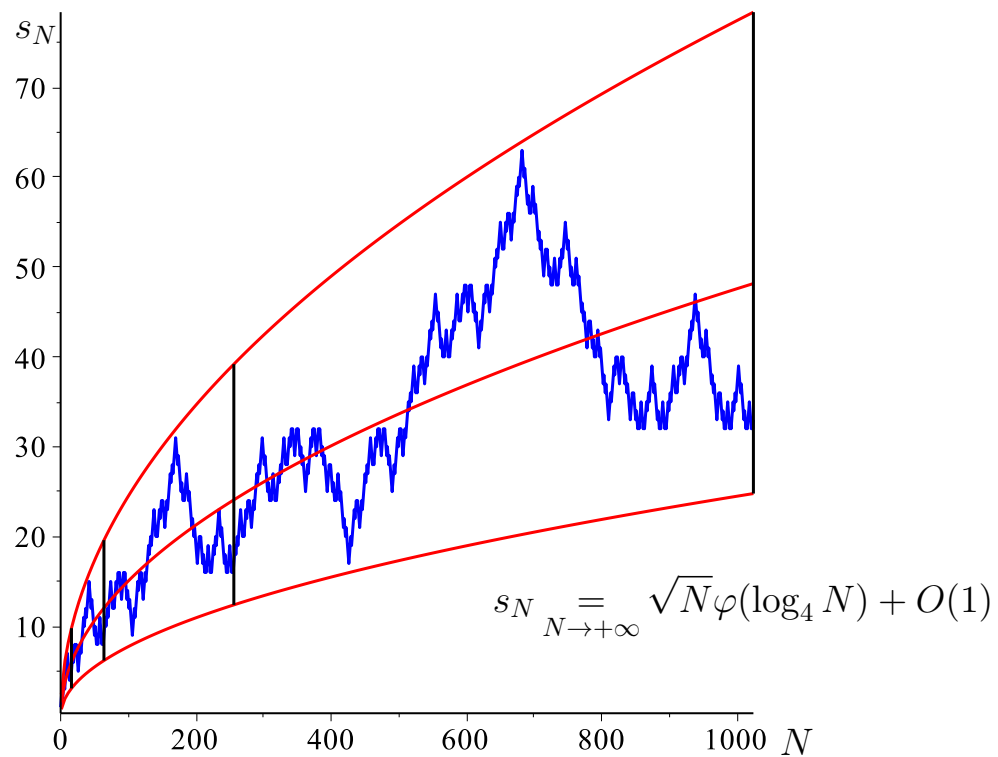


Diviser pour régner

Algèbre et analyse

Philippe Dumas
INRIA Saclay



Journées Aléa, CIRM 2016

Illustration de couverture. Harold Shapiro a traité en 1951 dans son mémoire de maîtrise [60] des problèmes d'extrémalité pour des opérateurs fonctionnels. L'un d'entre eux, repris en 1958 par Walter Rudin [58], s'énonce comme suit :

Trouver une constante A et pour chaque entier N un polynôme P de degré N à coefficients $\varepsilon_n = \pm 1$ qui vérifient

$$\max_{\vartheta \in \mathbb{R}} \left| \sum_{n=1}^N \varepsilon_n e^{in\vartheta} \right| \leq A\sqrt{N}.$$

La question fait sens parce que \sqrt{N} est un minorant de la norme uniforme sur le cercle unité d'un polynôme de la forme ci-dessus. Répondre positivement à la question signifie que cette minoration est de bonne qualité.

Une réponse possible [60, p. 40] est la constante $A = 2 + \sqrt{2}$ et les troncatrices d'une série $\sum_{n=0}^{+\infty} \varepsilon_n x^n$, dont les coefficients sont définis par

$$\varepsilon_0 = 1, \quad \varepsilon_{2n} = \varepsilon_n, \quad \varepsilon_{2n+1} = (-1)^n \varepsilon_n.$$

Cette suite $(\varepsilon_n)_{n \geq 0}$ est la suite de Rudin-Shapiro. Elle a aussi été introduite en 1951 par Marcel Golay dans un travail sur la spectroscopie en rayonnement infrarouge [40].

Le dessin de couverture montre le graphique de la fonction sommatoire $(s_N)_{N \geq 0}$ de cette suite, qui vérifie

$$\begin{aligned} s_{4N} &= 2s_N - \varepsilon_N, & s_{4N+1} &= 2s_N, \\ s_{4N+2} &= 2s_N + (-1)^N \varepsilon_N, & s_{4N+3} &= 2s_N. \end{aligned}$$

Ses comportements extrêmes ont été étudiés en 1978 par John Brillhart et Patrick Morton [18] par une approche élémentaire mais pleine de finesse. Puis en 1983 John Brillhart, Paul Erdős et Patrick Morton [17] ont obtenu le comportement asymptotique moyen de la suite par des méthodes de théorie analytique des nombres. La partie élémentaire est retracée dans [19] d'une manière très plaisante et qui restitue bien l'impression ressentie quand on étudie pour la première fois de telles suites.

Philippe Dumas
Équipe Specfun, INRIA Saclay
Philippe.Dumas@inria.fr

Document disponible à l'URL
<http://specfun.inria.fr/dumas/Research/DAC/>.

Version révisée du
27 octobre 2016

Table des matières

Introduction	1
Chapitre 1. Équations fonctionnelles	3
1. Des formes variées	3
2. Opérateurs	3
3. Définition des récurrences diviser pour régner	7
4. Comparaison des différentes formes	8
5. Récurrence bien fondée et conditions initiales	14
Chapitre 2. Bestiaire	17
1. Algorithmique	17
2. Mots	19
3. Théorie des nombres	19
Chapitre 3. Séries rationnelles	21
1. Séries rationnelles dans une base de numération	21
2. Propriétés de stabilité	24
3. Représentation linéaire	25
4. Cohérence et décalage	29
5. Lien avec la théorie des langages formels	36
Chapitre 4. Bornes	39
1. Résultats classiques	39
2. Sous-suites rationnelles au sens classique	41
3. Rayon spectral	41
Chapitre 5. Algèbre linéaire	45
1. Processus de calcul	46
2. Technique	46
3. Exemple développé	52
Annexe A. Questions	57
Annexe B. Réponses	61
Annexe. Bibliographie	71
Annexe. Index	75

Introduction

Les récurrences *diviser pour régner*, qui fréquemment relient les valeurs d'une suite en un entier et sa moitié, tirent leur nom de la stratégie diviser pour régner communément employée en algorithmique. Mais elles apparaissent aussi dans des problèmes de dénombrement liés à la combinatoire des mots ou à la combinatoire des partitions, ou encore en lien avec les séries algébriques à coefficients dans un corps fini, voire de manière inattendue dans des questions d'optimisation. Leur aspect exotique et les différentes formes qu'elles peuvent prendre leur confèrent un aspect déroutant.

Cette introduction élémentaire au domaine comporte deux parties. La première est algébrique et vise à donner une définition de ces récurrences à travers leurs différentes formes et à montrer que ces formes ont toutes la même capacité d'expression. Pour cela nous mettons en place des opérateurs linéaires qui traduisent les différentes manières de voir ces récurrences (chapitre 1). Quant aux preuves, elles consistent essentiellement en un calcul formel sur des polynômes dont les indéterminées sont soumises à des relations de commutation.

Après ce flot de technique, nous tentons de replacer ces récurrences dans les contextes variés où elles apparaissent (chapitre 2).

Toujours dans cette partie algébrique nous distinguons une famille de suites, introduite par Jean-Paul Allouche et Jeffrey Shallit [4] (chapitre 3). La raison en est que la grande majorité des suites satisfaisant à des récurrences diviser pour régner que l'on rencontre en pratique entre dans cette catégorie et que, de plus, elle est riche en propriétés.

Ensuite nous passons à l'analyse avec le but de déterminer le comportement asymptotique de suites solutions de ces récurrences. Nous commençons par quelques méthodes élémentaires, plus ou moins bien connues, qui fournissent des bornes (chapitre 4). Enfin, nous présentons une méthode basée sur l'algèbre linéaire, avec une approche relativement élémentaire donc, qui permet d'attraper les oscillations à l'abord surprenant que présentent ces suites, comme le montre l'illustration de couverture (chapitre 5). Cependant il existe d'autres méthodes d'attaque de la question, plus sophistiquées. Nous renvoyons à [33] pour une excellente introduction à l'usage de la théorie analytique des nombres dans l'analyse asymptotique de ces récurrences. Il existe aussi une approche par la théorie des probabilités dont [21] donne une brillante présentation.

L'ensemble se termine par quelques exercices (chapitre A), dont nous fournissons des solutions (chapitre B).

Nous avons muni ce texte de nombreux exemples dans l'espoir de le rendre moins aride et surtout concret. Aussi nous n'avons pas hésité à développer des points élémentaires, mais qui constituent une difficulté quand on aborde ces récurrences.

Équations fonctionnelles

Ce chapitre a pour but de fournir une définition des récurrences diviser pour régner linéaires. En effet cette terminologie, d'un usage fréquent en analyse d'algorithmes, est une expression usuelle mais qui n'a jamais reçu de définition mathématique. L'algèbre, non commutative, apporte une solution et permet de clarifier la question. Aussi, nous traitons, partiellement, la question de savoir si les équations fonctionnelles que nous rencontrons définissent des objets.

1. Des formes variées

Nous considérons des suites qui satisfont à des récurrences linéaires que nous pouvons appeler *récurrence diviser pour régner*. Par exemple, nous considérons la complexité au pire de l'algorithme de Karatsuba sur les polynômes, qui vérifie la relation de récurrence suivante écrite avec des fonctions plancher et plafond (développée dans l'exemple 12, page 18)

$$(1) \quad u_n = 2u_{\lceil \frac{n}{2} \rceil} + u_{\lfloor \frac{n}{2} \rfloor} + 4(n-1), \quad n \geq 2, \quad \text{avec } u_0 = 0, u_1 = 1,$$

ou encore l'interprétation en code binaire usuel du code de Gray (exemple 20, page 27) qui satisfait à la récurrence

$$\begin{aligned} u_{4n} &= 2u_{2n}, \\ u_{4n+1} &= -4u_n + 3u_{2n} + u_{2n+1}, \\ u_{4n+2} &= -4u_n + u_{2n} + 3u_{2n+1}, \\ u_{4n+3} &= 2u_{2n+1}, \end{aligned} \quad \text{avec } u_0 = 0.$$

Nous pouvons dire que le premier exemple est une récurrence de *type plancher-plafond*, alors que le second est de *type par cas*.

Évidemment nous pouvons récrire le premier exemple sous la forme par cas

$$(2) \quad \begin{aligned} u_{2n} &= 3u_n + 8n - 4, & \text{avec } u_0 = 0, \\ u_{2n+1} &= 2u_{n+1} + u_n + 8n, & \text{avec } u_1 = 1, \end{aligned}$$

en distinguant selon la parité de l'entier n . Par contre nous voyons mal comment mettre le second exemple dans une forme plancher-plafond. Ceci nous pose question : les deux formes ont-elles la même puissance d'expression ?

2. Opérateurs

Pour y voir clair, nous passons par un traitement algébrique d'opérateurs linéaires qui agissent sur les séries génératrices. À une suite de nombres $u = (u_n)$ dans un corps \mathbb{K} nous associons sa série génératrice ordinaire

$$(3) \quad u(x) = \sum_{n \geq 0} u_n x^n,$$

qui est dans l'espace des séries formelles $\mathbb{K}[[x]]$. Nous employons la même lettre pour la suite et sa série génératrice, mais cela ne créera pas d'ambiguïté car nous ferons référence aux noms des variables.

Nous définissons des opérateurs sur les séries. Pour disposer de propriétés de clôture nous sommes amenés à utiliser le corps des séries de Laurent formelles $\mathbb{K}((x))$, même si nous sommes intéressés par des séries formelles de $\mathbb{K}[[x]]$, dont le support est dans \mathbb{N} .

DÉFINITION 1. *L'opérateur de Mahler M_b ou simplement M associé à la base de numération $b \geq 2$ est l'opérateur de substitution de x^b à x sur l'espace des séries de Laurent, en formule*

$$(4) \quad M_b \sum_n u_n x^n = \sum_n u_n x^{bn}.$$

À chaque chiffre r de l'écriture des entiers en base b est associé un opérateur de section noté $T_{b,r}$, ou simplement T_r , qui extrait la partie de la série correspondant aux indices congrus à r modulo b ,

$$(5) \quad T_{b,r} \sum_n u_n x^n = \sum_k u_{bk+r} x^k.$$

L'opérateur de décalage avant S , qui est essentiellement la division par x , est défini par

$$(6) \quad S \sum_n u_n x^n = \sum_n u_{n+1} x^n.$$

L'opérateur de décalage arrière est la multiplication par x ,

$$(7) \quad x \sum_n u_n x^n = \sum_n u_{n-1} x^n.$$

Dans le cas $b = 2$, les deux opérateurs de section T_0 et T_1 extraient les parties paire et impaire de la série, mais avec une compression qui supprime les zéros.

2.1. Formulaire. Nous voyons tout de suite les propriétés suivantes.

PROPOSITION 1. *L'opérateur de Mahler $M = M_b$, les opérateurs de section $T_r = T_{b,r}$, $0 \leq r < b$, les opérateurs de décalage S et x sont tous linéaires. Ils sont liés par les formules suivantes,*

$$(8) \quad T_{b,r} T_{b',r'} = T_{bb',b'r+r'},$$

$$(9) \quad T_0 M = 1, \quad T_r M = 0 \quad (0 < r < b),$$

$$(10) \quad \sum_{0 \leq r < b} x^r M T_r = 1,$$

$$(11) \quad M x = x^b M,$$

$$(12) \quad S T_r = T_r S^b.$$

$$(13)$$

Les opérateurs de section vérifient une propriété de compatibilité avec le produit,

$$(14) \quad T_r(f(x)g(x)) = \sum_{s+t \equiv r \pmod{b}} x^{\lfloor \frac{s+t}{b} \rfloor} T_s f(x) T_t g(x)$$

et en particulier

$$(15) \quad T_r(f(x)Mg(x)) = (T_r f(x))g(x).$$

DÉMONSTRATION. Tout est élémentaire. La seule formule qui pose légèrement question est (14). Nous l'obtenons en nous basant sur la formule (10) et le calcul

$$\begin{aligned} f(x)g(x) &= \sum_{s,t} x^s T_s f(x^b) \times x^t T_t f(x^b) \\ &= \sum_r \sum_{s+t \equiv r} x^{s+t} T_s f(x^b) \times x^t T_t f(x^b) \\ &= \sum_r x^r \sum_{s+t \equiv r} x^{bq} T_s f(x^b) \times x^t T_t f(x^b), \end{aligned}$$

où nous avons noté $s+t = bq+r$, $0 \leq r < b$, la division euclidienne de $s+t$ par b . Le quotient $q = \lfloor \frac{s+t}{b} \rfloor$ ne peut prendre comme valeur que 0 ou 1. La formule (10) donne une autre écriture de $f(x)g(x)$ et par identification avec l'expression ci-dessus la formule (14). \square

La formule (10) dit comment il est possible de reconstruire une série à l'aide de ses sections. D'ailleurs elle pourrait servir de définition à la notion de section, car le membre de gauche n'a qu'une écriture possible, ce que nous venons d'utiliser dans la preuve ci-dessus. La formule (14) dit par exemple que la partie paire d'un produit s'obtient en additionnant le produit des parties paires et le produit des parties impaires, mais avec un décalage d'une unité pour ce dernier

$$T_{2,0}(f(x)g(x)) = T_{2,0}f(x)T_{2,0}g(x) + xT_{2,1}f(x)T_{2,1}g(x).$$

Une conséquence directe de (12) est l'invariance de $\mathbb{K}(x)$ par les sections.

PROPOSITION 2. *Les sections d'une fraction rationnelle sont des fractions rationnelles.*

DÉMONSTRATION. Une fraction rationnelle f a la propriété remarquable que ses images $S^k f$, $k \geq 0$, par le décalage avant restent dans un espace de dimension finie \mathcal{F} . C'est la raison pour laquelle son développement en série de Laurent se calcule par une usuelle récurrence linéaire à coefficients constants. Il en résulte que, pour $0 \leq r < b$, la série $T_r f$ a toutes ses décalées $S^k T_r f = T_r S^{bk} f$, $k \geq 0$, dans l'espace de dimension finie $T_r \mathcal{F}$ et est donc une fraction rationnelle. \square

EXEMPLE 1. Avec $b = 2$, nous calculons les parties paire et impaire de la fraction $(1+3x)/(x^3(1+2x))$,

$$T_{2,0} \frac{1+3x}{x^3(1+2x)} = \frac{1}{x(1-4x)}, \quad T_{2,1} \frac{1+3x}{x^3(1+2x)} = \frac{1-6x}{x^2(1-4x)},$$

et nous constatons bien (formule (10))

$$1 \times \frac{1}{x^2(1-4x^2)} + x \times \frac{1-6x^2}{x^4(1-4x^2)} = \frac{1+3x}{x^3(1+2x)}.$$

\triangle

$$\begin{array}{r|l}
xM^2 & + 1 + x & (1-x)M + 1 \\
-\frac{x^3}{1-x^3}M & + 1 + x & \frac{x}{1-x^3}M - \frac{x}{(1-x)(1-x^3)} \\
1 + x + \frac{x}{(1-x)(1-x^3)} & &
\end{array}$$

FIGURE 1. Une division dans l'anneau de polynômes tordus $\mathbb{Q}(x)[M]$ avec $b = 3$ (exemple 2).

2.2. Arithmétique. L'opérateur de Mahler M ne commute pas avec la multiplication par x . Nous avons seulement une relation de commutation $Mx = x^b M$, qu'il faut comprendre comme l'assertion *pour toute série* $u(x)$, $Mxu(x) = x^b Mu(x)$. Il n'en demeure pas moins que ces deux indéterminées x et M assujetties à cette relation de commutation définissent une structure assez riche. En effet, la formule

$$A = QB + R, \quad R = 0 \text{ ou } \deg_M R < \deg_M B,$$

(qui utilise $A = QB + R$ et non pas $A = BQ + R$) définit une division euclidienne à droite sur l'anneau $\mathbb{K}(x)[M]$, pour A et B des polynômes en M à coefficients des fractions rationnelles en x , avec $B \neq 0$. La structure obtenue est un *anneau de polynômes tordus* ou encore une *extension de Ore* [51].

EXEMPLE 2. Nous pouvons par exemple (figure 1) effectuer la division euclidienne

$$\begin{aligned}
x^2 M + (1 + x) &= \left(\frac{x}{1-x^3} M - \frac{x}{(1-x)(1-x^3)} \right) ((1-x)M + 1) \\
&\quad + \frac{1+x-x^2-x^3+x^5}{(1-x)(1-x^3)},
\end{aligned}$$

exactement comme nous procéderions pour une division de polynômes en une indéterminée sur un corps commutatif, en veillant seulement à respecter la relation de commutation. \triangle

Cette division euclidienne unilatérale permet de développer une arithmétique similaire à l'arithmétique usuelle des polynômes.

THÉORÈME 1. *L'algèbre $\mathbb{K}(x)[M]$ munie de la relation $Mx = x^b M$ a une structure d'anneau euclidien à gauche. En particulier les idéaux à gauche sont principaux.*

La conséquence directe de ce résultat est que les opérateurs de Mahler qui s'annulent sur une série donnée sont représentés par des polynômes tordus qui forment un idéal à gauche principal. Autrement dit tous ces polynômes sont les multiples d'un certain polynôme, que l'on peut qualifier de minimal. Ainsi il existe une notion d'équation de Mahler minimale pour une série.

De plus le PGCD (à droite) de plusieurs polynômes tordus s'interprète comme un polynôme annulateur pour l'intersection des espaces de solutions des opérateurs associés. Quant au PPCM (à gauche), il fournit un polynôme annulateur pour la somme des espaces solutions.

EXEMPLE 3. Les deux polynômes

$$L_1 = (1 + x^2) - (1 + x)^2 M, \quad L_2 = 1 - (1 - x)M,$$

avec $b = 2$, s'annulent respectivement sur la fraction rationnelle et le produit infini

$$f_1(x) = \frac{1-x}{1+x}, \quad f_2(x) = \prod_{k \geq 0} (1-x^{2^k}).$$

Leur PPCM

$$L = x(3+x^4) - (1+x)(3+x^2-x^3+2x^4-x^5)M + (1-x^4)(3+x^2)M^2$$

s'annule sur f_1 et f_2 . △

3. Définition des récurrences diviser pour régner

Les séries formelles étant d'un emploi plus facile que les suites, nous allons prendre comme point de référence les équations de Mahler pour définir la notion de récurrence diviser pour régner.

DÉFINITION 2. *Une équation de Mahler est une équation linéaire de la forme $L(x, M)u(x) = v(x)$ avec $L(x, M) = \ell_0(x) + \ell_1(x)M + \dots + \ell_d(x)M^d$, soit plus explicitement*

$$(16) \quad \ell_0(x)u(x) + \ell_1(x)u(x^b) + \dots + \ell_d(x)u(x^{b^d}) = v(x)$$

où $\ell_0(x), \ell_1(x), \dots, \ell_d(x)$ et $v(x)$ sont des polynômes de $\mathbb{K}[x]$.

Une récurrence diviser pour régner est la traduction en termes de suite d'une équation de Mahler.

Si elle ne se réduit pas à $0 = 0$, une équation de Mahler homogène exprime une relation de dépendance linéaire sur le corps des fractions rationnelles $\mathbb{K}(x)$ entre les séries $u, Mu, \dots, M^k u, \dots$ obtenues par itération de l'opérateur de Mahler sur u . Dans le cas non homogène, il convient d'ajouter 1 dans la famille considérée. Dans l'équation (16), les coefficients sont des polynômes et cette hypothèse n'est pas restrictive parce que nous pouvons toujours évacuer les dénominateurs d'une relation de dépendance.

Passons à la traduction en terme de suites et supposons que la série génératrice $u(x)$ soit solution de l'équation de Mahler $L(x, M)u(x) = v(x)$. Nous avons besoin d'une convention d'écriture que nous explicitons dans la définition suivante.

DÉFINITION 3. *Une suite $(u_n)_{n \geq 0}$ est étendue aux rationnels par la formule*

$$(17) \quad u_\nu = \begin{cases} u_n & \text{si } \nu \text{ est l'entier naturel } n, \\ 0 & \text{si } \nu \text{ n'est pas un entier naturel.} \end{cases}$$

Avec cette notation, le coefficient de x^m dans $x^j M^k u(x)$ est $u_{(m-j)/b^k}$. Si l'opérateur s'écrit

$$(18) \quad L(x, M) = \sum_{k=0}^d \sum_{j=0}^h \ell_{k,j} x^j M^k,$$

alors les coefficients de la série $u(x)$, élément de $\mathbb{K}[[x]]$, satisfont à la récurrence

$$(19) \quad \sum_{k=0}^d \sum_{j=0}^h \ell_{k,j} u_{\frac{m-j}{b^k}} = v_m, \quad m \geq 0.$$

Nous obtenons ainsi une troisième forme de récurrence. Nous pouvons la baptiser forme *fractionnaire*, parce qu'elle utilise l'indexation par des fractions.

