprend les notations 36 et 38. Supposons de plus que Φ'/Φ n'a pas de résidu entier positif. Alors, pour tout polynôme $\mathrm{R} \in \mathbb{K}[x]$ tel que $\deg_x \mathrm{R} < \delta$,*

$$(\exists \mathrm{K} \in \mathbb{K}(x)\ \mathrm{R}\Phi = (\mathrm{K}\Phi)') \iff \mathrm{R} = 0.$$

Algorithme Confinement(P,F)

Entrée Un polynôme $P \in \mathbb{K}[x]$, une fraction rationnelle $F = A/b$ telle que $\text{pgcd}(A, b) = 1$.

Sortie Un polynôme $R \in \mathbb{K}[x]$ de degré strictement inférieur à $\max(\deg(A), \deg(b)-1)$ et tel qu'il existe $Q \in \mathbb{K}[x]$ vérifiant $P = R + (Qb)' + QA$

$\delta \leftarrow \max(\deg(A), \deg(b)-1)$;
$d \leftarrow \deg(P) - \delta$;
Écrire $A = \sum_i a_i x^i$, $b = \sum_i b_i x^i$, $P = \sum_i p_i x^i$;
pour $i \leftarrow d$ à 0 **faire**
  $c \leftarrow a_\delta + (\delta + i + 1) b_{\delta+1}$;
  $q_i \leftarrow \frac{1}{c}\Big(p_{\delta+i} - \sum_{j=1}^{\delta} q_{i+j} a_{\delta-j}$
    $-(\delta + i + 1)\sum_{j=1}^{\delta+1} q_{i+j} b_{\delta+1-j}\Big)$;
$Q \leftarrow \sum_{i=0}^{d} q_i x^i$;
renvoyer $P - (Qb)' - QA$.

Algorithme 2: Confinement

Démonstration. L'implication réciproque est évidente. Pour l'implication directe, supposons qu'une telle fraction K existe. Alors l'équation se récrit

$$R = K' + K\frac{A}{b}. \tag{2.4}$$

Si K est un polynôme, cette égalité ne peut être satisfaite que si b divise K, auquel cas le résultat est une conséquence immédiate de l'unicité dans le lemme 37.

Mais si jamais K n'était pas un polynôme, K admettrait un pôle x_0 d'ordre $v > 0$. Alors l'équation (2.4) montre que A/b devrait avoir un pôle simple en x_0 avec résidu v, ce qui contredirait l'hypothèse faite sur les résidus de Φ'/Φ. □

La signification de cette proposition est qu'avec les bonnes hypothèses sur Φ, il n'y a pas de dérivée dont la forme normale (le confinement) est non-nulle. Cette propriété sera capitale pour les questions de minimalité des télescopeurs que l'on va calculer. Revenons sur la condition sur Φ dans la proposition. Si Φ'/Φ admet un résidu entier positif, cela signifie que l'on peut écrire $\Phi = P\tilde{\Phi}$ où P est un polynôme. Ainsi, informellement, dire que Φ'/Φ n'admet pas de résidu entier positif, c'est dire que dans l'écriture $\Psi = \mathscr{P}\Phi$, tous les polynômes ont été extraits de Φ et inclus dans $\mathscr{P}$.

2.2 Réduction de type Hermite

On passe désormais à la construction de la réduction à proprement parler. De même que pour la réduction de Hermite, on procède en une succession de réductions atomiques. On commence par un lemme technique, qui établit une propriété nécessaire pour amorcer la réduction.

Lemme 40. *On reprend les notations 36. Soit $f \in \mathbf{k}[x]$ un facteur sans carré du dénominateur de $\mathfrak{h}$. Alors, pour tout entier i,*

$$\operatorname{pgcd}\left(f, \mathrm{A} + b' - i\frac{bf'}{f}\right) = 1.$$

Démonstration. Si $\mathfrak{h} = 0$, le résultat est immédiat car nécessairement $f = 1$.

Dans le cas contraire, notons $\tilde{\mathrm{A}} = \mathrm{A} - ibf'/f$ et commençons par supposer que f est irréductible. Alors en écrivant $\mathfrak{h} = f^k\tilde{\mathfrak{h}}$ où le numérateur et le dénominateur de $\tilde{\mathfrak{h}}$ sont premiers avec f, on voit qu'il existe des polynômes $\mathfrak{h}_1, \mathfrak{h}_2 \in \mathbf{k}[x]$ tels que

$$\frac{\tilde{\mathrm{A}}}{b} = (nk - i)\frac{f'}{f} + \frac{\mathfrak{h}_1}{\mathfrak{h}_2} + \frac{\mathfrak{v}}{\mathfrak{w}},$$

avec $\operatorname{pgcd}(f, \mathfrak{h}_2) = 1$ et $b = \operatorname{ppcm}(f, \mathfrak{h}_2, \mathfrak{w})$. Écrivons $b = f^{\nu}\tilde{b}$ avec $\operatorname{pgcd}(f, \tilde{b}) = 1$. Alors

$$\tilde{\mathrm{A}} = (nk - i)f'f^{\nu-1}\tilde{b} + n\mathfrak{h}_1 f^{\nu}\frac{\tilde{b}}{\mathfrak{h}_2} + \mathfrak{v}\frac{f^{\nu}\tilde{b}}{\mathfrak{w}}$$

On en déduit la réduction de $\tilde{\mathrm{A}} + b'$ modulo f :

$$\tilde{\mathrm{A}} + b' \equiv (nk + \nu - i)f'f^{\nu-1}\tilde{b} + \mathfrak{v}\frac{f^{\nu}\tilde{b}}{\mathfrak{w}} \bmod f. \tag{2.5}$$

Comme f ne dépend pas de n, $f \mid \tilde{\mathrm{A}} + b'$ impliquerait qu'on a à la fois $f \mid f'f^{\nu-1}\tilde{b}$ et $f \mid \mathfrak{v}f^{\nu}\tilde{b}/\mathfrak{w}$. Pour vérifier la première relation de divisibilité, il faut que $\nu > 1$. Ceci n'est possible que si $f^{\nu} \mid \mathfrak{w}$, auquel cas la deuxième relation de divisibilité rendrait nécessaire $f \mid \mathfrak{v}$. Comme ceci contredirait le fait que $\operatorname{pgcd}(\mathfrak{v}, \mathfrak{w}) = 1$, on en déduit que $f \not| \tilde{\mathrm{A}} + b'$.

Maintenant, pour un facteur sans carré f du dénominateur de $\mathfrak{h}$ quelconque, tous les facteurs irréductibles de f sont inversibles modulo $\tilde{\mathrm{A}} + b'$ par ce qui précède, et donc f également par le théorème des restes Chinois. □

On est maintenant en mesure de prouver le lemme suivant, qui permet d'effectuer une étape atomique de la réduction. C'est l'analogue dans ce cadre mixte du lemme 20 p. 33.

Lemme 41. *On reprend les notations 36 et 38. Soit $\mathrm{P} \in \mathbb{K}[x]$ un polynôme, k un entier strictement positif, et $f \in \mathbf{k}[x]$ un facteur sans carré du dénominateur de $\mathfrak{h}$. Alors il existe une paire de polynômes $\mathrm{R}, \mathrm{Q} \in \mathbb{K}[x]$, avec*

$$\deg_x \mathrm{R} \leqslant \max(\deg_x \mathrm{P} - \deg_x f, \delta - 1), \quad \deg_x \mathrm{Q} < \deg_x f,$$

et tels que

$$\mathrm{P}\frac{\Phi}{f^k} = \mathrm{R}\frac{\Phi}{f^{k-1}} + \left(\mathrm{Q}b\frac{\Phi}{f^k}\right)'.$$

Démonstration. On note $\tilde{\Phi} = \Phi/f^k$. On a $\tilde{\Phi}'/\tilde{\Phi} = \tilde{\mathrm{A}}/b$ avec $\tilde{\mathrm{A}} = \mathrm{A} - kbf'/f$. Avec ces notations, on veut trouver R et Q tels que

$$\mathrm{P}\tilde{\Phi} = \mathrm{R}f\tilde{\Phi} + \left(\mathrm{Q}b\tilde{\Phi}\right)'.$$

Par le lemme 40, on a $\operatorname{pgcd}(f, \tilde{A} + b') = 1$, donc il existe $U, Q \in \mathbb{K}[x]$ tels que $\deg_x Q < \deg_x f$ et

$$P = Uf + Q\left(\tilde{A} + b'\right).$$

Considérons alors la dérivée

$$\frac{\left(Qb\tilde{\Phi}\right)'}{\tilde{\Phi}} = Q'b + Q(\tilde{A} + b') = (Q'b/f - U)f + P.$$

On voit qu'il suffit de poser $R = (P - (Qb)' - Q\tilde{A})/f$ et on a l'égalité attendue. De plus, cette définition de R rend apparente la borne annoncée sur son degré. □

À nouveau, la preuve est complètement effective. En particulier, avec les mêmes notations, on peut appliquer le lemme plusieurs fois et écrire

$$P\frac{\Phi}{f^k} = R\Phi + \left(Qb\frac{\Phi}{f^k}\right)',$$

pour un certain polynôme $Q \in \mathbb{K}[x]$. Cette opération est effectuée par l'algorithme RéducÉlém (algorithme 3).

Exemple 42. Regardons ce que signifie le lemme dans le cas particulier $\Phi = 1/g^n$, où $g \in \mathbf{k}[x]$ est un polynôme sans carré, et $f = g$, $k = 1$. Alors le lemme affirme qu'il existe des polynômes R et Q, avec $\deg_x R < \deg_x g$ tels que

$$\frac{P}{g^{n+1}} = \frac{R}{g^n} + \left(\frac{Q}{g^n}\right)'.$$

C'est tout à fait similaire à une étape élémentaire de la réduction de Hermite (lemme 20 p. 33), sauf que l'exposant dépend ici de n.

De plus, si l'on regarde la démonstration, $\tilde{A}$ est, ici, le numérateur de $(1/g^{n+1})'/(1/g^{n+1})$, c'est-à-dire $\tilde{A} = -(n+1)g'$. Le point clé de la preuve est donc une relation de Bézout entre g et g', ce qui est tout à fait analogue à la preuve du lemme 20.

C'est pour cette raison que l'on dit que cette réduction est « de type Hermite ».

La réduction complète s'effectue en utilisant de façon répétée le lemme précédent. Elle est décrite dans cette proposition, qui est l'analogue de la réduction de Hermite pour les fractions rationnelles (proposition 21 p. 33).

Proposition 43. *On reprend les notations 36 et 38. Notons également*

$$\delta_{\mathfrak{h}} = \max(\deg_x^{\infty} \mathfrak{h}, 0),$$

et soit $\mathfrak{h}_1/\mathfrak{h}_2$ *la forme réduite de* $\mathfrak{h}$.

Pour tout polynôme $P \in \mathbb{K}[x]$ *il existe une paire* $R, Q \in \mathbb{K}[x]$ *de polynômes avec*

$$\deg_x R \leqslant \max(\deg_x P + \delta_{\mathfrak{h}}, \delta - 1), \quad \deg_x Q < \deg_x \mathfrak{h}_2$$

et tels que

$$P\mathfrak{h}\Phi = R\Phi + \left(Qb\frac{\Phi}{\mathfrak{h}_2}\right)'.$$

Algorithme RéducÉlém(P,F,f,k)

Entrée Un polynôme $P \in \mathbb{K}[x]$, une fraction rationnelle $F = A/b \in \mathbb{K}(x)$, un facteur sans carré f de b tel que $\operatorname{pgcd}(f, A + b' - ibf'/f) = 1$ pour tout $i \in \mathbb{Z}$, un entier $k > 1$.

Sortie Un polynôme $R \in \mathbb{K}[x]$ tel que $P = f^k(R + (Qb)' + QA))$ pour un certain $Q \in \mathbb{K}[x][f^{-1}]$.

$R \leftarrow P$;
pour $i \leftarrow 1$ à k **faire**
  $C \leftarrow A + b' + (i-k-1)bf'/f$;
  Écrire $R = \tilde{Q}C + Vf$ avec $\deg_x \tilde{Q} < \deg_x f$;
  $R \leftarrow (R - \tilde{Q}'b - \tilde{Q}C)/f$; ▷ $\frac{P}{f^k}\Phi = \frac{R}{f^{k-i}}\Phi + (Qb\Phi)'$
renvoyer R.

Algorithme 3: Étape élémentaire de la réduction de type Hermite

Démonstration. On commence par décomposer $\mathfrak{h}$ en éléments simples. Étant donnée une décomposition sans carrés

$$\mathfrak{h}_2 = f_1 f_2^2 \dots f_m^m,$$

il existe des polynômes $u, u_1, u_2, \dots, u_m$ tels que

$$\mathfrak{h} = u + \sum_{i=1}^{m} \frac{u_i}{f_i^i},$$

avec $\deg_x u_i < i \deg_x f_i$, et $\deg_x u = \deg_x^\infty \mathfrak{h}$ si $u \neq 0$. De là, on calcule

$$P\mathfrak{h}\Phi = Pu\Phi + \sum_{i=1}^{m} Pu_i \frac{\Phi}{f_i^i}.$$

Maintenant, pour chaque terme de la somme, on applique répétitivement le lemme 41, ce qui produit des polynômes $R_1, R_2, \dots, R_m, Q_1, Q_2, \dots, Q_m$ avec

$$\deg_x R_i \leqslant \max(\deg_x P, \delta - 1), \quad \deg_x Q_i < i \deg_x f_i$$

et tels que

$$Pu_i \frac{\Phi}{f_i^i} = R_i\Phi + \left(Q_i b \frac{\Phi}{f_i^i}\right)'.$$

Il suffit donc de choisir pour Q le polynôme $\mathfrak{h}_2 \sum_{i=1}^m Q_i/f_i^i$, et

$$R = Pu + \sum_{i=1}^{m} R_i.$$

Les degrés des polynômes R et Q sont alors apparents de par leur construction. □

Algorithme Réduction(P,$\mathfrak{h}$,$\mathfrak{v}/\mathfrak{w}$)

Entrée Un polynôme $P \in \mathbf{k}(n)[x]$,
deux fractions rationnelles $\mathfrak{h} = \mathfrak{h}_1/\mathfrak{h}_2$ et $\mathfrak{v}/\mathfrak{w} \in \mathbf{k}(x)$.

Sortie Un polynôme $R \in \mathbf{k}(n)[x]$ tel que $P\mathfrak{h} = R + (Qb)' + QA$ pour un certain $Q \in \mathbf{k}(n,x)$, où $A/b = n\mathfrak{h}'/\mathfrak{h} + \mathfrak{v}/\mathfrak{w}$.

Calculer une décomposition sans carré du dénominateur de $\mathfrak{h}$: $\mathfrak{h}_2 = f_1 f_2^2 \dots f_m^m$;
Calculer la décomposition en éléments simples correspondante :
$\mathfrak{h} = u + \sum_{i=1}^{m} u_i / f_i^i$;
$K \leftarrow n\mathfrak{h}'/\mathfrak{h} + \mathfrak{v}/\mathfrak{w}$;
pour $i \leftarrow 1$ à m **faire**
  $r_i \leftarrow$ RéducÉlém(Pu_i, K, f_i, i) ;
renvoyer $Pu + r_1 + \dots + r_m$.

Algorithme 4: Réduction de type Hermite d'un terme mixte hypergéométrique et hyperexponentiel

À ce stade, prenons un peu de recul sur ce que signifient les résultats prouvés jusqu'ici. Le lemme 37 montre que l'on sait réduire $P\Phi$ vers un espace de dimension finie pour tout polynôme P, en posant $[P\Phi] = R$ pour le R du lemme. La proposition 43 montre que l'on sait réduire $P\mathfrak{h}\Phi$ pour tout polynôme P, en posant $[P\mathfrak{h}\Phi] = [R\Phi]$ pour le R de la proposition. On peut étendre la réduction à $P\mathfrak{h}^k\phi$ pour tout k en posant $[S_n^k\Phi] = [S_n[S_n^{k-1}\Phi]]$. Ceci sera suffisant pour arriver à nos fins (calculer un télescopeur), mais on pourrait aller plus loin en remarquant que la preuve de la proposition 43 s'adapte sans problème si l'on remplace $\mathfrak{h}$ par tout élément de $\mathbb{K}[x][\frac{1}{b^\star}]$. On peut donc faire de $[\cdot]$ une réduction sur $\mathbb{K}[x][\frac{1}{b^\star}, \Phi]$, qui a la propriété d'être confinée. De plus, la proposition 39 montre qu'il suffit que Φ'/Φ n'ait pas de résidu entier positif pour que la réduction soit normale (voir la définition 15 p. 31).

2.3 Algorithme TCMixte

Comme il a été expliqué dans la section 1.2, la réduction que l'on vient de construire mène à un algorithme pour calculer un télescopeur pour Ψ. La stratégie consiste à chercher une combinaison linéaire nulle entre les réductions de Ψ, $S_n\Psi$, $S_n^2\Psi$, … Le lemme suivant permet de suivre de façon précise la forme que prennent les réductions de ces décalages successifs, ce qui va nous permettre de prédire les degrés des coefficients du télescopeur.

Lemme 44. *On reprend les notations 36 et 38. Pour tout $i \in \mathbb{N}$, il existe des polynômes $R_i, Q_i \in \mathbb{K}[x]$, avec*

$$\deg_x R_i < \delta, \quad \deg_x Q_i < i \deg_x \mathfrak{h} + \max(\deg_x \mathscr{P} - \delta, 0),$$

et tels que

$$\mathscr{P}(n+i,x)\mathfrak{h}^i\Phi = \mathrm{R}_i\Phi + \left(\mathrm{Q}_i b\frac{\Phi}{\mathfrak{h}_2^i}\right)'. \tag{2.6}$$

Démonstration. On construit les polynômes R_i et Q_i par récurrence sur i.

Pour $i=0$, soit $\deg_x\mathscr{P} < \delta$ auquel cas il suffit de choisir $\mathrm{R}_0 = \mathscr{P}$ et $\mathrm{Q}_0 = 0$, soit $\deg_x\mathscr{P} \geqslant \delta$ et alors le lemme 37 appliqué à $\mathscr{P}$ fournit R_0 et Q_0.

Maintenant, donnons-nous un entier $i>0$ et supposons que R_{i-1} et Q_{i-1} ont déjà été construits. En remplaçant n par $n+1$ et i par $i-1$ dans l'équation (2.6), on obtient

$$\mathscr{P}(n+i,x)\mathfrak{h}^i\Phi = \mathrm{R}_{i-1}\mathfrak{h}\Phi + \left(\mathrm{Q}_{i-1}b\frac{\mathfrak{h}\Phi}{\mathfrak{h}_2^{i-1}}\right)'.$$

On peut alors appliquer la proposition 43 : il existe des polynômes $\tilde{\mathrm{R}}_i, \tilde{\mathrm{Q}}_i \in \mathbb{K}[x]$ tels que

$$\mathrm{R}_{i-1}\mathfrak{h}\Phi = \tilde{\mathrm{R}}_i\Phi + \left(\tilde{\mathrm{Q}}_i b\frac{\Phi}{\mathfrak{h}_2}\right)',$$

avec de plus

$$\deg_x\tilde{\mathrm{R}}_i \leqslant \delta - 1 + \delta_{\mathfrak{h}}, \quad \deg_x\tilde{\mathrm{Q}}_i < \deg_x\mathfrak{h}_2.$$

Si $\delta_{\mathfrak{h}} > 0$ on applique le lemme 37 et on obtient $\mathrm{R}_i, \overline{\mathrm{Q}}_i$ tels que

$$\tilde{\mathrm{R}}_i\Phi = \mathrm{R}_i\Phi + \left(\overline{\mathrm{Q}}_i b\Phi\right)',$$

avec $\deg_x\mathrm{R}_i < \delta$ et

$$\deg_x\overline{\mathrm{Q}}_i \leqslant \deg_x\tilde{\mathrm{R}}_i - \delta < \delta_{\mathfrak{h}}.$$

Si au contraire $\delta_{\mathfrak{h}} \leqslant 0$, on a déjà $\deg_x\tilde{\mathrm{R}}_i < \delta$. Dans ce cas on pose simplement $\mathrm{R}_i = \tilde{\mathrm{R}}_i$ et $\overline{\mathrm{Q}}_i = 0$. Enfin, on choisit

$$\mathrm{Q}_i = \mathfrak{h}_1\mathrm{Q}_{i-1} + \mathfrak{h}_2^{i-1}\tilde{\mathrm{Q}}_i + \mathfrak{h}_2^i\overline{\mathrm{Q}}_i,$$

et alors R_i et Q_i satisfont bien l'équation (2.6). De plus, Q_i satisfait l'inégalité du lemme puisque chacun des trois termes intervenant dans sa définition la vérifient séparément.

□

Théorème 45. *On reprend les notations 36 et 38. Le terme mixte Ψ admet un télescopeur L d'ordre $r \leqslant \delta$ et tel que*

$$\deg_n\mathrm{L} \leqslant r(\deg_n\mathscr{P} + \deg_x\mathfrak{h}) + \max(\deg_x\mathscr{P} - \delta, 0).$$

Démonstration. En utilisant le lemme 44, on construit pour tout $i \in \{0,1,\ldots,\delta\}$ des polynômes $\mathrm{R}_i, \mathrm{Q}_i \in \mathbb{K}[x]$ qui satisfont l'équation (2.6). Comme $\deg_x\mathrm{R}_i < \delta$ pour tout i, il existe $r \leqslant \delta$ minimal tel que la famille $(\mathrm{R}_0, \mathrm{R}_1, \ldots, \mathrm{R}_r)$ soit liée. Soient $c_0, c_1, \ldots, c_{r-1} \in \mathbb{K}(n)$ tels que

$$\sum_{i=0}^{r-1} c_i\mathrm{R}_i + \mathrm{R}_r = 0.$$

Algorithme TCMixte($\mathscr{P}, \mathfrak{h}, \mathfrak{v}/\mathfrak{w}$)

Entrée Un polynôme $\mathscr{P} \in \mathbf{k}(n)[x]$, deux fractions rationnelles $\mathfrak{h}$ et $\mathfrak{v}/\mathfrak{w} \in \mathbf{k}(x)$.

Sortie Un r-uplet $(c_0, \dots, c_{r-1})$ tel que $\mathscr{P}(n+r,x)\mathfrak{h}^r - \sum_{i=0}^{r-1} c_i \mathscr{P}(n+i,x)\mathfrak{h}^i = n\mathrm{Q}\mathfrak{h}'/\mathfrak{h} + \mathrm{Q}\mathfrak{v}/\mathfrak{w} + \mathrm{Q}'$ pour un certain $\mathrm{Q} \in \mathbf{k}(n,x)$.

$\mathrm{F} \leftarrow n\mathfrak{h}'/\mathfrak{h} + \mathfrak{v}/\mathfrak{w}$;
$\mathrm{R}_0 \leftarrow$ Confinement($\mathscr{P}$, F) ;
pour $k \leftarrow 0, \dots$ **faire**
  si $\mathrm{rang}_{\mathbf{k}(n)}(\mathrm{R}_0, \mathrm{R}_1, \dots, \mathrm{R}_k) < k+1$ **alors**
    Résoudre $\sum_{i=0}^{k-1} c_i \mathrm{R}_i = \mathrm{R}_k$ en $c_0, \dots, c_{k-1} \in \mathbf{k}(n)$;
    renvoyer $(c_0, \dots, c_{k-1})$.
  $\mathrm{P} \leftarrow \mathrm{R}_k|_{n \mapsto n+1}$;
  $\mathrm{P} \leftarrow$ Réduction(P, $\mathfrak{h}, \mathfrak{v}/\mathfrak{w}$) ;
  $\mathrm{R}_{k+1} \leftarrow$ Confinement(P, F) ;

Algorithme 5: Télescopage créatif mixte

Alors on a l'égalité

$$\sum_{i=0}^{r-1} c_i(n)\Psi(n+i,x) + \Psi(n+r,x) = \left(\mathrm{Q}b\frac{\Phi}{\mathfrak{h}_2^r}\right)', \tag{2.7}$$

où $\mathrm{Q} = \sum_{i=0}^{r-1} c_i \mathfrak{h}_2^{r-i}\mathrm{Q}_i + \mathrm{Q}_r$. On a donc le résultat sur l'existence et l'ordre du télescopeur, reste à estimer le degré des coefficients c_i. Pour ce faire on constate que, si l'on pose $\mathrm{Q} = \sum_{i=0}^{d_\mathrm{Q}} q_i x^i$, l'équation (2.7) peut être vue comme un système linéaire en les inconnues $c_0, c_1, \dots, c_{r-1}, q_0, q_1, \dots, q_{d_\mathrm{Q}}$. Dans ce système, les coefficients de $c_0, c_1, \dots, c_{r-1}$ sont de degré borné par $\deg_n \mathscr{P}$, et ceux de $q_0, q_1, \dots, q_s$ sont de degré au plus 1. L'inégalité de Hadamard (voir lemme 116 de l'annexe A) donne donc

$$\deg_n c_i \leqslant r \deg_n \mathscr{P} + d_\mathrm{Q} + 1$$

pour tout i. De plus, par le lemme 44 et la définition de Q dans l'équation (2.7), on peut choisir

$$d_\mathrm{Q} < r \deg_x \mathfrak{h} + \max(\deg_x \mathscr{P} - \delta, 0).$$

En combinant ces deux dernières inégalités, on obtient la borne annoncée sur $\deg_n \mathrm{L}$.

□

Le théorème précédent est implémenté par l'algorithme TCMixte (algorithme 5).

Théorème 46. *On reprend les notations 36. Supposons de plus que Φ'/Φ n'a pas de résidu entier positif. Alors l'algorithme* TCMixte(P,$\mathfrak{h}$,$\mathfrak{v}/\mathfrak{w}$) *calcule un télescopeur d'ordre minimal de Ψ.*

Démonstration. C'est une conséquence du corollaire 17 car la réduction est à la fois confinée (lemme 37) et normale (proposition 39).

□

2.4 Exemples

2.4.1 Inverse compositionnel d'une fraction rationnelle

Définition 47. Soit $f \in \mathbb{Q}(x)$ une fraction rationnelle régulière en 0 et telle que $f(0) = 0$ et $f'(0) \neq 0$. On définit l'*inverse compositionnel* de f, noté $f^{(-1)}$ comme étant l'unique élément de $\mathbb{Q}[[x]]$ vérifiant :

$$f \circ f^{(-1)} = f^{(-1)} \circ f = x.$$

Comme application des résultats de ce chapitre, je vais donner une généralisation d'un lemme de Manivel qui est utilisé dans un article de Furter[2]. Le résultat que je vais énoncer permet de calculer une récurrence satisfaite par les coefficients de l'inverse compositionnel d'une fraction rationnelle. Le lien entre cette question et les calculs d'intégrales de termes mixtes est établi par le lemme suivant, qui n'est autre qu'un cas particulier de la formule d'inversion de Lagrange.