EXEMPLE 4. Avec $b = 2$, l'équation de Mahler

$$(x + 2x^2)u(x) - (1 + x)u(x^2) + u(x^4) = 0$$

fournit la récurrence diviser pour régner sous forme fractionnaire

$$u_{m-1} + 2u_{m-2} - u_{\frac{m}{2}} - u_{\frac{m-1}{2}} + u_{\frac{m}{4}} = 0, \quad m \geq 0.$$

△

4. Comparaison des différentes formes

Nous disposons de trois formes d'écriture de récurrences :

- forme fractionnaire ;
- forme par cas ;
- forme plancher-plafond.

La forme fractionnaire est celle que nous avons prise comme définition des récurrences diviser pour régner. Elle est équivalente à l'écriture d'une équation de Mahler.

La forme par cas évoque une équation fonctionnelle basée sur les opérateurs de section. Pour être plus précis, nous avons besoin du lemme suivant.

LEMME 1. *Pour une suite $(u_n)_{n \geq 0}$ à support dans \mathbb{N} et pour un entier relatif s , la section que l'on peut appeler généralisée d'indice s s'exprime à l'aide des opérateurs de section de la définition 1 selon la formule*

$$(20) \quad \sum_{k \geq 0} u_{bk+s} x^k = x^{-q} T_{b,r} u(x) - x^{-q} \sum_{j=0}^{q-1} u_{bj+r} x^j,$$

en notant $s = bq + r$, $0 \leq r < b$, la division euclidienne naturelle de s par b . La formule est valable que l'entier q soit positif ou négatif, avec la convention usuelle des sommes vides.

Dans le cas $s \leq 0$ et même $s < b$, le terme correctif est nul. La formule est encore valable dans le cas $b = 1$.

EXEMPLE 5. Nous mettons facilement la récurrence de l'exemple 4 sous la forme par cas en récrivant la relation selon le résidu modulo 4 de l'entier m , plus précisément en posant successivement $m = 4k$, $m = 4k + 1$, $m = 4k + 2$, $m = 4k + 3$ avec $k \geq 0$,

$$\begin{aligned} u_{4k-1} + 2u_{4k-2} - u_{2k} - u_k &= 0, \\ u_{4k} + 2u_{4k-1} - u_{2k} &= 0, \\ u_{4k+1} + 2u_{4k} - u_{2k+1} &= 0, \\ u_{4k+2} + 2u_{4k+1} - u_{2k+1} &= 0. \end{aligned}$$

En multipliant le membre gauche de chaque équation par x^k et en sommant sur k entier naturel, nous obtenons le système

$$(21) \quad \begin{aligned} xT_{4,3}u + 2xT_{4,2}u - T_{2,0}u - u &= 0, \\ T_{4,0}u + 2xT_{4,3}u - T_{2,0}u &= 0, \\ T_{4,1}u + 2T_{4,0}u - T_{2,1}u &= 0, \\ T_{4,2}u + 2T_{4,1}u - T_{2,1}u &= 0. \end{aligned}$$

Nous avons utilisé les opérateurs de section en base 2 et 4 pour abrégé. Il est clair que nous pourrions n'utiliser que la base 2 en développant $T_{4,0} = T_{2,0}T_{2,0}$, $T_{4,1} = T_{2,0}T_{2,1}$, $T_{4,2} = T_{2,1}T_{2,0}$, $T_{4,3} = T_{2,1}T_{2,1}$. △

La proposition 2, sur la stabilité de $\mathbb{K}(x)$ par section, fournit aisément une caractérisation des solutions d'équations de Mahler en termes de sections.

THÉORÈME 2. *Si u est une série formelle solution d'une équation de Mahler non triviale, alors sous l'action des opérateurs de section elle engendre un espace de dimension finie sur $\mathbb{K}(x)$.*

Inversement si les sections itérées d'une série u reste dans un espace de dimension finie sur $\mathbb{K}(x)$, alors u est solution d'une équation de Mahler non triviale.

Avant de passer à une preuve, donnons deux exemples qui feront comprendre la démarche.

EXEMPLE 6. Reprenons l'équation de Mahler de l'exemple 4. Nous l'écrivons sous la forme

$$u(x) = -\frac{(-x-1)u(x^2)}{x(2x+1)} - \frac{u(x^4)}{x(2x+1)}.$$

Si maintenant nous considérons les expressions de la forme

$$c_0(x)u(x) + c_1(x)u(x^2)$$

avec des $c_k(x)$, $0 \leq k \leq 1$, rationnels, nous les récrivons en utilisant l'égalité ci-dessus sous la forme

$$c_0(x) \left(\frac{(1+x)u(x^2)}{x(2x+1)} - \frac{u(x^4)}{x(2x+1)} \right) + c_1(x)u(x^2)$$

ou encore, par regroupement des termes en $u(x^2)$ et $u(x^4)$,

$$\left(\frac{c_0(x)(1+x)}{x(2x+1)} + c_1(x) \right) u(x^2) - \frac{c_0(x)}{x(2x+1)} u(x^4).$$

L'application des opérateurs de section $T_{2,0}$ et $T_{2,1}$ donne les images

$$\begin{aligned} & \left(-\frac{T_{2,0}c_0(x)}{1-4x} + \frac{T_{2,1}c_0(x)(1-2x)}{1-4x} + T_{2,0}c_1(x) \right) u(x) \\ & \quad + \left(2\frac{T_{2,0}c_0(x)}{1-4x} - \frac{T_{2,1}c_0(x)}{1-4x} \right) u(x^2), \\ & \left(\frac{T_{2,0}c_0(x)(1-2x)}{(1-4x)x} - \frac{T_{2,1}c_0(x)}{1-4x} + T_{2,1}c_1(x) \right) u(x) \\ & \quad + \left(-\frac{T_{2,0}c_0(x)}{(1-4x)x} + 2\frac{T_{2,1}c_0(x)}{1-4x} \right) u(x^2). \end{aligned}$$

Ces expressions sont encore des combinaisons linéaires de $u(x)$, $u(x^2)$ à coefficients des fractions rationnelles. Ainsi l'espace vectoriel sur $\mathbb{K}(x)$ engendré par $u(x)$, $u(x^2)$ est stable par les opérateurs de section et, bien sûr, contient $u(x)$. \triangle

EXEMPLE 7. Le système (21) de l'exemple 5 se résout par rapport aux $T_{4,r}u$, $0 \leq r < 4$, en

$$\begin{aligned} T_{4,0}u &= \frac{1}{16x-1} (T_{2,0}u + 4xT_{2,1}u + 2u), \\ T_{4,1}u &= \frac{1}{16x-1} (-2T_{2,0}u + (8x-1)T_{2,1} - 4u), \\ T_{4,2}u &= \frac{1}{16x-1} (4T_{2,0}u + T_{2,1}u - 4u), \\ T_{4,3}u &= \frac{1}{x} \frac{1}{16x-1} ((8x-1)T_{2,0} - 2xT_{2,1}u - u). \end{aligned}$$

Au vu des ces égalités il est clair que l'espace des séries formelles engendré par u , $T_{2,0}u$, $T_{2,1}u$ est stable par section (figure 2), le corps de base étant le corps $\mathbb{K}(x)$ des fractions rationnelles. De manière équivalente, nous aurions pu considérer l'espace des suites engendré par (u_n) , (u_{2n}) et (u_{2n+1}) .

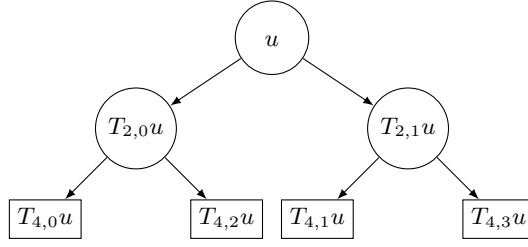


FIGURE 2. À partir d'une série formelle ou d'une suite u , nous fabriquons ses sections binaires. Si, par exemple, ses sections $T_{4,r}u$, $0 \leq r < 4$, se récrivent comme combinaisons linéaires de u , $T_{2,0}u$, $T_{2,1}u$, alors toutes les sections $T_{2^k,r}u$, $k \geq 0$, $0 \leq r < 2^k$, se récrivent en fonction de ces trois là et donc les sections engendrent un espace de dimension finie, en l'occurrence 3 au plus.

△

Passons à la démonstration. Elle est une reprise de [23, Th. 1] ou de [6, Th. 12.2.5] par une simple extension des scalaires de \mathbb{K} à $\mathbb{K}(x)$. Le point crucial est que le corps des coefficients est stable par section.

DÉMONSTRATION. Une équation de Mahler non triviale vérifiée par $u(x)$ exprime une relation de dépendance à coefficients dans $\mathbb{K}(x)$ entre la série 1 et les itérées $M^k u(x)$, $k \geq 0$. Nous pouvons l'écrire

$$(22) \quad u(x) = a(x) + a_1(x)Mu(x) + \cdots + a_d(x)M^d u(x),$$

avec $a(x)$ et les $a_k(x)$, $1 \leq k \leq d$, dans $\mathbb{K}(x)$. Considérons l'espace \mathcal{V} engendré sur $\mathbb{K}(x)$ par $1, u(x), \dots, M^{d-1}u(x)$. Un élément de cet espace s'écrit

$$(23) \quad \begin{aligned} v(x) &= c(x) + c_0(x)u(x) + c_1(x)Mu(x) + \cdots + c_{d-1}(x)M^{d-1}u(x) \\ &= (c(x) + c_0(x)a(x)) + (c_1(x) + c_0(x)a_1(x))Mu(x) + \cdots \\ &\quad + (c_{d-1}(x) + c_0(x)a_{d-1}(x))M^{d-1}u(x) + c_0(x)a_d(x)M^d u(x), \end{aligned}$$

avec $c(x)$, et les $c_k(x)$, $0 \leq k \leq d-1$ dans $\mathbb{K}(x)$. Si nous appliquons l'opérateur de section T_r , nous obtenons

$$(24) \quad \begin{aligned} T_r v(x) &= [T_r(c(x) + c_0(x)a(x))] + [T_r(c_1(x) + c_0(x)a_1(x))]u(x) + \cdots \\ &\quad + [T_r(c_{d-1}(x) + c_0(x)a_{d-1}(x))]M^{d-2}u(x) + [T_r c_0(x)a_d(x)]M^{d-1}u(x) \end{aligned}$$

et ceci montre que l'espace \mathcal{V} est stable par section, car les $T_r(c_k(x) + c_0(x)a_k(x))$, $0 \leq k \leq d-1$, $T_r c_0(x)a_d(x)$, sont des fractions rationnelles.

Inversement, supposons que u soit dans un espace \mathcal{V} qui est stable par les opérateurs de section et de dimension finie sur $\mathbb{K}(x)$, admettant une base $(v_k)_{0 \leq k \leq d-1}$. Cela amène une égalité

$$(25) \quad u(x) = \sum_{k=0}^{d-1} c_{0,k}(x)v_k(x).$$

Nous récrivons chacune des séries $v = v_k$ en fonction de ses sections selon (10),

$$(26) \quad v(x) = \sum_{0 \leq r < b} x^r T_r v(x^b)$$

et nous tenons compte du fait que les sections $T_r v(x)$ s'expriment elles-même dans la base. Nous obtenons une écriture

$$(27) \quad u(x) = \sum_{k=0}^{d-1} c_{1,k}(x) v_k(x^b)$$

avec des polynômes $c_{1,k}(x)$, $0 \leq k \leq d-1$. Nous itérons le passage de (25) à (27) en utilisant (26) appliqué en x^b au lieu de x , puis en x^{b^2} , etc. Cela donne des égalités

$$(28) \quad u(x) = \sum_{k=0}^{d-1} c_{m,k}(x) v_k(x^{b^m}), \quad m \geq 0.$$

Dans l'égalité numéro m avec $0 \leq m \leq d$, nous substituons $x^{b^{d-m}}$ à x d'où

$$(29) \quad u(x^{b^{d-m}}) = \sum_{k=0}^{d-1} c_{m,k}(x^{b^{d-m}}) v_k(x^{b^d}).$$

Ceci montre que les $d+1$ séries $u(x)$, $u(x^b)$, \dots , $u(x^{b^d})$ sont dans l'espace vectoriel sur le corps des fractions rationnelles engendré par les $v_k(x^{b^d})$, $0 \leq k \leq d-1$. Ceci prouve une dépendance linéaire qui se traduit par une équation de Mahler. \square

Le passage effectif d'une relation sur les sections à une équation de Mahler suppose la mise en place d'une structure d'algèbre linéaire puisque l'argument essentielle de la preuve qui précède est la dépendance linéaire. Nous traiterons un exemple en page 28.

Il reste une forme que nous n'avons pas traitée, la forme plancher-plafond. La formule

$$(30) \quad \left\lceil \frac{n}{b} \right\rceil = \left\lfloor \frac{n+b-1}{b} \right\rfloor$$

valable pour tout entier $b \geq 1$ et tout entier n montre qu'il suffit de considérer une forme qui n'utilise que la fonction plancher. De plus le lien entre suite et série génératrice est fourni par le lemme suivant.

LEMME 2. *Pour une suite $(u_n)_{n \geq 0}$ à support dans \mathbb{N} et pour un entier relatif s , est vérifiée la relation*

$$(31) \quad \sum_{n \geq 0} u_{\lfloor \frac{n+s}{b} \rfloor} x^n = x^{-s} (1 + x + \dots + x^{b-1}) u(x^b) - x^{-s} (1 + x + \dots + x^{b-1}) \sum_{n=0}^{q-1} u_n x^{bn} - x^{-r} \sum_{i=0}^{r-1} x^i u_q.$$

où $u(x)$ est la série génératrice de la suite (u_n) , en notant $s = bq + r$, $|r| < b$, $\text{sgn}(r) = \text{sgn}(s)$, la division euclidienne symétrisée de s par b . La formule est valable que l'entier q soit positif ou négatif, avec la convention usuelle des sommes vides.

La division que nous appelons symétrisée est la division usuelle dans le cas positif et la division usuelle de l'opposé dans le cas négatif. Dans le cas $s \leq 0$, le terme correctif est nul. La formule est encore valable dans le cas $b = 1$.

Rassemblons les résultats obtenus.

THÉORÈME 3. *Pour une suite (u_n) à support dans \mathbb{N} et pour sa série génératrice $u(x)$, avec un entier $b \geq 2$ donné,*

- *une récurrence de type fractionnaire ;*
- *une récurrence de type plancher-plafond ;*
- *une récurrence par cas ;*
- *une équation de Mahler ;*
- *un système sur les sections*

ont des capacités d'expression équivalentes.

DÉMONSTRATION. Nous avons pris comme définition des récurrences diviser pour régner les récurrences de type fractionnaire, qui ne sont que la traduction des équations de Mahler sur les séries génératrices. Comme nous l'avons remarqué dès le début, une récurrence de type fractionnaire se réécrit tout de suite en récurrence par cas. Nous avons ensuite vu qu'une récurrence par cas se réécrit, grâce au lemme 1, en un système sur les sections. Le théorème 2 dit qu'un tel système fournit une équation de Mahler. Nous obtenons ainsi les [flèches bleues](#) de la figure 3. Mais nous avons aussi vu qu'une récurrence fractionnaire peut se récrire en équation de Mahler et que, partant d'une équation de Mahler, nous savons obtenir un système sur les sections par le théorème 2. Bien sûr, un système sur les sections fournit une récurrence par cas. Nous disposons ainsi des [flèches vertes](#) de la figure 3. Enfin une récurrence plancher-plafond peut se récrire uniquement avec des planchers (formule (30)) et le lemme 2 donne alors une équation de Mahler. Inversement si nous avons une équation de Mahler, nous pouvons forcer la présence d'un facteur $x^{-s}(1 + x + \dots + x^{b-1})$ comme dans le lemme 2, par multiplication et division, pour faire apparaître des fonctions génératrices correspondant à des expressions de suites indexées par des plafonds. Bien sûr, une forme plancher-plafond se réécrit en une récurrence par cas, ce qui est une autre voie possible. Nous obtenons ainsi les [flèches noires](#) de la figure 3. Il faut noter que dans toutes ces manipulations, nous utilisons au besoin des fractions rationnelles comme coefficients des équations fonctionnelles, mais que pour passer aux écritures sur les suites nous chassons les dénominateurs. \square

EXEMPLE 8. Revenons sur la récurrence (1) liée à l'algorithme de Karatsuba qui nous a servi d'introduction (et qui sera prouvée dans l'exemple 12, page 18),

$$u_n = 2u_{\lfloor \frac{n}{2} \rfloor} + u_{\lfloor \frac{n}{2} \rfloor} + 4(n-1), \quad n \geq 2, \quad \text{avec } u(0) = 0, u(1) = 1.$$

D'après la formule (30), nous pouvons récrire la récurrence ($b = 2$ ici)

$$u_n = 2u_{\lfloor \frac{n+1}{2} \rfloor} + u_{\lfloor \frac{n}{2} \rfloor} + 4(n-1).$$

Avec le lemme 2 (successivement $s = 1, s = 0$), nous obtenons, en tenant compte des valeurs initiales et du fait que la sommation se fait pour $n \geq 2$, l'équation de Mahler

$$(32) \quad xu(x) - (1+x)(2+x)u(x^2) = -x^2 + 4\frac{x^3}{(1-x)^2}.$$

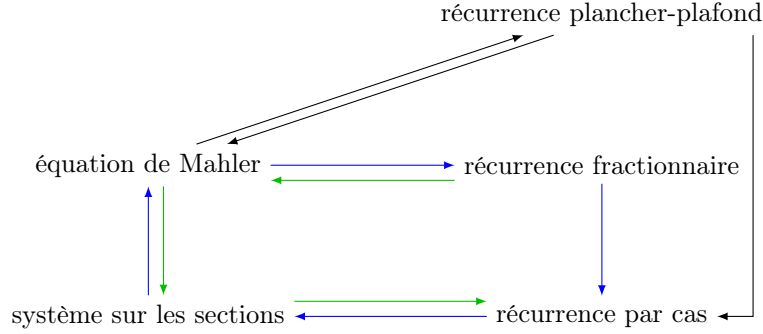


FIGURE 3. Les différentes formes des récurrences diviser pour régner.

En prenant le coefficient de x^m , $m \geq 3$, dans cette équation nous obtenons la récurrence sous forme fractionnaire

$$u_{m-1} - (2u_{\frac{m}{2}} + 3u_{\frac{m-1}{2}} + u_{\frac{m-2}{2}}) = 4(m-1).$$

Ceci se récrit par cas en

$$\begin{aligned} u_{2k-1} &= 2u_k + u_{k-1} + 8k - 4, & k \geq 2, \\ u_{2k} &= 3u_k + 8k, & k \geq 1, \end{aligned}$$

et n'est guère surprenant. Tout ceci est banal.

Reprenons plutôt l'équation de Mahler dans l'esprit du théorème 2 et de sa preuve. En appliquant les opérateurs de section aux deux membres de l'équation (32) écrite sous la forme

$$u(x) = \frac{(1+x)(2+x)}{x} u(x^2) - x + 4 \frac{x^2}{(1-x)^2}.$$

nous obtenons

$$T_{2,0}u(x) = 3u(x) + \frac{4x+4x^2}{(1-x)^2}, \quad T_{2,1}u(x) = \frac{2+x}{x}u(x) - \frac{1-10x+x^2}{(1-x)^2}.$$

Avec $T_{2,0}1 = 1$ et $T_{2,0}1 = 0$, ces relations montrent que le $\mathbb{Q}(x)$ -espace vectoriel \mathcal{V} engendré par 1 et $u(x)$ est stable par les opérateurs de section. Dans la base $(1, u(x))$, les endomorphismes induits ont pour matrices A_0 , A_1 et le vecteur $u(x)$ a pour matrice colonne de coordonnées C avec

$$A_0 = \begin{bmatrix} 1 & \frac{4x+4x^2}{(1-x)^2} \\ 0 & 3 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & -\frac{1-10x+x^2}{(1-x)^2} \\ 0 & \frac{2+x}{x} \end{bmatrix}, \quad C = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Nous reviendrons sur cet exemple à la page 26 en considérant que le corps des scalaires est \mathbb{Q} , alors qu'ici le corps de base est $\mathbb{Q}(x)$. \triangle

EXEMPLE 9. Le code de Gray ou code binaire réfléchi a la propriété que d'un entier au suivant un unique bit est modifié [55, Sec. 22.3]. L'interprétation du code Gray de l'entier n comme un code binaire usuel fournit une suite (u_n) , avec par exemple (figure 4)

$$u_4 = (\text{gray}(4))_2 = (0110)_2 = 6.$$

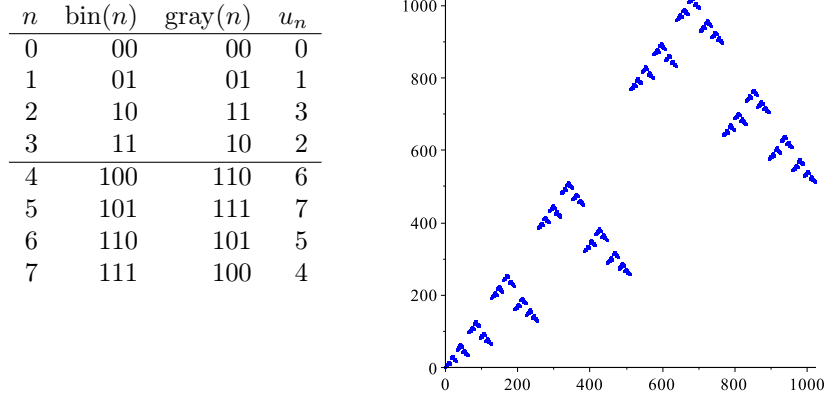


FIGURE 4. Le graphe de la suite (u_n) qui à un entier associe son code Gray vu comme un code binaire usuel (exemple 9).

Cette suite vérifie le système de quatre équations, qui avec la condition initiale $u_0 = 0$ la définit complètement,

$$\begin{aligned} u_{4n} &= 2u_{2n}, \\ u_{4n+1} &= -4u_n + 3u_{2n} + u_{2n+1}, \\ u_{4n+2} &= -4u_n + u_{2n} + 3u_{2n+1}, \\ u_{4n+3} &= 2u_{2n+1}. \end{aligned}$$

De cette récurrence il est possible de tirer une équation de Mahler (exemple 21, page 28)

$$x(1+x^2)u(x) - (1+x)(1+2x+2x^3+x^4)u(x^2) + 2(1+x)(1+x^2)(1+x^4)u(x^4) = 0.$$

Pour obtenir une récurrence de type plancher, nous utilisons la formule (31). Dans le terme en $y(x^2)$, le facteur $1+x$ convenable pour faire apparaître un expression avec plancher figure déjà. Il en est de même dans le terme en $y(x^4)$ d'après $(1+x)(1+x^2) = 1+x+x^2+x^3$. Nous voyons donc l'équation sous la forme

$$x(1+x^2)u(x) - (1+2x+2x^3+x^4) [(1+x)u(x^2)] + 2(1+x^4) [(1+x)(1+x^2)u(x^4)] = 0.$$

Le coefficient de x^{n+1} dans le membre gauche donne la formule de récurrence

$$u_n = -u_{n-2} + \left(u_{\lfloor \frac{n+1}{2} \rfloor} + 2u_{\lfloor \frac{n}{2} \rfloor} + 2u_{\lfloor \frac{n-2}{2} \rfloor} + u_{\lfloor \frac{n-3}{2} \rfloor} \right) - 2 \left(u_{\lfloor \frac{n+1}{4} \rfloor} + u_{\lfloor \frac{n-3}{4} \rfloor} \right).$$

Nous vérifions que les valeurs initiales $u_0 = 0$, $u_1 = 1$, $u_2 = 3$ garantissent une bonne définition de la suite. Nous pourrions introduire des fonctions plafond dans la formule, par exemple avec

$$u_{\lfloor \frac{n+1}{2} \rfloor} = u_{\lceil \frac{n}{2} \rceil}, \quad u_{\lfloor \frac{n-2}{2} \rfloor} = u_{\lceil \frac{n-3}{2} \rceil}, \quad u_{\lfloor \frac{n+1}{4} \rfloor} = u_{\lceil \frac{n-2}{4} \rceil}.$$

△

5. Récurrence bien fondée et conditions initiales

Nous sommes maintenant familiarisés avec les différentes écritures des récurrences diviser pour régner. Mais, quelle que soit la forme utilisée, ces récurrences sont des équations fonctionnelles dans un espace de suites ou de séries formelles et rien ne dit que ces équations possèdent des solutions. Commençons par un exemple.

EXEMPLE 10. Prenons l'équation de Mahler

$$x^3y(x) - (1 + 2x^2)y(x^2) + y(x^4) = 0.$$

Elle se traduit en la récurrence

$$(33) \quad u_{m-3} - u_{\frac{m}{2}} - 2u_{\frac{m-2}{2}} + u_{\frac{m}{4}} = 0, \quad m \geq 0.$$

Pour m assez grand, l'indice le plus grand parmi $m-3$, $m/2$, $m/2-1$, $m/4$ est $m-3$. Si les termes de la suite pour les indices 0 à $m-2$ sont définis, alors la formule détermine u_{m-3} d'une unique manière. Cette assertion est valable pour les m vérifiant

$$m-3 > \frac{m}{2}, \quad m-3 > \frac{m}{4}.$$

(Il est inutile d'écrire $m-3 > m/2-1$, qui découle de la première inégalité.) Ces contraintes imposent $m > 6$. Autrement dit, la récurrence est bien fondée à partir du rang $m = 7$. Pour le début, elle se traduit en un petit système (nous récrivons la formule (33) pour $m = 0, m = 1, \dots, m = 6$)

$$\begin{cases} 0 = 0, \\ 0 = 0, \\ -2u_0 - u_1 = 0, \\ u_0 = 0, \\ -u_2 = 0, \\ u_2 = 0, \\ u_2 = 0. \end{cases}$$

Celui-ci se résout en $u_0 = u_1 = u_2 = 0$ avec u_3 arbitraire. La récurrence est homogène et l'espace des solutions est une droite vectorielle engendrée par

$$u(x) = x^3 + 2x^5 + 2x^7 + 3x^9 + 2x^{11} + 4x^{13} + 3x^{15} + 4x^{17} + 2x^{19} + 4x^{21} + 4x^{23} + 6x^{25} + \dots$$

Si nous avons imposé $u_1 = 1$ par exemple, la récurrence n'aurait pas eu de solution. \triangle

Pour ce qui concerne les équations de Mahler, la question est résolue par le théorème suivant, extrait de [24].

THÉORÈME 4. Soit $\ell_0(x)y(x) + \ell_1(x)y(x^b) + \dots + \ell_d(x)y(x^{b^d}) = v(x)$ une équation de Mahler à coefficients polynomiaux, avec un coefficient $\ell_0(x)$ non nul. Si les valuations des polynômes $\ell_0(x), \ell_1(x), \dots, \ell_d(x)$ sont les entiers $\omega_0, \omega_1, \dots, \omega_d$, alors les éventuelles solutions de l'équation s'écrivent comme la somme d'une partie basse et d'une partie haute

$$y_b(x) = \sum_{n=0}^N y_n x^n, \quad y_h(x) = \sum_{n>N} y_n x^n.$$

La partie basse est déterminée par le système linéaire en les inconnues y_0, y_1, \dots, y_N dont les équations sont obtenues en extrayant le coefficient de x^m dans l'équation de Mahler pour $m = 0, m = 1, \dots, m = N + \omega_0$ avec

$$N = \left\lfloor \max_{1 \leq k \leq d} \frac{\omega_0 - \omega_k}{b^k - 1} \right\rfloor.$$

Si la partie basse existe, la partie haute s'obtient en déroulant la récurrence obtenue en extrayant le coefficient de x^m dans l'équation pour $m > N + \omega_0$.

EXEMPLE 11. Considérons l'équation de Mahler qui s'écrit

$$\begin{aligned} & x^6(1+x)(1-x-x^2)(1+x^2-x^6-x^{10}-x^{12})y(x) \\ & - x^2(1-x^2-x^4)(1+x+x^2+x^3-x^8-2x^9-2x^{12}-x^{13}+x^{14}-x^{15}-x^{16})y(x^2) \\ & + (1-x^2+x^4)(1-x^4-x^8)(1+x-x^3-x^5-x^6)y(x^4) = 0, \end{aligned}$$

ou encore

$$\begin{aligned} & x^6(1 - x^2 - x^3 - 2x^4 - x^5 - x^6 + 2x^8 + x^9 - x^{10} + x^{12} + x^{13} + 2x^{14} + x^{15})y(x) \\ & - x^2(1 + x - 2x^4 - 2x^5 - x^6 - x^7 - x^8 - 2x^9 + x^{10} + 2x^{11} - x^{12} + x^{13} + 3x^{14} + 2x^{17} + x^{19} + x^{20})y(x^2) \\ & + (1 + x - x^2 - 2x^3 + 2x^7 - x^8 - 3x^9 + x^{10} + 2x^{11} - 2x^{12} + 2x^{14} - x^{16} + x^{17} + x^{18})y(x^4) = 0. \end{aligned}$$

Les valuations des coefficients sont $\omega_0 = 6$, $\omega_1 = 2$ et $\omega_2 = 0$, d'où

$$N = \left\lfloor \max_{1 \leq k \leq d} \frac{\omega_0 - \omega_k}{b^k - 1} \right\rfloor = \left\lfloor \max\left(\frac{6-2}{2-1}, \frac{6-0}{4-1}\right) \right\rfloor = 4.$$

Nous regardons la matrice de taille $(1+4+6) \times (1+4)$, qui traduit la nullité du coefficient de x^m dans le membre gauche de l'équation pour $m = 0, \dots, m = 10$,

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -3 & 1 & 1 & 0 & 0 \\ -4 & 1 & 1 & 0 & 0 \\ 1 & -2 & -2 & 1 & 0 \\ 3 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Nous voyons tout de suite $y_0 = 0$, y_1 arbitraire, $y_2 = -y_1$, $y_3 = 0$, y_4 arbitraire. Autrement dit la partie basse de la solution s'écrit

$$y_b(x) = y_1x - y_1x^2 + y_4x^4$$

et nous pouvons choisir arbitrairement y_1 et y_4 . Ensuite nous pouvons calculer autant de termes que nous voulons de la suite (y_n) par une récurrence sans mystère mais passablement lourde à écrire, qui fournit

$$\begin{aligned} y(x) = & y_1(x - x^2 - 2x^5 - 2x^6 - 2x^7 - 6x^8 - 8x^9 - 12x^{10} - 22x^{11} - 34x^{12} + \dots) \\ & + y_4(x^4 + x^5 + 2x^6 + 3x^7 + 5x^8 + 8x^9 + 13x^{10} + 21x^{11} + 34x^{12} + \dots) \end{aligned}$$

△

Dans un souci de symétrie, il serait normal de traiter la cohérence des systèmes portant sur les sections d'une série. Mais la question de savoir si un tel système est bien fondé n'a pas reçu de réponse à ce jour. Une possibilité serait bien sûr de passer à une équation de Mahler, ce qui est en théorie possible, mais demande des calculs assez lourds. Une étude directe serait préférable. Nous reviendrons sur ce sujet dans un cas particulier (chapitre 3, section 4, page 29).

Bestiaire

Les récurrences diviser pour régner interviennent dans des domaines variés et nous tentons ici une classification, bien imparfaite et certainement non exhaustive.

1. Algorithmique

En algorithmique la stratégie *diviser pour régner* traite un problème de taille n en le cassant en b sous-problèmes de taille n/b , en traitant les b sous-problèmes récursivement, puis en fusionnant les résultats moyennant un coût t_n , ce qui amène une récurrence pour la complexité du calcul de la forme

$$u_n = bu_{n/b} + t_n.$$

Nous nous permettons ici une forme molle pour l'écriture de cette récurrence : la notation $u_{n/b}$ ne désigne pas l'écriture fractionnaire que nous avons utilisé auparavant, mais quelque chose qui hésite entre $u_{\lfloor n/b \rfloor}$ et $u_{\lceil n/b \rceil}$.

Donnons quelques exemples qui entre dans cette catégorie ou qui plus généralement utilise l'écriture des entiers dans une base de numération :

- (1) Tri [3] :
 - recherche binaire,
 - extrema,
 - k^e plus petit élément,
 - tri fusion,
 - tri rapide ;
- (2) Calcul algébrique [15] :
 - exponentiation binaire,
 - algorithme de Karatsuba,
 - algorithme de Toom-Cook,
 - algorithme de Schönhage–Strassen,
 - évaluation multipoint ;
- (3) Calcul matriciel [1, 30] :
 - produit de Strassen,
 - inversion d'une matrice triangulaire,
 - transformation de Fourier rapide,
 - décomposition en valeurs singulières,
 - valeurs et vecteurs propres de matrice symétrique tridiagonale ;
- (4) Géométrie algorithmique [54] :
 - enveloppe convexe,
 - paire la plus proche,
 - maximum en dimension $d \geq 2$,
 - diagramme de Voronoï.

Il existe une nette ambiguïté dans ces formulations car ces algorithmes ont de nombreuses variantes qui modifient l'écriture précise des récurrences. Nous allons détailler un exemple classique pour obtenir une formule solidement établie.

EXEMPLE 12 (Algorithme de Karatsuba). Nous voulons expliciter une formule de récurrence pour la complexité de l'algorithme de Karatsuba appliqué à la multiplication polynomiale. Nous considérons des polynômes a et b à coefficients dans un anneau commutatif \mathbb{A} . Nous utilisons comme paramètre de taille un entier n qui vérifie $\deg a < n$, $\deg b < n$. Avec des polynômes denses, n est le nombre de monômes de chacun des deux polynômes. L'appel récursif se fait en coupant en deux les deux polynômes. Cette assertion est floue et laisse différentes possibilités. Dans [1], le découpage des polynômes en deux parties se fait selon les sections, disons $p(x) = p_0(x^2) + xp_1(x^2)$. Ici, nous coupons les polynômes en une partie basse et une partie haute,

$$a = a_0(x) + x^k a_1(x), \quad b = b_0(x) + x^k b_1(x)$$

avec $0 < k < n - 1$ et des polynômes a_0, b_0 qui ont un degré strictement plus petit que k et des polynômes a_1, b_1 qui ont un degré strictement plus petit que $n - k$. Nous notons $M = \max(k, n - k)$, $m = \min(k, n - k)$. La méthode de Karatsuba consiste à calculer récursivement le produit ab par la formule

$$(34) \quad ab = a_0 b_0 + x^k ((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1) + x^{2k} a_1 b_1.$$

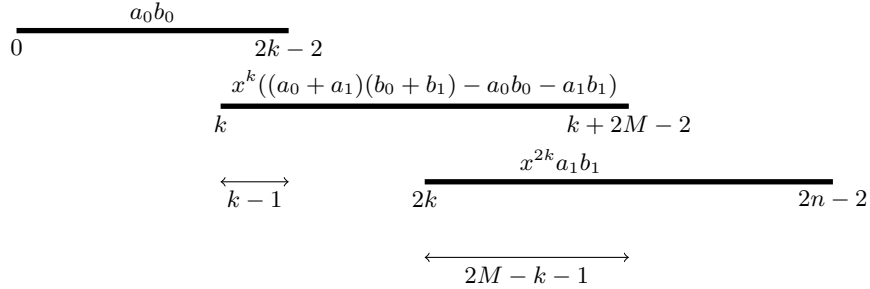


FIGURE 1. L'addition des trois termes de la formule de Karatsuba.

Notons u_n le coût de la multiplication de deux polynômes de degrés strictement plus petits que n par cette méthode en comptant une unité de coût pour chaque multiplication et chaque addition dans l'anneau de base \mathbb{A} . Pour appliquer la méthode nous calculons successivement

- les deux sommes $a_0 + a_1$ et $b_0 + b_1$, ce qui demande $2m$ additions ;
- les trois produits $a_0 b_0$, $a_1 b_1$, $(a_0 + a_1)(b_0 + b_1)$, qui ont respectivement comme coût u_k , u_{n-k} , u_M , soit globalement $u_k + u_{n-k} + u_M = 2u_M + u_m$;
- la soustraction à $(a_0 + a_1)(b_0 + b_1)$ de $a_0 b_0$, puis de $a_1 b_1$. L'une coûte $2k - 1$ et l'autre $2n - 2k - 1$, soit pour le tout $2n - 2$ additions ;
- enfin la somme des trois termes de la formule (34). Les deux premiers partagent un intervalle de degrés qui comporte $k - 1$ entiers (figure 1), alors que le deuxième et le troisième partage un intervalle de $2M - k - 1$ entiers, d'où un nombre d'additions égal à $2M - 2$.

Nous minimisons M en le prenant égal à $\lceil n/2 \rceil$, ce qui donne $k = M = \lceil n/2 \rceil$, $m = \lfloor n/2 \rfloor$. En additionnant les différents coûts, nous arrivons à la formule

$$(35) \quad u_n = 2u_{\lceil n/2 \rceil} + u_{\lfloor n/2 \rfloor} + 4n - 4, \quad n \geq 2,$$

avec $u_0 = 0$, $u_1 = 1$.

△

2. Mots

Dans le domaine des mots, les occurrences des suites diviser pour régner apparaissent de manière plus désordonnée. Nous pouvons citer comme première famille d'exemples les suites définies par un décompte de motifs ou plus généralement de configurations. En voici quelques exemples :

- nombre $e_1(n)$ de 1 dans l'écriture binaire de n ;
- suite de Golay-Rudin-Shapiro (nombre de 11) [60, 58] ;
- suite de Thue-Morse $((-1)^{e_1(n)})$ [5] ;
- mots sans recouvrement [20, 14].

Ensuite nous trouvons des exemples liés à des substitutions. Un exemple plaisant est le pliage de papier et ses variantes. Mais cela nous fait sortir de la numération ordinaire (substitutions à longueur non constante, fractal de Rauzy). Nous n'entrerons pas dans ce domaine extrêmement vaste [39].

Parmi ces suites, celles qui ne prennent qu'un nombre fini de valeurs sont b -automatiques : il existe un automate, constitué d'un état initial, de transitions étiquetées par les chiffres de la numération en base b , d'une fonction de sortie de l'ensemble des états dans un ensemble fini, qui permet le calcul de chaque terme de la suite. Pour un entier n , nous le décomposons en base b et nous utilisons cette décomposition pour voyager à partir de l'état initial dans l'automate. La fonction de sortie donne la valeur de la suite. Les deux sens de lecture du développement en base b (poids faible vers poids fort ou l'inverse) définissent la même classe de suites. Cette classe a été très largement étudiée [6].

EXEMPLE 13. Le nombre de 1 dans l'écriture binaire d'un entier est certainement la suite liée à la numération qui a été la plus étudiée. Cette suite (u_n) satisfait évidemment à la récurrence diviser pour régner

$$u_{2n} = u_n, \quad u_{2n+1} = u_n + 1, \quad u(0) = 0.$$

△

3. Théorie des nombres

La théorie des nombres est liée aux récurrences diviser pour régner à travers la numération [56]. La distinction entre arithmétique élémentaire et sophistiquée est passablement artificielle. Il suffit de penser aux partitions binaires d'entiers, qui n'emploient comme sommants que des puissances de 2, mais dont l'étude approfondie [29] est passablement sophistiquée.

- (1) Arithmétique élémentaire :
 - coefficients binomiaux impairs [33],
 - problème de Flavius Josèphe [41],
 - sommes de trois carrés,
 - approximation rationnelle (Stern-Brocot),
 - extrema de suite rationnelle dans une base de numération [17]
- (2) Arithmétique sophistiquée :
 - séries algébriques modulo p [22],
 - discrédance [34],
 - approximation rationnelle [2] ;
 - transcendance [8, 32].

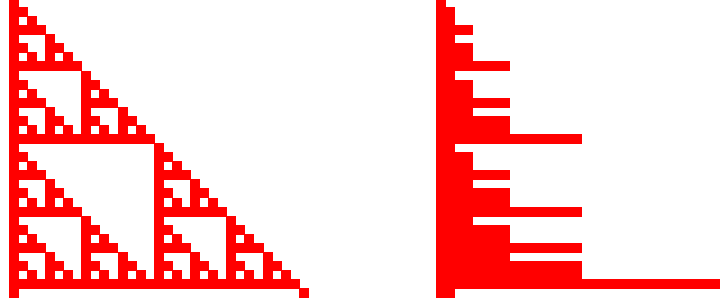


FIGURE 2. Le triangle de Pascal réduit modulo 2 (un carré rouge, respectivement blanc, représente 1, resp. 0). À droite le triangle est compressé pour mettre en valeur le nombre de 1 dans chaque ligne. Pour les puissances de 2, il vaut 2.

Nous fournissons un exemple élémentaire, qui nous l'espérons donnera au lecteur, à la lectrice, l'envie d'en savoir plus.

EXEMPLE 14. Le théorème de Lucas indique comment se comporte les coefficients binomiaux par rapport aux nombres premiers : pour deux entiers n et k qui ont comme développement en base le nombre premier p

$$n = (n_\ell \dots n_1 n_0)_p, \quad k = (k_\ell \dots k_1 k_0)_p$$

(le développement le plus court est complété à gauche par des zéros), nous avons [38]

$$\binom{n}{k} \equiv \binom{n_\ell}{k_\ell} \cdots \binom{n_1}{k_1} \binom{n_0}{k_0} \pmod{p}.$$

Nous voyons cela par un calcul modulo p

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} x^k &= (1+x)^n = (1+x)^{n_\ell p^\ell + \dots + n_1 p + n_0} = \prod_{r=0}^{\ell} (1+x)^{n_r p^r} = \prod_{r=0}^{\ell} (1+x^{p^r})^{n_r} \\ &= \prod_{r=0}^{\ell} \sum_{s_r=0}^{n_r} \binom{n_r}{s_r} x^{s_r p^r} = \sum_{s_0, s_1, \dots, s_\ell} \prod_{r=0}^{\ell} \binom{n_r}{s_r} x^{s_0 + s_1 p + \dots + s_\ell p^\ell} \\ &= \sum_{k=0}^n \sum_{\substack{s_0, s_1, \dots, s_\ell \\ s_0 + s_1 p + \dots + s_\ell p^\ell = k}} \prod_{r=0}^{\ell} \binom{n_r}{s_r} x^k. \end{aligned}$$

Pour la dernière égalité de la deuxième ligne, nous avons utilisé l'homomorphisme de Frobenius. À la troisième, nous écrivons qu'un produit de sommes est une somme de produits et en dernière ligne nous regroupons les termes suivants la puissance de x . Nous identifions ensuite les coefficients de x^k .

Particularisons la formule de Lucas au cas $p = 2$. Il n'y a que deux chiffres et d'après $\binom{0}{0} = 1$, $\binom{0}{1} = 0$, $\binom{1}{0} = 1$, $\binom{1}{1} = 1$ le produit

$$\binom{n_\ell}{k_\ell} \cdots \binom{n_1}{k_1} \binom{n_0}{k_0}$$

vaut 1 si et seulement si les bits égaux à 1 de k sont pris parmi les bits égaux à 1 de n . Donc si n a s_n bits égaux à 1, il y a 2^{s_n} entiers k entre 0 et n qui donnent un coefficient binomial égal à 1 dans la ligne numéro n du triangle de Pascal. Nous voyons ainsi surgir un lien entre arithmétique et diviser pour régner via la numération. \triangle

Séries rationnelles

Parmi les séries formelles, nous allons distinguer une classe particulière qui s'avère d'une occurrence fréquente.

1. Séries rationnelles dans une base de numération

DÉFINITION 4. Une série formelle (ou une suite) est rationnelle dans la base de numération b ou encore b -rationnelle, si sous l'action des opérateurs de section elle engendre un espace de dimension finie sur le corps \mathbb{K} .

Nous avons déjà rencontré une propriété similaire en section 4, mais alors le corps de base était le corps $\mathbb{K}(x)$ des fractions rationnelles. La notion est due à Jean-Paul Allouche et Jeffrey Shallit, qui parlent de suite k -régulière [4].

EXEMPLE 15. L'algorithme *dichopile* est une tentative pour trouver un équilibre entre temps et espace dans la génération aléatoire de mots d'un langage régulier [52, 53]. Les méthodes antérieures ont une complexité en temps $O(n)$ et utilise un espace de taille $O(n)$, alors que cette méthode dichopile a une complexité en temps $O(n \log n)$ et surtout utilise un espace de taille $O(\log n)$. La complexité en temps est donnée par la suite (u_n) définie par

$$u_n = n + v_n, \quad v_n = u_{\lfloor n/2 \rfloor - 1} + v_{\lceil n/2 \rceil}, \quad n \geq 2,$$

avec $u_1 = 1$, $v_1 = 0$ et nous complétons ces conditions initiales par $u_0 = 0$, $v_0 = 0$. Les relations précédentes se traduisent (lemme 2, page 11) sur les séries génératrices en

$$(36) \quad u(x) = \frac{x}{(1-x)^2} + v(x), \quad v(x) = x^2(1+x)u(x^2) + \frac{1+x}{x}v(x^2).$$

Si maintenant nous calculons les sections paires et impaires de $u(x)$ et $v(x)$, nous obtenons

$$\begin{aligned} T_{2,0}u(x) &= T_{2,0}v(x) + \frac{2x}{(1-x)^2}, & T_{2,0}v(x) &= x + v(x), \\ T_{2,1}u(x) &= T_{2,1}v(x) + \frac{1+x}{(1-x)^2}, & T_{2,1}v(x) &= x + \frac{v(x)}{x}. \end{aligned}$$

En poursuivant nous voyons rapidement que nous avons un espace de dimension au plus 7 sur \mathbb{Q} , engendré par $u(x)$, $v(x)$, $v(x)/x$, 1 , x , $1/(1-x)^2$, $x/(1-x)^2$, qui est stable sous l'action des opérateurs de section (figure 1). Si nous considérons que le corps de base est $\mathbb{Q}(x)$, à l'image de ce que nous avons fait dans les chapitres précédents, nous verrions un espace de dimension 2 et de base $(1, v(x))$.