Lemme 48. *Soit $f \in \mathbb{Q}(x)$ une fraction rationnelle régulière en 0 et telle que $f(0) = 0$. Écrivons son inverse compositionnel sous la forme*

$$f^{(-1)}(x) = \sum_{n \geqslant 1} u_n x^n.$$

Alors les coefficients u_n sont donnés sous forme intégrale par

$$u_n = \frac{1}{2\pi i n} \oint \frac{\mathrm{d}x}{f(x)^n}.$$

Démonstration. Par la formule de Cauchy,

$$u_n = \frac{1}{2\pi i} \oint f^{(-1)}(x) \frac{\mathrm{d}x}{x^{n+1}},$$

où le contour est un petit cercle autour de 0. En intégrant par parties, on obtient

$$u_n = \frac{1}{2\pi i n} \oint \frac{f^{(-1)'}(x)\mathrm{d}x}{x^n}.$$

Puis on fait le changement de variable $x = f(u)$. On a alors $\mathrm{d}u = f^{(-1)'}(x)\mathrm{d}x$, et donc

$$u_n = \frac{1}{2\pi i n} \oint \frac{\mathrm{d}u}{f(u)^n}.$$

□

2. FURTER, "Polynomial composition rigidity and plane polynomial automorphisms".

La représentation intégrale du lemme précédent rentre dans le cadre d'application de l'algorithme TCMixte. Ceci permet donc de calculer une récurrence pour les coefficients de l'inverse compositionnel. L'analyse de l'algorithme menée dans ce chapitre s'applique pour donner le théorème suivant.

Théorème 49. *Soit $f \in \mathbb{Q}(x)$ une fraction rationnelle régulière en 0 et telle que $f(0) = 0$ et $f'(0) \neq 0$. On écrit $f = p/q$, et la décomposition sans carré $p = p_1 p_2 \cdots p_m^m$. Notons également d_p, $d_p^\star$, d_q et $d_q^\star$ les degrés respectifs de p, $p^\star$, q et $q^\star$.*

Alors les coefficients de Taylor de $f^{(-1)}$ satisfont une récurrence d'ordre au plus

$$d_q^\star + d_p^\star - 1$$

et de degré rationnel en n au plus

$$\frac{(d_q^\star + d_p^\star)(d_q^\star + d_p^\star + 1)}{2}\left(\max(d_q - d_p, 0) + \sum_{p_k \neq 1} k\right) \cdot \left[\frac{1}{1}\right].$$

k	ordre	degré	coeffs	temps
5	10	61	1759	2.49
6	12	88	2440	4.64
7	14	120	3778	13.36
8	16	157	4666	33.89
9	18	199	6192	88.34
10	20	246	8364	260.59
11	22	298	10146	628.21
12	24	355	11802	1451.54

TABLE 2.1 – Ordre, degré, taille bit et temps pour l'exemple 50

Exemple 50. Dans la table 2.1 sont présentés des résultats expérimentaux pour une famille de fractions rationnelles

$$f_k(x) = x\frac{p_k(x)^2}{q_k(x)},$$

où p_k et q_k sont des polynômes denses de degré k à coefficients entiers bornés par 100 en valeur absolue. La première colonne donne l'indice k. La deuxième donne l'ordre du télescopeur d'ordre minimal, qui se comporte comme prédit dans le théorème 49. La troisième donne le degré du télescopeur ; elle met en évidence une croissance quadratique, comme prédit par le théorème 49. La quatrième colonne donne la taille en bits du plus grand coefficient du télescopeur ; sa croissance semble légèrement plus que quadratique. Enfin, la dernière colonne donne le temps (en secondes) pris par l'implémentation de l'algorithme TCMixte pour calculer le télescopeur.

2.5 Analyse de complexité de TCMixte

Cette section dédiée à l'analyse de la complexité de l'algorithme TCMixte est constituée de résultats particulièrement techniques. Cependant, le fil du raisonnement est très simple : on souhaite majorer le degré des entrées du système linéaire à résoudre. La majoration est obtenue en suivant les degrés des polynômes dans chacun des algorithmes intermédiaires, ce qui est un peu fastidieux, mais ne fait intervenir que des arguments élémentaires.

2.5.1 Confinement

Lemme 51. *On reprend les notations 36. Soit* $\mathrm{P} \in \mathbf{k}(n)[x]$ *un polynôme. Notons* $\mathrm{R} \in \mathbb{K}[x]$ *le polynôme renvoyé par l'algorithme* Confinement(P,A/b). *Alors, si* $\deg_x b \leqslant \deg_x \mathrm{A}+1$,

$$\mathrm{Rdeg}_n \mathrm{R} - \mathrm{Rdeg}_n \mathrm{P} \leqslant (\deg_x \mathrm{P} - \deg_x \mathrm{A} + 1) \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

et si $\deg_x b > \deg_x \mathrm{A}+1$,

$$\mathrm{Rdeg}_n \mathrm{R} - \mathrm{Rdeg}_n \mathrm{P} \leqslant \begin{bmatrix} \left\lfloor \frac{\deg_x \mathrm{P} - \deg_x \mathrm{B} + 1}{\deg_x \mathrm{B} - \deg_x \mathrm{A} - 1} \right\rfloor + 1 \\ 0 \end{bmatrix}.$$

Démonstration. On étudie séparément les deux cas en reprenant les notations de l'algorithme.

Si $\deg_x b \leqslant \deg_x \mathrm{A}+1$, la récurrence pour les q_i contient un terme $a_{\delta-1} q_{i+1}$, sauf lorsque $i = d$. Par ailleurs, c contient un terme a_δ. Ainsi, par une récurrence immédiate, le degré en n des numérateur et dénominateur de q_{d-i} augmentent de 1 à chaque étape. Comme il y a au total $d+1$ étapes, on en déduit que

$$\mathrm{Rdeg}_n \mathrm{Q} - \mathrm{Rdeg}_n \mathrm{P} \leqslant \begin{bmatrix} d \\ d+1 \end{bmatrix}.$$

En utilisant l'équation (2.3), le résultat sur R s'ensuit.

Si au contraire $\deg_x b > \deg_x \mathrm{A}+1$, les coefficients $a_{\delta-j}$ sont nuls pour $j < \delta - \deg_x \mathrm{A}$, et c ne dépend pas de n. Par récurrence sur i, le degré de q_{d-i} augmente de 1 chaque fois que $i \equiv 0 \mod \delta - \deg_x \mathrm{A}$ et reste constant sinon. Plus explicitement,

$$\mathrm{Rdeg}_n q_{d-i} - \mathrm{Rdeg}_n \mathrm{P} \leqslant \begin{bmatrix} \lfloor i/(\delta - \deg_x \mathrm{A}) \rfloor \\ 0 \end{bmatrix}.$$

À nouveau on en déduit le résultat pour R grâce à l'équation (2.3). □

Lemme 52. *On reprend les notations 36 et 38. Soit* $\mathrm{P} \in \mathbb{K}[x]$ *un polynôme. L'appel* Confinement(P,A/b) *effectue au plus*

$$\tilde{\mathrm{O}}(\delta \deg_x \mathrm{P})$$

opérations dans $\mathbb{K}$.

Démonstration. Chaque itération de la boucle nécessite $O(\delta)$ opérations dans $\mathbb{K}$, et la boucle est exécutée $\deg_x P - \delta + 1$ fois, ce qui fait au total $O(\delta \deg_x P)$ opérations. De là, les dernières multiplications et additions donnent R en $\tilde{O}(\deg_x P)$ opérations dans $\mathbb{K}$, ce qui permet de conclure. □

2.5.2 Réduction

Lemme 53. *On reprend les notations 36. Soit f un facteur irréductible du dénominateur de $\mathfrak{h}$, ν la valuation f-adique de b, et soit $P \in \mathbf{k}(n)[x]$ un polynôme. On se donne également un entier k et on note $\tilde{A} = A - kbf'/f$. Par le lemme 40, f est inversible modulo $\tilde{A} + b'$. Soit alors Q l'unique polynôme tel que $\deg_x Q < \deg_x f$ et*

$$P \equiv Q(\tilde{A} + b') \mod f$$

(Q est bien défini par le lemme 40).

Alors $\mathrm{Rdeg}_n Q - \mathrm{Rdeg}_n P$ *est majoré par*

$$\begin{cases} \left[\frac{0}{0}\right], & \text{si } \nu > 1; \\ \left[\frac{0}{1}\right], & \text{si } \nu = 1 \text{ et } f \not| \mathfrak{w}; \\ \left[\frac{\deg_x f - 1}{\deg_x f}\right], & \text{si } \nu = 1 \text{ et } f \mid \mathfrak{w}. \end{cases}$$

Démonstration. Ici, lorsque u est une classe modulo f, on notera u^{-1} l'inverse de u modulo f (avec $\deg u^{-1} < \deg f$). Remarquons tout d'abord que

$$\mathrm{Rdeg}_n Q - \mathrm{Rdeg}_n P = \mathrm{Rdeg}_n (\tilde{A} + b')^{-1}.$$

En effet, écrivons

$$p(n)P = P_0(x) + P_1(x)n + \cdots + P_d(x)n^d,$$

où $p(n)$ est le dénominateur de P. On voit que

$$p(n)Q = (\tilde{A} + b')^{-1}(P_0 \bmod f) + \cdots + (\tilde{A} + b')^{-1} n^d (P_d \bmod f)$$

a un degré rationnel borné par

$$\left[\frac{d}{0}\right] + \mathrm{Rdeg}_n (\tilde{A} + b')^{-1}.$$

Il suffit donc de borner $\mathrm{Rdeg}_n (\tilde{A} + b')^{-1}$. Pour ce faire, on observe de plus près l'équation (2.5).

Si $\nu > 1$, l'équation devient

$$\tilde{A} + b' \equiv \mathfrak{v} \frac{\tilde{b}}{\mathfrak{w}/f^\nu} \mod f,$$

et donc $(\tilde{A} + b')^{-1}$ ne dépend pas de n dans ce cas.

Si $\nu = 1$ et $f \not| \mathfrak{w}$, l'équation devient

$$\tilde{A} + b' \equiv (nk + 1) f' \tilde{b},$$

si bien que

$$(\tilde{A}+b')^{-1} \equiv \frac{(f'\tilde{b})^{-1}}{nk+\nu}.$$

Donc, dans ce cas,

$$\mathrm{Rdeg}_n(\tilde{A}+b')^{-1} = \left[\frac{0}{1}\right].$$

Enfin, si $\nu = 1$ et $f \mid \mathfrak{w}$, le résultat découle du lemme ci-dessous. □

Lemme 54. *Soient $p, q, r \in \mathbf{k}[x]$ des polynômes tels que r est premier avec au moins l'un de p et q. Soient $U, V \in \mathbf{k}(n)[x]$ tels que*

$$1 = U(pn+q) + Vr, \text{ avec } \deg_x U < \deg r. \tag{2.8}$$

Alors

$$\mathrm{Rdeg}_n U \leqslant \left[\frac{\deg_x r - 1}{\deg_x r}\right].$$

Démonstration. Notons $R(n) \neq 0$ le résultant en x de r et $pn+q$. Alors il existe $S, T \in \mathbf{k}[n,x]$ tels que $R = S(pn+q) + Tr$, avec également $\deg_x S < \deg_x r$. De plus, par la règle de Cramer appliquée à la matrice de Sylvester de r et $pn+q$, on a $\deg_n R \leqslant \deg_x r$ et $\deg_n S < \deg_x r$.

Maintenant, notons respectivement $\tilde{U}(n,x)$ et $d(n)$ le numérateur et le dénominateur de U. On aimerait montrer que $\deg_n d \leqslant \deg_x r$ et $\deg_n \tilde{U} < \deg_x r$. Les égalités

$$1 = U(pn+q) + Vr, \quad 1 = S/R(pn+q) + (T/R)r$$

impliquent par soustraction que r divise $(U - S/R)(pn+q)$. Comme r est premier avec $pn+q$, ceci implique que r divise $U - S/R$. Comme $\deg_x r > \deg_x(U - S/R)$, on en déduit que $U = S/R$. En particulier, d divise R. Il s'ensuit que $\deg_n d \leqslant \deg_n R \leqslant \deg_x r$ et $\deg_n \tilde{U} = \deg_n(dS/R) \leqslant \deg_n S < \deg_x r$, et la preuve est terminée. □

Lemme 55. *On reprend les notations du lemme 53, et on suppose que f divise le dénominateur de $\mathfrak{h}$ avec multiplicité k. Soit $R \in \mathbb{K}[x]$ le polynôme renvoyé par* RéducÉlém$(P, A/b, f, k)$. *Alors* $\mathrm{Rdeg}_n R - \mathrm{Rdeg}_n P$ *est majoré par*

$$\begin{cases} k\left[\frac{1}{0}\right], & \text{si } \nu > 1 ; \\ k\left[\frac{1}{1}\right], & \text{si } \nu = 1 \text{ et } f \not| \mathfrak{w} ; \\ k\deg_x(f)\left[\frac{1}{1}\right], & \text{si } \nu = 1 \text{ et } f \mid \mathfrak{w}. \end{cases}$$

Démonstration. À chaque étape de la boucle, le polynôme Q calculé par pgcd étendu a un degré rationnel dont une majoration est donnée par le lemme 53. Comme $\mathrm{Rdeg}_n C = \left[\frac{1}{0}\right]$ et il y a k étapes, le résultat s'ensuit. □

Lemme 56. *On reprend les notations 36. Soient $\mathfrak{h} = \mathfrak{h}_1/\mathfrak{h}_2$ la forme réduite de $\mathfrak{h}$. On décompose le dénominateur $\mathfrak{h}_2$ de la façon suivante :*

$$\mathfrak{h}_2 = fgh,$$

avec

$$f = \operatorname{pgcd}(\mathfrak{h}_2, \mathfrak{w}, \mathfrak{w}'), \quad g = \operatorname{pgcd}(\mathfrak{h}_2 / f, \mathfrak{w}).$$

Notons également m la plus grande multiplicité des racines de $\mathfrak{h}_2$, et soient $f = f_1 f_2^2 \cdots f_m^m$ et $h = h_1 h_2^2 \cdots h_m^m$ les décompositions sans carré de f et h respectivement.

Alors le polynôme $\mathrm{R} \in \mathbb{K}[x]$ renvoyé par Réduction$(\mathrm{P}, \mathfrak{h}, \mathfrak{v}/\mathfrak{w})$ *vérifie :*

$$\operatorname{Rdeg}_n \mathrm{R} \leqslant \operatorname{Rdeg}_n \mathrm{P} + \left\lceil \frac{\max_{f_k \neq 1} k + \sum_{h_k \neq 1} k + \deg_x g}{\sum_{h_k \neq 1} k + \deg_x g} \right\rceil.$$

Démonstration. Soit $g = g_1 g_2^2 \cdots g_m^m$ la décomposition sans carré de g. Par le lemme 55, on a

$$\operatorname{Rdeg}_n r_k \leqslant \operatorname{Rdeg}_n \mathrm{P} + \left\lceil \frac{k(\mathbf{1}_{f_k \neq 1} + \mathbf{1}_{h_k \neq 1} + \deg_x g_k)}{k(\mathbf{1}_{h_k \neq 1} + \deg_x g_k)} \right\rceil.$$

Il suffit alors de réduire $\mathrm{P}u + r_1 + r_2 + \cdots + r_m$ au même dénominateur et on obtient la borne annoncée. □

Lemme 57. *On reprend les notations 36 et 38. Soit $\mathrm{P} \in \mathbb{K}[x]$ un polynôme, f un facteur sans carré du dénominateur de $\mathfrak{h}$, et k un entier strictement positif.*

L'appel RéducÉlém$(\mathrm{P}, \mathrm{A}/b, f, k)$ *effectue au plus*

$$\tilde{\mathrm{O}}(k(\deg_x \mathrm{P} + \delta))$$

opérations dans $\mathbb{K}$.

Démonstration. Les étapes coûteuses sont les calculs de pgcd. Or, d'après la proposition 131, ceux-ci peuvent être calculés en $\tilde{\mathrm{O}}(\deg_x \mathrm{P} + \delta)$ opérations dans $\mathbb{K}$. Le résultat découle alors du fait qu'il y a k calculs de pgcd. □

Lemme 58. *On reprend les notations 36 et 38. $\mathfrak{h} = \mathfrak{h}_1/\mathfrak{h}_2$ la forme réduite de $\mathfrak{h}$, et $\mathfrak{h}_2 = f_1 f_2^2 \cdots f_m^m$ la décomposition sans carré de $\mathfrak{h}_2$. On note également*

$$\epsilon = \sum_{f_k \neq 1} k.$$

Alors l'appel Réduction$(\mathrm{P}, \mathfrak{h}, \mathfrak{v}/\mathfrak{w})$ *effectue au plus*

$$\tilde{\mathrm{O}}(\max(\epsilon \deg_x \mathrm{P}, d_{\mathfrak{h}}) + \deg_x \mathfrak{h}_2 + \epsilon\delta)$$

opérations dans $\mathbb{K}$.

Démonstration. Par la proposition 131, la décomposition sans carré de $\mathfrak{h}_2$ se calcule en $\tilde{\mathrm{O}}(\deg_x \mathfrak{h}_2)$ opérations, et le produit $\mathrm{P}u$ en $\tilde{\mathrm{O}}(\max(\deg_x \mathrm{P}, \deg_x^\infty \mathfrak{h}))$ opérations. De plus, on a vu dans le lemme 57 que le k-ième appel à RéducÉlém effectue $\tilde{\mathrm{O}}(k(\deg_x \mathrm{P} + \deg_x f_k + \delta))$ opérations dans $\mathbb{K}$. Il suffit alors de sommer ces complexités pour obtenir le résultat annoncé. □

2.5.3 TCMixte

Lemme 59. *On reprend les notations 36, 38, ainsi que celles de l'algorithme* TCMixte. *On note également* $d_{\mathfrak{h}} = \deg_x^{\infty} \mathfrak{h}$.

Pour tout $i \in \{1, 2, \dots, \delta\}$, *on a :*

$$\operatorname{Rdeg}_n \mathrm{R}_i \leqslant \deg_n \mathscr{P} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha + i(\beta + \gamma),$$

où

$$\alpha = \begin{cases} \max(\deg_x \mathscr{P} - \delta + 1, 0) \cdot \frac{[1]}{[1]} & \text{si } \delta = \deg_x \mathrm{A}, \\ \begin{bmatrix} \max\left(\left\lfloor \frac{\deg_x \mathscr{P} - \delta}{\delta - \deg_x \mathrm{A}} \right\rfloor + 1, 0\right) \\ 0 \end{bmatrix} & \text{sinon.} \end{cases}$$

$$\beta = \left\lceil \frac{\max_{e_k \neq 1} k + \sum_{h_k \neq 1} k + \deg_x f}{\sum_{h_k \neq 1} k + \deg_x f} \right\rceil$$

$$\gamma = \begin{cases} (d_{\mathfrak{h}} + 1) \cdot \frac{[1]}{[1]} & \text{si } d_{\mathfrak{h}} \geqslant 0 \text{ et } \delta = \deg_x \mathrm{A}, \\ \begin{bmatrix} \left\lfloor \frac{d_{\mathfrak{h}}}{\delta - \deg_x \mathrm{A}} \right\rfloor + 1 \\ 0 \end{bmatrix} & \text{si } d_{\mathfrak{h}} \geqslant 0 \text{ et } \delta = \deg_x b - 1, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. Par le lemme 51, le polynôme R_0 produit par le confinement initial vérifie

$$\operatorname{Rdeg}_n \mathrm{R}_0 \leqslant \operatorname{Rdeg}_n \mathscr{P} + \alpha.$$

Ensuite, l'algorithme Réduction est toujours utilisé avec un polynôme de degré strictement inférieur à δ comme argument. Par le lemme 56, on en déduit que chaque réduction produit un polynôme qui a un degré rationnel en n augmenté de β et un degré en x au plus δ si $d_{\mathfrak{h}} < 0$ et $\delta + d_{\mathfrak{h}}$ si $d_{\mathfrak{h}} \geqslant 0$. Dans ce dernier cas, le lemme 51 montre que le confinement augmente le degré rationnel en n de γ. Au total, on obtient le majorant annoncé. □

Théorème 60. *On reprend les notations 36 et 38. Notons également* $d_{\mathfrak{h}} = \deg_x^{\infty} \mathfrak{h}$ *et*

$$\begin{bmatrix} k \\ l \end{bmatrix} = \deg_n \mathscr{P} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha + \delta(\beta + \gamma), \quad \mu = \max(k, l).$$

Alors le nombre total d'opérations dans $\mathbf{k}$ *effectuées par l'appel* TCMixte$(\mathscr{P}, \mathfrak{h}, \mathfrak{v}/\mathfrak{w})$ *est*

$$\tilde{\mathrm{O}}(\mu(\epsilon\delta \deg_x \mathrm{P} + \delta \deg_x \mathfrak{h}_2 + \epsilon\delta^2 + \delta^{\omega})),$$

si $d_{\mathfrak{h}} < 0$, *ou*

$$\tilde{\mathrm{O}}(\mu(\epsilon\delta \deg_x \mathrm{P} + \delta \deg_x \mathfrak{h}_2 + \epsilon\delta^2 + \delta^3 + \delta^2 d_{\mathfrak{h}}))$$

si $d_{\mathfrak{h}} \geqslant 0$.

Démonstration. Les lemmes 51, 55, 56 et 59 montrent que tous les éléments de $\mathbf{k}(n)$ intervenant dans l'algorithme TCMixte ont un numérateur et un dénominateur de degré en n borné par μ. De là, la complexité de la construction du système linéaire à résoudre découle des lemmes 52 et 58. Enfin, par la proposition 136, la résolution du système linéaire nécessite $\tilde{\mathrm{O}}(\delta^{\omega}\mu)$ opérations dans $\mathbf{k}$. □

2.6 Implémentation

Une implémentation des algorithmes décrits dans ce chapitre est disponible en ligne[3]. Elle utilise le logiciel de calcul formel Maple, et est accompagnée d'une feuille de calcul montrant quelques exemples de calculs de télescopeurs. Parmi ceux-ci, l'exemple suivant illustre bien l'efficacité de la méthode.

Exemple 61. On considère le terme mixte

$$\left(1+\frac{x}{n^2+1}\right)\left(\frac{(x+1)^2}{(x-4)(x-3)^2(x^2-5)^3}\right)^n \sqrt{x^2-5}\, e^{\frac{x^3+1}{x(x-3)(x-4)^2}}.$$

Il rassemble plusieurs difficultés pour l'algorithme du point de vue de la complexité. En effet, les divers polynômes intervenant dans ce terme ont des pgcd non-triviaux. Pour cet exemple, l'algorithme TCMixte calcule un télescopeur d'ordre 9 et de degré 90 en 1,4 seconde. En comparaison, le seul autre code permettant d'effectuer ce calcul est le package `HolonomicFunctions`[4], qui calcul le télescopeur minimal pour une classe de fonctions bien plus générale et prend 3 minutes sur cet exemple. Ceci montre en particulier qu'il est avantageux de mettre au point des algorithmes spécifiques pour des classes de fonctions restreintes afin d'utiliser au maximum la structure à notre disposition pour accélérer les calculs.

Par ailleurs, on a déjà vu des temps d'exécution sur des exemples où le terme mixte n'a pas de partie exponentielle dans la table 2.1. Voici des temps d'exécution pour un exemple avec une partie exponentielle.

k	ordre	degré	coeffs	temps
5	9	26	709	0.63
6	11	40	1165	1.26
7	13	57	1801	2.74
8	15	77	2555	7.17
9	17	100	3378	20.20
10	19	126	4246	47.876
11	21	155	4928	113.96
12	23	187	6358	295.34

TABLE 2.2 – Ordre, degré, taille bit et temps pour l'exemple 62

Exemple 62. On présente dans la table 2.2 des résultats expérimentaux pour une famille de termes mixtes de la forme

$$\Phi_k(x) = \frac{1}{p_k(x)^n} \exp\left(\int \frac{1}{q_k(x)}\right),$$

3. http://mixedct.gforge.inria.fr
4. KOUTSCHAN, "Holonomic Functions in Mathematica".

où p_k et q_k sont des polynômes denses de degré k à coefficients entiers bornés par 100 en valeur absolue. À nouveau, la première colonne donne l'indice k. La deuxième donne l'ordre du télescopeur d'ordre minimal, dont on constate qu'il vaut $2k-1$, la valeur prédite par le théorème 45. La troisième colonne donne le degré du télescopeur qui coïncide avec $(3k-2)(k-1)/2$. Le théorème 45 est donc un peu pessimiste dans ce cas mais prédit bien un ordre de grandeur quadratique. La quatrième colonne donne la taille en bits du plus grand coefficient du télescopeur, qui croît de façon à peu près cubique. Enfin, la dernière colonne donne le temps de calcul en secondes. La croissance semble être plus rapide que ce que prédit la théorie, et potentiellement non-polynomiale. Ceci suggère que l'implémentation est encore imparfaite. Les causes peuvent en être diverses et n'ont pour le moment pas encore été étudiées.

Chapitre 3

Intégrales de fractions rationnelles bivariées

Nous avons vu que si $F \in \mathbf{k}(x,y)$ est une fraction rationnelle, alors $[y^{-1}]F(x,y)$ est une série algébrique (corollaire 9). Le but de ce chapitre est de rendre ce résultat effectif, c'est-à-dire de donner un algorithme qui calcule un polynôme annulateur pour cette série. La stratégie que nous allons adopter s'appuie sur la formule donnée par la proposition 8 :

$$[y^{-1}]F(x,y) = \sum_{i=1}^{s} \mathrm{Res}(F, y_i) \tag{3.1}$$

où $y_1, y_2, \ldots, y_s$ sont les petits pôles (voir la définition 6) de la fraction F. On divise alors le travail en deux étapes : on commence par calculer un polynôme qui annule chacun des résidus $\mathrm{Res}(F, y_i)$ dans la section 3.1, puis on en déduit un polynôme qui annule la somme des résidus dans la section 3.2. Ces algorithmes intermédiaires sont essentiellement appliqués à des fractions rationnelles univariées, on travaillera donc dans un corps $\mathbb{K}$ qui sera spécialisé plus tard à $\mathbb{K} = \mathbf{k}(x)$.

3.1 Polynôme annulant les résidus d'une fraction rationnelle

Dans cette section on souhaite, étant donnée une fraction rationnelle, calculer un polynôme qui annule une partie de ses résidus. Dans le cas des résidus aux pôles simples, c'est un résultat classique en intégration symbolique que l'on peut calculer un tel polynôme à l'aide d'un résultant introduit par Rothstein [1] et Trager [2]. Bronstein [3] a ensuite donné des formules similaires pour le cas de pôles multiples. Malheureusement, les résultants de Bronstein ne sont pas adaptés au calcul

1. ROTHSTEIN, "Aspects of symbolic integration and simplification of exponential and primitive functions".
2. TRAGER, "Algebraic Factoring and Rational Function Integration".
3. BRONSTEIN, "Formulas for series computations".

car la complexité de leur évaluation croît exponentiellement avec la multiplicité des pôles. Voici une méthode pour obtenir le résultat avec une complexité polynomiale.