△

Nous avons vu que la dépendance linéaire des sections se traduisaient en une équation de Mahler (théorème 2, page 9). L'énoncé utilisait comme corps de base le corps des fractions rationnelles $\mathbb{K}(x)$. Une dépendance sur \mathbb{K} étant aussi une dépendance sur $\mathbb{K}(x)$, l'énoncé suivant vient directement.

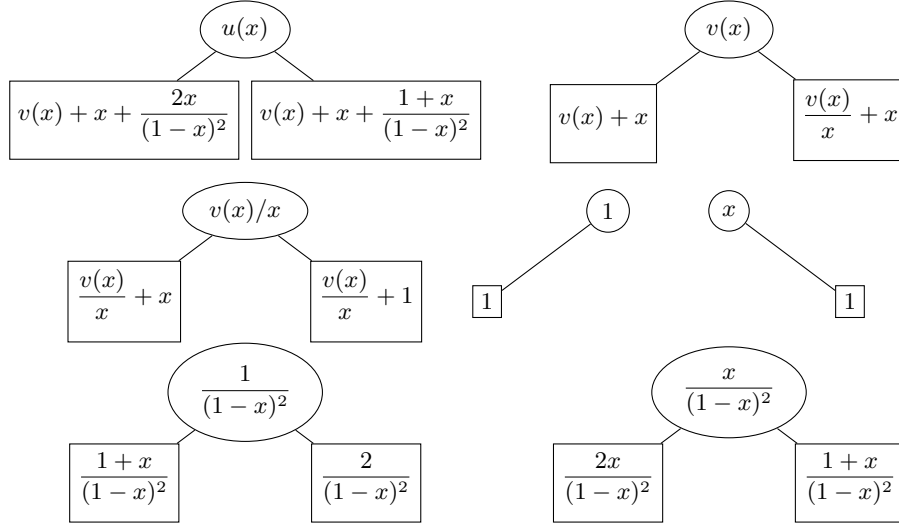


FIGURE 1. Une famille génératrice pour la complexité de l'algorithme dichopile (u_n). Le calcul de ses sections (section paire, fils gauche; section impaire, fils droit) montre la stabilité par section et le caractère 2-rationnel de la série génératrice $u(x)$ (exemple 15).

PROPOSITION 3. Une série b -rationnelle vérifie une équation de Mahler linéaire pour l'opérateur M relatif à la base de numération b .

Cependant, comme nous nous plaçons dans un cas particulier plus restrictif, en remplaçant $\mathbb{K}(x)$ par \mathbb{K} , nous n'avons pas la réciproque du théorème 2. Nous disposons cependant de l'énoncé suivant [36, 45]

THÉORÈME 5. Soit \mathbb{K} un corps de nombres et $f(x)$ une série formelle à coefficients dans \mathbb{K} qui satisfait à une équation de Mahler

$$\ell_0(x)f(x) + \ell_1(x)f(x^b) + \ell_d(x)f(x^{b^d}) = g(x),$$

avec des coefficients polynomiaux $\ell_k(x)$, $0 \leq k \leq d$, le coefficient $\ell_0(x)$ n'étant pas nul et un second membre polynomial $g(x)$.

Pour que la série $f(x)$ soit rationnelle en base b , il est suffisant que le coefficient $\ell_0(x)$ ait ses racines dans l'ensemble constitué de 0 et des racines de l'unité primitives d'ordre un entier qui n'est pas premier avec b .

Inversement cette condition est nécessaire si l'équation est une équation de Mahler homogène ($g(x) = 0$) minimale pour $f(x)$.

Pour le cas fréquent $b = 2$, la condition sur les racines de $\ell_0(x)$ est donc que ces racines peuvent être 0, -1 (ordre 2), $\pm i$ (ordre 4), $(1 \pm i\sqrt{3})/2$ (ordre 6), $(\pm 1 \pm i)/\sqrt{2}$ (ordre 8), ... L'adjectif *minimal* de la condition nécessaire fait référence au théorème 1, page 6.

EXEMPLE 16. Revenons sur l'algorithme dichopile (exemple 15). Nous voyons rapidement, par report de la première équation (36) dans la seconde, que la série $v(x)$ vérifie l'équation

$$v(x) = x^4 \frac{1+x}{(1-x)^2} + \frac{(1+x)(1+x^3)}{x} v(x^2).$$

Le théorème ne s'applique pas à cause du facteur $(1-x)^2$. La fraction rationnelle $x^4(1+x)/(1-x)^2$ est annulé par l'opérateur $x^4(1+x^2) - (1+x)^3M$. Nous multiplions à gauche l'opérateur $1 - (1+x)(1+x^3)/xM$ de l'équation précédente par cet opérateur et nous obtenons un nouvel opérateur et une équation homogène pour $v(x)$

$$x^6(1+x^2)v(x) - x^2(1+x)^2(1+x+x^3-x^4+2x^5-x^6+x^7)v(x^2) + (1+x)^3(1+x^2)^2(1-x^2+x^4)v(x^4) = 0.$$

Nous pouvons de même calculer d'abord une équation inhomogène pour $u(x)$ en utilisant celle que nous avons obtenu pour $v(x)$ et la première formule de (36). Nous annulons la partie inhomogène avec l'opérateur $x(1-x^2+x^4) - (1+x)^2(1-x+x^2)M$ et nous obtenons l'équation homogène

$$x^5(1+x^2)(1-x^2+x^4)u(x) - x(1+x-x^2-x^3+x^4+x^5+x^7-x^8+x^9+x^{11}-x^{12}+x^{13})u(x^2) + (1+x)^2(1+x^2)^3(1-x+x^2)u(x^4) = 0.$$

Pour chacune des deux équations, le coefficient d'indice 0 (au regard de M) a comme racines 0 et des racines de l'unité primitives d'ordre pair (ordre 4 pour $1+x^2$, ordre 12 pour $1-x^2+x^4$). Ceci montre que $u(x)$ et $v(x)$ sont rationnelles en base 2. \triangle

Cependant le cas particulier essentiel est celui où le coefficient $\ell_0(x)$ a au plus 0 comme racine.

PROPOSITION 4. *Une série formelle solution d'une équation de Mahler*

$$x^\omega u(x) = c_1(x)u(x^b) + \dots + c_d(x)u(x^{b^d}),$$

(ω est un entier naturel) avec des coefficients polynomiaux, est rationnelle en base b .

EXEMPLE 17. Reprenons la formule (32) de l'exemple 8

$$xu(x) - (1+x)(2+x)u(x^2) = -x^2 + 4\frac{x^3}{(1-x)^2}.$$

Le théorème 5 ne s'applique pas à cause du dénominateur $(1-x)^2$. L'opérateur sous-jacent à l'équation est $L = x - (1+x)(2+x)M$. Nous le multiplions à gauche par l'opérateur $x^3 - (1+x)^2M$, qui s'annule sur la fraction $x^3/(1-x)^2$, et nous obtenons l'opérateur

$$L' = x^4 - x^2(1+x)(1+3x+x^2)M + (1+x)^2(1+x^2)(2+x^2)M^2$$

ainsi que la nouvelle équation

$$x^4u(x) - x^2(1+x)(1+3x+x^2)u(x^2) + (1+x)^2(1+x^2)(2+x^2)u(x^4) = -x^5 + x^4(1+x)^2.$$

Elle montre que la complexité de l'algorithme de Karatsuba est une suite 2-rationnelle. \triangle

Il vaut la peine de récrire l'énoncé précédent en terme de suites.

PROPOSITION 5. *Une suite (u_n) qui satisfait à une relation de récurrence sous forme fractionnaire*

$$u_n = \sum_{k=1}^d \sum_{\ell=-s}^s c_{k,\ell} u_{\frac{n-\ell}{b^k}}$$

est rationnelle en base b .

DÉMONSTRATION. En effet les décalages qui apparaissent dans le membre droit correspondent à des multiplications par des monômes de Laurent (en x et $1/x$). En multipliant toute l'équation de Mahler qui traduit la récurrence par x^s nous retrouvons la forme de la proposition précédente. \square

Le point important est qu'il n'y a pas de décalage pour u_n mais seulement pour $u_{n/b}$, u_{n/b^2} , \dots . Nous pouvons dire que ces récurrences sont les *vraies récurrences diviser pour régner*.

2. Propriétés de stabilité

Les séries formelles qui sont rationnelles en base b forment un sous-ensemble de l'algèbre des séries formelles $\mathbb{K}[[x]]$. Cette algèbre possède de nombreuses propriétés de stabilité, qui ont justifié le titre de [4].

THÉORÈME 6. *Les séries formelles rationnelles en base b sont les éléments d'une sous-algèbre de $\mathbb{K}[[x]]$. Celle-ci est stable par la dérivation, par le produit de Hadamard, par le décalage arrière. Elle contient l'algèbre des polynômes.*

Rappelons qu'une série rationnelle est le développement en série formelle d'une fraction rationnelle qui n'a pas 0 comme pôle. Le résultat suivant [4, Th. 3.3] donne un exemple de série rationnelle dans une base de numération.

PROPOSITION 6. *Une série rationnelle est rationnelle dans une (et en fait toute) base de numération si et seulement la fraction rationnelle associée n'a comme pôles que des racines de l'unité (dans une extension de \mathbb{K}).*

EXEMPLE 18. La série caractéristique de l'ensemble des puissances de $b \geq 2$,

$$\chi(x) = \sum_{k \geq 0} x^{b^k}$$

est rationnelle en base b , par exemple parce qu'elle satisfait à $\chi(x) = x + \chi(x^b)$ et que ses sections sont données par $T_{b,0}\chi(x) = \chi(x)$, $T_{b,1}\chi(x) = 1$, $T_{b,r}\chi(x) = 0$ pour $1 < r < b$. Puisque $1/(1-x)$ est b -rationnelle, il en est donc de même de

$$\frac{1}{1-x}\chi(x) = \sum_{k \geq 0} x^{b^k} (1 + x + \dots + x^{b-1}),$$

qui est la série génératrice de la suite (u_n) qui vaut $k+1$ pour $b^k \leq n < b^{k+1}$, c'est-à-dire $u_n = 1 + \lceil \log_b n \rceil$ pour $n \geq 1$.

Dans la même veine, avec $b = 2$, la série

$$u(x) = \frac{x}{(1-x)^2} \sum_{k \geq 0} x^{2^k}$$

est 2-rationnelle. Elle est la série génératrice pour la complexité du tri fusion dans le cas le pire, qui est la solution de la récurrence

$$u_n = u_{\lfloor n/2 \rfloor} + u_{\lceil n/2 \rceil} + n - 1, \quad n \geq 2, \quad u_0 = u_1 = 0$$

et qui s'exprime donc explicitement en

$$u_n = \sum_{k=1}^n \lceil \log_2 k \rceil = n \lceil \log_2 n \rceil - 2^{\lceil \log_2 n \rceil} + 1, \quad n \geq 1.$$

△

3. Représentation linéaire

Puisque les sections d'une série rationnelle en base b demeurent dans un espace \mathcal{V} de dimension finie, nous pouvons par le choix d'une base de cet espace donner une représentation matricielle de l'action des sections sur la série. En fait, il n'est pas indispensable que la famille utilisée soit une base. Il suffit qu'elle soit une famille génératrice. Supposons donc que nous ayons une série u confinée dans un espace \mathcal{V} stable par section et muni d'une famille génératrice $(v_j)_{1 \leq j \leq d}$. Nous pouvons exprimer la suite u par un vecteur colonne C qui traduit le fait que u est combinaison linéaire des v_j , $1 \leq j \leq d$. De même les opérateurs de section $T_{b,r}$, $0 \leq r < b$, s'expriment par des matrices carrées A_r , $0 \leq r < b$. Enfin nous pouvons exprimer la forme linéaire qu'est l'évaluation en 0 par une matrice ligne L de taille d . L'intérêt de considérer ces quantités est lié au théorème suivant.

THÉORÈME 7. *Le coefficient d'indice N d'une série formelle $u(x)$ s'exprime par la formule*

$$(37) \quad u_N = T_{b,r_\ell} \cdots T_{b,r_0} u(0)$$

si l'entier N a pour écriture en base b le mot $r_\ell \dots r_0$ (avec les poids faibles à droite).

DÉMONSTRATION. Par application de l'opérateur de section $T_{b,r}$, la série $u(x)$, dont le terme constant est u_0 , devient la série

$$T_{b,r}u(x) = \sum_{k \geq 0} u_{bk+r} u_k,$$

dont le terme constant est u_r . Par itération de cette remarque, nous voyons que l'application des opérateurs de section liés à l'écriture en base b de l'entier N produit successivement comme termes constants les termes d'indices r_0 , $r_0 + br_1$, \dots et finalement $r_0 + br_1 + \dots + r_\ell b^\ell = N$. L'évaluation en 0 fournit donc bien u_N . \square

Nous aurions pu énoncer un résultat similaire pour les séries solutions d'une équation de Mahler non triviale. Nous aurions alors remplacé l'évaluation en 0 d'une série formelle par la prise du coefficient constant d'une série de Laurent.

La traduction en termes matriciels du théorème 7 donne, avec les notations définies auparavant, la formule $u_N = LA_{r_\ell} \cdots A_{r_0} C$, ce qui justifie la définition suivante.

DÉFINITION 5. *Une représentation linéaire d'une série $u(x)$ ou suite (u_n) rationnelle en base b est un triplet (L, A, C) constitué de*

- un vecteur ligne L ;
- une famille $(A_r)_{0 \leq r < b}$ de matrices carrées ;
- un vecteur colonne C ,

de tailles cohérentes et à coefficients dans \mathbb{K} , tel que le coefficient d'indice N de la série (ou le terme d'indice N de la suite) s'exprime comme le produit

$$(38) \quad u_N = LA_{r_\ell} \cdots A_{r_0} C.$$

Les éléments L , A , C sont respectivement les valeurs initiales, l'action, les coordonnées de la représentation linéaire.

Nous pouvons aussi noter que le vecteur ligne $LA_{r_\ell} \cdots A_{r_0}$ fournit les valeurs pour l'entier N des suites qui constituent la base ou famille génératrice.

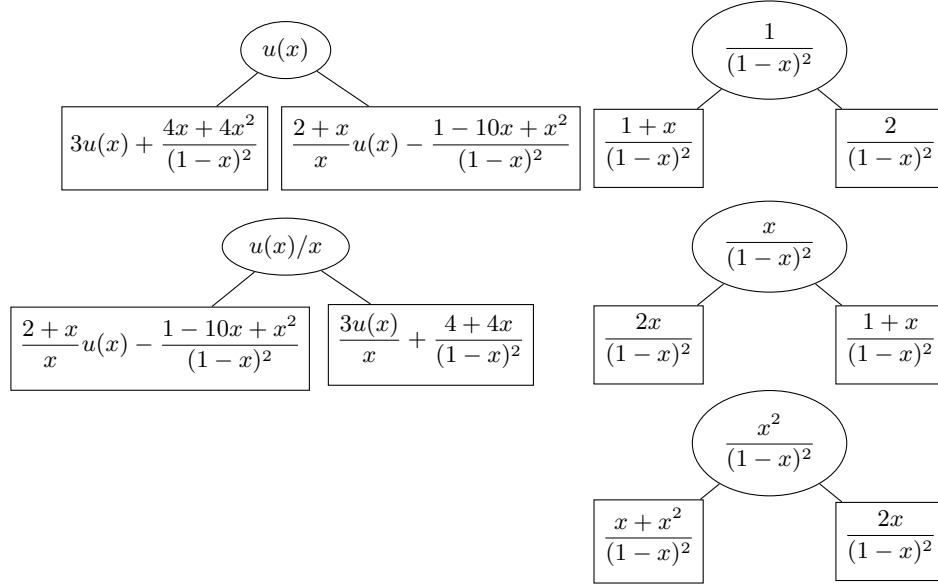


FIGURE 2. Une base et ses sections pour la complexité de l'algorithme de Karatsuba (u_n) (exemple 19).

EXEMPLE 19. Reprenons une fois de plus la formule (32) de l'exemple 8. Nous avons noté à l'exemple 17 qu'elle nous donnait, indirectement, le caractère 2-rationnel de la complexité de l'algorithme de Karatsuba. Nous pouvons être plus précis. En récrivant la formule sous la forme

$$u(x) = \frac{(1+x)(2+x)}{x}u(x^2) - x + 4\frac{x^2}{(1-x)^2},$$

nous trouvons rapidement que le \mathbb{Q} -espace vectoriel \mathcal{V} engendré par $u(x)$, $u(x)/x$, $1/(1-x)^2$, $x/(1-x)^2$ et $x^2/(1-x)^2$ est stable par section (figure 2). De plus si nous tronquons à l'indice 4 chacune des séries de cette famille, nous obtenons cinq vecteurs, qui constituent les cinq colonnes de la matrice inversible

$$\Delta = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 7 & 2 & 1 & 0 \\ 7 & 23 & 3 & 2 & 1 \\ 23 & 33 & 4 & 3 & 2 \\ 33 & 69 & 5 & 4 & 3 \end{bmatrix},$$

donc cette famille de cinq séries est libre et constitue une base de l'espace \mathcal{V} . L'expression des sections (figure 2) de ces séries dans la base, nous donne les matrices

$$A_0 = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 4 & 10 & 1 & 2 & 1 \\ 4 & -1 & 0 & 0 & 1 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 3 & 0 & 0 & 0 \\ -1 & 4 & 2 & 1 & 0 \\ 10 & 4 & 0 & 1 & 2 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

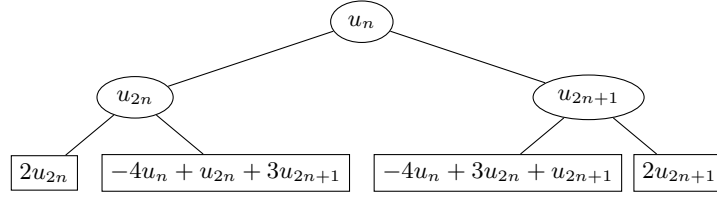


FIGURE 3. La suite (u_n) associée au code Gray est 2-rationnelle (exemple 20).

Nous n'avons pas de difficulté à compléter ce couple de matrices carrées avec les vecteurs ligne (première ligne de la matrice Δ) et colonne

$$L = [0 \quad 1 \quad 1 \quad 0 \quad 0], \quad C = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Nous disposons ainsi d'une représentation linéaire pour la complexité de l'algorithme de Karatsuba. \triangle

Une série formelle ou une suite u qui est rationnelle en base b engendre un sous-espace de dimension finie \mathcal{U} sous l'action des opérateurs de section. L'exhibition d'une famille génératrice finie d'un espace \mathcal{V} contenant u et stable par section suffit évidemment à prouver le caractère b -rationnel de u . Mais deux questions demeurent : la famille génératrice considérée est-elle une base de \mathcal{V} ? Le sous-espace \mathcal{V} est-il le sous-espace minimal \mathcal{U} ? Nous avons vu comment répondre à la première question dans l'exemple précédent. La seconde sera traitée à la fin de la section 5.

Nous privilégions dans ce texte l'emploi des séries formelles parce qu'elles permettent de capturer le comportement des suites pour les bases valeurs de l'indice. Quand les récurrences n'ont pas de conditions particulières dans leur début, il est équivalent d'employer les suites.

EXEMPLE 20. Nous avons déjà rencontré (exemple 9, page 13) la suite (u_n) associée au code de Gray et qui vérifie

$$\begin{aligned} u_{4n} &= 2u_{2n}, \\ u_{4n+1} &= -4u_n + 3u_{2n} + u_{2n+1}, \\ u_{4n+2} &= -4u_n + u_{2n} + 3u_{2n+1}, \\ u_{4n+3} &= 2u_{2n+1}. \end{aligned}$$

Ces formules montrent la 2-rationnalité de la suite (figure 3) et fournissent les matrices qui traduisent l'action des sections dans la base constituée des trois suites (u_n) , (u_{2n}) , (u_{2n+1}) , qui est bien une base comme le montrent les trois premiers termes de chacune de ces suites, et nous complétons la représentation en ajoutant à l'action les valeurs initiales et les coordonnées

$$(39) \quad A_0 = \begin{bmatrix} 0 & 0 & -4 \\ 1 & 2 & 3 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & -4 & 0 \\ 0 & 1 & 0 \\ 1 & 3 & 2 \end{bmatrix}, \quad L = [0 \quad 0 \quad 1], \quad C = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

\triangle

C'est le lieu de revenir sur un point que nous avons laissé pendant. Nous voulons voir effectivement fonctionner la démonstration du théorème 2, page 9, qui permet de passer d'un système sur les sections à une équation de Mahler. Nous présentons le calcul sur un exemple.

EXEMPLE 21. Nous partons de la représentation linéaire (39) obtenue à l'exemple précédent 20. Cette représentation exprime l'action des opérateurs de section dans l'espace de dimension 3 de base $v_1(x) = u(x)$, $v_2(x) = T_{2,0}u(x)$, $v_3(x) = T_{2,1}u(x)$. Nous exprimons les $v_k(x)$, $1 \leq k \leq 3$, en fonction de leurs sections $v(x) = \sum_{0 \leq r < b} x^r T_r v(x^b)$. Pour cela nous utilisons la représentation linéaire qui donne

$$\begin{aligned} [v_1(x) \quad v_2(x) \quad v_3(x)] &= [v_1(x^2) \quad v_2(x^2) \quad v_3(x^2)] \begin{bmatrix} 0 & 0 & -4 \\ 1 & 2 & 3 \\ 0 & 0 & 1 \end{bmatrix} \\ &\quad + x [v_1(x^2) \quad v_2(x^2) \quad v_3(x^2)] \begin{bmatrix} 0 & -4 & 0 \\ 0 & 1 & 0 \\ 1 & 3 & 2 \end{bmatrix} \end{aligned}$$

Ceci nous fait introduire le vecteur ligne et la matrice carrée

$$(40) \quad V(x) = [v_1(x) \quad v_2(x) \quad v_3(x)], \quad A(x) = A_0 + xA_1,$$

ce qui permet d'abrégier la formule précédente en

$$(41) \quad V(x) = V(x^2)A(x).$$

Quant à $u(x)$ nous l'obtenons comme le produit $u(x) = V(x)C$. Nous avons donc une écriture de $u(x)$ sous la forme

$$u(x) = V(x^2)A(x)C.$$

Nous itérons la transformation en déduisant $V(x^2) = V(x^4)A(x^2)$ de (41), d'où

$$u(x) = V(x^4)A(x^2)A(x)C,$$

puis par la même voie

$$u(x) = V(x^8)A(x^4)A(x^2)A(x)C.$$

Nous substituons à x une puissance x^{2^k} , $0 \leq k \leq 3$, dans chacune de ces formules pour obtenir

$$\begin{aligned} u(x^8) &= V(x^8)C, \\ u(x^4) &= V(x^8)A(x^4)C, \\ u(x^2) &= V(x^8)A(x^4)A(x^2)C, \\ u(x) &= V(x^8)A(x^4)A(x^2)A(x)C. \end{aligned}$$

Il faut noter que le calcul est ici légèrement simplifié parce que la représentation est à coefficients constants et les substitutions ne modifient pas le vecteur colonne C . Les quatre vecteurs colonnes en facteur de $V(x^8)$ sont liés puisqu'ils vivent dans un espace de dimension 3. Si $K(x) = (k_3(x), k_2(x), k_1(x), k_0(x))$ est un vecteur colonne qui exprime leur liaison, nous arrivons à l'équation de Mahler

$$(42) \quad k_0(x)u(x) + k_1(x)u(x^2) + k_2(x)u(x^4) + k_3(x)u(x^8) = 0.$$

Concrètement la matrice $A(x)$ vaut

$$A(x) = \begin{bmatrix} 0 & -4x & -4 \\ 1 & 2+x & 3 \\ x & 3x & 1+2x \end{bmatrix}$$

et nous ne considérons pas d'emblée la famille des quatre vecteurs colonnes. Nous utilisons successivement les familles (C) , puis $(C, A(x)C)$, puis $(C, A(x^2)C, A(x^2)A(x)C)$, en continuant avec $(C, A(x^4)C, A(x^4)A(x^2)C, A(x^4)A(x^2)A(x)C)$ jusqu'à trouver une relation de liaison. Ici la matrice dont les vecteurs colonnes sont les $\prod_{j=0..k} A(x^{2^{2-j}})C$, $0 \leq k \leq 3$, est

$$\Gamma(x) = \begin{bmatrix} 1 & 0 & -4x^2 - 4x^4 & -4x - 12x^2 - 8x^3 - 8x^4 - 12x^5 - 4x^6 \\ 0 & 1 & 2 + 3x^2 + x^4 & 4 + 5x + 7x^2 + 6x^3 + 2x^4 + 3x^5 + x^6 \\ 0 & x^4 & x^2 + 3x^4 + 2x^6 & x + 3x^2 + 2x^3 + 6x^4 + 7x^5 + 5x^6 + 4x^7 \end{bmatrix}$$

et une dépendance se produit avec la quatrième famille. Le vecteur colonne $K(x)$ vaut

$$K(x) = \begin{bmatrix} 0 \\ 2 \frac{(1+x)(1+x^4)}{x} \\ - \frac{(1+x)(1+2x+2x^3+x^4)}{x(1+x^2)} \\ 1 \end{bmatrix}$$

et nous arrivons à l'équation de Mahler d'ordre 2

$$x(1+x^2)u(x) - (1+x)(1+2x+2x^3+x^4)u(x^2) + 2(1+x)(1+x^2)(1+x^4)u(x^4) = 0.$$

△

4. Cohérence et décalage

Les suites divisées pour régner que l'on rencontre dans la littérature sont souvent définies par des récurrences linéaires qui portent sur leur sections. Il n'est pas immédiat que ces définitions fassent sens.

Imaginons que nous écrivions des relations linéaires entre les sections b -aires d'une suite (u_n) . Nous avons ainsi des relations entre des expressions de la forme $u_{b^k n+r}$. Pour n grand, proche de l'infini, certains termes dominent. Imaginons que pour chaque relation exactement un terme domine parce que le b^k qui apparaît dans son expression est strictement plus grand que ceux qui apparaissent dans les autres expressions. Nous voyons alors chaque relation comme une égalité orientée : dans le membre gauche figure le terme dominant et dans le membre droit une combinaison linéaire des autres termes. Cela nous permet de définir la suite d'une manière procédurale : pour calculer un terme, nous appelons la procédure sur des entiers strictement plus petits. Mais l'ensemble totalement ordonné des entiers naturels a deux bouts. Il ne suffit pas de regarder vers l'infini. Il faut aussi considérer la suite pour des indices proches de 0 car la domination n'est qu'asymptotique. Cela nous fait traiter un système linéaire qui correspond aux indices pour lesquels la domination du membre gauche sur le membre droit n'a pas lieu. Le système de relations sera cohérent si ce petit système a des solutions.

La vision précédente est assez incomplète. Une section d'une suite concerne des indices associés à une progression arithmétique. Pour que les sections considérées déterminent la suite il est suffisant que d'une part les progressions arithmétiques couvrent tous les entiers, d'autre part n'empiètent pas les unes sur les autres. La première condition est nécessaire à une bonne définition. Pour ce qui est de la seconde, elle fournit une certaine cohérence de la définition, mais n'est peut-être pas

nécessaire : il se pourrait que la redondance se résolve et n'introduise pas d'incohérence. Dans un souci de simplicité, nous faisons l'hypothèse que les progressions arithmétiques utilisées forment une partition de l'ensemble des entiers naturels.

Nous ne voulons cependant pas nous limiter aux sections b -aires d'une suite. En effet les cas concrets montrent des décalages. Par exemple, avec $b = 2$, les sous-suites (u_{2n}) et (u_{2n+1}) sont des sections d'une suite (u_n) , mais pas (u_{2n+2}) ou (u_{2n-1}) . Toujours avec $b = 2$, nous acceptons des relations comme

$$u_{4n+1} = u_{2n-2} + u_{2n+6} + u_{2n-29} + u_{n+10},$$

ce qui en termes de série génératrice s'énonce

$$T_{4,1}u(x) = \left(x + \frac{1}{x^3}\right) T_{2,0}u(x) + x^{15}T_{2,1}u(x) + \frac{1}{x^{10}}u(x).$$

Autrement dit, nous supposons que les coefficients des relations de dépendance linéaire qui portent sur les sections de la série génératrice $u(x)$ sont des polynômes de Laurent. Cette situation est moins générale que le cadre du chapitre 1 où les coefficients étaient des fractions rationnelles, mais plus générale que celle de la section 1 de ce chapitre où les coefficients étaient constants. En fait nous allons voir que la capacité d'expression est la même qu'en section 1 et la classe que nous sommes en train de définir n'est que la classe des suites rationnelles dans une base de numération. Ceci rejoint la remarque que nous faisons à la fin de la section 1 du chapitre 3 sur le fait que les suites b -rationnelles sont les vraies suites diviser pour régner parce que leurs récurrences exprime essentiellement leur valeur en n en fonction de n/b , n/b^2 , ... mais pas en fonction de $n - 1$, $n - 2$, ...

La formalisation des idées précédentes passe par la notion d'arbre, ce qui n'est guère surprenant au vu de l'emploi informel que nous en avons fait dans les dessins des pages précédentes.

DÉFINITION 6. *À la famille des sections b -aires d'une série formelle $u(x)$ est associé un arbre b -aire étiqueté : la section $T_{b^k,r}u(x)$, $k \geq 0$, $0 \leq r < b^k$, est l'étiquette du nœud à l'adresse qui est l'écriture en base b de l'entier r (lue en commençant par les poids faibles).*

Nous avons ainsi associé à une série formelle un arbre b -aire infini. Cependant il n'est pas rare que nous ayons à considérer plusieurs séries formelles en même temps et ceci fait apparaître une forêt.

Nous introduisons maintenant une définition qui exprime le fait que les arbres infinis précédents sont ramenés à des arbres finis par les relations entre sections et qui garantit que le système de relations est bien formé, bien posé.

DÉFINITION 7. *Un système de relations linéaires sur les sections b -aires d'une famille finie de séries formelles $(u_i(x))_{i \in I}$ est bien posé si*

- (1) *pour chaque série, un nombre fini de sections apparaissent, ce qui définit un arbre b -aire associé à cette série : les nœuds sont ou bien étiquetés par ces sections ou bien sont des ancêtres de tels nœuds ;*
- (2) *le système consiste en égalités dont le membre gauche est une section et le membre droit une combinaison linéaire de sections de séries de la famille à coefficients des polynômes de Laurent ;*
- (3) *les membres gauches sont les étiquettes des feuilles de la forêt ;*

- (4) les sections qui apparaissent dans les membres droits sont des étiquettes des nœuds internes de la forêt ;
- (5) pour chaque équation, le membre gauche étiquète un nœud de niveau strictement plus grand que les niveaux des nœuds étiquetés par les sections qui sont dans le membre droit.

Précisons, pour ce qui concerne le dernier point (5), que les racines des arbres sont toutes au niveau 0. Avec $b = 2$ et en supposant que nous ayons deux séries $u(x)$ et $v(x)$, nous pourrions donc avoir une relation

$$T_{4,2}u(x) = xT_{2,1}u(x) + T_{2,0}v(x) + u(x),$$

(en supposant que $T_{2,1}u(x)$ $T_{2,0}v(x)$, $u(x)$ correspondent à des nœuds internes) mais par contre la relation

$$T_{4,2}u(x) = xT_{2,1}u(x) + T_{4,0}v(x) + u(x),$$

ne rentre pas dans la définition d'un système bien posé, parce que les nœuds étiquetés par $T_{4,2}u(x)$ et $T_{4,0}v(x)$ sont au même niveau.

Avec cette définition, nous avons un système qui définit bien les suites impliquées pour de grandes valeurs de l'indice. Il reste à comprendre ce que nous faisons des petits indices.

EXEMPLE 22. Avec $b = 2$, considérons l'exemple simple suivant

$$u_{2n} = u_{n+2} + \lambda u_n, \quad u_{2n+1} = \mu u_{n+1},$$

avec λ, μ donnés et non nuls, qui satisfait bien aux conditions de la définition d'un système bien posé (il se réécrit $T_{2,0}u(x) = u(x)(1/x^2 + \lambda)$, $T_{2,1}u(x) = \mu u(x)/x$). Pour chacune des deux formules, le terme de gauche domine asymptotiquement les termes de droite. Pour chacun des deux cas, nous traçons les graphes (figure 4) des fonctions affines qui figurent en indice. Par exemple, pour le premier cas, nous utilisons les fonctions affines $m = 2n$, $m = n + 2$, $m = n$. Nous voyons que $m = 2n$ domine les deux autres pour $n > 2$. Ceci nous fournit trois équations, pour n allant de 0 à 2. Les valeurs de m qui ne correspondent pas à la domination sont les entiers de 0 à 4. Pour l'autre cas, il y a domination pour $n > 0$ et il n'y a qu'un entier m non concerné par la domination, qui est $m = 0$. Mais nous voyons que pour $n = 1$ et $m = 3$, alors qu'il y a domination, nous avons une équation qui concerne u_2 et u_3 , qui apparaissent dans l'autre cas avec $n = 3$ et $m = 6$. Nous considérons donc toutes les équations qui font intervenir des u_m avec $0 \leq m \leq 4$, c'est-à-dire dans le premier cas pour $n \leq 4$ et dans le second $n \leq 3$. Nous obtenons le système

$$\begin{array}{ll} u_0 = u_2 + \lambda u_0, & \text{pour } m = 0 \text{ et } n = 0, \\ u_2 = u_3 + \lambda u_1, & \text{pour } m = 2 \text{ et } n = 1, \\ u_4 = u_4 + \lambda u_2, & \text{pour } m = 4 \text{ et } n = 2, \\ u_6 = u_5 + \lambda u_3, & \text{pour } m = 6 \text{ et } n = 3, \\ u_8 = u_6 + \lambda u_4, & \text{pour } m = 8 \text{ et } n = 4, \\ u_1 = \mu u_1, & \text{pour } m = 1 \text{ et } n = 0, \\ u_3 = \mu u_2, & \text{pour } m = 3 \text{ et } n = 1, \\ u_5 = \mu u_3, & \text{pour } m = 5 \text{ et } n = 2, \\ u_7 = \mu u_4, & \text{pour } m = 7 \text{ et } n = 3. \end{array}$$

Dans ce système les inconnues u_n , $5 \leq n \leq 8$, sont les inconnues principales, alors que les inconnues u_n , $0 \leq n \leq 4$, sont les inconnues non principales. La compatibilité du système s'exprime sur ces dernières et c'est un choix cohérent des u_n , $0 \leq n \leq 4$, qui assure le caractère bien fondé de la récurrence. Les u_n , $5 \leq n \leq 8$, se déduisent alors des

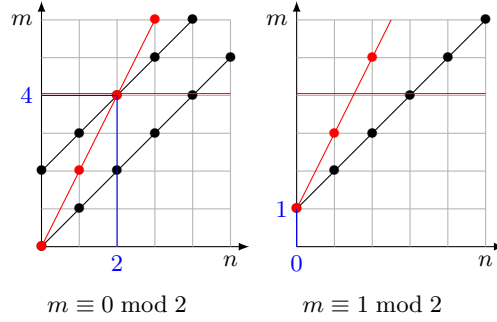


FIGURE 4. Un graphique élémentaire détermine le système qui assure la cohérence d'un système bien posé.

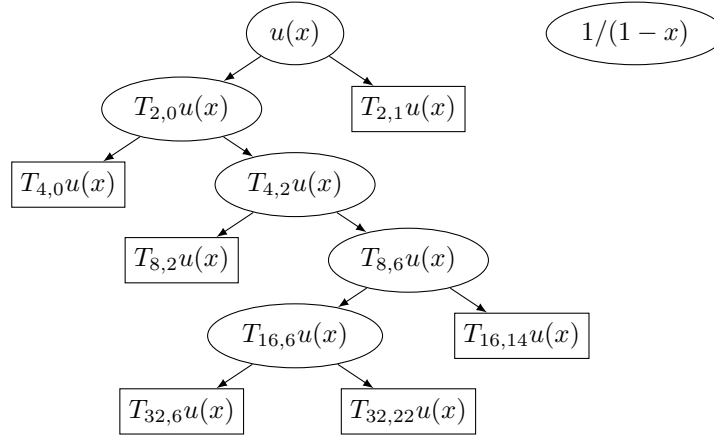


FIGURE 5. L'arbre binaire associé aux formules (43) de l'exemple 23.

précédents. Le système se résout en $u_m = 0$ pour $m = 0, 1, 2, 3$ et u_4 arbitraire d'où $u_m = 0$ pour $m = 5, 6$ et $u_7 = \mu u_4, u_8 = \lambda u_4$. Nous obtenons un espace de solution de dimension 1 dirigé par

$$u(x) = x^4 + \mu x^7 + \lambda x^8 + \mu x^{10} + \lambda x^{12} + \mu^2 x^{13} + \lambda \mu x^{14} + \lambda \mu x^{15} + \dots$$

△

EXEMPLE 23. La numération en base -2 utilise comme chiffres 0 et 1 [7, p. 2019]. Allouche et Shallit [6, exemple 16.1.4, p. 440] considèrent la somme des chiffres s_n d'un entier n dans ce système de numération. Par exemple de $14 = (10010)_{-2} = 1 \cdot (-2)^4 + 0 \cdot (-2)^3 + 0 \cdot (-2)^2 + 1 \cdot (-2)^1 + 0 \cdot (-2)^0$, nous tirons $s_{14} = 2$. Ils prouvent les formules

$$(43) \quad \begin{aligned} s_{2n+1} &= s_{2n} + 1, & s_{16n+14} &= s_{16n+6} - 1, \\ s_{4n} &= s_{2n}, & s_{32n+6} &= s_{2n+1} + 2, & n &\geq 0. \\ s_{8n+2} &= s_{2n+1} + 1, & s_{32n+22} &= s_{8n+6} + 1, \end{aligned}$$

Le système sur les sections est à coefficients constants :

$$(44) \quad \begin{aligned} T_{2,1}s(x) &= T_{2,0}s(x) + 1/(1-x), & T_{16,14}s(x) &= T_{16,6}s(x) - 1/(1-x), \\ T_{4,0}s(x) &= T_{2,0}s(x), & T_{32,6}s(x) &= T_{2,1}s(x) + 2/(1-x), \\ T_{8,2}s(x) &= T_{2,1}s(x) + 1/(1-x), & T_{32,22}s(x) &= T_{8,6}s(x) + 1/(1-x). \end{aligned}$$

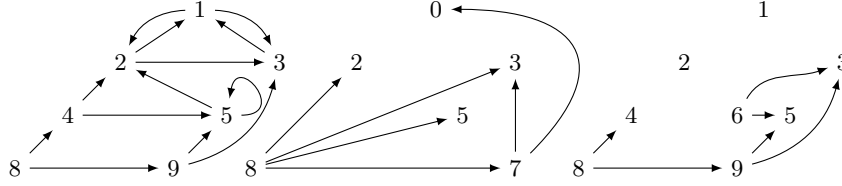


FIGURE 6. Les appels dans le calcul de u_8 pour l'exemple 24. Tout à gauche, la version d'origine, quasi bien posée, qui montre des cycles et une mauvaise définition. Au centre, le problème est résolu en passant à une récurrence bien posée et en fixant les valeurs u_n , $0 \leq n \leq 5$. À droite la version d'origine expurgée des cycles par l'étude de la version bien posée.

Il nous fait considérer une forêt d'arbres binaires (figure 5), dont l'un est atrophié parce que la fraction rationnelle $1/(1-x)$ est fixe par les opérateurs de section. Le système n'est pas bien posé car les deux sections $T_{2,1}s(x)$ et $T_{2,0}s(x)$ sont au même niveau. Il est vrai que sur l'écriture en suite, la question semble ténue.

△

Il semble, d'après l'exemple précédent, que la définition d'un système bien posé soit trop restrictive, puisqu'on y voit un système de relations entre sections qui ne respecte pas la condition (5) sur les niveaux.

DÉFINITION 8. *Un système de relations sur les sections b -aires d'une famille de séries formelles est quasi bien posé s'il satisfait aux conditions de la définition 7 à l'exception peut-être de la condition (5).*

EXEMPLE 24. Considérons le système suivant qui porte sur les sections binaires d'une suite (u_n)

$$\begin{aligned} u_{2n} &= 2u_n + u_{2n+1}, \\ u_{4n+1} &= u_{n+1} + u_{2n+3}, \quad n \geq 0. \\ u_{4n+3} &= u_{n-1} - u_{2n+1}, \end{aligned}$$

Il ne respecte pas la condition (5) et dès que nous tentons de calculer quelques valeurs, le flou s'instaure (figure 6, à gauche), car les appels récursifs tombent dans des cycles. Pour clarifier la situation et supprimer la dépendance d'un terme de la suite en des termes d'indice plus grands, nous éclatons la formule sur u_{2n} qui pose problème. Par remplacement, nous obtenons

$$\begin{aligned} u_{4n} &= 2u_{2n} + u_{4n+1} = u_{2n+3} + 2u_{2n+1} + u_{n+1} + 4u_n, \\ u_{4n+2} &= 2u_{2n+1} + u_{4n+3} = u_{2n+1} + u_{n-1}. \end{aligned}$$

Nous avons donc maintenant le système bien posé

$$\begin{aligned} u_{4n} &= u_{2n+3} + 2u_{2n+1} + u_{n+1} + 4u_n, \\ u_{4n+1} &= u_{n+1} + u_{2n+3}, \\ u_{4n+2} &= u_{2n+1} + u_{n-1}, \\ u_{4n+3} &= u_{n-1} - u_{2n+1}. \end{aligned}$$

Ceci ne suffit pas à garantir que la récurrence est bien fondée. Pour chacune des classes de congruence, nous traçons les graphes des fonctions affines qui apparaissent en indice (figure 7). Par exemple, pour les entiers m congrus à 0 modulo 4, nous voyons que la fonction affine $m = 4n$ qui apparaît dans le membre gauche de la relation de récurrence domine les fonctions affines $m = n$, $m = n + 1$, $m = 2n + 1$, $m = 2n + 3$ qui apparaissent

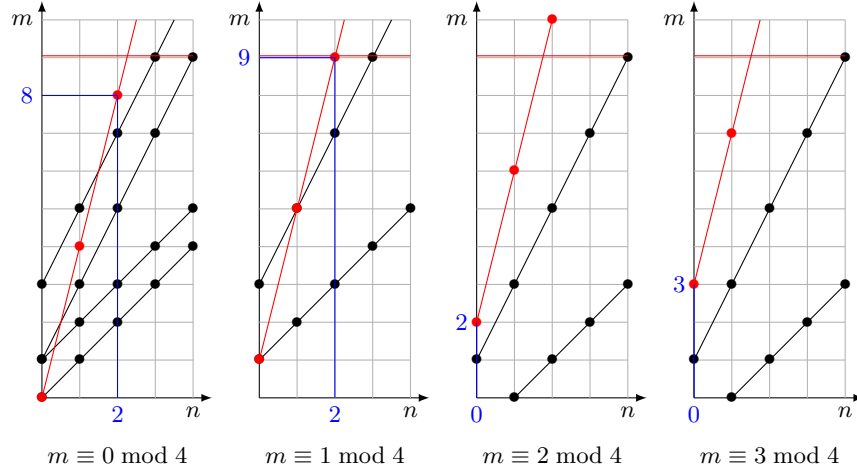


FIGURE 7. Des graphiques élémentaires permettent de déterminer les conditions initiales qui doivent être imposées à un système bien posé pour le rendre bien fondé (exemple 24).

dans le membre droit à partir de $n = 2$. Cela signifie que si l'initialisation de la récurrence est correcte, cette relation va déterminer les valeurs de la suite pour les entiers congrus à 0 modulo 4 à partir de $m = 8$. Nous procédons de même pour les trois autres classes de congruence, à l'imitation de l'exemple 22.

Nous constatons que sur les quatre cas à considérer la plus petite borne qui garantit la domination globale est $m = 9$ (trait rouge horizontal dans la figure 7). Les relations qui portent sur les u_m , $0 \leq m \leq 9$, sont obtenues pour $n \leq 9$ dans le cas $m \equiv 0 \pmod{4}$, pour $n \leq 8$ dans le cas $m \equiv 1 \pmod{4}$, pour $n \leq 10$ dans les cas $m \equiv 2$ ou $4 \pmod{4}$, respectivement à cause de l'occurrence des fonctions affines asymptotiquement les plus petites $m = n$, $m = n + 1$, $m = n - 1$. Nous avons ainsi un système de quarante et une équations d'inconnues principales les u_m , $10 \leq m \leq 38$ ou $42 \leq m \leq 43$, et d'inconnues non principales les u_m , $0 \leq m \leq 9$. Ce système se résout en

$$u(x) = \alpha x^4 + \alpha x^5 + 2\alpha x^8 + \alpha x^{10} + \alpha x^{12} + \alpha x^{13} - \alpha x^{15} + 5\alpha x^{16} + \alpha x^{17} + 5\alpha x^{20} + \alpha x^{21} + \dots$$

avec $u_4 = \alpha$ qui paramètre la solution. Ainsi nous avons exactement l'espace des solutions de la récurrence bien posée.

Cependant dans le passage de la première récurrence à la seconde, nous avons procédé par implication et donc agrandi a priori l'espace des solutions. Il nous faut vérifier que la solution obtenue est bien solution de la récurrence originelle. Supposons que nous ayons une solution (u_n) du système bien posé. Cela signifie qu'elle satisfait à

$$\begin{aligned} u_{4n} &= u_{2n+3} + 2u_{2n+1} + u_{n+1} + 4u_n, & n \geq 2, \\ u_{4n+1} &= u_{n+1} + u_{2n+3}, & n \geq 2, \\ u_{4n+2} &= u_{2n+1} + u_{n-1}, & n \geq 0, \\ u_{4n+3} &= u_{n-1} - u_{2n+1}, & n \geq 0, \end{aligned}$$

avec les conditions initiales indiquées plus haut. Le système originel s'écrit

$$\begin{aligned} u_{2n} &= 2u_n + u_{2n+1}, \\ u_{4n+1} &= u_{n+1} + u_{2n+3}, & n \geq 0. \\ u_{4n+3} &= u_{n-1} - u_{2n+1}, \end{aligned}$$

Le problème est de savoir si la première équation est satisfaite. Notons $\mathcal{P}(n)$ le système de ces trois équations. Il est immédiat de vérifier que $\mathcal{P}(n)$ implique $\mathcal{P}(2n)$ pour $n \geq 2$ et que $\mathcal{P}(n)$ implique $\mathcal{P}(2n+1)$ pour $n \geq 0$. Du coup tout revient à savoir si l'initialisation est satisfaite, c'est-à-dire si $\mathcal{P}(0)$ et $\mathcal{P}(2)$ sont vérifiées. Cela se traduit par les contraintes supplémentaires $u_0 + u_1 = 0$, $u_4 = 2u_2 + u_5$, qui ici sont déjà satisfaites dans la solution du système bien posé. \triangle

L'expérience fournie par cet exemple nous mène aisément aux deux propositions qui suivent.