On se donne deux polynômes $p, q \in \mathbb{K}[y]$ premiers entre eux, et on note $f = p/q$. Fixons un diviseur $\hat{q}$ de q tel que $\hat{q}$ et $q/\hat{q}$ soient premiers entre eux. En pratique, cela signifie que l'on sépare les racines de q en deux groupes : les racines de $\hat{q}$ dont on veut un polynôme annulateur pour les résidus, et les racines de $q/\hat{q}$ qui ne nous intéressent pas. On cherche donc à calculer un polynôme $\rho \in \mathbb{K}[z]$ dont les racines incluent tous les résidus de f aux racines de $\hat{q}$. Notons $q = q_1 q_2^2 \cdots q_m^m$ la décomposition sans carré de q. Définissons également pour tout $i \in \{1, 2, \ldots, m\}$

$$\mathrm{V}_i(y,t) = \frac{q_i(y+t) - q_i(y)}{t}, \quad \mathrm{F}_i(y,t) = \frac{f(y+t)q_i^i(y+t)}{\mathrm{V}_i^i(y,t)}.$$

Notre nouvel algorithme (PolynômeRésidus, page 65) est fondé sur la proposition suivante, qui permet de ramener le calcul de résidu d'une fraction singulière à un calcul de coefficient dans le développement d'une fraction régulière :

Proposition 63. *Soit $i \in \{1, 2, \ldots, m\}$ et α une racine de q_i dans $\overline{\mathbb{K}}$. Alors*

1. *$\mathrm{F}_i(\alpha, t)$ est régulière en $t = 0$;*
2. *$\mathrm{Res}(f, \alpha) = [t^{i-1}]\mathrm{F}_i(y,t)_{|y=\alpha}$.*

Démonstration. *(1)* Comme les q_i sont premiers entre eux deux à deux, il est immédiat que la fraction $f(\alpha+t)q_i^i(\alpha+t)$ est régulière en 0. Il suffit donc de vérifier que $\mathrm{V}_i(\alpha, 0) \neq 0$. Mais le développement de Taylor $\mathrm{V}_i(\alpha, t) = q_i'(\alpha) + \mathrm{O}(t)$ montre que $\mathrm{V}_i(\alpha, 0) = q_i'(\alpha) \neq 0$ puisque q_i est un polynôme sans carré.

(2) Il suffit de remarquer que $\mathrm{F}_i(\alpha, t) = f(\alpha+t) \cdot t^i$, d'où l'on déduit :

$$\mathrm{Res}(f, \alpha) = [t^{-1}] f(\alpha+t) = [t^{i-1}]\mathrm{F}_i(\alpha, t).$$

□

Corollaire 64. *Soit $i \in \{1, 2, \ldots, m\}$ et $a_i, b_i \in \mathbb{K}[y]$ des polynômes tels que*

$$[t^{i-1}]\mathrm{F}_i(y,t) = \frac{a_i}{b_i}.$$

Alors tous les résidus de f aux racines de q_i sont annulés par le polynôme

$$\rho_i(z) = \mathrm{Résultant}_y(a_i - z b_i, q_i).$$

Démonstration. Soit α une racine de q_i dans $\overline{\mathbb{K}}$. On a vu dans la proposition précédente que $\mathrm{Res}(f, \alpha) = a_i(\alpha)/b_i(\alpha)$. Or ces nombres sont exactement les racines de ρ_i. En effet, cela se voit sur la formule explicite pour le résultant rappelée dans la proposition 128 :

$$\rho_i(z) = c \prod_{q_i(\alpha)=0} (a_i(\alpha) - z b_i(\alpha)),$$

où c une constante par rapport à z (et y) qu'il est inutile d'expliciter. □

Algorithme **PolynômeRésidus**$(p/q, \hat{q})$

Entrée trois polynômes $p, q, \hat{q} \in \mathbb{K}[y]$ tels que $\hat{q} \mid q$ et $\operatorname{pgcd}(\hat{q}, q/\hat{q}) = 1$

Sortie un polynôme en z qui annule les résidus de p/q en toutes les racines de $\hat{q}$

Calculer la décomposition sans carré $\hat{q} = q_1 q_2^2 \cdots q_m^m$;
pour $i \leftarrow 1$ à m **faire**
  si $\deg_y q_i = 0$ **alors** $\rho_i \leftarrow 1$
  sinon
    $u_i(y) \leftarrow q(y)/q_i^i(y)$;
    $V_i(y,t) \leftarrow (q_i(y+t) - q_i(y))/t$;
    Développer $\frac{p(y+t)}{u_i(y+t)V_i^i(y,t)} = s_0 + s_1 t \cdots + s_{i-1} t^{i-1} + O(t^i)$;
    Écrire $s_{i-1}(y) = a_i(y)/b_i(y)$ avec a_i et b_i premiers entre eux ;
    $\rho_i(z) \leftarrow \text{Résultant}_y(a_i - z b_i, q_i)$;
renvoyer $\rho_1 \rho_2 \cdots \rho_m$

Algorithme 6: Polynôme annulant une partie des résidus d'une fraction rationnelle

Pour $i = 1$, on calcule un polynôme $\rho_1(z)$ dont les racines sont les résidus aux pôles simples de f. La formule de la proposition 63 donne alors pour tout pôle simple α de f :

$$\operatorname{Res}(f, \alpha) = F_1(\alpha, 0) = \frac{p(\alpha)}{q_1'(\alpha) q_2(\alpha)^2 \cdots q_m(\alpha)^m} = \frac{p(\alpha)}{q'(\alpha)}.$$

On retrouve donc la formule classique pour les résidus aux pôles simples, et le résultant correspondant n'est autre que le résultant de Rothstein et Trager.

Le correction de l'algorithme PolynômeRésidus découle du corollaire 64.

Exemple 65. Soit d un entier positif, et soit $G_d \in \mathbb{Q}[x](y)$ la fraction rationnelle définie par

$$G_d(x, y) = \frac{y^d}{(y - y^2 - x)^{d+1}}.$$

Ses pôles sont d'ordre $d+1$. Sur cet exemple, l'algorithme peut-être effectué à la main pour d quelconque. En reprenant les notations de l'algorithme, on a la décomposition sans carré avec $m = d+1$ et $Q_m = y - y^2 - x$, les autres Q_i valant 1. De là, on calcule $V_m = 1 - 2y - t$, et il faut donc développer

$$\frac{(y+t)^d}{(1-2y-t)^{d+1}} = \frac{(y+t)^d}{(1-2y)^{d+1}\left(1 - \frac{t}{1-2y}\right)^{d+1}}.$$

En utilisant le développement des séries binomiales, on trouve que le coefficient de t^d vaut $\frac{A_m}{B_m}$, avec

$$A_m = \sum_{k=0}^{d} \binom{d}{k}\binom{d+k}{k} y^k (1-2y)^{d-k}, \quad B_m = (1-2y)^{2d+1}.$$

Les résidus sont donc annulés par $\mathrm{R}_m = \mathrm{Résultant}_y(\mathrm{A}_m - z\mathrm{B}_m, \mathrm{Q}_m)$. Pour calculer ce résultant, remarquons que

$$\mathrm{A}_m = \sum_{k=0}^{\lfloor d/2 \rfloor} \binom{d}{2k}\binom{2k}{k}(y-y^2)^k.$$

Pour se convaincre de cela, on peut vérifier que les deux membres de cette égalité satisfont la récurrence

$$(2y-1)^2(d+1)u_d - (2d+3)u_{d+1} + (d+2)u_{d+2} = 0, \quad u_0 = u_1 = 1.$$

En particulier, on en déduit que

$$\mathrm{A}_m \bmod \mathrm{Q}_m = \sum_{k=0}^{\lfloor d/2 \rfloor} \binom{d}{2k}\binom{2k}{k}x^k.$$

Par ailleurs, on a

$$\mathrm{B}_m \bmod \mathrm{Q}_m = (1-4x)^d(1-2y).$$

On obtient donc la formule explicite

$$\mathrm{R}_m = (1-4x)^{2d+1}z^2 - \left(\sum_{k=0}^{\lfloor d/2 \rfloor} \binom{d}{2k}\binom{2k}{k}x^k\right)^2.$$

3.1.1 Bornes

Par la suite, on voudra appliquer l'algorithme 6 à un polynôme bivarié, auquel cas le résultat obtenu est également un polynôme bivarié. Afin d'analyser son bidegré, on décortique les deux étapes principales de l'algorithme : l'extraction de coefficient dans le développement en série d'une fraction rationnelle, et le calcul final de résultant. Pour cette dernière, on dispose de bornes classiques pour le degré d'un résultant rappelées dans l'annexe A. Pour ce qui est de l'extraction de coefficient, il se trouve que le développement en série d'une fraction rationnelle est très structuré : on va montrer que les degrés des coefficients croissent au plus linéairement.

Notation 66. Soit $q \in \mathbb{K}[x]$ un polynôme, et $\alpha \in \mathbb{R}$. On note $\mathscr{E}_\alpha(q)$ le sous-ensemble de $\mathbb{K}(x)[[t]]$ des séries de la forme

$$c_0 + c_1\frac{t}{q} + \cdots + c_n\frac{t^n}{q^n} + \ldots,$$

où $c_n \in \mathbb{K}[x]$ et $\deg_x c_n \leqslant n\alpha$ pour tout n (rappelons que si $\alpha < 0$ on utilise la convention $\deg_x 0 = -\infty$).

Cette notation se généralise lorsque x est un k-uplet de variables en remplaçant α par un k-uplet de réels.

On va voir que le développement en série d'une fraction rationnelle appartient toujours à $\mathscr{E}_\alpha(q)$ pour certains α et q. C'est une conséquence des propriété de clôture de $\mathscr{E}_\alpha(q)$, qui font l'objet de la proposition suivante.

Proposition 67. *Soient* $q, r \in \mathbb{K}[x]$, $\alpha, \beta \in \mathbb{R}$ *et* $f \in \mathbb{K}[[t]]$.

1. *L'ensemble* $\mathscr{E}_\alpha(q)$ *est un sous-anneau de* $\mathbb{K}(x)[[t]]$;
2. *Soit* $S \in \mathscr{E}_\alpha(q)$ *telle que* $S(0) = 0$. *Alors* $f(S) \in \mathscr{E}_\alpha(q)$;
3. *Les produits vérifient*

$$\mathscr{E}_\alpha(q) \cdot \mathscr{E}_\beta(r) \subset \mathscr{E}_{\max(\alpha+\deg_x r, \beta+\deg_x q)}(qr).$$

Démonstration. Pour *(3)*, si $f = \sum_n a_n t^n/q^n$ et $g = \sum_n b_n t^n/r^n$ appartiennent respectivement à $\mathscr{E}_\alpha(q)$ et $\mathscr{E}_\beta(r)$, alors le n-ième coefficient de leur produit est une somme de termes de la forme

$$\frac{a_i(x) q^{n-i} b_{n-i}(x) r^i}{(qr)^n}.$$

Le degré de leur numérateur est donc majoré par

$$i(\alpha + \deg_x r) + (n-i)(\beta + \deg_x q),$$

et le résultat s'ensuit.

Le *(1)* se prouve de la même façon, puisque le n-ième coefficient du produit de $f = \sum_n a_n t^n/q^n$ par $g = \sum_n b_n t^n/q^n$ est une somme de termes de la forme

$$\frac{a_i b_{n-i}}{q^n}.$$

Pour le *(2)*, la condition $S(0) = 0$ rend la série $f(S)$ bien définie. Le résultat est alors une conséquence directe du *(1)*. □

Corollaire 68. *Soit* $Q \in \mathbb{K}[x,t]$ *tel que* $Q(0,0) \neq 0$. *Soit* $Q^\star$ *une partie sans carré de* Q. *Alors*

$$\frac{1}{Q(x,t)} \in \frac{1}{Q(x,0)} \mathscr{E}_{\min(\deg_x(Q^\star), \deg t(Q^\star)-1)}(Q^\star(x,0)).$$

Démonstration. Pour tout i, le coefficient de t^i dans Q a un degré au plus

$$\min(\deg_x Q, \deg t Q - i).$$

Ainsi,

$$r := \frac{(Q(x,t) - Q(x,0))}{Q(x,0)} \in \mathscr{E}_{\min(\deg_x(Q), \deg t(Q)-1)}(Q(x,0)).$$

En écrivant $Q(x,t) = Q(x,0)(1+r)$ et en utilisant le *(2)* de la proposition 67 avec $f = 1/(1+y)$ fournit le résultat lorsque Q est sans carré. Avec $f = 1/(1+y)^i$, on obtient le résultat pour une puissance pure grâce au *(1)* de la proposition. Le cas général découle alors du *(3)* par récurrence sur le nombre de facteurs dans la décomposition sans carré de Q, et en utilisant l'additivité du degré et du degré total. □

On a maintenant les outils nécessaires pour analyser l'algorithme 3.

Théorème 69. *Soit* $\mathrm{P}(x,y)/\mathrm{Q}(x,y) \in \mathbf{k}(x,y)_{d_x,d_y}$. *Soit* $\hat{\mathrm{Q}}$ *un diviseur de* Q, $\hat{\mathrm{Q}}^\star$ *la partie sans carré de* $\hat{\mathrm{Q}}$ *par rapport à* y, *et on note* m *le nombre de facteurs dans la décomposition sans carré de* $\hat{\mathrm{Q}}$. *Soit* $(d_x^\star, d_y^\star)$ *une borne sur le bidegré de* $\mathrm{Q}^\star$. *Alors le polynôme calculé par l'appel* PolynômeRésidus$(\mathrm{P}/\mathrm{Q}, \hat{\mathrm{Q}})$ *(algorithme 6) a un degré en* z *majoré par* $\deg_y \hat{\mathrm{Q}}^\star$ *et un degré en* x *majoré par*

$$2d_x^\star(d_y+1) + 2(d_y^\star - 1)d_x - 2d_x^\star d_y^\star.$$

On remarquera que la borne sur le degré en x peut se réécrire sous la forme

$$2d_x d_y - 2(d_x - d_x^\star)(d_y - d_y^\star + 1).$$

En particulier, ce degré est borné indépendamment des multiplicités par $2d_x d_y$.

Démonstration. On note, comme précédemment,

$$\mathrm{F}_i = \frac{\mathrm{P}(x, y+t)}{\mathrm{U}_i(x,y+t)\mathrm{V}_i(x,y,t)^i},$$

où

$$\mathrm{U}_i(x,y) = \frac{\mathrm{Q}(x,y)}{\mathrm{Q}_i(x,y)^i}, \quad \mathrm{V}_i(x,y,t) = \frac{\mathrm{Q}_i(x,y+t) - \mathrm{Q}_i(x,y)}{t}.$$

En utilisant les bidegrés par rapport à (x,y), on constate que

$$\operatorname{bideg}\mathrm{U}_i^\star = \operatorname{bideg}\mathrm{Q}^\star - \operatorname{bideg}\mathrm{Q}_i, \quad \operatorname{bideg}\mathrm{V}_i \leqslant \operatorname{bideg}\mathrm{Q}_i - (0,1).$$

Le degré total en (y,t) se comporte de la même façon : celui de $\mathrm{U}_i^\star(x,y+t)$ est $\deg_y \mathrm{Q} - \deg_y \mathrm{Q}_i$, tandis que celui de $\mathrm{V}_i(x,y,t)$ est $\deg_y \mathrm{Q}_i - 1$. Le corollaire 68 donne alors

$$\frac{1}{\mathrm{U}_i(x,y+t)} \in \frac{1}{\mathrm{U}_i(x,y)} \mathscr{E}_{\operatorname{bideg}\mathrm{Q}^\star - \operatorname{bideg}\mathrm{Q}_i - (0,1)}(\mathrm{U}_i^\star(x,y)), \tag{3.2}$$

$$\frac{1}{\mathrm{V}_i(x,y,t)^i} \in \frac{1}{\mathrm{V}_i(x,y,0)^i} \mathscr{E}_{\operatorname{bideg}\mathrm{Q}_i - (0,2)}(\mathrm{V}_i(x,y,0)). \tag{3.3}$$

De là, la partie *(3)* de la proposition 67 montre que le produit de ces séries appartient à

$$\frac{1}{\mathrm{U}_i(x,y)\mathrm{V}_i(x,y,0)^i} \mathscr{E}_{\operatorname{bideg}\mathrm{Q}^\star - (0,2)}(\mathrm{U}_i^\star(x,y)\mathrm{V}_i(x,y,0)).$$

Ainsi, le coefficient S_{i-1} de t^{i-1} dans le développement en série de F_i peut s'écrire $\mathrm{A}_i/\mathrm{B}_i$, avec

$$\mathrm{B}_i = \mathrm{U}_i(x,y)\mathrm{V}_i(x,y,0)^i \mathrm{U}_i^\star(x,y)^{i-1}\mathrm{V}_i(x,y,0)^{i-1},$$

Et, finalement,

$$\begin{aligned} \operatorname{bideg}\mathrm{A}_i &\leqslant \operatorname{bideg}\mathrm{P} + (i-1)\operatorname{bideg}\mathrm{Q}^\star - 2(i-1)(0,1), \\ \operatorname{bideg}\mathrm{B}_i &\leqslant \operatorname{bideg}\mathrm{Q} + (i-1)\operatorname{bideg}\mathrm{Q}^\star - (2i-1)(0,1), \end{aligned} \tag{3.4}$$

d'où

$$\operatorname{bideg}(\mathrm{A}_i - z\mathrm{B}_i) \leqslant \max(\operatorname{bideg}\mathrm{P}, \operatorname{bideg}\mathrm{Q} - (0,1)) + (i-1)(\operatorname{bideg}\mathrm{Q}^\star - (0,2)).$$

On peut alors borner le bidegré de R_i par la proposition 130 :

$$\begin{aligned}\deg_x \mathrm{R}_i \leqslant \deg_y \mathrm{Q}_i \big(&\max(\deg_x \mathrm{P}, \deg_x \mathrm{Q}) + (i-1)\deg_x \mathrm{Q}^\star\big) \\ &+ \deg_x \mathrm{Q}_i \Big(\max(\deg_y \mathrm{P}, \deg_y \mathrm{Q} - 1) + (i-1)(\deg_y \mathrm{Q}^\star - 2)\Big).\end{aligned}$$

Maintenant, on somme sur les indices i correspondant aux facteurs de $\hat{\mathrm{Q}}$, ce qui donne pour le degré en x du résultat de l'algorithme la borne

$$\begin{aligned}&\deg_y \hat{\mathrm{Q}}^\star \max(\deg_x \mathrm{P}, \deg_x \mathrm{Q}) + (\deg_y \hat{\mathrm{Q}} - \deg_y \hat{\mathrm{Q}}^\star)\deg_x \mathrm{Q}^\star \\ &\qquad + \deg_x \hat{\mathrm{Q}}^\star \max(\deg_y \mathrm{P}, \deg_y \mathrm{Q} - 1) + (\deg_x \hat{\mathrm{Q}} - \deg_x \hat{\mathrm{Q}}^\star)(\deg_y \mathrm{Q}^\star - 2).\end{aligned}$$

Étant donné que cette borne est une fonction croissante de chacun des degrés, elle reste vraie si on les remplace eux-mêmes par des majorants respectifs. On en déduit la borne

$$d_y^\star d_x + (d_y - d_y^\star)d_x^\star + d_x^\star d_y + (d_x - d_x^\star)(d_y^\star - 2),$$

qui se récrit comme celle annoncée dans le théorème. □

3.1.2 Complexité

Théorème 70. *Soit* $\mathrm{P}(x,y)/\mathrm{Q}(x,y) \in \mathbf{k}(x,y)_{d_x,d_y}$. *Soit* $\hat{\mathrm{Q}}$ *un diviseur de* Q, $\hat{\mathrm{Q}}^\star$ *une partie sans carré de* $\hat{\mathrm{Q}}$ *par rapport à* y, *et on note* m *le nombre de facteurs dans la décomposition sans carré de* $\hat{\mathrm{Q}}$. *Soit* $(d_x^\star, d_y^\star)$ *une borne sur le bidegré de* $\mathrm{Q}^\star$. *Alors l'appel* PolynômeRésidus$(\mathrm{P}/\mathrm{Q}, \hat{\mathrm{Q}})$ *effectue au plus*

$$\mathrm{O}(m^2 d_x^\star d_y^\star (m^2 + d_y^{\star 2}))$$

opérations dans $\mathbf{k}$.

Démonstration. D'après la proposition 135, la décomposition sans carré de $\hat{\mathrm{Q}}$ peut être calculée en $\tilde{\mathrm{O}}(d_x^2 d_y)$ opérations dans $\mathbf{k}$. On s'intéresse maintenant aux calculs effectués lors de la i-ème itération de la boucle. Pour ce faire, on note $(d_x^{(i)}, d_y^{(i)})$ le bidegré de Q_i. Le calcul de U_i nécessite une division exacte de polynômes de bidegré au plus (d_x, d_y) ; cette division peut se faire par évaluation et interpolation en $\tilde{\mathrm{O}}(d_x d_y)$ opérations (voir proposition 133). De même, le polynôme trivarié V_i peut être calculé par évaluation et interpolation par rapport à (x,y) en $\tilde{\mathrm{O}}(d_x^{(i)}(d_y^{(i)})^2)$ opérations. Ensuite, l'équation (3.4) montre que $\mathrm{A}_i(x,y)$ et $\mathrm{B}_i(x,y)$ ont tous deux un bidegré au plus $(\mathrm{D}_x^{(i)}, \mathrm{D}_y^{(i)})$, où $\mathrm{D}_x^{(i)} = d_x + i d_x^\star$ et $\mathrm{D}_y^{(i)} = d_y + i d_y^\star$. Ils peuvent être calculés par évaluation et interpolation en $\tilde{\mathrm{O}}(i\mathrm{D}_x^{(i)}\mathrm{D}_y^{(i)})$ opérations. Enfin, le résultant $\mathrm{R}_i(x,z)$ a un bidegré au plus $(d_x^{(i)}\mathrm{D}_y^{(i)} + d_y^{(i)}\mathrm{D}_x^{(i)}, d_y^{(i)})$, par la proposition 130. Le coût total de la boucle est donc $\tilde{\mathrm{O}}(\mathrm{L})$, où

$$\mathrm{L} = \sum_{i=1}^{m} \Big((i + (d_y^{(i)})^2)\mathrm{D}_x^{(i)}\mathrm{D}_y^{(i)} + d_x^{(i)} d_y^{(i)} (\mathrm{D}_y^{(i)})^2\Big).$$

En utilisant les bornes (brutales) $\mathrm{D}_x^{(i)} \leqslant \mathrm{D}_x^{(m)}$, $\mathrm{D}_y^{(i)} \leqslant \mathrm{D}_y^{(m)}$, $\sum_{i=1}^m (d_y^{(i)})^2 \leqslant d_y^{\star 2}$ et $\sum_{i=1}^m d_x^{(i)} d_y^{(i)} \leqslant d_x^\star d_y^\star$, on en déduit que L est majoré par

$$\mathrm{D}_x^{(m)}\mathrm{D}_y^{(m)} \sum_{i=1}^m (i + (d_y^{(i)})^2) + (\mathrm{D}_y^{(m)})^2 \sum_{i=1}^m d_x^{(i)} d_y^{(i)} \leqslant \mathrm{D}_x^{(m)}\mathrm{D}_y^{(m)}(m^2 + d_y^{\star 2}) + (\mathrm{D}_y^{(m)})^2 d_x^\star d_y^\star.$$

Il ne reste qu'à utiliser les inégalités $\mathrm{D}_x^{(m)} \leqslant 2md_x^\star$ et $\mathrm{D}_y^{(m)} \leqslant 2md_y^\star$ pour voir que

$$\mathrm{L} = \mathrm{O}(m^2 d_x^\star d_y^\star (m^2 + d_y^{\star 2})),$$

et la preuve est terminée. □

Remarque 71. *En relâchant la borne du théorème précédent, on voit que la complexité peut également être majorée indépendamment des multiplicités par*

$$\tilde{\mathrm{O}}(d_x^\star d_y^\star d_y).$$

3.2 Polynôme annulateur pour une somme composée pure

On passe maintenant au deuxième sous-problème : à partir d'un polynôme annulant chacun des résidus, calculer un polynôme qui annule la somme d'un certain nombre de résidus. Je commence cette section avec un rappel sur les sommes de Newton attachée à un polynôme. C'est un objet très classique qui va intervenir de façon fondamentale pour attaquer ce problème.

3.2.1 Sommes de Newton d'un polynôme

Définition 72. Soit $p \in \mathbb{K}[y]$ un polynôme de degré d, que l'on factorise sur $\overline{\mathbb{K}}$:

$$p = a \prod_{i=1}^d (y - \alpha_i),$$

avec $\alpha_1, \alpha_2, \ldots, \alpha_d \in \overline{\mathbb{K}}$. La quantité

$$\alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n \in \mathbb{K}$$

est appelée la n-ième somme de Newton de p. On utilisera la notation $\mathscr{N}(p)$ pour désigner la série génératrice ordinaire des sommes de Newton de p. Plus précisément,

$$\mathscr{N}(p) = \sum_{n \geqslant 0} \left(\alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n\right) y^n \in \mathbb{K}[[x]].$$

Rappelons quelques propriétés élémentaires bien connues des sommes de Newton. On utilise la notation $\mathrm{rec}(p)$ pour désigner le polynôme réciproque de p.

Proposition 73. *Soit $p \in \mathbb{K}[y]$ un polynôme unitaire de degré d. Alors*

1.
$$\forall \lambda \in \mathbb{K}\ \mathscr{N}(\lambda p) = \mathscr{N}(p)\ ;$$

2.
$$\mathscr{N}(p) = \frac{\mathrm{rec}(p')}{\mathrm{rec}(p)}\ ;$$

3.
$$\mathrm{rec}(p) = \exp\left(\int \frac{d - \mathscr{N}(p)}{y}\,\mathrm{d}y\right).$$

Démonstration. (1) Évident car λp et p ont les mêmes racines.
(2) Écrivons $p = \prod_{i=1}^{d}(y - \alpha_i)$. Alors on a

$$\frac{p'}{p} = \sum_{i=1}^{d} \frac{1}{y - \alpha_i},$$

et donc

$$\frac{\mathrm{rec}(p')}{\mathrm{rec}(p)} = \frac{1}{y} \cdot \frac{p'\left(\frac{1}{y}\right)}{p\left(\frac{1}{y}\right)} = \sum_{i=1}^{d} \frac{1}{1 - \alpha_i y} = \sum_{i=1}^{d} \sum_{n \geqslant 0} \alpha_i^n y^n = \sum_{n \geqslant 0} \left(\sum_{i=1}^{d} \alpha_i\right) y^n = \mathscr{N}(p).$$

(3) D'après le calcul précédent, on a

$$\frac{d - \mathscr{N}(p)}{y} = \frac{1}{y}\left(d - \sum_{i=1}^{d} \frac{1}{1 - \alpha_i y}\right) = \sum_{i=1}^{d} \frac{-\alpha_i}{1 - \alpha_i y}.$$

En intégrant puis en prenant l'exponentielle, il vient

$$\exp\left(\int \frac{d - \mathscr{N}(p)}{y}\,\mathrm{d}y\right) = \prod_{i=1}^{d} (1 - \alpha_i y) = \mathrm{rec}(p).$$

□

Cette proposition montre qu'un polynôme p unitaire de degré d est entièrement déterminé par la série tronquée $\mathscr{N}(p) \bmod y^{d+1}$. De plus, le passage d'une structure de données à l'autre est algorithmiquement efficace par la proposition 131 de l'annexe B.

3.2.2 Somme composée pure d'un polynôme

Jusqu'à la fin de cette section, on se donne $p \in \mathbb{K}[y]$ un polynôme de degré d, et on fixe un entier positif $c \leqslant d$. On note également $\alpha_1, \alpha_2, \ldots, \alpha_d$ les racines de p dans $\overline{\mathbb{K}}$.

Définition 74. On appelle somme composée pure d'ordre c le polynôme noté $\Sigma_c p$ et défini par

$$\Sigma_c p = \prod_{i_1 < i_2 < \cdots < i_c} (y - (\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_c})).$$

Proposition 75.

1. $\Sigma_c p \in \mathbb{K}[y]$;
2. $\deg_y \Sigma_c p = \binom{d}{c}$.

Démonstration. *(1)* Le polynôme $\Sigma_c p$ vu comme élément de $\mathbb{K}[y][\alpha_1, \alpha_2, \ldots, \alpha_d]$ est symétrique en les racines de p. Donc, par la proposition 126, ses coefficients appartiennent au corps engendré par les coefficients de p, qui n'est autre que $\mathbb{K}$.

(2) Évident. □

La définition de $\Sigma_c p$ à partir de p est certes très simple en théorie. Cependant, en pratique, il n'est pas du tout évident au premier abord de calculer $\Sigma_c p$ pour un p donné par la liste de ses coefficients. Comme souvent pour ce genre d'opération, il se trouve que la série génératrice des sommes de Newton est une meilleure structure de données pour effectuer le calcul. On trouve cette idée pour une opération similaire, qu'on pourrait appeler par analogie le « produit composé pur », chez Banderier et Flajolet[4]. L'algorithme que je vais présenter pour le calcul de la somme composée pure est une variante de leur algorithme Platypus. Par ailleurs, on trouve l'idée chez Bostan, Flajolet *et al.*[5] que les séries génératrices ordinaires sont utiles pour manipuler les opérations de type « produit composé », alors que les « sommes composées » se manipulent mieux par l'intermédiaire de la série génératrice exponentielle

$$\mathscr{N}(p) \odot \exp(y) = \sum_{n \geqslant 0} \left(\alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n\right) \frac{y^n}{n!} = \sum_{i=1}^{d} \exp(\alpha_i y).$$

Bien sûr, il est aisé de jongler entre séries génératrices ordinaires et exponentielles puisque l'on passe de l'une à l'autre en multipliant ou en divisant par des factorielles.

Proposition 76. *Soit $p \in \mathbf{k}[y]$ un polynôme de degré d. On note $\mathrm{S} = \mathscr{N}(p) \odot \exp(y)$. Soit $\Psi_c \in \mathbf{k}[t_1, \ldots, t_c]$ le polynôme défini par*

$$\Psi_c(t_1, t_2, \ldots, t_c) = [z^c] \exp\left(\sum_{n \geqslant 1} (-1)^{n-1} t_n \frac{z^n}{n}\right).$$

Alors

$$\mathscr{N}(\Sigma_c p) \odot \exp(y) = \Psi_c(\mathrm{S}(y), \mathrm{S}(2y), \ldots, \mathrm{S}(cy)).$$

Démonstration. On part de la série génératrice exponentielle des sommes de Newton de $\Sigma_c p$.

$$\begin{aligned} \mathscr{N}(\Sigma_c p) \odot \exp(y) &= \sum_{i_1 < \cdots < i_c} \exp\left((\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_c}) y\right) \\ &= [z^c] \prod_{i=1}^{d} \left(1 + z \exp(\alpha_i y)\right). \end{aligned}$$

4. BANDERIER et FLAJOLET, "Basic Analytic Combinatorics of Directed Lattice Paths".
5. BOSTAN, FLAJOLET et al., "Fast Computation of Special Resultants".

Algorithme **SommeCompPure**(p, c)

Entrée Un polynôme $p \in \mathbb{K}[y]$ de degré d, un entier positif $c \leqslant d$

Sortie Le polynôme $\Sigma_c p$

$\mathrm{D} \leftarrow \binom{d}{c}$;
$\mathscr{N}(p) \leftarrow \mathrm{rec}(p')/\mathrm{rec}(p) \bmod y^{\mathrm{D}+1}$;
$\mathrm{S} \leftarrow \mathscr{N}(p) \odot \exp(y) \bmod y^{\mathrm{D}+1}$;
$\mathrm{F} \leftarrow \exp\left(\sum_{n=1}^{c} (-1)^{n-1} \frac{\mathrm{S}(ny)}{n} z^n\right) \bmod (y^{\mathrm{D}+1}, z^{c+1})$;
$\mathscr{N}(\Sigma_c p) \leftarrow ([z^c]\mathrm{F}) \odot \sum n! y^n \bmod y^{\mathrm{D}+1}$;
renvoyer $\mathrm{rec}\left(\exp\left(\int \frac{\mathrm{D} - \mathscr{N}(\Sigma_c p)}{y} \mathrm{d}y\right) \bmod y^{\mathrm{D}+1}\right)$.

Algorithme 7: Polynôme annulant une somme composée pure

Cette expression se récrit

$$[z^c] \exp\left(\sum_{i=1}^{d} \log(1 + z\exp(\alpha_i y))\right) = [z^c] \exp\left(\sum_{i=1}^{d} \sum_{m \geqslant 1} (-1)^{m-1} \exp(\alpha_i m y) \frac{z^m}{m}\right)$$
$$= [z^c] \exp\left(\sum_{m \geqslant 1} (-1)^{m-1} \mathrm{S}(my) \frac{z^m}{m}\right),$$

et le membre de droite n'est autre que $\Psi_c(\mathrm{S}(y), \mathrm{S}(2y), \ldots, \mathrm{S}(cy))$.

□

Correction de l'algorithme 7
C'est direct avec les propositions 73, 75 et 76. □

3.2.3 Somme composée pure d'un polynôme bivarié

À nouveau, on va appliquer l'algorithme 7 à un polynôme bivarié et on souhaite être capable de prédire le bidegré du résultat.

Théorème 77. *Soit* $\mathrm{P} \in \mathbf{k}[x, y]_{d_x, d_y}$*, et soit* $c \leqslant d_y$ *un entier positif. Soit également* $a \in \mathbb{K}[x]$ *le coefficient dominant de* P *par rapport à* y*. On note*

$$\mathrm{D}_x := \binom{d_y - 1}{c - 1}, \qquad \mathrm{D}_y := \binom{d_y}{c}.$$

Alors $a^{\mathrm{D}_x} \cdot \Sigma_c \mathrm{P}$ *est un polynôme de* $\mathbf{k}[x, y]$ *qui annule toutes les sommes* $\alpha_{i_1} + \cdots + \alpha_{i_c}$ *de* c *racines de* P*, avec* $i_1 < \cdots < i_c$*, et vérifie*

$$\deg_x(a^{\mathrm{D}_x} \cdot \Sigma_c \mathrm{P}) \leqslant d_x \mathrm{D}_x, \quad \deg_y(a^{\mathrm{D}_x} \cdot \Sigma_c \mathrm{P}) = \mathrm{D}_y.$$

Démonstration. On choisit des notations pour les coefficients et les racines de P :

$$\mathrm{P} = a(x)y^{d_y} + \sum_{i=0}^{d_y-1} a_i(x)y^i = a(x)\prod_{i=1}^{d_y}(y-\alpha_i(x)).$$

Soient $\sigma_1(x),\sigma_2(x),\ldots,\sigma_{d_y}(x)$ les fonctions symétriques élémentaires associées à $\alpha_1,\alpha_2,\ldots,\alpha_{d_y}$. Alors les fonctions symétriques associées $\alpha_{i_1}+\alpha_{i_2}+\cdots+\alpha_{i_c}$ de $\Sigma_c\mathrm{P}$ ont un degré $\binom{d_y-1}{c-1}$ en chacun des α_i. Par la proposition 126, on en déduit que les coefficients de $\Sigma_c\mathrm{P}$ sont des polynômes de degré total au plus $\binom{d_y-1}{c-1}$ en $\sigma_1,\sigma_2,\ldots,\sigma_{d_y}$. On obtient alors la borne annoncée sur $\deg_x(a^{\mathrm{D}_x}\cdot\Sigma_c\mathrm{P})$ en utilisant les relations (voir proposition 124)

$$(-1)^i\sigma_i = \frac{a_{d_y-i}}{a}.$$

La borne sur le degré en y a déjà été vue dans la proposition 75. □

3.2.4 Complexité

Théorème 78. *On reprend les notations du théorème 77. Alors l'appel* SommeCompPure(P, c) *calcule la somme composée pure d'ordre de c de* P *en*

$$\tilde{\mathrm{O}}(cd_x\mathrm{D}_x\mathrm{D}_y)$$

opérations dans **k**.

Démonstration. Le calcul est effectué par évaluation et interpolation pour $1+d_x\mathrm{D}_x$ valeurs de x. D'après la proposition 131, pour chacune de ces valeurs, le calcul des séries tronquées $\mathscr{N}(\mathrm{P})$ et S à l'ordre $1+\mathrm{D}_y$ nécessite $\tilde{\mathrm{O}}(\mathrm{D}_y)$ opérations dans **k** ; il en va de même pour les calculs de $\mathscr{N}(\Sigma_c\mathrm{P})$ et pour la dernière étape. L'étape la plus coûteuse est le calcul de F, en $\tilde{\mathrm{O}}(c\mathrm{D}_y)$ opérations dans **k**. Comme il doit être effectué $\mathrm{O}(d_x\mathrm{D}_x)$ fois, le coût total du calcul est $\tilde{\mathrm{O}}(cd_x\mathrm{D}_x\mathrm{D}_y)$ opérations dans **k**. □

3.3 Polynôme annulateur pour une intégrale de fraction rationnelle bivariée

3.3.1 Algorithme

Dans cette section, on se donne une fraction rationnelle $\mathrm{F}\in\mathbf{k}[x,y]$ de degrés respectifs d_x et d_y en x et y, et on souhaite calculer un polynôme annulateur de $[y^{-1}]\mathrm{F}(x,y)$. On repart de la formule (3.1) :

$$[y^{-1}]\mathrm{F}(x,y) = \sum_{i=1}^{c}\mathrm{Res}(\mathrm{F},y_i),$$

où $y_1,y_2,\ldots,y_c$ les petits pôles de F. L'algorithme PolynômeRésidus p. 65 permet de calculer un polynôme qui annule tous les $\mathrm{Res}(\mathrm{F},y_i)$. Pour ensuite calculer un

Algorithme **PolIntFRat**(A/B)

Entrée Deux polynômes $A, B \in \mathbf{k}[x, y]$

Sortie Un polynôme $\Phi \in \mathbf{k}[x, y]$ tel que $\Phi(x, [y^{-1}]A/B) = 0$

$R \leftarrow$ **PolynômeRésidus**$(A/B, B)$;
$c \leftarrow$ nombre de petites branches B ;
$\Phi(x, y) \leftarrow$ numer(**SommeCompPure**(R, c)) ;
renvoyer $\Phi(x, y)$

Algorithme 8: Polynôme annulant une intégrale de fraction rationnelle bivariée

polynôme annulateur pour la somme en utilisant l'algorithme SommeCompPure, il suffit de connaître le nombre c de petits pôles de F.

Cette information peut être lue directement sur le polygone de Newton du dénominateur de F, dont la définition est rappelée dans l'annexe A.3 (définition 121). Il est classique que les valuations des racines d'un polynôme sont les opposés des pentes apparaissant dans le polygone de Newton. Ainsi, le nombre de petits pôles de F est simplement la largeur de la partie de pente strictement négative du polygone de Newton de son dénominateur.

On en déduit donc l'algorithme PolIntFRat qui calcule un polynôme annulateur pour $[y^{-1}]F(x, y)$.

3.3.2 Bornes

L'algorithme PolIntFRat consiste essentiellement en deux appels à PolynômeRésidus et SommeCompPure mis bout-à-bout. Ce nouvel algorithme peut donc être analysé à partir des résultats déjà obtenus dans les sections précédentes.

Théorème 79. *Soient* $A, B \in \mathbf{k}[x, y]_{d_x, d_y}$ *deux polynômes premiers entre eux. Soit également* $d_y^\star$ *une borne sur le degré de la partie sans carré de* B *et* c *son nombre de petites branches. Notons*

$$D_x = 2d_x^\star(d_y + 1) + 2(d_y^\star - 1)d_x - 2d_x^\star d_y^\star.$$

Alors le polynôme Φ *calculé par l'appel* PolIntFRat(A/B) *vérifie*

$$\deg_x \Phi \leqslant D_x \binom{d_y^\star - 1}{c}, \quad \deg_y \Phi = \binom{d_y^\star}{c}.$$

Démonstration. D'après le théorème 69, $\deg_y R = d_y^\star$ et $\deg_x R \leqslant D_x$. On applique ensuite le théorème 77, qui donne $\deg_y \Phi = \binom{d_y^\star}{c}$ et

$$\deg_x \Phi \leqslant D_x \binom{d_y^\star - 1}{c}.$$

□

3.3.3 Complexité

Théorème 80. *On reprend les notations du théorème 79. Alors l'appel* PolIntFRat(A/B) *calcule le polynôme* Φ *en*

$$\tilde{\mathrm{O}}\left(c\mathrm{D}_x\binom{d_y^\star}{c}^2 + d_x d_y^5\right)$$

opérations dans **k**.

Démonstration. D'après la remarque 71, le calcul de R coûte $\tilde{\mathrm{O}}(d_x d_y^5)$ opérations. Le nombre de petites branches quant à lui est obtenu gratuitement à partir de la décomposition sans carré de B calculée par l'algorithme 6. Enfin, par le théorème 78, la somme composée pure est calculée en $\tilde{\mathrm{O}}(c\mathrm{D}_x\mathrm{D}_y^2)$ opérations. □

Chapitre 4

Diagonales de fractions rationnelles bivariées

Les algorithmes du chapitre précédent s'appliquent presque directement pour calculer un polynôme annulant une diagonale de fraction rationnelle bivariée. Le point clé est le fait qu'elles ont une représentation sous forme d'intégrale de fraction rationnelle. Nous avons déjà évoqué cela sommairement dans l'introduction et dans le premier chapitre. Dans la première section de ce chapitre, nous allons revenir sur la définition et les propriétés de base des diagonales. La deuxième section présente une solution algorithmique au calcul d'un polynôme annulateur. La méthode est très similaire à l'algorithme PolIntFRat à cela près que l'on peut apporter une optimisation supplémentaire en utilisant la forme particulière que prennent les représentations intégrales des diagonales. Enfin, on étudiera en fin de chapitre le polynôme minimal de la diagonale d'une fraction rationnelle F dans le cas générique et montrerons en particulier que son degré est génériquement exponentiel en le bidegré de F.

4.1 Généralités

Définition 81. Soit $F \in \mathbf{k}(x, y)$ une fraction rationnelle régulière en $(0,0)$. On peut alors développer F dans $\mathbf{k}[[x, y]]$:

$$F(x, y) = \sum_{i,j \geqslant 0} a_{i,j} x^i y^j,$$

avec $a_{i,j} \in \mathbf{k}$ pour tous i et j. On définit alors la *diagonale* de F, notée ΔF, comme étant la série univariée

$$\Delta F(t) = \sum_{i \geqslant 0} a_{i,i} t^i \in \mathbf{k}[[t]].$$

Commençons par une première remarque très simple mais fondamentale dans les calculs de diagonales.

Lemme 82. *Soit* $\mathrm{F} \in \mathbf{k}(x,y)$ *une fraction rationnelle régulière en* $(0,0)$. *Alors*

$$\Delta\mathrm{F}(t) = [y^{-1}]\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right).$$

Démonstration. Écrivons le développement de F en série entière :

$$\mathrm{F}(x,y) = \sum_{i,j\geqslant 0} a_{i,j}x^i y^j,$$

avec $a_{i,j} \in \mathbf{k}$ pour tous i et j. Alors le changement de variable $x \to t/y$ donne

$$\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right) = \sum_{i,j\geqslant 0} a_{i,j}t^i y^{j-i-1}.$$

Ceci est une égalité entre éléments de $\mathbf{k}((y))((t))$, on peut donc en extraire le coefficient de $[y^{-1}]$ au sens de la définition 7 :

$$[y^{-1}]\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right) = \sum_{i\geqslant 0} a_{i,i}t^i = \Delta\mathrm{F}(t).$$

□

Remarque 83. *Cette formule peut aussi être lue dans l'autre sens. En effet, supposons que l'on a écrit une série* $f \in \mathbf{k}[[t]]$

$$f(t) = [y^{-1}]\mathrm{F}(t,y),$$

pour une certaine fraction rationnelle $\mathrm{F} \in \mathbf{k}(t,y)$. *Alors, le lemme 82 montre que*

$$f(t) = \Delta\left\{y\mathrm{F}(xy,y)\right\},$$

pour peu que la fraction rationnelle $y\mathrm{F}(xy,y)$ *soit régulière en* $(0,0)$.

Proposition 84. *Soit* $\mathrm{F} \in \mathbf{k}(x,y)$ *une fraction rationnelle. Notons* $y_1, y_2, \ldots, y_c$ *les petits pôles de la fraction*

$$\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right)$$

en y.

Alors

$$\Delta\mathrm{F}(t) = \sum_{i=1}^{c} \mathrm{Res}\left(\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right), y_i\right).$$

Ce résultat est une généralisation à un corps de caractéristique 0 quelconque d'un résultat de Furstenberg[1].

1. FURSTENBERG, "Algebraic Functions over Finite Fields".

Démonstration. On part de l'expression de ΔF comme résidu (lemme 82) :

$$\Delta F(t) = [y^{-1}]\frac{1}{y}F\left(\frac{t}{y}, y\right).$$

On calcule alors le membre droit à l'aide de la formule des résidus (proposition 8 p. 27), ce qui donne le résultat escompté.

□

Corollaire 85. *Soit* $F \in \mathbf{k}(x,y)$ *une fraction rationnelle bivariée. Alors la diagonale de* F *est une série univariée algébrique.*

Démonstration. C'est un cas particulier du corollaire 9 p. 28. □

Il est naturel de se demander si la réciproque est vraie : une série algébrique étant donnée, peut-on toujours trouver une fraction rationnelle bivariée dont elle est la diagonale ? La proposition suivante, due à Furstenberg [2], montre que c'est en effet le cas si l'on considère une série algébrique qui satisfait une bonne condition de séparation par rapport à ses conjuguées.

Proposition 86. *Soit* $P \in \mathbf{k}[t][y]$ *un polynôme tel que*

$$P(0,0) = 0, \quad \textit{et} \quad \partial_y P(0,0) \neq 0.$$

Soit f *l'unique racine de* P *dans* $\mathbf{k}[[t]]$ *telle que* $f(0) = 0$. *Alors la fraction rationnelle*

$$F(x,y) = y^2 \partial_y P(xy, y)/P(xy, y)$$

est régulière en $(0,0)$ *et*

$$f = \Delta F.$$

Démonstration. Si l'on note $d = \deg_y P$ et $f_1 = f, f_2, \ldots, f_d$ les d racines de P dans $\overline{\mathbf{k}(x)}$, on a

$$\frac{\partial_y P(x,y)}{P(x,y)} = \sum_{i=1}^{d} \frac{1}{y - f_i}.$$

On déduit que

$$y\frac{\partial_y P(x,y)}{P(x,y)} = \sum_{i=1}^{d} \frac{y}{y - f_i} = d + \sum_{i=1}^{d} \frac{f_i}{y - f_i}.$$

Mais par la proposition 122 de l'annexe A.3, l'hypothèse de séparation des racines de P implique que f est l'unique petit pôle de $y\partial_y P/P$, et le résidu de cette fraction en f vaut f. La proposition 8 donne alors

$$[y^{-1}]\left\{\frac{y\partial_y P(x,y)}{P(x,y)}\right\} = f.$$

Le résultat attendu découle ensuite de la remarque 83. Il faut simplement s'assurer que la fraction F est régulière en $(0,0)$. Mais ceci découle des hypothèses faites sur P. En effet, comme $P(0,0) = 0$, $P(xy,y)/y$ est un polynôme dont on vérifie facilement que la valeur en $(0,0)$ n'est autre que $\partial_y P(0,0)$. □

2. Ibid., Prop. 2.

Bien évidemment, ce lemme ne s'applique pas pour une série algébrique f générale. Mais Mechik[3] a montré qu'il est toujours possible de se ramener à la situation du lemme en développant f assez loin pour qu'elle se sépare de ses conjuguées. Plus précisément, il a prouvé que la queue du développement de f à l'ordre α est solution d'un polynôme satisfaisant les hypothèses du lemme, pour peu que l'on choisisse α assez grand. Cependant, sa méthode ne donne aucune information sur une valeur suffisante de α. Adamczewski et Bell[4] ont établi une version quantitative de ce résultat dans un cadre bien plus général, qui donne accès à une estimation d'un ordre de développement α suffisant. Le lemme suivant est une spécialisation de leur théorème au cas qui nous intéresse. J'en redonne la preuve en détail, d'une part parce qu'elle peut s'exprimer en des termes plus simples dans ce cas particulier, et également pour rectifier une légère imprécision dans la preuve d'Adamczewski et Bell.

Lemme 87. *Soit* $\mathrm{P} \in \mathbf{k}(x)[y]$ *un polynôme sans carré tel que* $\mathrm{P}(0,0) = 0$, $\partial_y \mathrm{P}(0,0) = 0$ *et admettant une racine* $f \in \mathbf{k}[[x]]$ *telle que* $f(0) = 0$. *On note*

$$\alpha = \mathrm{val}_x \, \text{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P}),$$

et on écrit

$$f(x) = r(x) + x^\alpha g(x),$$

où $r(x) = f \bmod x^{\alpha+1}$.

Alors $g(x)$ *est annulée par un polynôme* $\mathrm{Q} \in \mathbf{k}[x,y]$ *tel que*

$$\mathrm{Q}(0,0) = 0, \quad \textit{et} \quad \partial_y \mathrm{Q}(0,0) \neq 0.$$

Démonstration. On pose $\mathrm{R} = \text{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P})$. De par sa définition, la série g est annulée par le polynôme $\mathrm{P}(x, r(x) + x^\alpha y)$. Par la formule de Taylor, on peut récrire ce polynôme :

$$\mathrm{P}(x, r + x^\alpha y) = \mathrm{P}(x,r) + x^\alpha y \partial_y \mathrm{P}(x,r) + x^{2\alpha} y^2 \mathrm{H}(x,y), \tag{4.1}$$

pour un certain polynôme $\mathrm{H} \in \mathbf{k}[x,y]$. En évaluant cette égalité en g, on obtient

$$\mathrm{P}(x,r) = -x^\alpha g \partial_y \mathrm{P}(x,r) - x^{2\alpha} g^2 \mathrm{H}(x,r). \tag{4.2}$$

Comme $g(0) = 0$, ceci implique en particulier que

$$\mathrm{val}_x \, \mathrm{P}(x,r) > \alpha.$$

Maintenant, les propriétés élémentaires du résultant font qu'il existe des polynômes $\mathrm{U}, \mathrm{V} \in \mathbf{k}[x,y]$ tels que

$$\mathrm{R}(x) = \mathrm{U}(x,y)\mathrm{P}(x,y) + \mathrm{V}(x,y)\partial_y \mathrm{P}(x,y)$$

3. MECHIK, "Sur la constante d'Eisenstein".
4. ADAMCZEWSKI et BELL, "Diagonalization and rationalization of algebraic Laurent series".

(voir la proposition 129 de l'annexe A.5). Comme $\mathrm{val}_x \mathrm{R} = \alpha$ et $\mathrm{val}_x \mathrm{P} > \alpha$, cette égalité implique que $\mathrm{val}_x(\mathrm{V}(x,r)\partial_y \mathrm{P}(x,r)) = \alpha$, et donc

$$\mathrm{val}_x \partial_y \mathrm{P}(x,r) \leqslant \alpha.$$

(À noter que cette inégalité peut être stricte, c'est là l'imprécision dans la preuve originelle.) Posons $\beta = \mathrm{val}_x \partial_y \mathrm{P}(x,r)$. Alors en réinspectant l'égalité (4.2), on constate que

$$\mathrm{val}_x \mathrm{P}(x,r) \geqslant \min(\alpha+\beta+1, 2\alpha+2) = \alpha+\beta+1.$$

Ceci et l'égalité (4.1) montrent que le polynôme $\mathrm{P}(x, r+x^\alpha y)$ est divisible par $x^{\alpha+\beta}$. On pose donc

$$\mathrm{Q}(x,y) = \frac{\mathrm{P}(x, r+x^\alpha y)}{x^{\alpha+\beta}} \in \mathbf{k}[x,y].$$

Par construction, on a $\mathrm{Q}(x, g(x)) = 0$. De plus, l'égalité (4.1) se récrit

$$\mathrm{Q}(x,y) = \frac{\mathrm{P}(x,r)}{x^{\alpha+\beta}} + y\frac{\partial_y \mathrm{P}(x,r)}{x^\beta} + x^{\alpha-\beta}y^2 \mathrm{H}(x,y).$$

En évaluant cette égalité en $(0,0)$, on obtient $\mathrm{Q}(0,0) = 0$ puisque $\mathrm{val}_x(\mathrm{P}(x,r)/x^{\alpha+\beta}) \geqslant 1$. En la dérivant et en évaluant en $(0,0)$, on obtient

$$\partial_y \mathrm{Q}(0,0) = \frac{\partial_y \mathrm{P}(x,r)}{x^\beta}(0,0) \neq 0$$

par définition de β. □

Remarque 88. *Si l'on note (d_x, d_y) le bidgré de* P*, la proposition 130 donne une majoration de l'entier* α *du lemme :*

$$\alpha = \mathrm{val}_x \mathrm{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P}) \leqslant \deg_x \mathrm{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P}) \leqslant 2d_x d_y.$$

Grâce aux deux lemmes précédents, on obtient la réciproque du théorème de Furstenberg.

Proposition 89. *Soit* $\mathrm{P} \in \mathbf{k}[t,y]$ *un polynôme admettant une série* $f \in \mathbf{k}[[t]]$ *comme solution.*

Alors il existe une fraction rationnelle $\mathrm{F} \in \mathbf{k}(x,y)$ *régulière en* $(0,0)$ *telle que*

$$f = \Delta \mathrm{F}.$$

Démonstration. On peut sans perte de généralité supposer que P est sans carré, quitte à le remplacer par un facteur sans carré annulant f. De plus, on peut supposer que $\mathrm{P}(0,0) = 0$ (il suffit pour cela que $f(0) = 0$). En effet, si l'on écrit $f(x) = f(0) + x\tilde{f}(x)$, on remarque que si $\tilde{f} = \Delta\tilde{\mathrm{F}}$, alors $f = \Delta\{f(0) + \tilde{\mathrm{F}}\}$. Il suffit donc de montrer la proposition pour $\tilde{f}$ qui vérifie $\tilde{f}(0) = 0$.