PROPOSITION 7. *Un système quasi bien posé peut être transformé en un système bien posé.*

DÉMONSTRATION. Nous considérons à la forêt b -aire qui traduit le système. Si le membre gauche d'une équation étiquète un nœud qui est strictement plus haut qu'un nœud étiqueté par un terme du membre droit, nous appliquons à chaque membre de l'équation les opérateurs de section $T_{b,r}$, $0 \leq r < b$, ce qui fait descendre les nœuds d'un niveau et augmente la taille de l'arbre. Pour les nœuds qui sont des feuilles, nous remplaçons dans l'équation l'étiquette par la combinaison linéaire fournie par le système et qui utilise les nœuds internes de la forêt initiale. Dans cette transformation nous n'avons pas augmenté la hauteur de la forêt, car nous n'avons pas à traiter les feuilles les plus basses pour lesquelles la condition sur les niveaux est automatiquement satisfaite. De plus les nœuds qui sont associés aux membres droits des équations demeurent parmi les nœuds internes de la forêt initiale. Nous itérons la transformation tant que le système n'est pas bien posé. Comme la hauteur de la forêt est fixée, le processus termine nécessairement. \square

PROPOSITION 8. *Le caractère bien fondé d'un système quasi bien posé peut être obtenu comme suit :*

- (1) *fabriquer le système bien posé associé, donné par la proposition 7;*
- (2) *déterminer les limites de validité des formules par comparaison de fonctions affines. Ceci définit les inconnues non principales u_m , $0 \leq m \leq m_0$;*
- (3) *déterminer les conditions initiales en considérant toutes les formules utilisant les inconnues non principales à la fois pour le système bien posé et pour le système initial.*

DÉMONSTRATION. Nous ne faisons que traduire la démarche que nous avons suivi dans l'exemple. \square

Ayant accumulé ces résultats, nous pouvons énoncer le théorème lyonnais.

THÉORÈME 8. *Une famille de séries formelles définie par un système quasi bien posé sur leurs sections b -aires est une famille de séries rationnelles en base b .*

DÉMONSTRATION. L'hypothèse sous-entend que le système est bien fondé puisque nous en considérons une solution. Le système se traduit par des équations sur des sections des éléments de la famille et nous pouvons supposer que ce système est bien posé grâce à la proposition 7. Nous exprimons donc des sections comme des combinaisons linéaires à coefficients des polynômes de Laurent de sections d'ordre strictement inférieur. La méthode employée dans la preuve du théorème 2, page 9, fonctionne ici sans problème parce que les sections contractent les polynômes de Laurent en rapprochant les degrés extrêmes de 0. Nous avons déjà remarqué que

la propriété utile des coefficients était qu'ils forment un espace stable par section (page 10). Ici nous utilisons les polynômes de $\mathbb{K}[x, 1/x]$ dont les degrés sont bornés en valeur absolue par le maximum des valeurs absolues des degrés des coefficients des équations du système bien posé. Comme cet espace est de dimension finie, nous passons de relations dont les coefficients sont des polynômes de Laurent à des relations à coefficients constants. \square

Ce théorème, s'il est élémentaire, a le mérite de correspondre à la pratique des suites rationnelles dans une base de numération. En effet il n'est pas rare que les formules de récurrence n'utilisent pas seulement les opérateurs de section, mais aussi des décalages qui demandent sur chaque exemple quelques calculs pour disparaître. Le théorème précédent nous dit qu'il n'y a pas à s'en inquiéter. Tout au plus ils grossissent l'espace engendré par la suite ou la série sous l'action des sections.

EXEMPLE 25. La suite de Stern-Brocot [50], ou suite diatomique de Stern, peut être définie par

$$u_0 = 0, u_1 = 1, \quad u_{2n} = u_n, \quad u_{2n+1} = u_n + u_{n+1}.$$

Dans [4, exemple 7, p. 187], les auteurs montrent que cette suite est 2-rationnelle et pour cela font disparaître le terme décalé u_{n+1} . Le calcul est simple : nous évaluons d'abord $u_{4n+1} = u_{2n} + u_{2n+1}$ puis $u_{4n+3} = u_{2n+1} + u_{2n+2}$. Le terme u_{2n+2} n'est pas typique d'une suite 2-rationnelle, mais les auteurs le remplacent par $u_{n+1} = u_{2n+1} - u_n$, d'où $u_{4n+3} = 2u_{2n+1} - u_n$ et tout est en ordre.

Si nous exprimons cet exemple à l'aide des sections de la série génératrice $u(x)$, nous voyons que nous sommes passés de

$$T_{2,0}u(x) = u(x), \quad T_{2,1}u(x) = \left(1 + \frac{1}{x}\right)u(x)$$

à

$$T_{2,0u(x)} = u(x), \quad T_{4,1}u(x) = T_{2,0}u(x) + T_{2,1}u(x), \quad T_{4,3}u(x) = 2T_{2,1}u(x) - u(x),$$

le changement essentiel étant que dans la première formulation les coefficients sont des polynômes de Laurent alors que dans la seconde ils sont constants. \triangle

5. Lien avec la théorie des langages formels

La section précédente a mis en valeur l'intervention du développement en base b des entiers dans l'emploi des séries rationnelles en base b . Ceci nous pousse à considérer non pas les entiers mais les mots que sont les développements de ces entiers. Ainsi à chaque mot sur l'alphabet de la numération en base b nous associons une valeur dans le corps \mathbb{K} . Nous considérons donc des séries au sens de la théorie des langages formels,

$$s = \sum_{w \in [0, b]^*} s_w w.$$

Ici l'alphabet est l'intervalle d'entiers $[0, b[= \{0, \dots, b-1\}$ et le monoïde des mots est noté selon l'usage avec une étoile $*$. Nous dérogeons cependant à l'usage car la notation standard des linguistes formels est (s, w) pour le coefficient du mot w . Nous préférons garder une notation indexée.

Si nous regardons l'action des opérateurs de section $T_{b,r}$, $0 \leq r < b$, sur les mots, nous voyons, en revenant à la définition 1, page 4,

$$T_{b,r} \sum_{n \geq 0} u_n x^n = \sum_{k \geq 0} u_{bk+r} x^k$$

que nous avons supprimé dans la série les entiers dont le chiffre des unités n'est pas r , c'est-à-dire les mots dont le chiffre de poids faible n'est pas r . De plus pour les entiers congrus à r modulo b , nous avons effectué la division euclidienne $n = bk + r$ et nous avons remplacé n par k , autrement dit pour les mots qui finissent par la lettre r , nous avons gommé cette lettre. Cette opération est l'opération d'effacement classiquement notée $s \mapsto sr^{-1}$. La notion de série b -rationnelle n'est donc qu'un avatar de la notion de série reconnaissable de la théorie des langages formels, vue à travers la numération des entiers dans une base de numération. Quant à la notion de représentation linéaire, elle est calquée de la notion de représentation linéaire d'une série reconnaissable. Enfin, le théorème de Schützenberger affirme qu'une série est reconnaissable si et seulement si elle est rationnelle, au sens de la théorie de la théorie des langages formels. C'est pourquoi nous employons l'adjectif *rationnel*. Pour toutes ces notions, nous renvoyons au chapitre 1 de [11, 12]. Le lien entre théorie des langages formels et séries rationnelles dans une base de numération est développé dans [10, chap. 5].

Finalement, toute la machinerie de ce chapitre n'est que la composition du développement en base b des entiers et d'une série formelle au sens de la théorie des langages formels. Cependant une petite nuance surgit : nous n'employons jamais les mots qui commencent par un zéro. Précisons que le développement de zéro est le mot vide (ce qui correspond à la relation $u_0 = LC$ dans la formule (38), page 25). Pourtant ce point ne pose pas de problème parce que l'application de l'opérateur de section $T_{b,0}$ ne change pas le terme constant de la série à laquelle il s'applique : $T_{b,0}u(0) = u(0)$. Il en résulte que les représentations linéaires que nous fabriquons vérifient $LA_0 = L$. Du coup les zéros à gauche n'ont pas d'effet dans le calcul de la formule (38).

DÉFINITION 9. *Une représentation linéaire (L, A, C) est insensible aux zéros à gauche (insensitive to the leftmost zeroes, zero-insensitive) si elle vérifie $LA_0 = L$.*

Autrement dit, nous considérons une série définie sur les mots qui ne commencent pas par un zéro et l'insensibilité aux zéros à gauche la prolonge naturellement aux mots qui commencent par un zéro.

Pour chaque choix d'un sous-espace \mathcal{V} de dimension finie stable par section et contenant la série b -rationnelle $u(x)$ que nous considérons et pour chaque choix d'une famille génératrice de cet espace, nous obtenons une (voire plusieurs si la famille n'est pas une base) représentation linéaire de $u(x)$. Nous avons ainsi une multitude de représentations linéaires, mais la question a déjà été débrouillée par les linguistes formels : pour une série rationnelle de la théorie des langages formels, il y a une taille minimale pour ses représentations linéaires et toutes les représentations linéaires de cette taille, qui sont dit *réduites*, sont semblables. De plus il existe un algorithme de réduction qui fait passer d'une représentation linéaire à une représentation linéaire réduite (voir le chapitre 2 de [11, 12]). Nous disposons d'un résultat similaire pour les représentations linéaires de séries b -rationnelles à la condition de ne considérer que des représentations linéaires insensibles aux zéros à gauche, ce qui répond à la question posée en page 27.

DÉFINITION 10. *Une représentation linéaire d'une série $u(x)$ rationnelle dans une base de numération est réduite si elle est insensible aux zéros à gauche et de taille minimale parmi toutes les représentations linéaires qui ont cette propriété.*

Ainsi nous avons choisi que les représentations linéaires réduites des séries ou suites rationnelles dans une base de numération soient par définition insensibles aux zéros à gauche.

PROPOSITION 9. *Deux représentations linéaires (L, A, C) et (L', A', C') d'une série b -rationnelle qui sont réduites sont semblables, ce qui signifie qu'il existe une matrice carrée inversible de taille adéquate satisfaisant à*

$$L' = LP, \quad A'_r = P^{-1}A_rP, \quad 0 \leq r < b, \quad C' = P^{-1}C.$$

Enfin, les séries rationnelles de la théorie des langages formels utilisant un alphabet qui ne comporte qu'une lettre sont les séries rationnelles usuelles. En effet, dans ce cas, la numération employée est la numération en base 1 : un entier naturel n est représenté par n bâtons. Le gommage de la lettre la plus à droite se traduit en le décalage avant sur les séries. Les séries qui engendrent un espace de dimension finie sous l'effet du décalage sont les séries rationnelles usuelles (chapitre 4 de [11, 12]). Elles admettent une représentation linéaire qui ne comporte qu'une matrice carrée. Les séries rationnelles usuelles sont donc les séries 1-rationnelles et les séries b -rationnelles avec $b \geq 2$ que nous avons considérées en sont une généralisation directe.

Bornes

Nous entamons ici l'étude du comportement asymptotique des suites diviser pour régner. Ceci suppose bien sûr que le corps \mathbb{K} soit un corps de nombres, un sous-corps du corps \mathbb{C} des nombres complexes. Nous voulons étudier le comportement asymptotique de suites (u_n) qui sont définies par une récurrence diviser pour régner où u_n dépend de termes en $n/b, n/b^2, \dots$ et leurs décalées mais pas de décalées de u_n . Dans le cas d'une récurrence homogène, il s'agit typiquement des suites rationnelles en base b du chapitre précédent.

Cela nous fait par exemple exclure la suite du nombre de partitions binaires, dont la série génératrice

$$u(x) = \prod_{k \geq 0} \frac{1}{1 - x^{2^k}}$$

est solution de l'équation $(1-x)u(x) = u(x^2)$, soit $u_n - u_{n-1} = u_{n/2}$. Ses coefficients ont un comportement essentiellement en [29]

$$\exp\left(\frac{1}{2 \log 2} \left(\log \frac{n}{\log n}\right)^2\right).$$

1. Résultats classiques

Pour ce qui concerne les récurrences diviser pour régner liées à l'algorithmique, il est un énoncé que l'on voit extrêmement répandu et dont certains semblent être esclaves. Il a pour source [9] mais est généralement cité comme [26, Th. 4.1]. Dans [1, Prop. 5.1.1], il est assorti de considération non seulement sur la complexité mais sur la place mémoire. Dans [63] est proposé une approche élémentaire (*The pedagogical advantage of avoiding calculus for computer science students is obvious.* [63, p. 16]), dont la clé est de voir les suites, a priori définies sur les entiers, comme des fonctions de variable réelle. De plus cet article offre un bon panorama des variations sur le thème. Mais nous préférons la version suivante [15, Th. 2], qui a le mérite de mettre en valeur qu'il s'agit de traiter des suites majorantes.

THÉORÈME 9. Soit (c_n) une suite réelle positive vérifiant la condition

$$(45) \quad c_n \leq \begin{cases} ac_{\lceil \frac{n}{b} \rceil} + t_n, & \text{si } n \geq n_0 \geq b, \\ \kappa & \text{sinon,} \end{cases}$$

avec

- b un entier au moins égal à 2 ;
- a un réel strictement positif ;
- κ un réel positif ;
- t une fonction de péage
 - croissante,
 - qui vérifie $a't_n \leq t_{bn} \leq a''t_n$ pour des constantes $a'' \geq a' > 1$,

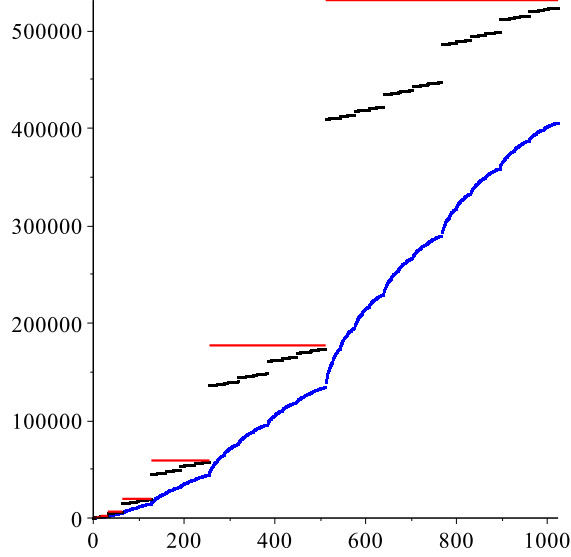


FIGURE 1. Comparaison des graphes de la complexité (u_n) dans l'algorithme de Karatsuba (en bleu), de la suite majorante (v_n) (en noir) et la suite super majorante (w_n) (en rouge) (exemple 26).

alors avec $\alpha = \log_b a$, $\alpha' = \log_b a'$, la suite (c_n) vérifie

$$(46) \quad c_n \underset{n \rightarrow \infty}{=} \begin{cases} O(t_n) & \text{si } a' > a, \\ O(t_n \log n) & \text{si } a' = a, \\ O(n^{\alpha - \alpha'} t_n) & \text{si } a' < a. \end{cases}$$

DÉMONSTRATION. La preuve cale l'entier n entre deux puissances de b et déroule la « récurrence » sur (c_n) , ce qui fait apparaître une somme sur la suite (t_n) . Les hypothèses sur cette suite permettent de conclure. \square

Que de tels énoncés soient utiles est indéniable, cependant ils ne peuvent pas rendre compte des oscillations que l'on observe.

EXEMPLE 26. Nous avons vu que le coût dans le cas le pire de la multiplication de polynômes par l'algorithme de Karatsuba suit la récurrence

$$u_n = 2u_{\lceil \frac{n}{2} \rceil} + u_{\lfloor \frac{n}{2} \rfloor} + 4(n-1), \quad n \geq 2, \quad \text{avec } u_0 = 0, u_1 = 1.$$

Nous pouvons majorer la suite (u_n) en remplaçant la récurrence par l'inégalité récurrente

$$(47) \quad v_n \leq 3v_{\lceil \frac{n}{2} \rceil} + 4n, \quad n \geq 2, \quad \text{avec } v_0 = 0, v_1 = 1.$$

Le théorème 9 donne, avec $b = 2$, $a = 3$, $a' = a'' = 2$, $n_0 = 2$, $\kappa = 1$, $\alpha = \log_2 3$, $\alpha' = \log_2 2 = 1$,

$$(48) \quad v_n \underset{n \rightarrow \infty}{=} O(n^{\log_2 3}).$$

Comme il est montré dans [15], il est possible de travailler plus finement pour obtenir

$$(49) \quad u_n \leq w_n = 9 \cdot 3^{\lceil \log_2 n \rceil},$$

mais cela ne fournit pas les oscillations visibles sur la figure 1.

\triangle

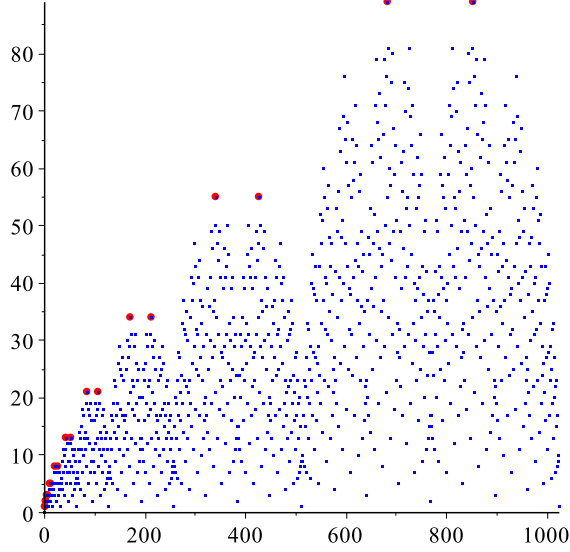


FIGURE 2. Le graphe de la suite de Stern-Brocot (exemple 27), avec, marqués en rouge, les points extrémaux dans les intervalles entre deux puissances consécutives de 2.

si $(r_\ell \dots r_0)_b$ est le développement en base b de N .

Introduisons une norme matricielle subordonnée, c'est-à-dire une norme sur les matrices qui provient d'une norme sur l'espace \mathbb{K}^d où d est la dimension de la représentation par la formule $\|M\| = \sup_{v \neq 0} \|Mv\|/\|v\|$. Une telle norme a la propriété $\|Mv\| \leq \|M\|\|v\|$ pour toute matrice M et tout vecteur colonne v . Nous obtenons tout de suite

$$(50) \quad |u_N| \leq \|L\| \|A_{r_\ell}\| \cdots \|A_{r_0}\| \|C\|.$$

Nous avons utilisé le caractère multiplicatif d'une norme subordonnée : pour M_1 et M_2 dans $M_d(\mathbb{K})$, $\|M_1 M_2\| \leq \|M_1\| \|M_2\|$. Si a est une borne pour les normes $\|A_r\|$, $0 \leq r < b$, nous obtenons ainsi pour $N \geq 1$

$$|u_N| \leq \|L\| \|C\| a^{\ell+1} = \|L\| \|C\| a^{\lceil \log_b N \rceil} \leq KN^{\log_b a},$$

avec $K = \|L\| \|C\| a$. Nous obtenons le résultat suivant [4, Th. 2.10].

PROPOSITION 10. *Une suite b -rationnelle a une croissance au plus polynomiale.*

L'idée peut-être poussée plus loin. Introduisons une norme multiplicative $\|\cdot\|$, qui n'est pas nécessairement une norme subordonnée d'ailleurs. Nous pouvons considérer la suite des

$$\hat{\rho}_\ell(A) = \max_{w \in \mathbb{Z}^\ell} \|A_w\|^{1/\ell},$$

qui dépend de la norme multiplicative utilisée. Cette suite est convergente [57, 44].

PROPOSITION 11. *Soit $A = (A_z)_{z \in \mathbb{Z}}$ une famille finie de matrices carrées à coefficients dans un corps de nombres. La suite $(\hat{\rho}_\ell(A))$ converge vers*

$$(51) \quad \hat{\rho}(A) = \lim_{\ell \rightarrow +\infty} \hat{\rho}_\ell(A) = \inf_{\ell} \hat{\rho}_\ell(A).$$

De plus la limite est indépendante de la norme utilisée.

DÉMONSTRATION. La preuve est directe dans le cas particulier où tous les produits de longueur ℓ sont nuls à partir d'un certain rang. Sinon, la preuve utilise le lemme de Fekete : si une suite de réels (a_ℓ) est sous-additive, alors la suite (a_ℓ/ℓ) est convergente de limite l'infimum des a_ℓ/ℓ , $\ell \geq 1$. Le lemme est appliqué à la suite des $\log \max_{w \in \mathcal{Z}^\ell} \|A_w\|$, $\ell \geq 1$. La limite est indépendante de la norme multiplicative utilisée parce que deux telles normes sont équivalentes. En effet elles diffèrent au plus d'un facteur multiplicatif $k > 0$ qui disparaît dans le passage à la limite. \square

DÉFINITION 12. La limite annoncée dans la proposition précédente est le rayon spectral $\hat{\rho}(A)$ (joint spectral radius) de la famille A .

PROPOSITION 12. Une suite b -rationnelle (u_n) qui admet une représentation linéaire (L, A, C) a un comportement asymptotique

$$(52) \quad u_N \underset{N \rightarrow +\infty}{=} O(N^{\log_b \hat{\rho}(A) + \varepsilon}) \quad \text{pour tout } \varepsilon > 0$$

où $\hat{\rho}(A)$ est le rayon spectral de l'action A .

DÉMONSTRATION. D'après la proposition précédente, la suite des $\hat{\rho}_\ell(A)$ converge vers $\hat{\rho}(A)$ qui est l'infimum de la suite, donc pour tout $\varepsilon > 0$ et pour ℓ assez grand, l'inégalité $\hat{\rho}_\ell(A) < \hat{\rho}(A) + \varepsilon$ est satisfaite. Notons $\rho = \hat{\rho}(A) + \varepsilon$ pour alléger l'écriture. Sachant que le nombre de chiffres d'un naturel $N > 0$ en base b est $1 + \lfloor \log_b N \rfloor$, de l'inégalité précédente nous tirons pour N assez grand ($\ell = \lfloor \log_b N \rfloor$)

$$|u_N| \leq \|L\| \rho^{1+\ell} \|C\| \leq \|L\| \rho \|C\| \times \rho^{\log_b N} = \|L\| \rho \|C\| \times N^{\log_b \rho}.$$

\square

Il est connu que le rayon spectral est difficile à calculer [44, Th 2.4], mais il existe tout de même des bornes assez simples à obtenir [62, chap. 6]. En particulier, puisque le rayon spectral est l'infimum des normes des produits de longueur ℓ à la puissance $1/\ell$, un majorant se calcule facilement.

EXEMPLE 28. Nous avons obtenu à l'exemple 19 une représentation linéaire pour la complexité de l'algorithme de Karatsuba. Nous calculons les normes des produits de longueur ℓ pour ℓ allant de 1 à 10 et pour les normes d'indice 1 et ∞ (qui sont les normes subordonnées des normes vectorielles 1 et ∞) ainsi que pour la norme de Frobenius (qui n'est pas une norme subordonnée, mais est multiplicative)

$$\|M\|_1 = \max_j \sum_i |M_{i,j}|, \quad \|M\|_\infty = \max_i \sum_j |M_{i,j}|, \quad \|M\|_F = \left(\sum_{i,j} |M_{i,j}|^2 \right)^{1/2}.$$

La plus petite des valeurs numériques obtenues est $\hat{\rho}_{10}(A) = 562615^{1/10} \simeq 3.76$ pour la norme d'indice 1 et 3.76 est donc un majorant de $\hat{\rho}(A)$ (figure 3).

\triangle

Cependant les représentations linéaires que l'on rencontre dans les applications sont souvent structurées, ce qui permet des approches plus raffinées. Citons par exemple le résultat suivant [44, Prop. 1.5].

PROPOSITION 13. Si les matrices d'une famille finie $A = (A_z)_{z \in \mathcal{Z}}$ peuvent être simultanément trigonalisées par blocs

$$P^{-1} A_z P = \begin{pmatrix} B_z & C_z \\ 0 & D_z \end{pmatrix}, \quad z \in \mathcal{Z},$$

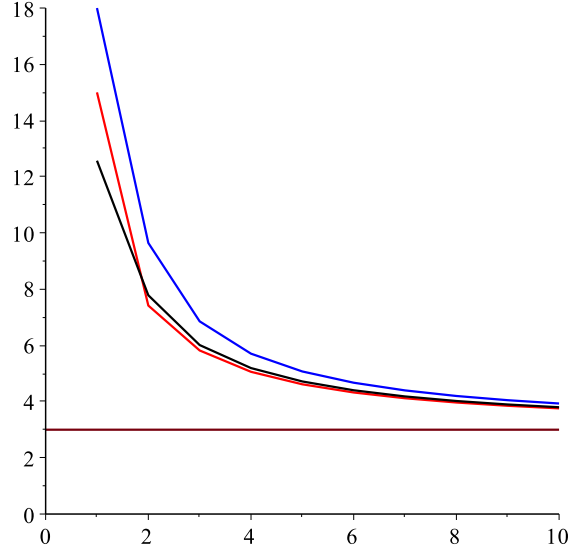


FIGURE 3. Les suites $(\hat{\rho}_\ell(A))$ pour la complexité de l'algorithme de Karatsuba (exemple 28), avec $1 \leq \ell \leq 10$ et pour la norme d'indice 1 (trait rouge), la norme d'indice ∞ (trait bleu), la norme de Frobenius (trait noir).

par une matrice inversible P , alors le rayon spectral de la famille A vaut le maximum des rayons spectraux des deux familles de blocs diagonaux,

$$\hat{\rho}(A) = \max(\hat{\rho}(B), \hat{\rho}(D)).$$

EXEMPLE 29. Reprenons l'exemple 28 précédent. La famille de matrices (A_0, A_1) est triangulaire par blocs, disons de la forme

$$A_0 = \begin{bmatrix} B_0 & 0 \\ C_0 & D_0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} B_1 & 0 \\ C_1 & D_1 \end{bmatrix}.$$

Nous obtenons tout de suite $\hat{\rho}(A) = \max(\hat{\rho}(B), \hat{\rho}(D))$. Pour le premier rayon spectral, qui concerne

$$B_0 = \begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix},$$

la matrice inversible P qui suit trigonalise simultanément B_0 et B_1 ,

$$P = \begin{bmatrix} 2/3 & 1/3 \\ -2/3 & 2/3 \end{bmatrix}, \quad P^{-1}B_0P = \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix}, \quad P^{-1}B_1P = \begin{bmatrix} 1 & -1 \\ 0 & 3 \end{bmatrix}.$$

En réitérant l'argument sur ces matrices triangulaires, nous obtenons $\hat{\rho}(B) = 3$. Pour le deuxième rayon spectral, nous trouvons de même $\hat{\rho}(D) = 2$. Le rayon spectral est donc $\hat{\rho}(A) = \max(3, 2) = 3$, ce qui est cohérent avec le calcul numérique de l'exemple 28. \triangle

Algèbre linéaire

Nous considérons une suite b -rationnelle et nous voulons étudier son comportement asymptotique. Nous allons mettre en valeur ses éventuelles oscillations, que ne peuvent attraper les méthodes du chapitre précédent (figure 1, page 40), par un raisonnement basé sur l'algèbre linéaire.

EXEMPLE 30. La suite (u_n) qui donne la complexité de l'algorithme de Karatsuba comptée en nombres d'additions et de multiplications est théorique. Il est tentant de la comparer avec le temps de calcul réel. C'est ce que nous avons fait (ordinateur portable muni d'Intel Core i5, 2.8 GHz, 3MB) en tirant au pseudo-hasard des coefficients entiers de valeurs absolues plus petites que 99 et en appliquant l'algorithme pour des polynômes de taille n allant de 1 à 1024. Ceci nous a donné une suite de temps $(t_n)_{1 \leq n \leq 1024}$ exprimés en secondes. Ensuite nous avons comparé par ajustement linéaire les deux suites (u_n) et (t_n) , ce qui a fournit la formule

$$t_n \simeq 4 \cdot 10^{-6} u_n.$$

Les graphes des deux suites (t_n) et $(4 \cdot 10^{-6} u_n)$ sont représentés (figure 1) dans l'intervalle $32 \leq n \leq 1024$. L'accord entre les deux est frappant. Qui plus est, nous voyons que les deux suites majorantes rencontrées au chapitre précédent, page 40, ne peuvent absolument pas décrire les oscillations observées.

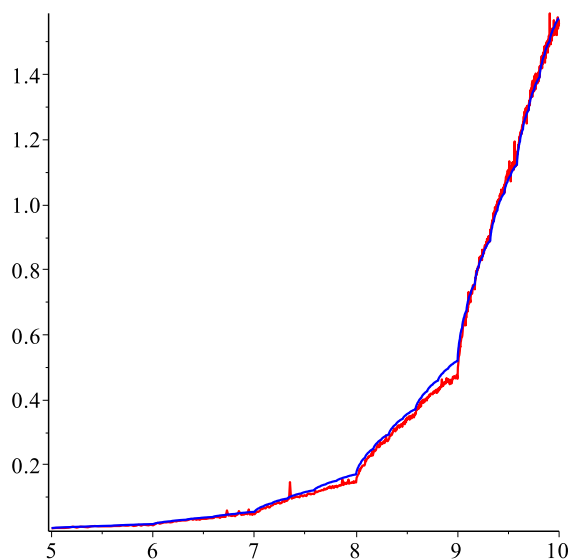


FIGURE 1. La complexité théorique (u_n) représente bien le temps de calcul dans l'algorithme de Karatsuba (exemple 30).

△

1. Processus de calcul

Nous allons décrire un procédé fondé sur l'algèbre linéaire qui fournit un développement asymptotique d'une suite b -rationnelle [37]. L'idée de base est de voir la suite étudiée (u_n) comme la suite sommatoire de la suite de ses différences arrière $\delta_n = u_n - u_{n-1}$ (avec $u_{-1} = 0$). Nous écrivons donc

$$u_N = \sum_{n=0}^N \delta_n.$$

La suite (δ_n) est b -rationnelle comme la suite (u_n) et nous utilisons une représentation linéaire (L, A, C) de la suite (δ_n) . Nous reprenons cette vieille idée simpliste qui consiste à regarder la suite (u_n) au puissance de b , précisément à l'indice $b^k - 1$. Les écritures des entiers de 0 à $b^k - 1$ utilisent tous les mots de longueur au plus k sur l'alphabet de la numération en base b , si l'on veut bien négliger le fait que nous n'utilisons que les mots ne commençant pas par 0. Puisque qu'un terme δ_n vaut $LA_w C$, en notant w l'écriture b -aire de n , la somme des δ_n entre les puissances b^{k-1} et $b^k - 1$ est essentiellement

$$\sum_{|w|=k} LA_w C = L(A_0 + A_1 + \dots + A_{b-1})^k C = LQ^k C,$$

où Q est la somme des matrices de l'action. Avec cette somme nous avons affaire à une suite rationnelle au sens classique. Le comportement de cette suite va dépendre des valeurs propres de la matrice Q et de la représentation du vecteur C sur une base de vecteurs propres, disons. Le spectre de la matrice Q va donc être un ingrédient important du procédé.

Cependant nous n'avons considéré que les puissances de b . Il nous faut interpoler le comportement de la suite entre deux puissances de b . Pour cela nous montrons que les sommes partielles de la suite (δ_n) sont directement liées à un somme indexée par des mots sur l'alphabet de la numération en base b . Cette somme satisfait à une équation fonctionnelle qui est une récurrence. Par passage à la limite nous obtenons ce que l'on appelle une équation de dilatation, une équation linéaire basée sur les opérateurs $f(x) \mapsto f(bx - r)$, $0 \leq r < b$. Plus précisément il y a une équation de dilatation par valeur propre. L'existence d'une solution à cette équation est garantie, par un théorème de point fixe, dès que la valeur propre est plus grande en module que le rayon spectral $\hat{\rho}$ de la représentation. Ceci amène une dichotomie dans les valeurs propres. Celles qui ont un module ρ plus grand que le rayon spectral vont fournir des termes en $\rho^{\log_b N} = N^{\log_b \rho}$. Celles qui ont un module égal ou inférieur au rayon spectral vont contribuer à un terme d'erreur en $O(N^{\log_b \hat{\rho} + \varepsilon})$.

2. Technique

Nous introduisons pour K entier naturel la somme

$$(53) \quad s_K(x) = \sum_{\substack{|w|=K \\ (0.w)_b \leq x}} LA_w C.$$

Dans cette écriture, x représente un réel de $[0, 1]$. Nous notons $|w|$ la longueur du mot w et si w s'écrit $w_1 \dots w_K$ alors $(0.w)_b$ est le nombre b -adique $w_1/b + \dots + w_K/b^K$. Enfin A_w est le produit matriciel $A_{w_1} \dots A_{w_K}$ (définition 11, page 41).

LEMME 3. Soit (L, A, C) une représentation linéaire insensible aux zéros à gauche pour la suite (δ_n) des différences arrière d'une suite b -rationnelle (u_n) . Alors la suite (u_n) s'exprime par

$$(54) \quad u_N = s_{K+1}(b^{\{\log_b N\}-1}),$$

en notant $K = \lfloor \log_b N \rfloor$ et $\{t\} = t - \lfloor t \rfloor$ la partie fractionnaire d'un réel t .

DÉMONSTRATION. Si nous écrivons les développements en base b des nombres de la forme n/b^{K+1} avec $0 \leq n \leq N$, nous obtenons après la virgule (qui tend à devenir un point) les écritures des entiers n avec $0 \leq n \leq N$ complétées à gauche par des 0 pour arriver à la longueur $K + 1$. Mais ces zéros à gauche n'ont pas d'importance puisque la représentation linéaire est insensible aux zéros à gauche. En notant que N s'écrit

$$N = b^{\log_b N} = b^{K+1} b^{\log_b(N) - (K+1)},$$

nous arrivons à la formule annoncée. \square

L'étude du comportement asymptotique de (u_n) se ramène donc à l'étude de la suite de fonctions $(s_K(x))$. Introduisons maintenant

$$S_K(x) = \sum_{\substack{|w|=K \\ (0.w)_b \leq x}} A_w C,$$

ce qui permet de réexprimer $s_K(x)$ sous la forme $s_K(x) = LS_K(x)$.

LEMME 4. La suite des sommes $S_K(x)$ vérifie la formule de récurrence

$$(55) \quad S_{K+1}(x) = \sum_{r_1 < x_1} A_{r_1} Q^K C + A_{x_1} S_K(bx - x_1),$$

pour $x = (0.x_1 x_2 \dots)_b$ dans $[0, 1[$.

DÉMONSTRATION. Nous rangeons les nombres de l'intervalle $[0, x]$ selon le préfixe de leur écriture en base b , ce qui nous fait casser la somme

$$S_{K+1}(x) = \sum_{\substack{|w|=K+1 \\ (0.w)_b \leq x}} A_w C$$

en morceaux. Nous avons d'abord les mots dont le premier chiffre r_1 est strictement plus petit que x_1 , qui fournissent la somme

$$\sum_{r_1 < x_1} \sum_{\substack{|w|=K \\ (0.r_1 w)_b \leq x}} A_w C = \sum_{r_1 < x_1} A_{r_1} Q^K C.$$

Ensuite nous avons les mots dont le premier chiffre est x_1 mais dont le second r_2 est strictement plus petit que x_2 et la somme

$$\sum_{r_2 < x_2} \sum_{\substack{|w|=K-1 \\ (0.r_1 r_2 w)_b \leq x}} A_w C = \sum_{r_2 < x_2} A_{r_1} A_{r_2} Q^{K-1} C.$$

En continuant ainsi nous obtenons la décomposition

$$S_{K+1}(x) = \sum_{r_1 < x_1} A_{r_1} Q^K C + \sum_{r_2 < x_2} A_{r_1} A_{r_2} Q^{K-1} C + \dots + \sum_{r_{K+1} \leq x_{K+1}} A_{x_1} A_{x_2} \dots A_{x_{K+1}} C$$

et nous voyons

$$S_{K+1}(x) = \sum_{r_1 < x_1} A_{r_1} Q^K C + A_{r_1} S_K(bx - x_1).$$

□

Le lemme 4 est le résultat crucial. C'est lui qui va faire apparaître la dichotomie sur les valeurs propres de $Q = A_0 + A_1 + \dots + A_{b-1}$. Cependant la technique devient un peu lourde à ce stade et pour simplifier la présentation nous allons supposer que la matrice Q est diagonalisable.

L'idée est de décomposer le vecteur C sur une base de vecteurs propres et de traiter séparément chaque composante. Regardons d'abord le cas d'un vecteur propre associé à une petite valeur propre.

LEMME 5. *Soit un V un vecteur propre de Q associé à une valeur propre ρw de module ρ inférieur au rayon spectral de la représentation linéaire. Alors la somme associée à V*

$$S_K(x) = \sum_{\substack{|w|=K \\ (0.w)_b \leq x}} A_w V$$

est un $O(r^K)$ uniformément par rapport à x pour $r > \hat{\rho}(A) \geq \rho$.

DÉMONSTRATION. La formule du lemme 4 donne pour toute norme subordonnée

$$\|S_{K+1}(x)\| \leq \rho^K \sum_{r_1 < x_1} \|A_{r_1}\| \|V\| + \|A_{r_1}\| \|S_K(bx - x_1)\|$$

et en considérant le supremum

$$\|S_{K+1}\|_\infty \leq \rho^K \sum_{r_1 < x_1} \|A_{r_1}\| \|V\| + \|A_{r_1}\| \|S_K\|_\infty.$$

Si nous avons $\|A_{r_1}\| \leq r$ pour tout r_1 , une preuve par récurrence termine la question. Sinon nous effectuons un changement de base de numération en passant de b à b^ℓ avec ℓ assez grand pour garantir que tous les produits A_w de longueur ℓ ont une norme plus petite que r , ce qui est possible d'après la définition du rayon spectral. □

Passons aux grandes valeurs propres. Nous avons d'abord besoin d'un résultat d'existence et d'unicité pour une équation de dilatation, aussi nommée équation de raffinement ou équation à deux échelles (*refinement equation, two-scale difference equation*). La définition de [27] est la suivante.

DÉFINITION 13. *Une équation de dilatation est une équation fonctionnelle de la forme*

$$f(x) = \sum_{n=0}^N c_n f(\alpha x - \beta_n)$$

avec $\alpha > 1$, $\beta_0 < \beta_1 < \dots < \beta_N$. La variable x est réelle et les coefficients c_n , $0 \leq n \leq N$, sont complexes.

De telles équations apparaissent dans la théorie des ondelettes [27, 28, 61] et dans la théorie des schémas de raffinement [35, 48, 31]. Les équations de dilatation que nous considérons ne sont pas scalaires mais vectorielles et pourvues de conditions aux limites.

LEMME 6. Dans l'hypothèse $\rho > \hat{\rho}(A)$, l'équation de dilatation

$$(56) \quad \rho\omega F(x) = \sum_{0 \leq r < b} A_r F(bx - r)$$

avec les conditions aux limites

$$(57) \quad F(x) = 0 \quad \text{pour } x \leq 0, \quad F(x) = V \quad \text{pour } x \geq 1,$$

où V est un vecteur propre de $Q = A_0 + \dots + A_{b-1}$ associé à la valeur propre $\rho\omega$ de module ρ , possède une unique solution continue de \mathbb{R} dans \mathbb{C}^d . De plus cette solution est Hölder d'exposant $\log_b(\rho/r)$ pour tout $r > \hat{\rho}(A)$.

DÉMONSTRATION. L'idée de la preuve est d'écrire l'équation sous la forme

$$F(x) = \frac{1}{\rho\omega} \sum_{0 \leq r < b} A_r F(bx - r)$$

et le passage du membre gauche au moins droit est essentiellement un opérateur contractant. \square

Ce résultat nous permet de revenir vers la somme qui nous intéresse.

LEMME 7. Soit V un vecteur propre associé à une valeur propre $\rho\omega$ de Q de module ρ strictement supérieur au rayon spectral de la représentation linéaire, alors la somme associée à V

$$S_K(x) = \sum_{\substack{|w|=K \\ (0.w)_b \leq x}} A_w V$$

a un comportement asymptotique

$$(58) \quad S_K(x) \underset{K \rightarrow \infty}{=} (\rho\omega)^K F(x) + O(r^K)$$

pour $\rho > r > \hat{\rho}(A)$ et uniformément par rapport à x .

DÉMONSTRATION. Nous mélangeons la formule de récurrence du lemme 4, l'équation de dilatation (56) et le caractère contractant utilisé dans la pseudo-preuve précédente. \square

La formule (55) n'est pas homogène alors que l'équation de dilatation (56) est homogène. Ceci peut sembler curieux. Si nous récrivons la relation (55), en tenant compte du fait la somme est associée à un vecteur propre V et une valeur propre $\rho\omega$, sous la forme

$$\begin{aligned} \frac{1}{(\rho\omega)^K} S_{K+1}(x) &= \frac{1}{(\rho\omega)^K} \sum_{r_1 < x_1} A_{r_1} Q^K V + A_{x_1} \frac{1}{(\rho\omega)^K} S_K(bx - x_1) \\ &= \sum_{r_1 < x_1} A_{r_1} V + A_{x_1} \frac{1}{(\rho\omega)^K} S_K(bx - x_1) \end{aligned}$$

nous obtenons par passage à la limite

$$(59) \quad \rho\omega F(x) = \sum_{r_1 < x_1} A_{r_1} V + A_{x_1} F(bx - x_1).$$

Mais pour $x_1/b \leq x < (x_1 + 1)/b$ et pour $r_1 < x_1$, le réel $bx - r_1$ est supérieur ou égal à 1 et nous retrouvons bien l'équation de dilatation (56). Les conditions aux limites ont permis de rendre l'équation homogène.

Nous pouvons maintenant assembler les résultats précédents.

THÉORÈME 10. *Soit (u_n) une suite b -rationnelle dont la suite des différences arrière est définie par une représentation linéaire. Alors la suite (u_n) admet un développement asymptotique qui est une somme de termes de la forme*

$$N^{\log_b \rho} \binom{\log_b N}{m} \times e^{i\vartheta \log_b N} \times \varphi(\log_b N).$$

Dans cette écriture, $\rho e^{i\vartheta}$ est une valeur propre de la matrice $Q = A_0 + A_1 + \dots + A_{b-1}$ dont le module ρ est strictement plus grand que le rayon spectral de la représentation linéaire. L'entier m est borné par la taille maximale des blocs de Jordan relatifs à la valeur propre $\rho e^{i\vartheta}$. La fonction $\varphi(t)$ est 1-periodique est hölderienne d'exposant $\log_b(\rho/r)$ pour $\rho > r > \hat{\rho}(A)$. Le terme d'erreur est un $O(N^{\log_b r})$ pour $r > \hat{\rho}(A)$.

DÉMONSTRATION. Nous reprenons la formule (58) et nous opérons la substitution qui correspond à la formule (54). Avec $t = \log_b N$, $K = \lfloor \log_b N \rfloor$, cela donne un terme

$$S_{K+1}(b^{\{t\}-1}) = (\rho e^{i\vartheta})^{K+1} F(b^{\{t\}-1}) + O(r^K) = (\rho e^{i\vartheta})^t (\rho e^{i\vartheta})^{1-\{t\}} F(b^{\{t\}-1}) + O(r^K)$$

soit

$$(60) \quad N^{\log_b \rho} e^{i\vartheta \log_b N} \Phi(t) + O(N^{\log_b r})$$

en posant

$$(61) \quad \Phi(t) = (\rho e^{i\vartheta})^{1-\{t\}} F(b^{\{t\}-1}).$$

La fonction $\Phi(t)$ est hölderienne de même exposant que $F(x)$, sauf peut-être aux entiers à cause de la présence des parties fractionnaires, qui empêchent de garantir sa continuité aux entiers. La continuité de $\varphi(t) = L\Phi(t)$ résulte des formules $\Phi(1^-) = F(1) = V$ et $\Phi(0^+) = F(1/b)\rho\omega = A_0V$ et de l'insensibilité aux zéros à gauche. \square

Nous avons supprimé dans l'énoncé les hypothèses inutiles comme l'insensibilité aux zéros à gauche, mais si celle-ci n'est pas satisfaite il faut bien sûr en tenir compte dans les calculs. De même nous avons enlevé l'hypothèse que la matrice Q est diagonalisable. Un traitement complet demande l'emploi d'une réduite de Jordan et de vecteurs propres généralisés. Nous renvoyons à [37] pour une version expurgée de ces hypothèses.

Le développement asymptotique utilise des fonctions définies comme solutions d'équation de dilatation. Ces équations les définissent complètement mais elles sont à ce stade assez éthérées. Nous pouvons calculer les valeurs d'une telle fonction aux points de la forme j/b^k avec k entier naturel et $0 \leq j \leq b^k$. Pour simplifier l'expression supposons que la base b soit égale à 2. Nous connaissons les valeurs de la fonction en 0 et 1, d'après les conditions aux limites. L'équation de dilatation

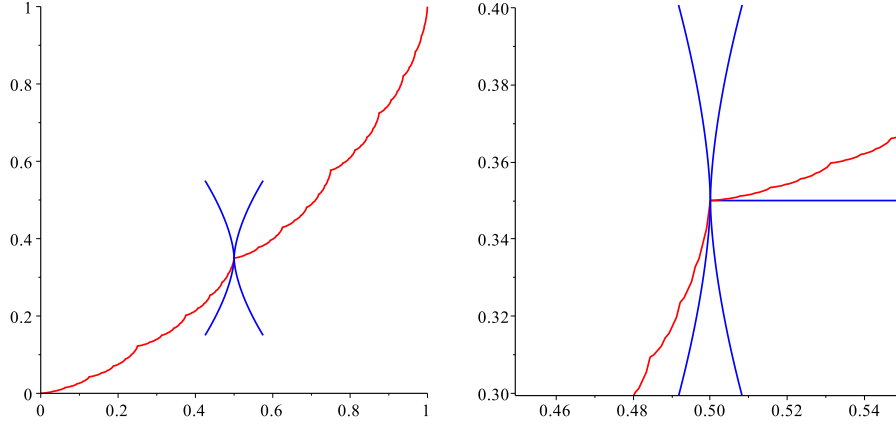


FIGURE 2. La fonction de répartition pour un jeu de pile ou face infini est solution d'une équation de dilatation (exemple 31).

nous donne les valeurs en $1/2$, puis $1/4$ et $3/4$, ensuite $1/8$, $3/8$, $5/8$, $7/8$, etc. Ce procédé est l'algorithme en cascade (*cascade algorithm*) [27, § 4].