Maintenant, si de plus $\partial_y \mathrm{P}(0,0) \neq 0$, on peut conclure directement par le lemme 86. Si au contraire $\partial_y \mathrm{P}(0,0) = 0$, on utilise le lemme 87 pour écrire

$$f(x) = r(x) + x^\alpha g(x),$$

de telle sorte que g est annulée par un polynôme Q satisfaisant les hypothèses du lemme 86. g est alors la diagonale de la fraction

$$\mathrm{G}(x,y) = y^2 \frac{\partial_y \mathrm{Q}(xy,y)}{\mathrm{Q}(xy,y)}.$$

On en déduit que f est la diagonale de la fraction rationnelle

$$\mathrm{F}(x,y) = r(xy) + (xy)^{\alpha}\mathrm{G}(x,y).$$

□

4.2 Polynôme annulateur pour une diagonale de fraction rationnelle bivariée

Jusqu'à la fin du chapitre, on se donne une fraction rationnelle $\mathrm{F} \in \mathbf{k}(x,y)$ régulière en $(0,0)$. On a vu que la diagonale de F est une série algébrique (corollaire 85). Il est alors naturel de chercher à calculer un polynôme annulateur de $\Delta\mathrm{F}$. Le point de départ est la formule

$$\Delta\mathrm{F}(t) = [y^{-1}]\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right).$$

On peut donc appliquer directement l'algorithme PolIntFRat à la fraction rationnelle $\mathrm{G}(t,y) = \mathrm{F}(t/y,y)/y$ pour obtenir un polynôme annulateur. Cependant, on peut faire mieux, en prenant en compte la structure particulière de la fraction G qui et obtenue à partir du changement de variables $x \mapsto t/y$ dans F. Dans le paragraphe suivant, on va prédire la forme de G, ce qui permet dans certains cas de prédire une factorisation du polynôme qui serait calculé par l'algorithme PolIntFRat. Ceci conduit à une variante de cet algorithme qui calcule directement le facteur qui nous intéresse.

4.2.1 Effet du changement de variables

Pour suivre l'impact du changement de variables $x \mapsto t/y$ sur un polynôme, on introduit la notion de degré diagonal.

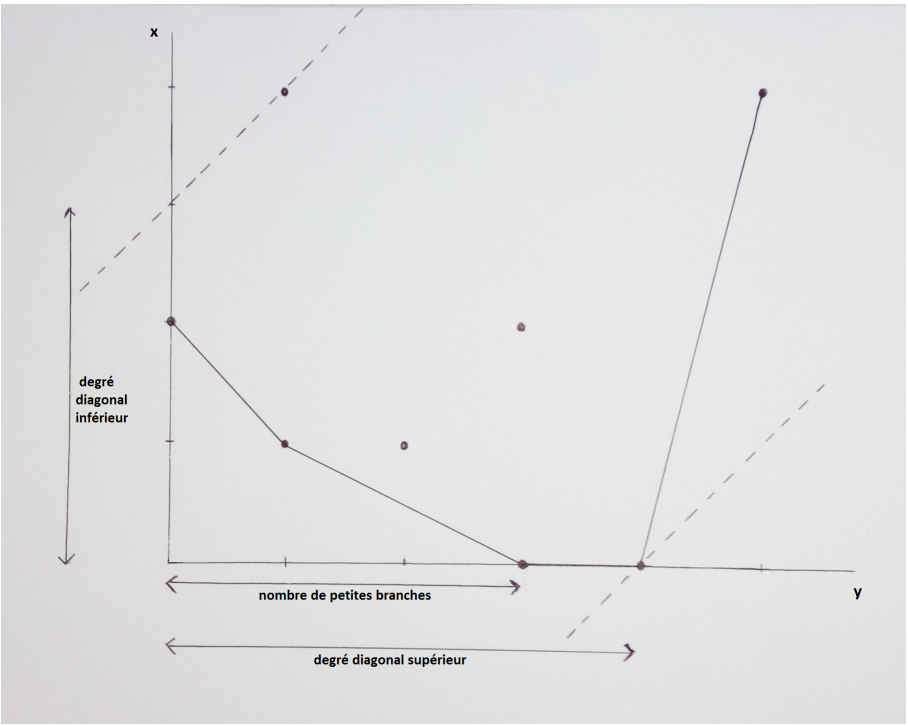
Définition 90. Soit $\mathrm{P} \in \mathbf{k}[x,y]$ un polynôme, que l'on écrit

$$\mathrm{P}(x,y) = \sum_{i,j} a_{i,j} x^i y^j.$$

On définit le *degré diagonal inférieur* et le *degré diagonal supérieur* de P, respectivement notés $\mathrm{ddeg}^-(\mathrm{P})$ et $\mathrm{ddeg}^+(\mathrm{P})$ par

$$\begin{aligned} \mathrm{ddeg}^-(\mathrm{P}) &= \sup\{i-j \mid a_{i,j} \neq 0\} \\ \mathrm{ddeg}^+(\mathrm{P}) &= \sup\{j-i \mid a_{i,j} \neq 0\} \end{aligned} \tag{4.3}$$

Plus concrètement, comme illustré dans le dessin ci-dessous, le degré diagonal inférieur d'un polynôme peut se lire sur son polygone de Newton de la façon suivante : on fait descendre une droite de pente 1 depuis l'infini jusqu'à rencontrer un point du support des coefficients du polynôme. Le degré diagonal inférieur est l'ordonnée à l'origine de cette droite. Le degré diagonal supérieur est obtenu en faisant monter une droite de pente 1 depuis l'infini jusqu'à rencontrer le support du polynôme, et en lisant l'abscisse du point d'intersection de cette droite avec l'axe horizontal.



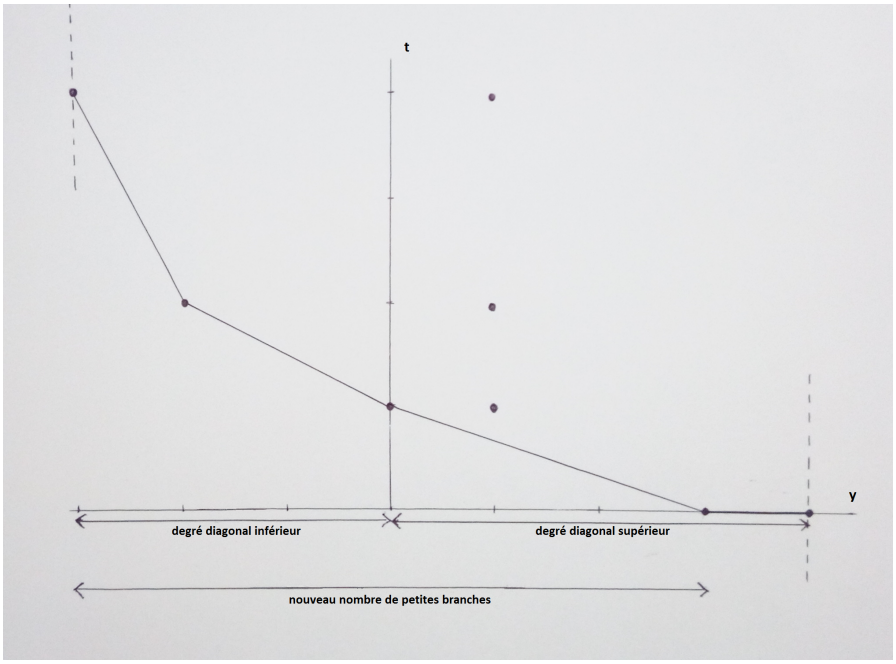
Lecture du degré diagonal d'un polynôme sur son polygone de Newton

La proposition suivante rassemble les propriétés importantes du degré diagonal dans notre contexte. (On rappelle que la notation $(\cdot)^\star$ désigne la prise de partie sans carré.)

Lemme 91. *Pour tous polynômes* $P, Q \in \mathbb{K}[x,y]$,

1. $\mathrm{ddeg}^-(P) \leqslant \deg_x P$ *et* $\mathrm{ddeg}^+(P) \leqslant \deg_y P$ *;*
2. $\mathrm{ddeg}^\pm(PQ) = \mathrm{ddeg}^\pm(P) + \mathrm{ddeg}^\pm(Q)$ *;*
3. *il existe un polynôme* $\tilde{P} \in \mathbb{K}[t,y]$ *tel que* $P(t/y, y) = y^{-\mathrm{ddeg}^-(P)}\tilde{P}(t,y)$, *avec* $\tilde{P}(t,0) \neq 0$ *et*
$$\mathrm{bideg}_{t,y}(\tilde{P}) = (\deg_x P, \mathrm{ddeg}^-(P) + \mathrm{ddeg}^+(P)) \ ;$$
4. $\mathrm{bideg}_{t,y}((\tilde{P})^\star) = (\deg_x P^\star, \mathrm{ddeg}^-(P^\star) + \mathrm{ddeg}^+(P^\star))$.

Avant de démontrer ce lemme, illustrons ce résultat en appliquant le changement de variable $x \mapsto t/y$ au polynôme dont le polygone de Newton était dessiné dans l'illustration précédente. Sur l'image ci-dessous, on constate notamment que le point de coordonnées (i, j) est envoyé sur le point $(i, j-i)$. En particulier, le degré diagonal inférieur et supérieur donnent la valuation et le degré en y du polynôme de Laurent obtenu par ce changement de variable.



Polygone de Newton après le changement de variable $x \mapsto t/y$

Démonstration. Le *(1)* est immédiat. Les quantités $\mathrm{ddeg}^-(\mathrm{P})$ et $\mathrm{ddeg}^+(\mathrm{P})$ ne sont autres que $-\mathrm{val}_y \mathrm{P}(t/y, y)$ et $\deg_y \mathrm{P}(t/y, y)$, ce qui rend limpides le *(2)* et le *(3)*. De là, on obtient l'égalité $\widetilde{\mathrm{PQ}} = \tilde{\mathrm{P}}\tilde{\mathrm{Q}}$ pour P et Q quelconques, d'où $(\tilde{\mathrm{P}})^\star = \widetilde{\mathrm{P}^\star}$. Le *(4)* est alors une conséquence de *(1)* et *(3)*. □

Par ailleurs, pour utiliser l'algorithme SommeCompPure de la section 3.2, on a également besoin de connaître le nombre de petites branches du dénominateur après le changement de variables. Comme on l'a déjà rappelé, le nombre de petites branches d'un polynôme est exactement la largeur totale des pentes strictement négatives dans son polygone de Newton. Dans le lemme suivant, on note Nsmall(P) le nombre de petites branches d'un polynôme P.

Lemme 92. *Soit* $\mathrm{P} \in \mathbf{k}[x, y]$ *un polynôme tel que* $\mathrm{P}(0, y) \neq 0$. *Alors*

$$\mathrm{Nsmall}\left(y^{\mathrm{ddeg}^-(\mathrm{P})}\mathrm{P}(t/y, y)\right) = \mathrm{Nsmall}(\mathrm{P}^\star) + \mathrm{ddeg}^-(\mathrm{P}^\star).$$

Démonstration. Écrivons $\mathrm{P}(x, y) = \sum_{i,j} a_{i,j} x^i y^j$. On a déjà vu que le changement de variables $x \mapsto t/y$ change les coordonnées du point correspondant à $a_{i,j}$ en

$(i, j-i)$. Cette transformation envoie les sommets du polygone de Newton de P sur les sommets du polygone de Newton du polynôme de Laurent $\mathrm{P}(t/y, y)$. De plus, l'hypothèse $\mathrm{P}(0, y) \neq 0$ fait que le point le plus à droite de la partie de pente strictement négative du polygone de Newton est invariant par la transformation (puisque sur l'axe des abscisses). Ainsi, la largeur des pentes négatives est augmentée exactement de $\mathrm{ddeg}^-(\mathrm{P})$ (voir le dessin ci-dessus). La multiplication par $y^{\mathrm{ddeg}^-(\mathrm{P})}$, ne fait qu'une translation du polygone, le résultat est donc démontré. □

On peut maintenant utiliser les deux lemmes précédents pour prévoir la forme de la fraction rationnelle $\mathrm{G}(t, y)$.

Proposition 93. *Soient* $\mathrm{A}, \mathrm{B} \in \mathbf{k}[x, y]_{d_x, d_y}$ *deux polynômes premiers entre eux et tels que* $\mathrm{B}(0,0) \neq 0$. *Soit* $(d_x^\star, d_y^\star)$ *une borne sur le bidegré de la partie sans carré de* B. *Notons* $\mathrm{F} = \mathrm{A}/\mathrm{B}$ *et*

$$\mathrm{G}(t, y) = \frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right).$$

Alors il existe des polynômes $\mathrm{P}, \mathrm{Q} \in \mathbf{k}[t, y]$ *tels que*

$$\mathrm{G}(t, y) = y^\alpha \frac{\mathrm{P}(t, y)}{\mathrm{Q}(t, y)},$$

où

$$\begin{gathered} \alpha = \mathrm{ddeg}^-(\mathrm{B}) - \mathrm{ddeg}^-(\mathrm{A}) - 1, \qquad (4.4) \\ \mathrm{bideg}\,\mathrm{P} \leqslant (d_x, \mathrm{ddeg}^-(\mathrm{A}) + \mathrm{ddeg}^+(\mathrm{A})), \quad \mathrm{bideg}\,\mathrm{Q} \leqslant (d_x, \mathrm{ddeg}^-(\mathrm{B}) + \mathrm{ddeg}^+(\mathrm{B})), \\ \mathrm{bideg}\,\mathrm{Q}^\star = (d_x^\star, \mathrm{ddeg}^-(\mathrm{B}^\star) + \mathrm{ddeg}^+(\mathrm{B}^\star)), \\ \mathrm{Nsmall}(\mathrm{Q}) = \mathrm{ddeg}^-(\mathrm{B}^\star). \end{gathered}$$

Démonstration. C'est une application directe des lemmes 91 et 92, en prenant pour P et Q les polynômes $\tilde{\mathrm{A}}$ et $\tilde{\mathrm{B}}$. Pour le nombre de petites branches, on utilise en plus le fait que comme $\mathrm{B}(0,0) \neq 0$, $\mathrm{Nsmall}(\mathrm{B}^\star) = 0$ (son polygone de Newton n'a que des pentes positives). □

4.2.2 Algorithme

On garde les mêmes notations que dans la proposition précédente, et on revient au calcul d'un polynôme annulateur pour $\Delta\mathrm{F}$. Il y a une légère différence entre les cas $\alpha \geqslant 0$ et $\alpha < 0$: dans le second cas le dénominateur admet 0 comme petite branche supplémentaire. Notons $r \in \mathbf{k}(t)$ le résidu de G en 0 si $\alpha < 0$, et $r = 0$ si $\alpha \geqslant 0$. Alors la formule de la proposition 84 se récrit

$$\Delta\mathrm{F}(t) = r(t) + \tilde{f}(t),$$

où, en notant $c = \mathrm{Nsmall}(\mathrm{Q})$ et $y_1, y_2, \ldots, y_c$ les petites branches de Q,

$$\tilde{f}(t) = \sum_{i=1}^{c} \mathrm{Res}\left(\mathrm{G}, y_i\right).$$

Algorithme **PolynômeDiagonale**(A/B)

Entrée Deux polynômes $A, B \in \mathbf{k}[x, y]$, avec $B(0,0) \neq 0$

Sortie Un polynôme $\Phi \in \mathbf{k}[t, y]$ tel que $\Phi(t, \Delta\{A/B\}) = 0$

$P, Q, \alpha \leftarrow y^{\mathrm{ddeg}^-(A)} A(\frac{t}{y}, y),\ y^{\mathrm{ddeg}^-(B)} B(\frac{t}{y}, y),\ \mathrm{ddeg}^-(B) - \mathrm{ddeg}^-(A) - 1$;
si $\alpha < 0$ **alors**
  $r \leftarrow$ **PolynômeRésidus**$(P / y^{-\alpha} Q, y)$;
  $R \leftarrow$ **PolynômeRésidus**$(P / y^{-\alpha} Q, Q)$;
sinon
  $R \leftarrow$ **PolynômeRésidus**$(y^{\alpha} P / Q, Q)$;
$c \leftarrow$ nombre de petites branches de Q ;
$\Phi(t, y) \leftarrow \mathrm{numer}($**SommeCompPure**$(R, c))$;
si $\alpha < 0$ **alors**
  $\Phi(t, y) \leftarrow \mathrm{numer}(\Phi(t, y - r))$;
renvoyer $\Phi(t, y)$

Algorithme 9: Polynôme annulant la diagonale d'une fraction rationnelle. La notation ddeg est définie dans l'équation (4.3) p. 82

Ainsi, pour obtenir un polynôme Φ annulant ΔF, on commence par calculer un polynôme R annulant les $\mathrm{Res}(G, y_i)$ en appliquant l'algorithme PolynômeRésidus p. 65 à $((y^{\alpha} P)/Q, Q)$ si $\alpha \geqslant 0$, et à $(P/y^{-\alpha} Q), Q)$ dans le cas contraire. On obtient ensuite un polynôme $\tilde{\Phi}$ annulant $\tilde{f}$ en appliquant l'algorithme SommeCompPure à (R, c). On en déduit que le polynôme $\Phi(t, y) = \tilde{\Phi}(t, y - r(t))$ annule ΔF.

Cette méthode est implémentée par l'algorithme PolynômeDiagonale (algorithme 9).

Exemple 94. Soit d un entier positif, et soit $F_d \in \mathbb{Q}(x, y)$ la fraction rationnelle définie par

$$F_d(x, y) = \frac{1}{(1 - x - y)^{d+1}}.$$

Sur cet exemple simple, on peut calculer explicitement la diagonale par un développement direct :

$$\Delta F_d(t) = \sum_{n \geqslant 0} \binom{2n + d}{n} \binom{n + d}{d} t^n.$$

D'après le lemme 82 et le corollaire 85, c'est une série algébrique qui est égale à la somme des résidus de la fraction rationnelle G_d de l'exemple 65 à ses petites branches (avec x remplacé par t). Ici, comme le dénominateur est $y - t - y^2$, il n'a qu'une seule petite branche. La diagonale ΔF_d est donc annulée par le polynôme

$$(1 - 4t)^{2d+1} y^2 - \left(\sum_{k=0}^{\lfloor d/2 \rfloor} \binom{d}{2k} \binom{2k}{k} x^k \right)^2.$$

Exemple 95. Soit d un entier strictement positif, et soit $\mathrm{F}_d \in \mathbb{Q}(x,y)$ la fraction rationnelle définie par

$$\mathrm{F}_d(x,y) = \frac{x^{d-1}}{1-x^d-y^{d+1}}$$

C'est une fraction de bidegré $(d,d+1)$. La première étape de l'algorithme 9 produit

$$\mathrm{G}_d(t,y) = y^\alpha \frac{\mathrm{P}}{\mathrm{Q}} = \frac{t^{d-1}}{y^d - t^d - y^{2d+1}},$$

qui est de bidegré $(d,2d+1)$, et dont le dénominateur est irréductible et possède d petites branches. De là, l'algorithme calcule des polynômes Φ_d annulant $\Delta\mathrm{F}_d$. Expérimentalement, ces polynômes sont irréductibles et leurs bidegrés pour $d = 1,2,3,4$ sont $(2,3)$, $(18,10)$, $(120,35)$, $(700,126)$.

À partir de ces valeurs, il est facile de conjecturer que le bidegré est donné par

$$\left(d(d+1)\binom{2d-1}{d-1}, \binom{2d+1}{d}\right),$$

ce qui met en évidence une croissance exponentielle en d. Nous allons voir avec le théorème 97 que, dans le cas général, la croissance du bidegré est au plus du même ordre de grandeur que dans cet exemple.

Exemple 96. Cet exemple est tiré d'une solution trouvée avec Bostan et Lairez à un exercice proposé dans l'American Mathematical Monthly par Gessel[5]. La question est de prouver l'égalité :

$$[x^n y^n] \frac{1}{(1-3y)(1-x-3y+3y^2)} = 9^n. \tag{4.5}$$

On remarque immédiatement que le membre de gauche est le n-ième coefficient de la diagonale de la fraction

$$\mathrm{F}(x,y) = \frac{1}{(1-3y)(1-x-3y+3y^2)}.$$

On peut donc appliquer l'algorithme PolynômeDiagonale à F, ce qui produit un polynôme annulateur pour $\Delta\mathrm{F}(t)$:

$$(9t-1)^3((1-9t)y+3)((1-9t)y-1)^3.$$

On en déduit que

$$\Delta\mathrm{F}(t) = -\frac{3}{1-9t}, \text{ ou bien } \Delta\mathrm{F}(t) = \frac{1}{1-9t}.$$

Mais comme il est évident que $\Delta\mathrm{F}(0) = 1$, la seule possibilité est

$$\Delta\mathrm{F}(t) = \frac{1}{1-9t},$$

5. "Problems and Solutions". Dans : *The American Mathematical Monthly* 123 (4) (avr. 2016), p. 399–406.

ce qui est équivalent à l'équation (4.5).

Il se trouve que pour cet exemple, on peut retrouver le résultat à la main. En effet, le changement de variable $x \mapsto t/y$ donne ici :

$$\Delta F(t) = [y^{-1}] \frac{1}{(1-3y)(y-3y^2+3y^3-t)}$$

(c'est le lemme 82). Le dénominateur de cette fraction a une forme très particulière : le polynôme

$$P(t,y) = y - 3y^2 + 3y^3 - t$$

admet une unique racine f telle que $f(0) = 0$, qui n'est autre que l'inverse du polynôme $y - 3y^2 + 3y^3$ pour la composition des séries. Ceci se voit également sur le polygone de Newton de P. Maintenant, on sait par la proposition 84 que

$$\Delta F = \mathrm{Res}\left(\frac{1}{(1-3y)P(t,y)}, f\right).$$

Comme f est un pôle simple, un calcul classique (voir aussi la remarque sous le corollaire 64) donne :

$$\mathrm{Res}\left(\frac{1}{(1-3y)P(t,y)}, f\right) = \frac{1}{\partial_y\{(1-3y)P\}(t,f)} = \frac{1}{(1-3f)\partial_y P(t,f)} = \frac{1}{1-9f+27f^2-27f^3},$$

et comme $f - 3f^2 + 3f^3 = t$, on en déduit à nouveau que

$$\Delta F(t) = \frac{1}{1-9t}.$$

4.2.3 Bornes

On dispose déjà de tous les outils nécessaires pour analyser l'algorithme PolynômeDiagonale. L'étape du changement de variables a été analysée dans le paragraphe 4.2.1, et les algorithmes PolynômeRésidus et SommeCompPure ont été analysés dans le chapitre précédent.

Théorème 97. *Soient* $A, B \in \mathbf{k}[x,y]_{d_x,d_y}$ *des polynômes premiers entre eux tels que* $B(0,0) \neq 0$. *Soit* $B^\star$ *la partie sans carré de* B, *de bidegré majoré par* $(d_x^\star, d_y^\star)$. *Alors le polynôme* $\Phi(t,y)$ *calculé par l'appel* PolynômeDiagonale(A/B) *vérifie*

$$\deg_t \Phi \leqslant D_x \begin{pmatrix} D_y \\ c \end{pmatrix}, \quad \deg_y \Phi = \begin{pmatrix} D_y \\ c \end{pmatrix},$$

où

$$c = \mathrm{ddeg}^-(B^\star),$$
$$D_x = 2d_x(d_x+d_y+1) + d_x - 2(d_x - d_x^\star)(d_x - d_x^\star + d_y - d_y^\star + 1),$$
$$D_y := \mathrm{ddeg}^-(B^\star) + \mathrm{ddeg}^+(B^\star).$$

Démonstration. D'après le théorème 69, quel que soit le signe de α l'appel à PolynômeRésidus produit un polynôme de degré

$$\mathrm{D}_y := \mathrm{ddeg}^-(\mathrm{B}^\star) + \mathrm{ddeg}^+(\mathrm{B}^\star). \tag{4.6}$$

Puis, par le théorème 77, on en déduit que

$$\deg_y \Phi = \binom{\mathrm{D}_y}{c}.$$

Pour majorer le degré de Φ en t, on peut ignorer l'optimisation qui consiste à prendre en compte la petite branche en 0 et appliquer l'algorithme PolynômeRésidus à $(y^\alpha \mathrm{P}, \mathrm{Q}, \mathrm{Q})$ ou $(\mathrm{P}, y^{-\alpha}\mathrm{Q}, y^{-\alpha}\mathrm{Q})$ selon que $\alpha \geqslant 0$ ou $\alpha < 0$. En effet, le polynôme obtenu de cette façon est clairement un multiple de celui calculé par l'algorithme. Par le théorème 69, comme les bidegrés de P, y^αP, Q et $y^{-\alpha}$Q sont tous majorés par $(d_x, d_x + d_y + 1)$, on calcule un polynôme R de degré en x majoré par D_x. Ensuite, on fait appel au théorème 77 appliqué à (R, c) ou $(\mathrm{R}, c+1)$ selon le signe de α. Dans les deux cas, on obtient

$$\deg_y \Phi = \binom{\mathrm{D}_y}{c}.$$

□

4.2.4 Complexité

Théorème 98. *On reprend les notations du théorème 97. Alors l'appel* PolynômeDiagonale(A/B) *est effectué en*

$$\tilde{\mathrm{O}}\left(c\mathrm{D}_x\binom{\mathrm{D}_y}{c}^2 + (d_x + d_y)^6\right)$$

opérations dans **k**.

Démonstration. Le calcul de P et Q ne nécessite aucune opération. Ensuite, d'après la remarque 71, le calcul de R et r se fait en $\tilde{\mathrm{O}}((d_x + d_y)^6)$ opérations. Le nombre de petits pôles est obtenu gratuitement à partir de la décomposition sans carré calculée par l'algorithme PolynômeRésidus. De là, comme le degré en x de R est borné par D_x (voir la preuve du théorème 97), le théorème 78 montre que l'appel à l'algorithme SommeCompPure coûte $\tilde{\mathrm{O}}(c\mathrm{D}_x\binom{\mathrm{D}_y}{c}^2)$ opérations. Enfin, si une translation de la variable est requise, elle peut être effectuée par évaluation et interpolation en $\tilde{\mathrm{O}}(\mathrm{D}_x\binom{\mathrm{D}_y}{c}^2)$ opérations. (On pourrait également évaluer et interpoler par rapport à x et utiliser de meilleurs algorithmes pour la translation univariée[6].) □

6. BOSTAN, FLAJOLET et al., "Fast Computation of Special Resultants", §5.

4.3 Degré du polynôme minimal dans le cas générique

La borne du théorème 97 sur le bidegré de Φ est légèrement pessimiste en t, mais génériquement atteinte en y. Cette dernière affirmation fait l'objet de la proposition 100 ci-dessous. On commence tout d'abord par démontrer un lemme de théorie de Galois, dans lequel on utilise la notation $\mathfrak{S}_n$ pour désigner le groupe symétrique de degré n.

Lemme 99. *Soit $\mathbb{K}$ un corps de caractéristique 0, et $p \in \mathbb{K}[y]$ un polynôme de degré d, dont le groupe de Galois sur $\mathbb{K}$ est $\mathfrak{S}_d$. On suppose que les racines $\alpha_1, \ldots, \alpha_d$ de p dans $\overline{\mathbb{K}}$ sont algébriquement indépendantes sur $\mathbb{Q}$. Alors, pour tout $c \leqslant d$, le polynôme $\Sigma_c p$ de degré $\binom{d}{c}$ est irréductible sur $\mathbb{K}$.*

($\Sigma_c p$ a été défini dans le paragraphe 3.2.2.)

Démonstration. Comme $\Sigma = \alpha_1 + \cdots + \alpha_c$ est une racine de $\Sigma_c p$, il suffit de montrer que le degré de $\mathbb{K}(\Sigma)$ sur $\mathbb{K}$ vaut $\binom{d}{c}$. Les α_i étant algébriquement indépendants sur $\mathbb{Q}$, toute permutation $\sigma \in \mathfrak{S}_d$ des α_i par laquelle Σ est invariant doit également fixer les ensembles $\{\alpha_1, \ldots, \alpha_c\}$ et $\{\alpha_{c+1}, \ldots, \alpha_d\}$. Réciproquement, toute permutation ayant cette propriété induit un automorphisme de $\mathbb{K}(\alpha_1, \ldots, \alpha_d)$ par lequel Σ est invariant. En d'autres termes, le groupe de Galois de $\mathbb{K}(\alpha_1, \ldots, \alpha_d)$ sur $\mathbb{K}(\Sigma)$ est égal à $\mathfrak{S}_c \times \mathfrak{S}_{d-c}$. On en déduit que $\mathbb{K}(\alpha_1, \ldots, \alpha_d)$ a un degré $c!(d-c)!$ sur $\mathbb{K}(\Sigma)$ et $d!$ sur $\mathbb{K}$, de telle sorte que $\mathbb{K}(\Sigma)$ a un degré $\binom{d}{c}$ sur $\mathbb{K}$. □

Proposition 100. *Soit $A \in \mathbb{Q}[x, y]$ un polynôme. Soient d_x et d_y des entiers positifs, $s^- \leqslant d_x$, $s^+ \leqslant d_y$, et*

$$B(x, y) = \sum_{i=0}^{s^-} b_i^{(x)} x^i + \sum_{j=1}^{s^+} b_j^{(y)} y^j + \sum_{\substack{i \leqslant d_x, j \leqslant d_y \\ -s^- \leqslant j-i \leqslant s^+}} b_{i,j} x^i y^j \in \mathbb{Q}[(b_i^{(x)}), (b_j^{(y)}), x, y],$$

où les $b_i^{(x)}$ et $b_j^{(y)}$ sont des indéterminées et $b_{i,j} \in \mathbb{Q}$.

Alors le polynôme $\Phi(t, y)$ calculé par l'appel PolynômeDiagonale(A/B) *est irréductible de degré $\binom{s^- + s^+}{s^-}$ sur $\mathbb{K} = \mathbb{Q}[(b_i^{(x)}), (b_j^{(y)}), t, y]$.*

Démonstration. On reprend les notations de l'algorithme PolynômeDiagonale. D'après sa définition dans l'algorithme, le polynôme Q vaut

$$Q(t, y) = \sum_{i=0}^{s^-} b_i^{(x)} t^i y^{s^- - i} + \sum_{j=1}^{s^+} b_j^{(y)} y^{s^- + j} + \sum_{i,j} b_{i,j} t^i y^{s^- - i + j}.$$

Notons $d = s^- + s^+$. Alors le polynôme $Q(1, y)$ a la forme $\sum_{j \leqslant d} t_j y^j$ où chacun des t_j est la somme de l'une des indéterminées et de nombres rationnels. Ceci implique que les t_j sont algébriquement indépendants sur $\mathbb{Q}$. Donc $Q(1, y)$ admet $\mathfrak{S}_d$ pour groupe de Galois sur $\mathbb{Q}(t_0, \ldots, t_d)$ et ses racines sont algébriquement indépendantes

sur $\mathbb{Q}$ [7]. Cette propriété s'étend à $\mathrm{Q}(t,y)$ [8], qui a donc $\mathfrak{S}_d$ comme groupe de Galois et des racines algébriquement indépendantes, notées $y_1,\dots,y_d$.

Maintenant, on définit le polynôme $\mathrm{R}(t,y) = \prod_i (y - \tilde{\mathrm{P}}(t,y_i)/\partial_y \mathrm{Q}(t,y_i))$, où $\tilde{\mathrm{P}} = y^\alpha \mathrm{P}$ si $\alpha \geqslant 0$ et $\tilde{\mathrm{P}} = \mathrm{P}$ sinon. Comme toutes les racines de Q sont simples, R est exactement le polynôme calculé par l'algorithme PolynômeRésidus. Alors la famille $\{\mathrm{P}(t,y_i)/\partial_y \mathrm{Q}(t,y_i)\}$ est algébriquement indépendante sur $\mathbb{Q}$, puisque toute relation algébrique entre ses éléments en induirait également une pour les y_i en réduisant au même dénominateur. En particulier, le morphisme naturel $\mathrm{Gal}(\mathrm{Q}/\mathbb{K}) = \mathfrak{S}_d \to \mathrm{Gal}(\mathrm{R}/\mathbb{K})$ est injectif, et donc un isomorphisme. (Ici, on note $\mathrm{Gal}(\mathrm{P}/\mathbb{K})$ le groupe de Galois sur $\mathbb{K}$ de $\mathrm{P} \in \mathbb{K}[y]$.) Comme une simple inspection du polygone de Newton de Q montre qu'il a s^- petites branches, on peut conclure en utilisant le lemme 99 et le fait qu'une translation de la variable ne change en rien l'irréductibilité de Φ. □

La proposition 100 doit être comprise comme un résultat d'optimalité. En effet, pour une fraction rationnelle A/B générique, comme dans la proposition, on a $\mathrm{B} = \mathrm{B}^\star$, $\mathrm{ddeg}^-(\mathrm{B}) = s^-$, $\mathrm{ddeg}^+(\mathrm{B}) = s^+$ et B a s^- petites branches. Ceci montre que la borne du théorème 97 est optimale dans ce cas (générique).

Si l'on croit au fait que les exemples aléatoires devraient se comporter comme le cas générique, alors la proposition 100 met en évidence que le polynôme calculé par l'algorithme 9 sera irréductible la plupart du temps.

À titre d'exemple, on considère le cas particulier de la proposition 100 où $s^- = s^+ = d_x = d_y = d$. On a alors $\deg_y \Phi = \binom{2d}{d}$.

Exemple 101. Illustrons ce résultat davantage en observant le degré du polynôme minimal sur des diagonales de fractions rationnelles tirées au hasard. On considère une fraction rationnelle $\mathrm{F}(x,y) = 1/\mathrm{B}(x,y)$, où $\mathrm{B}(x,y)$ est un polynôme dense de bidegré (d,d) choisi au hasard. Pour $d = 1,2,3,4$, la sortie de l'algorithme 9 est irréductible de bidegré $(2,2)$, $(16,6)$, $(108,20)$, $(640,70)$. Ces valeurs correspondent à la formule

$$\left(2d^2\binom{2d-2}{d-1}, \binom{2d}{d}\right). \tag{4.7}$$

On constate donc que la borne sur $\deg_y \Phi$ est fine dans ce cas, et l'irréductibilité de la sortie indique que la proposition 100 ne peut être améliorée.

7. WAERDEN, *Modern Algebra*, §57.
8. Ibid., §61.

Chapitre 5

Développement des séries génératrices des marches unidimensionnelles

Informellement, une marche est une suite de déplacements élémentaires effectués dans un ensemble (par exemple sur une grille). L'étude combinatoire des marches est un sujet très riche, qui touche à de nombreux domaines des mathématiques (combinatoire des mots, physique statistique, probabilités, dénombrements, ...) et qui peut-être abordé avec des points de vue variés. C'est un domaine où les méthodes de calcul formel ont connu un certain succès, certes en offrant la possibilité d'expérimenter par le calcul, mais aussi dans certains cas comme outil de preuve. C'est ainsi par exemple qu'une conjecture de Gessel sur une famille particulière de marches dans le plan a été prouvée rigoureusement à l'aide de l'ordinateur en 2009 [1], alors que la première preuve « humaine » n'est apparue que très récemment, en 2016 [2]. Ici, je vais m'intéresser à un problème d'ordre calculatoire sur les marches unidimensionnelles. Dans l'exemple 24 p. 35, nous étions parvenus à calculer les valeurs d'une suite de probabilités b_n. Il se trouve que les nombres b_n sont liés au comptage d'une famille de marches unidimensionnelles, et on aimerait généraliser ce type de dénombrement à d'autres familles de marches. Ce problème a déjà été abordé par Banderier et Flajolet [3]. Après avoir discuté les avantages et inconvénients de leur méthode, je vais présenter une nouvelle méthode pour compter les marches unidimensionnelles. Sans plus attendre, définissons plus précisément les marches à étudier et le vocabulaire associé.

1. KAUERS, KOUTSCHAN et ZEILBERGER, "Proof of Ira Gessel's Lattice Path Conjecture".
2. BOSTAN, KURKOVA et RASCHEL, "A human proof of Gessel's lattice path conjecture".
3. BANDERIER et FLAJOLET, "Basic Analytic Combinatorics of Directed Lattice Paths".

5.1 Définitions et énoncé du problème

Définition 102.

1. On appelle *pas* tout vecteur de la forme $(1, u)$, avec $u \in \mathbb{Z}$.

2. Si S est un ensemble fini de pas, une S-*marche* est une suite $(A_0, A_1, \ldots, A_n)$ de points de $\mathbb{Z}^2$ telle que

   · $A_0 = (0,0)$;

   · $\overrightarrow{A_{k-1}A_k}$ est un pas appartenant à S.

   n est alors la *longueur* de la marche. Pour tout $k \geqslant 0$, l'ordonnée de A_k est l'*altitude* de la marche au temps k. L'altitude au temps n est appelée l'*altitude finale* de la marche.

3. Si S est un ensemble fini de pas, on définit le *polynôme caractéristique* de S, noté χ_S par

$$\chi_S(y) = \sum_{(1,u)\in S} y^u.$$

Remarquons que les marches qui viennent d'être définies, bien qu'évoluant dans la grille $\mathbb{Z}^2$, sont essentiellement unidimensionnelles. En effet, on peut les voir comme des marches sur $\mathbb{Z}$, l'axe vertical, alors que l'axe horizontal ne sert qu'à représenter le temps qui augmente de 1 à chaque pas.

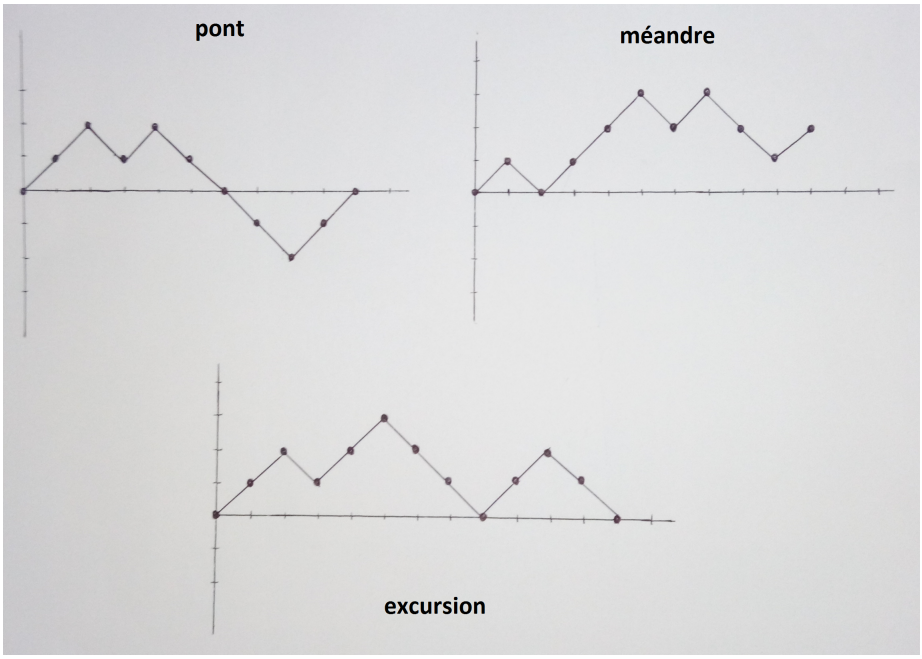
À l'instar de Banderier et Flajolet, nous considérons trois familles particulières de marches, illustrées dans le dessin ci-dessous.

Définition 103. Soit S un ensemble de pas, et soit $\mathscr{M}$ une S-marche. On dit que $\mathscr{M}$ est

1. un *pont* si son altitude finale est 0 ;

2. un *méandre* si son altitude est positive après chaque pas ;

3. une *excursion* si c'est à la fois un pont et un méandre.



Les trois familles de marches ($S = \{-1, 1\}$)

Définition 104. Soit S un ensemble fini de pas.

1. On note $W_S \in \mathbb{Q}[[x, y]]$ la série génératrice des S-marches indexées par leur longueur et leur altitude finale, c'est-à-dire

$$W_S(x, y) = \sum_{n,k \geqslant 0} w_{n,k} x^n y^k,$$

où $w_{n,k}$ est le nombre de marches de longueur n ayant pour altitude finale k.

2. On note $B_S \in \mathbb{Q}[[x]]$ (resp. E_S, M_S) la série génératrice des ponts (resp. excursions, méandres) indexés par leur longueur, c'est-à-dire

$$B_S(x) = \sum_{n \geqslant 0} b_n x^n,$$

où b_n est le nombre de ponts de longueur n. (Idem pour les excursions et les méandres.)

Lorsque le contexte sera clair, on omettra de préciser l'ensemble S de pas en indice.

Exemple 105. (1) L'exemple intéressant le plus simple est $S = \{-1, 1\}$. Les S-excursions ne sont autres que les chemins de Dyck, bien-connus en combinatoire. Les chemins de Dyck sont en bijection avec les mots bien parenthésés sur l'alphabet $\{(,)\}$: on peut voir tous les pas 1 comme des parenthèses ouvrantes et les pas -1

comme des parenthèses fermantes. La condition de positivité des excursions traduit le fait que le nombre de parenthèses ouvrantes doit être plus grand que le nombre de parenthèses fermantes dans tout préfixe.

(2) Si $\mathrm{S} = \{-1, 0, 1\}$, les S-marches sont exactement les déroulements possibles d'un scrutin à deux candidats (exemple 24). En effet, les pas 1 et -1 correspondent aux votes respectifs pour les deux candidats, tandis que les pas 0 correspondent aux votes blancs. L'altitude finale mesure alors le score de l'élection. Ainsi, les S-ponts sont les déroulements qui se terminent par une égalité.

On rappelle maintenant quelques résultats classiques sur les séries génératrices des diverses familles de marches unidimensionnelles.

Proposition 106. *Les séries* W, B, E *et* M *vérifient les propriétés suivantes :*

1. $\mathrm{W}(x, y)$ *est une série rationnelle. Explicitement :*
$$\mathrm{W}(x, y) = \frac{1}{1 - x\chi(y)}.$$
2. $\mathrm{B}(x)$, $\mathrm{E}(x)$ *et* $\mathrm{M}(x)$ *sont des séries algébriques.*
3. $\mathrm{B}(x) = [y^0]\mathrm{W}(x, y)$.
4. $$\mathrm{E}(x) = \exp\left(\int \frac{\mathrm{B}(x) - 1}{x}\,\mathrm{d}x\right).$$

Démonstration. Ces résultats sont tous prouvés chez Banderier et Flajolet[4]. □

5.2 Calcul des séries génératrices

À partir de maintenant, on fixe un ensemble fini de pas S. On note u^- (resp. u^+) le plus grand entier $u \in \mathbb{Z}$ tel que $(1, -u) \in \mathrm{S}$ (resp. $(1, u) \in \mathrm{S}$). On définit également $d = u^+ + u^-$. L'entier d mesure l'amplitude verticale de S ; ceci fait de d une bonne échelle pour la complexité des algorithmes à venir. On supposera de plus que u^+ et u^- sont tous les deux strictement positifs, car dans le cas contraire l'étude des ponts, excursions et méandres devient triviale. (Par exemple si $u^- < 0$, alors il n'y a ni ponts ni excursions, et toutes les marches sont des méandres.)

La question à laquelle nous souhaitons répondre est la suivante :

Problème 107. *Soit* N *un entier naturel. Calculer en bonne complexité les* $\mathrm{N} + 1$ *premiers termes de la suite* (u_n)*, où* u_n *est le nombre de ponts (resp. excursions, méandres) de longueur* n*.*

5.2.1 Méthode directe

Notons $w_{n,k}$ le nombre de marches de longueur n et d'altitude finale k. Alors la définition des marches donne directement la récurrence

$$w_{n,k} = \sum_{(1,u)\in \mathrm{S}} w_{n-1,k-u}, \tag{5.1}$$

4. BANDERIER et FLAJOLET, "Basic Analytic Combinatorics of Directed Lattice Paths", §2.1-2.2.

avec les conditions initiales $w_{n,k} = 0$ si $n < 0$, et $w_{0,0} = 1$. Si l'on note $\tilde{w}_{n,k}$ le nombre de méandres de longueur n et d'altitude finale k, alors $\tilde{w}_{n,k}$ satisfait également la récurrence (5.1), mais avec les conditions initiales supplémentaires $\tilde{w}_{n,k} = 0$ si $k < 0$. Alors les ponts (resp. excursions, méandres) sont comptés par les nombres $w_{n,0}$ (resp. $\tilde{w}_{n,0}$, $\sum_k \tilde{w}_{n,k}$).

On peut calculer ces quantités en déroulant la récurrence (5.1). Chaque utilisation de la récurrence requiert $O(d)$ opérations, et dans le pire des cas on a besoin de calculer $O(d\mathrm{N}^2)$ termes de la suite (si l'ensemble des pas est $\mathrm{S} = \{(1,1),\dots,(1,d)\}$ par exemple). Avec cette méthode, on calcule donc les N premiers termes d'une des trois séries en $O(d^2\mathrm{N}^2)$ opérations dans $\mathbb{Q}$.

Cette complexité quadratique en N n'est pas satisfaisante, et toute méthode qui repose sur le développement complet de la série génératrice $\mathrm{W}(x,y)$ sera inéluctablement quadratique en N par nature. Les deux autres méthodes que je vais présenter ont pour principal atout d'avoir une complexité linéaire ou quasi-linéaire en N. Comme il sera expliqué, cette amélioration a lieu au prix d'un pré-calcul. Lors de l'analyse de la complexité des algorithmes, ce pré-calcul doit bien sûr être pris en compte, et nous allons voir qu'il a son importance : il peut dominer la complexité si l'on ne prend pas garde.

5.2.2 En passant par une équation algébrique

On a vu dans la proposition 106 que les séries B, E, et M sont algébriques. Banderier et Flajolet [5] ont esquissé une méthode reposant sur ce fait pour effectuer le calcul des N premiers termes. Les séries E et M peuvent être exprimées comme des produits de petites branches du polynôme caractéristique χ_S (voir leur théorème [6] pour un énoncé précis). De là, une équation algébrique peut être obtenue à l'aide de l'algorithme Platypus qui calcule un polynôme annulant un produit de racines d'un polynôme donné. À partir d'une équation $\mathrm{P}(x,\mathrm{E}(x)) = 0$, on peut trouver un polynôme annulant B à l'aide de la formule $\mathrm{B} = x\mathrm{E}'/\mathrm{E} + 1$, à savoir $\mathrm{Résultant}_{\mathrm{E}}((\mathrm{B}-1)\mathrm{E}\partial_y\mathrm{P} + x\partial_x\mathrm{P}, \mathrm{P})$.

Une fois que l'on connaît un polynôme pour l'une de ces trois séries, il peut être utilisé pour calculer une récurrence linéaire à coefficients polynomiaux satisfaite par ses coefficients (voir le théorème 117 de l'annexe A et la proposition 25). La méthode directe exposée ci-dessus permet de calculer assez de conditions initiales pour dérouler la récurrence (il en faut au plus un nombre polynomial en le degré de l'équation algébrique calculée d'après la proposition 34 p. 40). Ainsi, cette approche permet de calculer les N premiers termes de B, E et M en O(N) opérations. Pour que ceci soit une amélioration par rapport à la méthode naïve, il faut que la dépendance en d de la constante dans le O() ne soit pas trop grande et que le pré-calcul ne soit pas trop coûteux.

En effet, le coût du pré-calcul d'une équation algébrique n'est pas négligeable. Bousquet-Mélou [7] a obtenu la borne $\binom{d}{u^-}$ sur le degré de l'équation pour les excursions et a montré que cette borne est génériquement atteinte. Le degré de l'équa-

5. Ibid., §2.3.
6. Ibid., Th. 1.
7. BOUSQUET-MÉLOU, "Discrete excursions", §2.1.

tion algébrique peut donc être exponentiellement grand par rapport à d. Empiriquement, on constate que les équations algébriques pour B et M peuvent elles aussi avoir un degré exponentiellement grand.

Notre première contribution est de remarquer que la situation pour les équations différentielles et les récurrences est différente : B satisfait une équation différentielle dont le degré n'est que polynomial (voir ci-dessous), alors que (empiriquement) celles de E et M peuvent avoir une taille exponentielle. Qui dit grosse équation différentielle dit grosse récurrence, ce qui entraîne une grosse constante dans la complexité du pré-calcul et dans le déroulement da la récurrence. Le théorème 111 du paragraphe suivant montre que l'on peut se contenter d'un pré-calcul de complexité polynomiale avec une nouvelle méthode, ce qui est une amélioration importante dès que d devient non-négligeable.

Exemple 108. Avec l'ensemble de pas $S = \{(1,d),(1,1),(1,-d)\}$ et $d \geqslant 2$, la série génératrice W_S vaut

$$W_S(x,y) = \frac{y^d}{y^d - x(1+y^{d+1}+y^{2d})}.$$

Les expériences mettent en évidence que le bidegré du polynôme minimal de B_S est $\left(2d\binom{2d-2}{d-1}, \binom{2d}{d}\right)$, ce qui montre bien une croissance exponentielle en d. Par ailleurs, on constate expérimentalement que B_S satisfait une équation différentielle d'ordre $2d-1$ avec des coefficients de degré d^2+3d-2 lorsque d est pair, et d^2+3d-4 si d est impair.

5.2.3 Nouvelle méthode

Je vais maintenant présenter une méthode, mise au point avec Bostan et Salvy[8] qui a une complexité quasi-linéaire en N et qui évite le pré-calcul d'une équation algébrique. Elle repose sur le fait que les coefficients constants de fractions rationnelles, comme celui du point *3* de la proposition 106, satisfont des équations différentielles de taille polynomiale en le degré de la fraction rationnelle[9]. Nous allons traiter les trois séries B, E et M au cas par cas, et les résultats seront résumés dans le théorème 111.

5.2.4 Ponts

Pour développer $B(x)$, on utilise la formule *(3)* de la proposition 106, que l'on peut réécrire :

$$B(x) = [y^{-1}]\frac{W(x,y)}{y}.$$

De plus, $W(x,y)/y$ est de la forme P/Q, où $\operatorname{bideg} Q \leqslant (1,d)$ et $\operatorname{bideg} P \leqslant (0,d-1)$. Les conditions sont réunies pour appliquer le théorème 23 : l'algorithme Hermite-Telescoping de Bostan, Chen *et al.*[10] permet de calculer un télescopeur minimal

8. Bostan, Dumont et Salvy, "Algebraic Diagonals and Walks".
9. Bostan, Chen, Chyzak et Li, "Complexity of creative telescoping for bivariate rational functions".
10. Ibid., Fig. 3.

pour P/Q d'ordre au plus d et de degré $O(d^2)$ en $\tilde{O}(d^5)$ opérations dans $\mathbb{Q}$. Ce télescopeur n'est autre que la résolvante différentielle de B que l'on peut convertir en temps quasi-optimal en une récurrence d'ordre $O(d^2)$ (proposition 25).

À ce stade, on est donc capable de calculer $B(x) \bmod x^{N+1}$ en $O(d^2N)$ dès lors que l'on connaît un nombre suffisant de conditions initiales pour lancer la récurrence. La proposition suivante donne un majorant du nombre de telles conditions initiales à calculer.

Proposition 109. *Soit* S *un ensemble fini de pas, et* $d = \max_{(1,u),(1,v)\in S} |u-v|$. *Soit* P *le polynôme minimal de* B_S, *et* L_P *sa résolvante différentielle.*

Alors l'exposant de L_P *est au plus* $O(d^3)$.

Démonstration. À la lumière de la proposition 8, la formule

$$B(x) = [y^{-1}]\frac{W(x,y)}{y}$$

implique que B est une somme de résidus de la fraction $W(x,y)/y$. Notons alors R le polynôme qui annule ces résidus calculé par l'algorithme PolynômeRésidus (p. 65), et L_R sa résolvante différentielle. Comme W a un bidegré $(1,d)$ le théorème 69 montre que le bidegré de R est au plus $(O(d),d)$.

Maintenant, comme B est annulée par $\Sigma_c R$ (voir définition 74 p. 71) pour un certain c, P est un diviseur de $\Sigma_c R$. Donc toutes les racines de P sont des sommes de racines de R, ce qui implique en particulier que toutes les solutions de L_P sont des solutions de L_R. De là, le lemme 32 et la proposition 34 donnent la majoration attendue. □

Ainsi, on peut calculer un nombre suffisant de conditions initiales par la méthode directe en $O(d^5)$ opérations dans $\mathbb{Q}$. Le coût total du pré-calcul est donc $\tilde{O}(d^5)$.

5.2.5 Excursions

Si $B(x) \bmod x^{N+1}$ est connu, il est alors possible d'en déduire $E(x) \bmod x^{N+1}$ en utilisant la formule *(4)* de la proposition 106. Développer $E(x)$ se ramène alors au calcul de l'exponentielle d'une série, ce qui peut se faire en $\tilde{O}(N)$ opérations dans $\mathbb{Q}$ par la proposition 131 de l'annexe B.

5.2.6 Méandres

De même que dans le cas des excursions, la dérivée logarithmique de $M(x)$ peut être obtenue comme un coefficient constant. Ceci fait l'objet de la proposition suivante.

Proposition 110. *Soit* S *un ensemble fini de pas. On définit la série* $A_S \in \mathbb{Q}[[x]]$ *de la façon suivante :*

$$A_S(x) = [y^{-1}]\frac{W(x,y)}{1-y}.$$

Alors la série génératrice $\mathrm{M_S}(x)$ *des méandres est reliée à* $\mathrm{A_S}(x)$ *par la formule*

$$\mathrm{M_S}(x) = \frac{\exp\left(-\int \frac{\mathrm{A_S}(x)}{x}\mathrm{d}x\right)}{1 - x\chi_{\mathrm{S}}(1)}.$$

Démonstration. Notons $y_1, y_2, \ldots, y_{u^-}$ les petites branches du polynôme $y^{u^-} - xy^{u^-}\chi(y)$. Banderier et Flajolet ont montré [11] que

$$\mathrm{M}(x) = \frac{1}{1 - x\chi(1)} \prod_{i=1}^{u^-} (1 - y_i). \tag{5.2}$$

Par ailleurs, la définition de $\mathrm{A}(x)$ et la proposition 8 donnent

$$\mathrm{A}(x) = [y^{-1}]\frac{\mathrm{W}(x,y)}{1-y}\mathrm{d}y = \sum_{i=1}^{u^-} \mathrm{Res}\left(\frac{1}{(1-y)(1-x\chi(y))}, y_i\right) = -\sum_{i=1}^{u^-} \frac{1}{(1-y_i)x\chi'(y_i)}.$$

Ensuite, en dérivant l'équation $1 - x\chi(y) = 0$ par rapport à x, on obtient

$$-x\chi'(y_i) = \frac{1}{xy_i'},$$

et donc

$$\mathrm{A}(x) = x\sum_{i=1}^{u^-} \frac{y_i'}{1-y_i}.$$

En prenant l'exponentielle de cette égalité, il vient

$$\prod_{i=1}^{u^-} (1 - y_i) = \exp\left(-\int \frac{\mathrm{A}(x)}{x}\mathrm{d}x\right).$$

En combinant cette égalité et l'équation (5.2), on obtient bien le résultat attendu. □

À la lumière de ce dernier résultat, on peut appliquer la même méthode que dans le cas des excursions. On commence par calculer une équation satisfaite par $\mathrm{A}(x)$ en utilisant les méthodes de Bostan, Chyzak *et al.* et on la convertit en récurrence. Le calcul des conditions initiales pour A peut être effectué naïvement en développant $y\mathrm{W}(x,y)/(1-y)$. La formule de la proposition 110 permet alors de calculer $\mathrm{M}(x)$ mod $x^{\mathrm{N}+1}$ à partir de $\mathrm{A}(x)$ mod $x^{\mathrm{N}+1}$. L'analyse de complexité est tout à fait similaire : le pré-calcul s'effectue en $\tilde{\mathrm{O}}(d^5)$ opérations dans $\mathbb{Q}$.

5.2.7 Algorithme

Les discussions des trois paragraphes précédents sont résumées par le théorème suivant, implémenté en pratique par l'algorithme Marches (algorithme 10).

Théorème 111. *Soit* S *un ensemble fini de pas, et* $d = u^- + u^+$. *Il est possible de développer la série* $\mathrm{B_S}$ *(resp.* $\mathrm{E_S}$, $\mathrm{M_S}$*) à l'ordre* N *en* $\mathrm{O}(d^2\mathrm{N})$ *(resp.* $\tilde{\mathrm{O}}(d^2\mathrm{N})$*) opérations dans* $\mathbb{Q}$, *après un pré-calcul en* $\tilde{\mathrm{O}}(d^5)$ *opérations dans* $\mathbb{Q}$.

11. BANDERIER et FLAJOLET, "Basic Analytic Combinatorics of Directed Lattice Paths", Cor. 1.

Algorithme **Marches**(S, N)

Entrée Un ensemble de pas S et un entier positif N

Sortie $B_S, E_S, M_S \bmod x^{N+1}$

F ← $W(x,y)/y$ [cas B, E] ou $W(x,y)/(1-y)$ [cas M] ;
D ← **HermiteTelescoping**(F) [a] ;
R ← la récurrence d'ordre r associée à D ;
I ← $[y^0]W(x,y) \bmod x^{r+1}$ [cas B, E]
$[y^0]yW(x,y)/(1-y) \bmod x^{r+1}$ [cas M] ;
B ← $[y^0]W(x,y) \bmod x^{N+1}$ (à partir de R, I) ;
A ← $[y^0]yW(x,y)/(1-y) \bmod x^{N+1}$ (à partir de R, I) ;
E ← $\exp\left(\int (B(x)-1)/x\,dx\right) \bmod x^{N+1}$;
M ← $\exp\left(-\int (A(x)/x)/(1-\chi(1)x)\,dx\right) \bmod x^{N+1}$;
renvoyer B, E, M

a. BOSTAN, CHEN, CHYZAK et LI, "Complexity of creative telescoping for bivariate rational functions", Fig. 3.

Algorithme 10: Développement des séries génératrices des ponts, méandres et excursions

Perspectives

Je conclus ce texte en proposant quelques questions liées aux sujets abordés jusqu'ici, dont j'estime qu'elles constituent des sujets de recherche intéressants.

Création télescopique par réduction

Les algorithmes de création télescopique par réduction font l'objet d'une grande activité depuis quelques années, et il reste encore du travail pour généraliser ces méthodes. Une première direction consiste à étendre les classes de fonctions pour lesquelles on dispose de réduction. Par exemple, dans le cas de l'intégration d'une fonction dépendant d'un paramètre continu, on dispose de la réduction de Hermite pour les fractions rationnelles bivariées, qui a été étendue dans plusieurs directions : aux fonctions algébriques [12], aux fonctions hyperexponentielles [13], et aux fractions rationnelles de plus de variables [14]. Un des idéaux dans ce cadre consiste à trouver une réduction qui s'appliquerait à une fonction différentiellement finie générale.

Une autre direction consiste à étendre les contextes dans lesquels on dispose de réductions. Par exemple, on a vu dans le chapitre 2 une réduction pour l'intégration de termes mixtes hypergéométriques hyperexponentiels. Il y a un bon espoir de trouver par des méthodes similaires une réduction pour le problème associé de la sommation de ces mêmes termes.

Toujours dans la même veine, on pourrait tenter de trouver un analogue des résultats du chapitre 2 en remplaçant les termes mixtes hypergéométriques et hyperexponentiels par des termes mixtes hypergéométriques et algébriques. Il semble alors prometteur d'appliquer un analogue de la réduction de Trager des fonctions algébriques pour faire de la création télescopique. Un cas particulier intéressant est l'intégrale

$$\oint \frac{f(x)}{x^{n+1}}\mathrm{d}x,$$

où f est une fonction algébrique. Calculer un télescopeur pour cette intégrale

12. Chen, Kauers et Koutschan, "Reduction-Based Creative Telescoping for Algebraic Functions".
13. Bostan, Chen, Chyzak, Li et Xin, "Hermite reduction and creative telescoping for hyperexponential functions".
14. Bostan, Lairez et Salvy, "Creative telescoping for rational functions using the Griffiths-Dwork method" ; Lairez, "Computing periods of rational integrals".

donne une récurrence pour les coefficients de Taylor de f. Si l'on dispose d'un algorithme dont l'analyse fournit des bornes sur l'ordre du télescopeur minimal, on peut espérer démontrer une conjecture de Bostan :

Conjecture 112. Soit $f(x) = \sum_{n\geqslant 0} a_n x^n \in \mathbf{k}[[x]]$ une série algébrique, annulée par un polynôme $P \in \mathbf{k}[x,y]$ de bidegré (d_x, d_y).

Alors la suite (a_n) satisfait une récurrence à coefficients polynomiaux d'ordre $d_x(d_y-1)$.

On retrouvera certaines questions posées dans ce paragraphe ainsi que d'autres problèmes ouverts pour la création télescopique en général chez Chen et Kauers [15].

Constantes d'Eisenstein

Si $f \in \mathbb{Q}[[x]]$ est une série algébrique telle que $f(0) = 0$, alors Eisenstein a montré [16] qu'il existe toujours un entier c tel que $f(cx) \in \mathbb{Z}[[x]]$. On dit alors que c est une *constante d'Eisenstein* pour f. Trouver une estimation de la plus petite constante d'Eisenstein pour une fonction f donnée est un problème important. Par exemple, les constantes d'Eisenstein interviennent pour estimer la complexité de l'algorithme de Newton-Puiseux [17]. À l'heure actuelle, la meilleure estimation est due à Dwork et van der Poorten [18]. Une approche possible pour calculer effectivement une constante d'Eisenstein consiste à utiliser la proposition 89 afin d'écrire f comme une diagonale de fraction rationnelle. Il est alors aisé de lire une constante d'Eisenstein sur cette fraction. Mechik [19] a montré comment tirer de cette méthode un algorithme de calcul d'une constante d'Eisenstein. Cependant, il reste encore à étudier la méthode d'un point de vue quantitatif, ce qui mènerait potentiellement à une estimation qu'il serait intéressant de comparer à celles qui existent déjà.

Trous dans les développements de fonctions algébriques

Les premières idées qui ont plus tard mené aux résultats du chapitre 2 trouvent leurs origines dans une tentative échouée de démontrer une conjecture due à Furter [20].

Conjecture 113. Soit $p \in \mathbb{C}[x]$ un polynôme de degré $m+1$ tel que $p(0) = 0$. On note $p^{(-1)}$ l'inverse de p pour la composition des séries.

Si m coefficients consécutifs de $p^{(-1)}$ sont nuls, alors $p(x) = x$.

15. CHEN et KAUERS, "Some Open Problems related to Creative Telescoping".
16. EISENSTEIN, "Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen".
17. WALSH, "A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function".
18. DWORK et POORTEN, "The Eisenstein constant".
19. MECHIK, "Sur la constante d'Eisenstein".
20. FURTER, "Polynomial composition rigidity and plane polynomial automorphisms", Conj. 1.6.

Le lien entre cette conjecture et le chapitre 2 peut paraître flou au premier abord, mais il devient plus clair en étudiant la tentative de preuve de sa conjecture par Furter. L'idée est que les coefficients de $p^{(-1)}$ satisfont une récurrence d'ordre m. C'est un lemme dû à Manivel qui est un cas particulier du théorème 49. Dès lors que l'on a dépassé les singularités du coefficient de tête de cette récurrence, on en déduit que la nullité de m coefficients consécutifs entraîne la nullité de tous les suivants. Ceci permet avec un peu plus de travail de démontrer la conjecture pour $m = 2$, mais échoue à cause du problème des singularités pour m plus grand. C'est en essayant d'étudier de plus près les récurrences données par le lemme de Manivel et sa preuve que l'on a été amenés à étudier les intégrales du type

$$\oint \frac{\mathrm{d}x}{p(x)^n},$$

où p est un polynôme, puis à généraliser à d'autres termes mixtes hypergéométriques et hyperexponentiels.

Cependant, la barrière créée par les singularités des récurrences reste encore infranchissable à ce jour, et la conjecture de Furter reste ouverte. Plus généralement, cette conjecture est généralisée par la variante originelle de la conjecture 112 :

Conjecture 114. Soit $f \in \mathbf{k}[[x]]$ une série algébrique annulée par un polynôme $P \in \mathbf{k}[x, y]$ de bidegré (d_x, d_y).

Si f admet $d_x(d_y - 1)$ coefficients nuls consécutifs, alors f est un polynôme.

Cette conjecture signifie que les "trous" d'une fonction algébrique ne peuvent pas être trop grands.

Diagonales modulo p

Dans le chapitre 4, nous avons vu comment calculer un polynôme annulateur pour une diagonale de fraction rationnelle bivariée, en caractéristique nulle. Maintenant, dans un corps de caractéristique strictement positive, la même question se pose, d'autant plus qu'alors toutes les diagonales de fractions rationnelles sont algébriques, quel que soit le nombre de variables. Ceci a été prouvé par Furstenberg[21], et sa preuve suggère un algorithme pour calculer un polynôme annulateur de la diagonale. Il est intéressant d'étudier cet algorithme du point de vue de la complexité, notamment lorsque le nombre de variables augmente.

En particulier, une première étape de l'analyse consiste à estimer la taille du polynôme calculé. En d'autre termes, on aimerait savoir quel est le degré d'algébricité d'une diagonale donnée lorsqu'on la considère modulo p, pour diverses valeurs de p. Une première réponse a fait l'objet de travaux d'Adamczewski et Bell[22] qui ont déjà été cités plus haut. Ils ont prouvé que la croissance du degré d'algébricité est au plus p^{A}, où A est une certaine constante dépendant de la diagonale considérée. Ils ont également mis en évidence des familles de diagonales pour lesquelles la croissance est effectivement en p^{B} pour B arbitrairement grand. Mais la

21. Furstenberg, "Algebraic Functions over Finite Fields", Th. 1.
22. Adamczewski et Bell, "Diagonalization and rationalization of algebraic Laurent series".

route n'est pas encore terminée dans cette direction, car la constante A n'est en général pas optimale, et ne reflète donc pas nécessairement la taille effective du polynôme calculé.

Par ailleurs, on a vu qu'en caractéristique nulle l'équation algébrique minimale satisfaite par une diagonale peut être exponentiellement plus grande que l'équation différentielle ou la récurrence minimale. Cette disparité existe-t-elle encore modulo p ? En fonction de la réponse à cette question, il est à nouveau intéressant de comparer les deux structures de données pour le problème du calcul des N premiers termes d'une diagonale modulo p. Il est tout à fait imaginable que la méthode la plus efficace modulo p ne soit pas la même qu'en caractéristique nulle. En effet, pour le problème apparenté du calcul direct du N-ième terme du développement d'une série algébrique, le meilleur algorithme en caractéristique nulle a une complexité $\tilde{O}(\sqrt{N})$, alors que modulo p il a été prouvé récemment [23] que l'on peut atteindre une complexité $O(\log N)$ avec un pré-calcul quasi-linéaire en p.

23. BOSTAN, CHRISTOL et DUMAS, "Fast Computation of the Nth Term of an Algebraic Series over a Finite Prime Field".

Annexes

Annexe A

Rappels de résultats classiques d'algèbre

A.1 Inégalité de Hadamard

Lors de la résolution de systèmes linéaires à coefficients dans $\mathbb{K}[x]$, il est utile de pouvoir prédire a priori le degré des solutions du système. C'est possible grâce à ce lemme, qui est une variante de l'inégalité de Hadamard [1].

Lemme 115. *Soit* M *une matrice carrée de taille* n*, dont les entrées sont dans* $\mathbb{K}(x)_d$*. Notons* $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n$ *les colonnes de* M*.*

Alors son déterminant est une fraction rationnelle dont le degré vérifie

$$\deg_x(\det \mathrm{M}) \leqslant \sum_{i=1}^{n} \deg_x \mathrm{C}_i.$$

Démonstration. C'est une conséquence immédiate de la formule de développement par rapport à une colonne et des propriétés du degré. □

Le lemme suivant est utile en pratique, il permet de majorer le degré d'une base du noyau gauche d'une matrice polynomiale rectangulaire dont les entrées sont séparées en deux blocs de degrés différents.

Lemme 116. *Soit* M *une matrice de taille* $n \times m$ *avec* $n > m$ *et de rang* r*, dont les entrées sont dans* $\mathbb{K}(x)$ *On suppose de plus que* $\mathrm{M} = (\mathrm{M}_1\ \mathrm{M}_2)$*, où* M_1 *et* M_2 *ont* m_1 *et* m_2 *colonnes respectivement, et ont des entrées de degrés* d_1 *et* d_2 *respectivement.*

Alors il existe une base $(\mathrm{V}_1, \mathrm{V}_2, \ldots, \mathrm{V}_r)$ *du noyau à gauche de* M *telle que, pour tout* $i \in \{1, 2, \ldots, r\}$*,*

$$\deg_x \mathrm{V}_i \leqslant m_1 d_1 + m_2 d_2.$$

(Les coefficients des V_i *sont des fractions rationnelles.)*

1. HADAMARD, "Résolution d'une question relative aux déterminants".

Démonstration. C'est un résultat classique qu'une base de noyau à gauche peut être lue sur les entrées de la matrice de transformation de M vers sa forme échelonnée, et que ces entrées sont toutes des mineurs de M. Il suffit alors d'appliquer l'inégalité de Hadamard (lemme précédent) à ces mineurs. □

A.2 Les fonctions algébriques sont différentiellement finies

Il est rapporté dans ses œuvres complètes[2] qu'Abel déjà aurait constaté le fait que toute série univariée algébrique est différentiellement finie. Plus précisément, on a le résultat suivant :

Théorème 117. *Soit* $\mathrm{P} \in \mathbf{k}[x][y]$ *un polynôme sans carré. Alors il existe un opérateur différentiel* L_P *dont l'espace des solutions est engendré par les racines de* P.

Démonstration. On trouvera la preuve de ce résultat chez Cormier, Singer, *et al.*[3] □

Définition 118. Soit $\mathrm{P} \in \mathbf{k}(x)[y]$ un polynôme sans carré. Alors l'opérateur unitaire d'ordre minimal satisfaisant la propriété du théorème précédent est appelé la résolvante différentielle de P.

Rappelons également une estimation de l'ordre et du degré de la résolvante différentielle d'un polynôme bivarié due à Bostan, Chyzak *et al.*[4].

Théorème 119. *Soit* $\mathrm{P} \in \mathbf{k}[x, y]$ *un polynôme sans carré de bidegré* (d_x, d_y). *On note* L_P *la résolvante différentielle de* P, *et* r *son ordre. Alors*

$$r \leqslant d_y, \quad \deg \mathrm{L}_\mathrm{P} = \mathrm{O}(r d_x d_y).$$

A.3 Séries de Puiseux et polygone de Newton

Lorsqu'on se donne un polynôme $\mathrm{P} \in \mathbf{k}(x)[y]$, il est souvent utile de développer ses racines en séries de Puiseux, c'est-à-dire des séries en $x^{1/n}$ où n est un certain entier positif. Le fait que ceci soit toujours possible est assuré par le théorème suivant :

Théorème 120. *Soit* $\mathbf{k}$ *un corps de caractéristique* 0. *Notons* $\overline{\mathbf{k}}$ *une clôture algébrique de* $\mathbf{k}$. *Alors le corps des séries de Puiseux sur* $\overline{\mathbf{k}}$,

$$\overline{\mathbf{k}}\langle\langle x\rangle\rangle = \bigcup_{n=0}^{\infty} \overline{\mathbf{k}}((x^{\frac{1}{n}})),$$

est algébriquement clos.

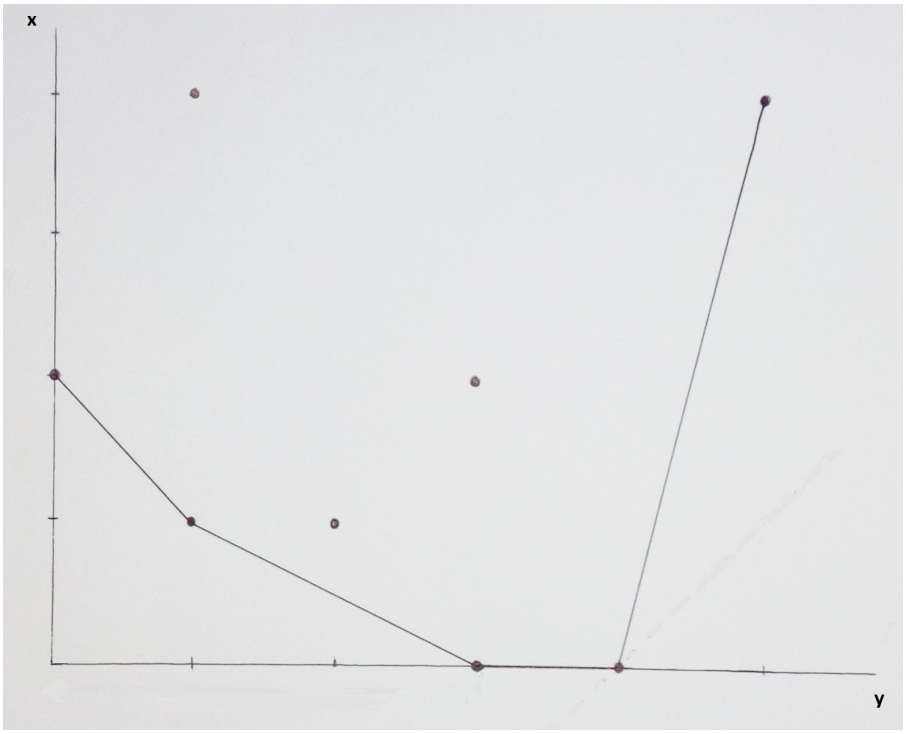
2. ABEL, *Œuvres Complètes*, p. 287.
3. CORMIER et al., "Linear differential operators for polynomial equations", §2.
4. BOSTAN, CHYZAK et al., "Differential equations for algebraic functions".

Démonstration. Ce théorème est dû à Puiseux[5], et on trouvera la preuve expliquée très clairement chez Walker[6]. □

En regardant de plus près la preuve du théorème, dans la présentation de Walker par exemple, on constate qu'elle n'est autre qu'un algorithme permettant de calculer le développement en série de Puiseux des racines d'un polynôme. En particulier, une conséquence très importante de la construction est que les valuations des racines d'un polynôme P peuvent être déterminées facilement grâce à son polygone de Newton, dont je rappelle maintenant la définition. C'est un cas typique où un dessin vaut bien mieux qu'un long discours, la définition est donc suivie d'un dessin du polygone de Newton pour l'exemple du polynôme $x^2+(2x+x^4)y+4xy^2+(1+x^2)y^3+5y^4+x^4y^5$.

Définition 121. Soit $P \in \mathbf{k}(x)[y]$ un polynôme de degré d_y. On écrit $P = \sum_{i=0}^{d_y} a_i(x)y^i$. Dans le plan cartésien, on considère les points E_i de coordonnées $(i, \mathrm{val}_x(a_i))$, pour tous les entiers $i \in \{0,1,\ldots,d_y\}$ tels que $a_i(x) \neq 0$.

Alors le *polygone de Newton* de P est défini comme étant la ligne polygonale joignant E_0 à E_{d_y} en ne passant que par des E_i et de telle sorte que tous les E_i soient au-dessus d'elle. (Si E_0 n'est pas défini, on part du premier point qui est défini.)



Exemple de polygone de Newton

5. PUISEUX, "Recherches sur les fonctions algébriques."
6. WALKER, *Algebraic Curves*, Chap. IV, Th. 3.1.

Pour obtenir les valuations des racines de P, il suffit alors d'utiliser la proposition suivante :

Proposition 122. *Soit* $P \in \mathbf{k}(x)[y]$ *un polynôme. Alors les valuations des racines de* P *sont exactement les opposés des pentes apparaissant dans le polygone de Newton de* P.

Démonstration. Comme annoncé précédemment, c'est une conséquence de la preuve du théorème de Puiseux[7]. □

A.4 Théorème fondamental des polynômes symétriques

Définition 123. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des indéterminées. On appelle k-ième fonction symétrique élémentaire associée à $\alpha_1, \alpha_2, \ldots, \alpha_n$, notée σ_k, le polynôme défini par

$$\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i_1 < i_2 < \cdots < i_k} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k}.$$

On rappelle le résultat ultra-classique reliant les coefficients d'un polynôme et les fonctions symétriques élémentaires associées à ses racines.

Proposition 124. *Soit* $p = a_n \prod_{i=1}^{n} (x - \alpha_i)$ *un polynôme de degré* n*, que l'on écrit également sous forme développée*

$$p = \sum_{i=0}^{n} a_i x^i.$$

Soient $\sigma_1, \sigma_2, \ldots, \sigma_n$ *les fonctions symétriques élémentaires associées à* $\alpha_1, \alpha_2, \ldots, \alpha_n$.
Alors, pour tout $i \in \{1, 2, \ldots, n\}$*, on a :*

$$\sigma_i = (-1)^i \frac{a_{n-i}}{a_n}.$$

Définition 125. Soit $p \in \mathbb{K}[\alpha_1, \alpha_2, \ldots, \alpha_n]$. On dit que p est un polynôme *symétrique* si pour toute permutation ϕ de l'ensemble $\{1, 2, \ldots, n\}$ on a

$$p(\alpha_{\phi(1)}, \alpha_{\phi(2)}, \ldots, \alpha_{\phi(n)}) = p(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

La proposition suivante est une version effective d'un résultat classique[8] sur les polynômes symétriques.

Proposition 126. *Soient* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *des indéterminées, et* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *les fonctions symétriques élémentaires associées. Soit* $p \in \mathbb{K}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *un polynôme symétrique tel que, pour tout* $i \in \{1, 2, \ldots, n\}$*,*

$$\deg_{\alpha_i} p \leqslant d.$$

7. WALKER, *Algebraic Curves*, preuve du Th. 3.1.
8. YAP, *Fundamental Problems of Algorithmic Algebra*, Th. 6.21.

Alors il existe un polynôme $\tilde{p} \in \mathbb{K}[\sigma_1, \sigma_2, \ldots, \sigma_n]$ *tel que*

$$\sum_{i=1}^{n} \deg_{\sigma_i} \tilde{p} \leqslant d$$

et

$$p(\alpha_1, \alpha_2, \ldots, \alpha_n) = \tilde{p}(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Démonstration. C'est une conséquence de la forme de la matrice de changement de bases des fonctions symétriques élémentaires vers les fonctions symétriques monomiales, telle que décrite par exemple par Stanley[9]. Comme p est symétrique et a degré au plus d par rapport à chaque variable, on peut l'écrire comme une combinaison linéaire de fonctions symétriques monomiales de la forme

$$\sum_{i_1 < \cdots < i_k} \alpha_{i_1}^{\lambda_1} \ldots \alpha_{i_k}^{\lambda_k},$$

où $\lambda_i \leqslant d$ pour tout i. Ces fonctions symétriques monomiales peuvent à leur tour être écrites comme des combinaisons linéaires de fonctions symétriques élémentaires de la forme $\sigma_{\mu_1} \cdots \sigma_{\mu_l}$ où $l \leqslant d$ ce qui est le résultat annoncé. □

A.5 Résultant

Les résultants sont des objets très utilisés en calcul formel car ils permettent d'effectuer en pratique beaucoup d'opérations sur les nombres (ou les fonctions) algébriques. Je rappelle ici une définition possible ainsi que les propriétés utiles à l'exposé. Les preuves ainsi qu'une présentation plus complète peuvent être trouvées par exemple dans le livre de von zur Gathen et Gerhard[10] ou celui de Lang[11].

Définition 127. Soient $p, q \in \mathbf{k}[x]$ deux polynômes de degrés respectifs d et e, que l'on écrit

$$p = \sum_{i=0}^{d} p_i x^i, \quad q = \sum_{i=0}^{e} q_i x^i.$$

On définit le *résultant* en x de p et q, noté $\text{Résultant}_x(p, q)$, comme étant le déterminant de la matrice de Sylvester :

$$\begin{pmatrix}
p_d & p_{d-1} & \cdots & p_0 & & & \\
 & p_d & p_{d-1} & \cdots & p_0 & & \\
 & & \ddots & \ddots & & \ddots & \\
 & & & p_d & p_{d-1} & \cdots & p_0 \\
q_e & q_{e-1} & \cdots & q_0 & & & \\
 & q_e & q_{e-1} & \cdots & q_0 & & \\
 & & \ddots & \ddots & & \ddots & \\
 & & & q_e & q_{e-1} & \cdots & q_0
\end{pmatrix} \tag{A.1}$$

9. STANLEY, *Enumerative combinatorics*, preuve du Th. 7.4.4.
10. GATHEN et GERHARD, *Modern computer algebra*, §6.3.
11. LANG, *Algebra*, Ch. IV §8.

où les e premières lignes contiennent les coefficients de p et les d dernières les coefficients de q.

Le résultant satisfait les propriétés fondamentales suivantes :

Proposition 128. *Soient $p, q \in \mathbf{k}[x]$ deux polynômes de degrés respectifs d et e, que l'on écrit*

$$p(x) = p_d \prod_{i=1}^{d} (x - \alpha_i), \quad q(x) = q_e \prod_{i=1}^{e} (x - \beta_i).$$

Alors le résultant de p et q vaut

$$\text{Résultant}_x(p,q) = (-1)^{de} \text{Résultant}_x(q,p) = p_d^e \prod_{i=1}^{d} q(\alpha_i).$$

Proposition 129. *Soient $p, q \in \mathbf{k}[x]$ deux polynômes. Alors il existe des polynômes $u, v \in \mathbf{k}[x]$ tels que le résultant de p et q s'écrit*

$$\text{Résultant}_x(p,q) = pu + qv.$$

On termine cette section avec une proposition permettant de majorer le degré du résultant de deux polynômes bivariés. On en redonne la preuve car elle n'est énoncée que dans une variante légèrement plus faible dans le livre de von zur Gathen et Gerhard (quoique leur preuve s'adapterait sans problème pour démontrer cette version du résultat).

Proposition 130. *Soient $\mathrm{P}, \mathrm{Q} \in \mathbf{k}[x, y]$ des polynômes de bidegrés respectifs $(d_x^{\mathrm{P}}, d_y^{\mathrm{P}})$ et $(d_x^{\mathrm{Q}}, d_y^{\mathrm{Q}})$. Alors,*

$$\deg \text{Résultant}_y(\mathrm{P}(x,y), \mathrm{Q}(x,y)) \leqslant d_x^{\mathrm{P}} d_y^{\mathrm{Q}} + d_x^{\mathrm{Q}} d_y^{\mathrm{P}},$$

et c'est une égalité dès lors que d_x^{Q} ou d_x^{P} est nul..

Démonstration. C'est une application directe du lemme 115 à la transposée de la matrice de Sylvester (A.1). □

Annexe B

Résultats de complexité pour les opérations de base

Dans cette annexe sont rappelés des résultats classiques de complexité qui servent de briques de base pour les diverses analyses de complexité tout au long du texte. Rappelons que les complexités sont évaluées en comptant le nombre d'opérations arithmétiques dans le corps $\mathbf{k}$ de caractéristique 0 et que la notation $\tilde{\mathrm{O}}(\cdot)$ indique que des facteurs polylogarithmiques sont omis.

B.1 Opérations univariées

La plupart des opérations sur les polynômes, fractions rationnelles et séries entières en une variable peuvent être effectuées en temps quasi-linéaire. Les preuves des résultats assemblés dans la proposition ci-dessous pourront être trouvées dans les livres usuels de référence [1].

Proposition 131. *Les opérations suivantes peuvent être effectuées en* $\tilde{\mathrm{O}}(n)$ *opérations dans* $\mathbf{k}$.

1. *somme, produit et dérivation dans* $\mathbf{k}[x]_n$, $\mathbf{k}(x)_n$ *et* $\mathbf{k}[[x]]_n$ *; intégration dans* $\mathbf{k}[x]_n$ *et* $\mathbf{k}[[x]]_n$ *;*
2. *pgcd étendu, décomposition sans carré et résultant dans* $\mathbf{k}[x]_n$ *;*
3. *évaluation en* $\mathrm{O}(n)$ *points de* $\mathbf{k}$ *d'éléments de* $\mathbf{k}[x]_n$ *et* $\mathbf{k}(x)_n$ *; interpolation dans* $\mathbf{k}[x]_n$ *et* $\mathbf{k}(x)_n$ *à partir de* n *(resp.* $2n-1$*) valeurs en des points deux à deux distincts de* $\mathbf{k}$ *;*
4. *inverse, logarithme, exponentielle dans* $\mathbf{k}[[x]]_n$ *(quand ceux-ci sont définis) ;*
5. *conversion entre* $\mathrm{P} \in \mathbf{k}[x]_n$ *et* $\mathscr{N}(\mathrm{P}) \bmod x^n \in \mathbf{k}[x]_n$. *(voir la proposition 73)*

1. Bürgisser, Clausen et Shokrollahi, *Algebraic complexity theory*; Gathen et Gerhard, *Modern computer algebra.*

B.2 Opérations multivariées

Les opérations de base sur les polynômes, fractions rationnelles et séries entières multivariés sont des questions difficiles d'un point de vue algorithmique. Par exemple, on ne connaît pas encore d'algorithme général quasi-optimal pour calculer des résultants de polynômes bivariés (il en existe tout de même dans certains cas particuliers importants[2]).

B.2.1 Multiplication

La multiplication est l'opération non-triviale la plus simple dans ce contexte. Le résultat suivant peut être prouvé en utilisant la substitution de Kronecker[3].

Proposition 132. *Soit m un entier. On peut multiplier des polynômes dans $\mathbf{k}[x_1,\dots,x_m]_{d_1,\dots,d_m}$ et des séries entières dans $\mathbf{k}[[x_1,\dots,x_m]]_{d_1,\dots,d_m}$ en $\tilde{\mathrm{O}}(2^m d_1\cdots d_m)$ opérations dans $\mathbf{k}$.*

On remarquera que pour un nombre de variables $m = \mathrm{O}(1)$ fixé, ce résultat est quasi-optimal. Pour un grand nombre de variables, ou lorsque l'on s'intéresse à des supports monomiaux plus compliqués, il existe des méthodes plus sophistiquées[4].

B.2.2 Évaluation et interpolation

Pour la méthode d'évaluation et interpolation, le cas le plus simple est lorsque les points forment une grille qui est un produit m-dimensionnel $\mathrm{I}_1\times\cdots\times\mathrm{I}_m$, où I_j est un ensemble de cardinal d_j. Ce cas est traité dans la proposition suivante, due à Pan[5] ; elle se généralise à des sous-grilles de grilles produit[6].

Proposition 133. *Un polynôme de $\mathbf{k}[x_1,\dots,x_m]_{d_1,\dots,d_m}$ peut être évalué et interpolé en $d_1\cdots d_m$ points d'une grille-produit m-dimensionnelle en $\tilde{\mathrm{O}}(md_1\cdots d_m)$ opérations dans $\mathbf{k}$.*

À nouveau, cette complexité est quasi-optimale pour $m = \mathrm{O}(1)$ fixé.

B.2.3 Résultant

Une méthode générale (bien que non-optimale) pour traiter des opérations plus compliquées sur des objets multivariés consiste à utiliser l'évaluation et l'interpolation de polynômes pour se ramener à des opérations sur des objets univariés. Pour mettre en œuvre cette stratégie, il est nécessaire de maîtriser la taille du

2. BOSTAN, FLAJOLET et al., "Fast Computation of Special Resultants".
3. GATHEN et GERHARD, *Modern computer algebra*, §8.4.
4. CANNY, KALTOFEN et LAKSHMAN, "Solving Systems of Nonlinear Polynomial Equations Faster" ; PAN, "Simple multivariate polynomial multiplication" ; LECERF et SCHOST, "Fast multivariate power series multiplication in characteristic zero" ; HOEVEN et SCHOST, "Multi-point evaluation in higher dimensions".
5. PAN, "Simple multivariate polynomial multiplication".
6. HOEVEN et SCHOST, "Multi-point evaluation in higher dimensions".

résultat de l'opération. On illustre cette idée dans le résultat suivant sur l'exemple du calcul de résultants.

Proposition 134. *Soient* $P, Q \in \mathbf{k}[x_1, \ldots, x_m, y]_{d_1,\ldots,d_m,d}$ *deux polynômes. Alors* $R = \text{Résultant}_y(P, Q)$ *appartient à* $\mathbf{k}[x_1, \ldots, x_m]_{D_1,\ldots,D_m}$*, où* $D_i = 1+2(d-1)(d_i-1)$*. De plus, les coefficients de* R *peuvent être calculés en* $\tilde{O}(2^m d_1 \cdots d_m d^{m+1})$ *opérations dans* $\mathbf{k}$*.*

Démonstration. Les bornes sur les degrés proviennent de la proposition 130. Pour calculer R, on procède par évaluation et interpolation. P et Q sont évalués à $D = D_1 \cdots D_m$ points $(x_1, \ldots, x_m)$ formant une grille-produit m-dimensionnelle ; D résultants univariés dans $\mathbf{k}[y]$ sont calculés ; R est ensuite reconstruit par interpolation. Par la proposition 133, les étapes d'évaluation et d'interpolation coûtent $\tilde{O}(mD)$ opérations dans $\mathbf{k}$. Les calculs de résultants coûtent $\tilde{O}(dD)$ opérations dans $\mathbf{k}$ par la proposition 131.On conclut alors par l'inégalité $D \leqslant 2^m d_1 \cdots d_m d^m$. □

B.2.4 Décomposition sans carré

Proposition 135. *La décomposition sans carré d'un polynôme dans* $\mathbf{k}[x, y]_{d_x,d_y}$ *peut-être calculée en* $\tilde{O}(d_x^2 d_y)$ *opérations dans* $\mathbf{k}$*.*

On trouvera la preuve de ceci chez Lecerf[7].

B.2.5 Algèbre linéaire

Pour résoudre les systèmes linéaires à coefficients polynomiaux, on dispose de l'algorithme de Storjohann et Villard[8] :

Proposition 136. *Le noyau d'une matrice de taille* $s \times (s+1)$ *à entrées polynomiales dans* $\mathbb{K}[x]_d$ *peut être calculé en* $\tilde{O}(s^\omega d)$ *opérations dans* $\mathbb{K}$*.*

7. LECERF, "Fast separable factorization and applications".
8. STORJOHANN et VILLARD, "Computing the Rank and a Small Nullspace Basis of a Polynomial Matrix".

Bibliographie

Niels. H. ABEL. *Œuvres Complètes*. T. II. Éditions Jacques Gabay, 1992.

Boris ADAMCZEWSKI et Jason P. BELL. "Diagonalization and rationalization of algebraic Laurent series". Dans : *Annales Scientifiques de l'École Normale Supérieure* 46 (6) (2013), p. 963–1004.

Gert ALMKVIST et Doron ZEILBERGER. "The method of differentiating under the integral sign". Dans : *Journal of Symbolic Computation* 10 (6) (1990), p. 571–591.

Moa APAGODU et Doron ZEILBERGER. "Multi-variable Zeilberger and Almkvist-Zeilberger algorithms and the sharpening of Wilf-Zeilberger theory". Dans : *Advances in Applied Mathematics* 37 (2) (2006), p. 139–152.

Cyril BANDERIER et Philippe FLAJOLET. "Basic Analytic Combinatorics of Directed Lattice Paths". Dans : *Theoretical Computer Science* 281 (1-2) (2002), p. 37–80.

Alin BOSTAN, Shaoshi CHEN, Frédéric CHYZAK et Ziming LI. "Complexity of creative telescoping for bivariate rational functions". Dans : *Proceedings ISSAC'10*. ACM, 2010, p. 203–210.

Alin BOSTAN, Shaoshi CHEN, Frédéric CHYZAK, Ziming LI et Guoce XIN. "Hermite reduction and creative telescoping for hyperexponential functions". Dans : *Proceedings ISSAC'13*. ACM, 2013, p. 77–84.

Alin BOSTAN, Gilles CHRISTOL et Philippe DUMAS. "Fast Computation of the Nth Term of an Algebraic Series over a Finite Prime Field". Dans : *Proceedings ISSAC'16*. ACM, 2016, p. 119–126.

Alin BOSTAN, Frédéric CHYZAK, Grégoire LECERF, Bruno SALVY et Éric SCHOST. "Differential equations for algebraic functions". Dans : *Proceedings ISSAC'07*. ACM, 2007, p. 25–32.

Alin BOSTAN, Louis DUMONT et Bruno SALVY. "Algebraic Diagonals and Walks". Dans : *Proceedings ISSAC'15*. ACM, 2015, p. 77–84.

Alin BOSTAN, Louis DUMONT et Bruno SALVY. "Efficient Algorithms for Mixed Creative Telscoping". Dans : *Proceedings ISSAC'16*. ACM, 2016, p. 127–134.

Alin BOSTAN, Philippe FLAJOLET, Bruno SALVY et Éric SCHOST. "Fast Computation of Special Resultants". Dans : *Journal of Symbolic Computation* 41 (1) (2006), p. 1–29.

Alin BOSTAN, Irina KURKOVA et Kilian RASCHEL. “A human proof of Gessel’s lattice path conjecture”. Dans : *Transactions of the American Mathematical Society* 369 (2) (2017), p. 1365–1393.

Alin BOSTAN, Pierre LAIREZ et Bruno SALVY. “Creative telescoping for rational functions using the Griffiths-Dwork method”. Dans : *Proceedings ISSAC’13*. ACM, 2013, p. 93–100.

Alin BOSTAN et Éric SCHOST. “Polynomial evaluation and interpolation on special sets of points”. Dans : *Journal of Complexity* 21 (4) (2005), p. 420–446.

Mireille BOUSQUET-MÉLOU. “Discrete excursions”. Dans : *Séminaire Lotharingien de Combinatoire* 57 (2008), Art. B57d, 1–23.

Mireille BOUSQUET-MÉLOU. “Rational and algebraic series in combinatorial enumeration”. Dans : *International Congress of Mathematicians*. EMS, 2006, p. 789–826.

Manuel BRONSTEIN. “Formulas for series computations”. Dans : *AAECC* 2 (3) (1992), p. 195–206.

Peter BÜRGISSER, Michael CLAUSEN et Amin SHOKROLLAHI. *Algebraic complexity theory*. Grundlehren der Mathematischen Wissenschaften 315. Springer, 1997.

John F. CANNY, Erich KALTOFEN et Yagati N. LAKSHMAN. “Solving Systems of Nonlinear Polynomial Equations Faster”. Dans : *Proceedings ISSAC’89*. 1989, p. 121–128.

Shaoshi CHEN, Frédéric CHYZAK, Ruyong FENG, Guofeng FU et Ziming LI. “On the existence of telescopers for mixed hypergeometric terms”. Dans : *Journal of Symbolic Computation* 68, Part 1 (2015), p. 1–26.

Shaoshi CHEN et Manuel KAUERS. “Order-degree curves for hypergeometric creative telescoping”. Dans : *Proceedings ISSAC’12*. ACM, 2012, p. 122–129.

Shaoshi CHEN et Manuel KAUERS. “Some Open Problems related to Creative Telescoping”. Dans : *Journal of Systems Science and Complexity* (to appear).

Shaoshi CHEN et Manuel KAUERS. “Trading order for degree in creative telescoping”. Dans : *Journal of Symbolic Computation* 47 (8) (2012), p. 968–995.

Shaoshi CHEN, Manuel KAUERS et Christoph KOUTSCHAN. “Reduction-Based Creative Telescoping for Algebraic Functions”. Dans : *Proceeding ISSAC’16*. ACM, 2016, p. 175–182.

Gilles CHRISTOL. “Diagonales de fractions rationnelles et équations de Picard-Fuchs”. Dans : *Groupe d’étude d’analyse ultramétrique*. T. XII. n°13. 1984-85, p. 1–12.

Gilles CHRISTOL. “Diagonales de fractions rationnelles et équations différentielles”. Dans : *Groupe d’étude d’analyse ultramétrique*. T. X. n°18. 1982-83, p. 1–10.

Frédéric CHYZAK. “An extension of Zeilberger’s fast algorithm to general holonomic functions”. Dans : *Discrete Mathematics* 217 (1) (2000), p. 115–134.

Frédéric CHYZAK. “Fonctions holonomes en calcul formel”. Inria, TU 0531. Thèse de doct. École polytechnique, 1998.

Frédéric CHYZAK. “The ABC of Creative Telescoping — Algorithms, Bounds, Complexity”. Thèse d’habilitation à diriger des recherches. École polytechnique, 2014.

Frédéric CHYZAK et Bruno SALVY. “Non-commutative elimination in Ore algebras proves multivariate identities”. Dans : *Journal of Symbolic Computation* 26 (2) (1998), p. 187–227.

Olivier CORMIER, Michael F. SINGER, Barry M. TRAGER et Felix ULMER. “Linear differential operators for polynomial equations”. Dans : *Journal of Symbolic Computation* 34 (5) (2002), p. 355–398.

Bernard M. DWORK et Alfred J. van der POORTEN. “The Eisenstein constant”. Dans : *Duke Mathematical Journal* 65 (1) (jan. 1992), p. 23–43.

Gotthold EISENSTEIN. “Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen”. Dans : *Bericht Königl. Preuss. Akad. Wiss.* (1852), p. 441–443.

Mary Celine FASENMYER. “A Note on Pure Recurrence Relations”. Dans : *The American Mathematical Monthly* 56 (1) (1949), p. 14–17.

Mary Celine FASENMYER. “Some generalized hypergeometric polynomials”. Dans : *Bulletin of the American Mathematical Society* 53 (8) (août 1947), p. 806–812.

Michel FLIESS. “Sur divers produits de séries formelles”. Dans : *Bulletin de la Société Mathématique de France* 102 (1974), p. 181–191.

Harry FURSTENBERG. “Algebraic Functions over Finite Fields”. Dans : *Journal of Algebra* 7 (2) (1967), p. 271–277.

Jean-Philippe FURTER. “Polynomial composition rigidity and plane polynomial automorphisms”. Dans : *Journal of the London Mathematical Society. Second Series* 91 (1) (2015), p. 180–202.

Joachim von zur GATHEN et Jürgen GERHARD. *Modern computer algebra*. Third edition. Cambridge University Press, 2013.

Ira M. GESSEL. “A factorization for formal Laurent series and lattice path enumeration”. Dans : *Journal of Combinatorial Theory. Series A* 28 (3) (1980), p. 321–337.

R. William GOSPER. “Decision Procedure for Indefinite Hypergeometric Summation”. Dans : *Proceedings of the National Academy of Sciences of the United States of America* 75 (1) (1978), p. 40–42.

Jacques HADAMARD. “Résolution d’une question relative aux déterminants”. Dans : *Bulletin des Sciences Mathématiques* (17) (1893), p. 240–246.

Charles HERMITE. “Sur l’intégration des fractions rationnelles”. Dans : *Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale* 11 (1872), p. 145–148.

Joris van der HOEVEN et Éric SCHOST. “Multi-point evaluation in higher dimensions”. Dans : *Applicable Algebra in Engineering, Communication and Computing* 24 (1) (2013), p. 37–52.

Ellis HOROWITZ. “Algorithms for Partial Fraction Decomposition and Rational Function Integration”. Dans : *Proceedings SYMSAC ’71*. ACM, 1971, p. 441–457.

Edward L. INCE. *Ordinary differential equations*. Reprint of the 1926 edition. Dover Publications, 1956.

Manuel KAUERS, Christoph KOUTSCHAN et Doron ZEILBERGER. “Proof of Ira Gessel’s Lattice Path Conjecture”. Dans : *Proceedings of the National Academy of Sciences* 106 (28) (juil. 2009), p. 11502–11505.

Manuel KAUERS et Lily YEN. “On the length of integers in telescopers for proper hypergeometric terms”. Dans : *Journal of Symbolic Computation* 66 (2015), p. 21–33.

Christoph KOUTSCHAN. “A Fast Approach to Creative Telescoping”. Dans : *Mathematics in Computer Science* 4 (2) (2010), p. 259–266.

Christoph KOUTSCHAN. “Holonomic Functions in Mathematica”. Dans : *ACM Communications in Computer Algebra* 47 (3-4) (jan. 2014), p. 179–182.

Pierre LAIREZ. “Computing periods of rational integrals”. Dans : *Mathematics of Computation* 85 (300) (2014), p. 1719–1752.

Pierre LAIREZ. “Periods of rational integrals : algorithms and applications”. Thèse de doct. École polytechnique, 2014.

Serge LANG. *Algebra*. Graduate Texts in Mathematics 211. Springer New York, 2002.

Grégoire LECERF. “Fast separable factorization and applications”. Dans : *Applicable Algebra in Engineering, Communication and Computing* 19 (2) (2008), p. 135–160.

Grégoire LECERF et Éric SCHOST. “Fast multivariate power series multiplication in characteristic zero”. Dans : *SADIO Electronic Journal on Informatics and Operations Research* 5 (2003), p. 1–10.

Leonard M. LIPSHITZ. “The diagonal of a D-finite power series is D-finite”. Dans : *Journal of Algebra* 113 (2) (1988), p. 373–378.

Rachid MECHIK. “Sur la constante d’Eisenstein”. Dans : *Annales mathématiques Blaise Pascal* 15 (1) (jan. 2008), p. 87–108.

Mikhail OSTROGRADSKY. “De l’intégration des fractions rationnelles”. Dans : *Bulletin de la classe physico-mathématique de l’Académie Impériale des Sciences de Saint-Pétersbourg* (4) (1845), p. 145–167, 286–300.

Victor Y. PAN. “Simple multivariate polynomial multiplication”. Dans : *Journal of Symbolic Computation* 18 (3) (1994), p. 183–186.

George PÓLYA. “Sur les séries entières, dont la somme est une fonction algébrique”. Dans : *L’Enseignement Mathématique* 22 (1921), p. 38–47.

“Problems and Solutions”. Dans : *The American Mathematical Monthly* 123 (4) (avr. 2016), p. 399–406.

Victor PUISEUX. “Recherches sur les fonctions algébriques.” Dans : *Journal de Mathématiques Pures et Appliquées* (1850), p. 365–480.

Marius van der PUT et Michael F. SINGER. *Galois Theory of Difference Equations*. Lecture Notes in Mathematics 1666. Springer, 1997.

Marius van der PUT et Michael F. SINGER. *Galois Theory of Linear Differential Equations*. Grundlehren der mathematischen Wissenschaften 328. Springer, 2003.

Michael ROTHSTEIN. "Aspects of symbolic integration and simplification of exponential and primitive functions". Thèse de doct. University of Wisconsin-Madison, 1976.

Richard P. STANLEY. *Enumerative combinatorics*. T. II. Cambridge University Press, 1999.

Arne STORJOHANN et Gilles VILLARD. "Computing the Rank and a Small Nullspace Basis of a Polynomial Matrix". Dans : *Proceedings ISSAC'05*. ACM, 2005, p. 309–316.

Volker STRASSEN. "Gaussian Elimination is Not Optimal". Dans : *Numerische Mathematik* 13 (4) (août 1969), p. 354–356.

Barry M. TRAGER. "Algebraic Factoring and Rational Function Integration". Dans : *Proceedings SYMSAC'76*. ACM, 1976, p. 219–226.

Bartel L. van der WAERDEN. *Modern Algebra*. T. I. Frederick Ungar Publishing Company, 1949.

Robert J. WALKER. *Algebraic Curves*. Princeton University Press, 1950.

P. Gary WALSH. "A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function". Dans : *Mathematics of Computation* (69) (fév. 2000).

Herbert S. WILF et Doron ZEILBERGER. "An alorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities". Dans : *Inventiones Mathematicae* 108 (3) (1992), p. 575–633.

Chee Keng YAP. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press Inc., 2000.

Lily YEN. "Contributions to the proof theory of hypergeometric identities". Thèse de doct. University of Pennsylvania, 1993.

Doron ZEILBERGER. "A fast algorithm for proving terminating hypergeometric identities". Dans : *Discrete Mathematics* 80 (2) (1990), p. 207–211.

Doron ZEILBERGER. "A holonomic systems approach to special functions identities". Dans : *Journal of Computational and Applied Mathematics* 32 (3) (1990), p. 321–368.

université PARIS-SACLAY
ÉCOLE DOCTORALE
Sciences et technologies de l'information et de la communication (STIC)

Titre : Algorithmes rapides pour le calcul symbolique de certaines intégrales de contour à paramètre

Mots clés : calcul formel, intégrale, création télescopique, diagonale, marche

Résumé : Cette thèse traite de problèmes d'intégration symbolique en calcul formel. L'objectif principal est de mettre au point des algorithmes permettant de calculer rapidement des fonctions qui sont présentées sous la forme d'intégrales de contour dépendant d'un paramètre.

On commence par aborder le problème du calcul de l'intégrale d'une fraction rationnelle bivariée par rapport à l'une de ses variables. Le résultat est alors une fonction algébrique qui s'exprime comme une somme de résidus de l'intégrande. On met au point deux algorithmes qui calculent efficacement un polynôme annulateur pour chacun des résidus, et ensuite pour la somme, ce qui donne accès à un polynôme annulateur pour l'intégrale elle-même.

Ces algorithmes s'appliquent presque directement au calcul d'un polynôme annulateur pour la diagonale d'une fraction rationnelle bivariée, c'est-à-dire la série univariée obtenue à partir du développement en série d'une fraction rationnelle bivariée en ne gardant que les coefficients diagonaux. En effet, ces diagonales peuvent s'écrire comme des intégrales de fractions rationnelles. Dans une autre application, on donne un nouvel algorithme pour le développement des séries génératrices de plusieurs familles de marches unidimensionnelles sur les entiers. Il repose sur une analyse fine des tailles des équations algébriques et différentielles satisfaites par ces séries.

Dans un second temps, on s'intéresse au calcul de l'intégrale d'un terme mixte hypergéométrique et hyperexponentiel. Cette fois-ci le résultat est une suite polynomialement récursive. On élabore une méthode pour mettre sous forme normale les divers décalages d'un terme donné. Ceci permet d'appliquer la méthode du télescopage créatif par réductions pour calculer efficacement une récurrence à coefficients polynomiaux satisfaite par l'intégrale.

Title : Efficient algorithms for the symbolic computation of certain contour integrals with one parameter

Keywords : symbolic computation, integral, creative telescoping, diagonal, walk

Abstract : In this thesis, we provide solutions to some symbolic integration problems in computer algebra. The main objective is to effectively and efficiently compute functions that appear as contour integrals depending on one parameter.

First, we consider the computation of the integral of a bivariate rational function with regard to one of the variables. The result is then an algebraic function that can be expressed as a sum of residues of the integrand. We design two algorithms that efficiently compute an annihilating polynomial for each residue, and then for their sum, which yields an annihilating polynomial for the integral itself.

These algorithms apply almost directly to the computation of an annihilating polynomial for the diagonal of a rational function, that is, the univariate power series obtained from the expansion of a bivariate rational function by only keeping the diagonal coefficients. Indeed, these diagonals can be written as integrals of rational functions. In another application, we give a new algorithm for the Taylor expansion of the generating functions for several families of unidimensional lattice walks. It relies on a fine analysis of the sizes of the algebraic and differential equations satisfied by these generating functions.

Secondly, we consider integrals of mixed hypergeometric and hyperexponential terms. In this case, the result is a polynomially recursive sequence. We devise a method to rewrite the various shifts of a given term under a normal form. This allows us to apply the method of reduction-based creative telescoping in order to efficiently compute a recurrence with polynomial coefficients for the integral.