EXEMPLE 31. Dans [13, exemple 31.1, p. 407], Patrick Billingsley considère un lancer de pièces répété à l'infini, c'est-à-dire une suite infinie $(T_n)_{n \geq 1}$ de variables aléatoires de Bernoulli indépendantes et équidistribuées. Plus précisément la loi est $\mathbf{P}(T = 0) = p_0$, $\mathbf{P}(T = 1) = p_1$ avec $p_0 + p_1 = 1$ et les conditions $0 < p_0, p_1 < 1$. Si nous considérons les tirages finis nous avons une série rationnelle qui admet la représentation linéaire $L = (1)$, $A_0 = (p_0)$, $A_1 = (p_1)$, $C = (1)$ de dimension 1. Avec les notations que nous avons employées, nous trouvons $Q = (1)$, $\rho = 1$, $\hat{\rho}(A) = \max(p_0, p_1)$. La fonction de répartition $F(x)$ de la variable aléatoire

$$X = \sum_{n \geq 1} \frac{T_n}{2^n},$$

est exactement la solution de l'équation de dilatation (56), ici

$$F(x) = p_0 F(2x) + p_1 F(2x - 1).$$

En effet nous avons, respectivement pour $0 \leq x < 1/2$ et pour $1/2 \leq x < 1$,

$$F(x) = \mathbf{P}(X \leq x) = \mathbf{P}(T_1 = 0, \sum_{n \geq 2} \frac{T_n}{2^{n-1}} \leq 2x) = p_0 F(2x)$$

$$F(x) = \mathbf{P}(X \leq x) = \mathbf{P}(T_1 = 0) + \mathbf{P}(T_1 = 1, \sum_{n \geq 2} \frac{T_n}{2^{n-1}} \leq 2x - 1) = p_0 + p_1 F(2x - 1),$$

ce qui est l'équation de dilatation dans la version non homogène (59). Il en résulte que cette fonction est hõlderienne d'exposant $\log_2(1/\hat{\rho}(A))$. Dans le dessin de la figure 2, les paramètres sont $p_0 = 7/20$, $p_1 = 13/20$ d'où $\hat{\rho}(A) = 13/20$ et un exposant de Hõlder $\log_2 20/13 \simeq 0.62$. Nous avons dessiné pour le point $x = 1/2$ deux arcs de pseudo-parabole qui matérialisent l'encadrement de Hõlder. Cependant l'exposant est valable uniformément sur tout l'intervalle. Il est possible de raffiner la notion à la fois en considérant une notion locale et en distinguant droite et gauche. Alors, en un point dyadique, l'exposant précédent est un exposant de Hõlder à gauche et on peut montrer que 0 est un exposant de Hõlder à droite, ce qui est visible sur le dessin et sur le grossissement qui en est proposé.

△

3. Exemple développé

Nous traitons pas à pas le cas de la complexité de l'algorithme de Karatsuba.

3.1. Représentation linéaire. Nous avons besoin d'une représentation linéaire pour la série formelle $\delta(x) = (1-x)u(x)$. La formule (32) de l'exemple 8 donne par simple remplacement

$$\delta(x) = \frac{(2+x)}{x}\delta(x^2) - \frac{x-6x^2+x^3}{1-x}.$$

Nous calculons à l'aide de cette équation les sections

$$T_{2,0}\delta(x) = \delta(x) + \frac{5x-x^2}{1-x}, \quad T_{2,1}\delta(x) = 2\frac{\delta(x)}{x} - \frac{1-5x}{1-x}$$

$(\delta(x)/x)$ est bien une série formelle à cause des égalités $\delta_0 = u_0 = 0$) et nous voyons qu'un \mathbb{Q} -sous-espace stable par section et contenant $\delta(x)$ est le sous-espace engendré par la famille $(\delta(x), \delta(x)/x, 1/(1-x), x/(1-x), x^2/(1-x), x^3/(1-x))$. Nous en tirons la représentation linéaire en dimension 6,

$$L = [0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0], \quad A_0 = \begin{bmatrix} B_0 & 0 \\ C_0 & D_0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

avec

$$A_1 = \begin{bmatrix} B_1 & 0 \\ C_1 & D_1 \end{bmatrix},$$

$$B_0 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix},$$

$$C_0 = \begin{bmatrix} 0 & -1 \\ 5 & 5 \\ -1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C_1 = \begin{bmatrix} -1 & 5 \\ 5 & -1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},$$

$$D_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad D_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

3.2. Calcul du rayon spectral. Comme dans l'exemple 29, page 44, les deux matrices A_0 et A_1 sont bloc-triangulaires, ce qui fournit tout de suite (proposition 13, page 43) $\hat{\rho}(A) = \max(\hat{\rho}(B), \hat{\rho}(D))$. Mais les matrices B_0 et B_1 sont triangulaires inférieures et les matrices D_0 et D_1 sont triangulaires supérieures. Il suffit donc de considérer le maximum des éléments diagonaux pour trouver $\hat{\rho}(A) = 2$. Cette valeur indique que nous allons obtenir un développement asymptotique avec un terme d'erreur $O(N^{1+\varepsilon})$ avec $\varepsilon > 0$ aussi près que l'on veut de 0.

3.3. Réduction de Jordan. Un calcul de réduite de Jordan effectué sur la matrice Q donne la matrice de passage P et la réduite Q' ,

$$P = \begin{bmatrix} 0 & 0 & 0 & 24 & 0 & 0 \\ 8 & 0 & 0 & -24 & 0 & 0 \\ 48 & -96 & -96 & 120 & 24 & 179 \\ 16 & 0 & 96 & -96 & -48 & -334 \\ 0 & 0 & 0 & -24 & 24 & 131 \\ 0 & 0 & 0 & 0 & 0 & 24 \end{bmatrix}, \quad Q' = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Il faut noter que le changement de base ne change pas le rayon spectral, qui est intrinsèque. Seule la valeur propre 3 a un module strictement plus grand que le rayon spectral $\hat{\rho}(A) = 2$. Ceci nous fait prévoir un terme de la forme $N^{\log_2 3} \Phi(\log_2 N)$ dans le développement asymptotique.

Nous appliquons le changement de base à la représentation linéaire, ce qui donne la nouvelle représentation

$$L' = [56 \quad -96 \quad -96 \quad 96 \quad 24 \quad 179], \quad A'_0 = \begin{bmatrix} 2 & 0 & 0 & -3 & 0 & 0 \\ 1/3 & 1 & 0 & -2 & 0 & 0 \\ 1/4 & 0 & 1 & 1/4 & -1/4 & -155/96 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$A'_1 = \begin{bmatrix} 1 & 0 & 0 & 3 & 0 & 0 \\ -1/3 & 1 & 0 & 2 & 0 & 0 \\ -1/4 & 0 & 0 & 3/4 & 1/4 & 155/96 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad C' = \begin{bmatrix} 1/8 \\ 1/12 \\ 1/24 \\ 1/24 \\ 1/24 \\ 0 \end{bmatrix}.$$

Il est possible de travailler avec l'ancienne ou la nouvelle représentation. Les composantes du vecteur C' montre que le vecteur de coordonnées C de la représentation a une composante égale à $1/8$ sur le vecteur propre associé à la valeur propre 3, qui est $V = 8E_2 + 48E_3 + 16E_4$, d'après la première colonne de la matrice P . Nous utilisons donc le vecteur propre $V = E_2 + 6E_3 + 2E_4$.

3.4. Équation de dilatation. Nous traitons la valeur propre 3, l'unique valeur propre strictement plus grande que le rayon spectral. Pour cela nous avons à « résoudre » l'équation de dilatation

$$3F(x) = A_0F(2x) + A_1F(2x - 1).$$

L'inconnue $F(x)$ est une fonction vectorielle à valeurs dans \mathbb{R}^d , avec $d = 6$ qui est la dimension de la représentation linéaire. Elle est définie sur tout \mathbb{R} , mais avec les conditions aux limites

$$F(x) = 0 \quad \text{pour } x \leq 0, \quad F(x) = E_2 + 6E_3 + 2E_4 \quad \text{pour } x \geq 1.$$

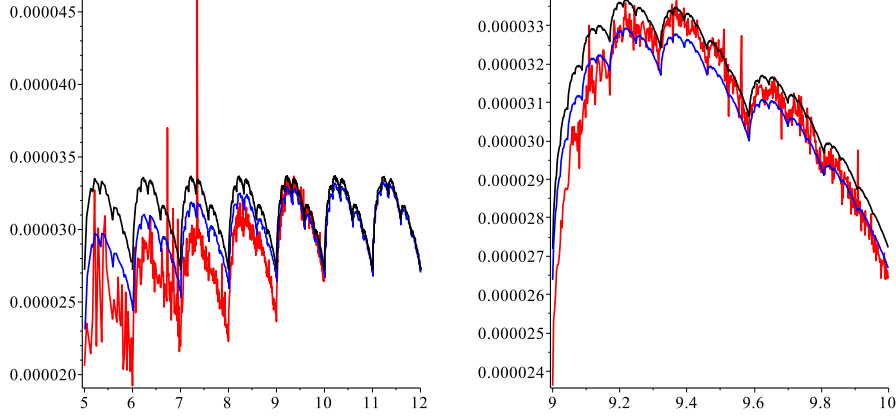


FIGURE 3. La complexité de l'algorithme de Karatsuba empirique (trait rouge), théorique (trait bleu), normalisées grâce à une division par $N^{\log_2 3}$ et une échelle logarithmique pour les abscisses, comparées avec la fonction périodique hölderienne d'exposant 0.58 (trait noir) que révèle l'analyse asymptotique.

L'équation s'explique en le système

$$\begin{aligned}
 f_1(x) &= \frac{2}{3}f_1(2x) - f_4(2x), \\
 f_2(x) &= \frac{1}{9}f_1(2x) + \frac{1}{3}f_2(2x) - \frac{2}{3}f_4(2x) + \frac{2}{3}f_1(2x-1) + \frac{1}{3}f_2(2x-1), \\
 f_3(x) &= \frac{1}{12}f_1(2x) + \frac{1}{3}f_3(2x) + \frac{1}{12}f_4(2x) - \frac{1}{12}f_5(2x) - \frac{155}{288}f_6(2x) \\
 &\quad - \frac{1}{3}f_1(2x-1) + \frac{5}{3}f_2(2x-1) + \frac{1}{3}f_3(2x-1) + \frac{1}{3}f_4(2x-1), \\
 f_4(x) &= \frac{1}{3}f_4(2x) + \frac{5}{3}f_1(2x-1) - \frac{1}{3}f_2(2x-1) + \frac{1}{3}f_5(2x-1) + \frac{1}{3}f_6(2x-1), \\
 f_5(x) &= \frac{1}{3}f_6(2x), \\
 f_6(x) &= 0.
 \end{aligned}$$

La fonction scalaire utile est $f(x) = LF(x) = f_2(x) + f_3(x)$. Selon le théorème 10, nous arrivons à la formule

$$u_N \underset{N \rightarrow \infty}{=} N^{\log_2 3} \varphi(\log_2 N) + O(N^{1+\varepsilon})$$

avec $\varepsilon > 0$ et une fonction $\varphi(t)$ qui est déterminée par

$$\varphi(t) = 3^{1-\{t\}} f(2^{\{t\}-1}).$$

Nous savons calculer cette fonction sur tous les réels t qui sont, à un entier près, des logarithmes en base 2 d'entiers naturels non nuls. En effet un tel réel s'écrit $t = T + \log_2 N$ avec T entier relatif et N entier naturel non nul. Si l'entier N vérifie $2^K \leq N < 2^{K+1}$, alors la partie entière du logarithme base 2 de N est K et nous

obtenons $\{t\} - 1 = \log_2(N/2^{K+1})$, d'où

$$2^{\{t\}-1} = \frac{N}{2^{K+1}}.$$

Ces points sont exactement ceux pour lesquels nous pouvons appliquer l'algorithme en cascade. Cet algorithme a fourni le graphique (en noir) de la fonction $\varphi(t)$ dans la figure 3. À côté de cela nous avons (en bleu) le graphique de la suite $(u_n/n^{\log_2 3})$ et nous voyons bien la convergence attendue. Plus précisément la fonction et la suite précédente ont été multipliées par le coefficient $4 \cdot 10^{-6}$ que nous avons rencontré en début de ce chapitre (figure 1, page 45). Ceci permet une comparaison avec la fonction empirique obtenue en divisant le temps de calcul réel sur machine par $n^{\log_2 3}$, représenté en rouge. L'accord est merveilleux.

Questions

EXERCICE 1 — Une méthode efficace, dans le cas $b > 2$, pour calculer une section $T_{b,r}f(x)$ d'une fraction rationnelle $f(x)$ consiste en

- (1) développer en série la fraction rationnelle à un ordre adéquat ;
- (2) fabriquer un développement de la section en attrapant les termes $f_{bk+r}x^k$;
- (3) construire la section en calculant un approximant de Padé [42, sec. 12.4].

Il est admis que le numérateur et le dénominateur de la section n'ont pas un degré plus grand que celui du numérateur et du dénominateur de la fraction originelle. Testez avec $b = 3$ et

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

EXERCICE 2 — La recherche du maximum et du minimum des valeurs dans une liste, disons d'entiers, a_1, a_2, \dots, a_n , peut se faire par une stratégie diviser pour régner :

- dans le cas $n = 1$, alors a_1 est à la fois le maximum et le minimum ;
- dans le cas $n > 1$, nous coupons la liste en deux moitiés de taille $\lfloor n/2 \rfloor$, $\lceil n/2 \rceil$, nous traitons chacune des moitiés, puis nous comparons les maxima et les minima pour obtenir le maximum et le minimum de la liste originelle.

Le coût, compté en nombre de comparaisons, est donc fourni par la suite (u_n) définie par

$$u_0 = 0, \quad u_1 = 0, \quad u_n = u_{\lfloor n/2 \rfloor} + u_{\lceil n/2 \rceil} + 2, \quad n \geq 2.$$

Donnez une équation de Mahler vérifiée par la série génératrice $u(x)$ de la suite (u_n) .

EXERCICE 3 — **1.** La suite (u_n) définie par $u_0 = 0, u_1 = 1, u_2 = 2$ et la relation de récurrence

$$u_n = -u_{n-3} + u_{\lfloor n/2 \rfloor}, \quad n \geq 3$$

est-elle rationnelle dans une base de numération ?

2. La suite sommatoire de la suite (u_n) , définie par $s_0 = u_0, s_n = s_{n-1} + u_n$ pour $n \geq 1$, est-elle rationnelle dans une base de numération ?

EXERCICE 4 — Donald Knuth propose [46, exercices 14 et 14, sec. 5.2.2] l'étude de la suite des différences $\delta_n = u_{n+1} - u_n$ où (u_n) est la suite des coûts, comptés en nombre de comparaisons, de la méthode de tri de Batcher. Cette suite $(u_n)_{n \geq 0}$ commence par 0, 0, 1, 3, 5... La suite des différences vérifie

$$\delta_{2n} = \delta_n + \lambda_n + 1, \quad n \geq 1; \quad \delta_{2n+1} = \delta_n + 1, \quad n \geq 0,$$

avec $\lambda_n = \lfloor \log_2 n \rfloor$. Fournissez une représentation linéaire de la suite (δ_n) et montrez que la suite (u_n) est rationnelle en base 2.

EXERCICE 5 — La suite de Stern-Brocot a été définie et pourvue d'une représentation linéaire à l'exemple 27, page 41. En vous inspirant de l'exemple 21, page 28, donnez un équation de Mahler pour sa série génératrice.

EXERCICE 6 — La série génératrice de la suite de Stern-Brocot est le produit infini

$$u(x) = x \prod_{k \geq 0} (1 + x^{2^k} + x^{2^{k+1}}).$$

Fournissez une récurrence de type plancher-plafond pour cette suite.

EXERCICE 7 — La suite de Stern-Brocot montre dans chaque intervalle entre deux puissances de 2 une valeur maximale atteinte en deux points symétriques dans l'intervalle (figure 2, page 42) qui sont placés à peu près aux tiers de l'intervalle. Dans l'intervalle $[2^r, 2^{r+1}]$, le premier point est

$$n_r = \frac{4 \cdot 2^r - (-1)^r}{3}$$

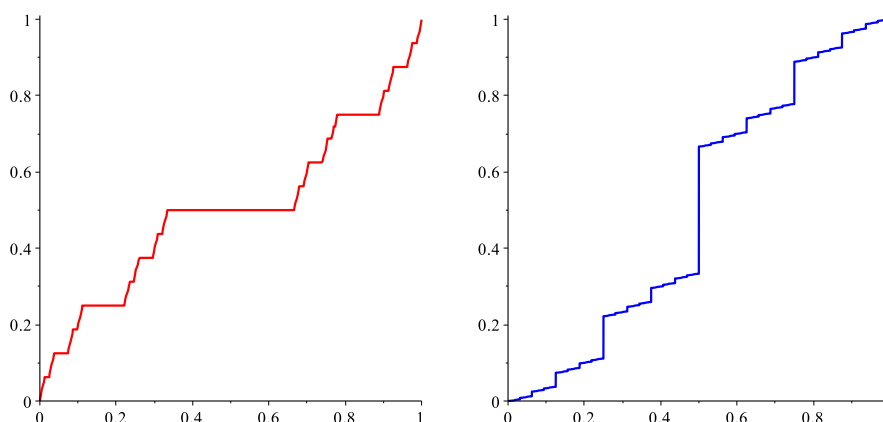
et le second est $n_r^* = 3 \cdot 2^r - n_r$. Quelle est la valeur du maximum m_r ?

EXERCICE 8 — Tout réel x de $[0, 1]$ admet un développement triadique

$$x = \frac{c_1}{3} + \frac{c_2}{3^2} + \cdots, \quad c_k \in \{0, 1, 2\}.$$

L'ensemble de Cantor \mathcal{C} est défini comme l'ensemble des points de $[0, 1]$ tels qu'aucun des c_k , $k \geq 1$, ne soit égal à 1. Par analogie, la suite caractéristique de Cantor $(\chi_n)_{n \geq 0}$ est définie par $\chi_n = 1$ si le développement triadique de n ne contient pas de 1 et $\chi_n = 0$ sinon [6, ex. 12.1.5, p. 353]. Donnez une récurrence vérifiée par cette suite, puis de là une équation de Mahler satisfaite par sa série génératrice $\chi(x)$. En jouant sur l'homomorphisme de Frobenius qui donne $\chi(x^3) \equiv \chi(x)^3 \pmod{3}$, obtenez un lien entre la suite (χ_n) et la suite des coefficients binomiaux centraux.

EXERCICE 9 — La suite de Cantor $(c_n)_{n \geq 0}$ est la suite strictement croissante des entiers qui n'utilisent pas le chiffre 1 dans leur développement triadique [4, ex. 3, p. 186]. Elle commence avec $c_0 = 0$, $c_1 = 2$, $c_2 = 6$, $c_3 = 8$. Donnez une formule de récurrence pour cette suite et montrez ainsi qu'elle est rationnelle en base 2. De là tirez une équation de Mahler pour sa série génératrice, d'abord inhomogène, puis homogène.

FIGURE 1. La fonction de Cantor $C(x)$ et sa fonction inverse $C^*(y)$.

EXERCICE 10 — La suite de Newman-Coquet [49, 25] est définie par $u(n) = (-1)^{s_2(3n)}$, où $s_2(n)$ est la somme des chiffres de l'écriture binaire de n . Cette suite est 4-rationnelle et admet la représentation linéaire (associée à la famille $(u(n), u(4n+2), u(4n+3))$)

$$A_0 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$L = [1 \quad 1 \quad 1], \quad A_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -1 & 1 \end{bmatrix}.$$

Quel est le rayon spectral de la famille $(A_r)_{0 \leq r < 4}$?

EXERCICE 11 — À chaque réel x de $[0, 1]$ est associé un ou deux développements triadiques, $x = (0.c_1c_2\dots)_3$. La fonction de Cantor C est définie comme suit : pour x dans $[0, 1]$, soit k_x le plus petit entier k pour lequel le chiffre c_k vaut 1, avec $k_x = \infty$ pour un x qui est dans \mathcal{C} (exercice 8), alors

$$C(x) = \frac{1}{2} \left(\frac{c_1}{2} + \dots + \frac{c_{k_x-1}}{2^{k_x-1}} \right) + \frac{1}{2^{k_x}}.$$

Bien que le développement dyadique d'un réel ne soit pas nécessairement unique, la définition est correcte car une suite infinie de chiffres triadiques 2 est envoyée sur une suite infinie de chiffres dyadiques 1. Le graphe de C (figure 1 à gauche) est appelé escalier du diable. Montrez que cette fonction est solution d'une équation de dilatation.

EXERCICE 12 — La suite de Rudin-Shapiro (que nous avons rencontrée en couverture, page ii) vérifie l'égalité $u_n = (-1)^{e_{2;11}(n)}$ où $e_{2;11}(n)$ est le nombre d'occurrences (possiblement chevauchantes) du motif 11 dans le développement binaire de

l'entier n [16]. Elle est 2-rationnelle : elle admet la famille génératrice (u_n, u_{2n+1}) et la représentation linéaire insensible aux zéros à gauche

$$L = \begin{bmatrix} 1 & 1 \end{bmatrix}, \quad A_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & 0 \\ 1 & -1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Quel est le rayon spectral de la famille A ? Quelles sont les valeurs propres de la matrice $Q = A_0 + A_1$. Donnez la forme d'un développement asymptotique de la suite (u_n) .

EXERCICE 13 — La fonction de Cantor envoie l'ensemble de Cantor sur le segment $[0, 1]$ et chaque nombre dyadique (c'est-à-dire avec un développement dyadique fini) est l'image d'un intervalle (par exemple $1/2$ est l'image de l'intervalle $[1/3, 2/3]$). La fonction de Cantor n'est pas injective et n'admet donc pas de fonction réciproque, c'est-à-dire pas d'inverse à gauche. Il est cependant possible de définir une fonction que l'on appelle (à tort) réciproque C^* . C'est l'unique fonction continue à droite qui à un nombre dyadique associe le plus grand de ses antécédents [47]. Ainsi C possède un inverse à droite C^* . Explicitement si y dans $[0, 1]$ a pour développement dyadique

$$y = \frac{b_1}{2} + \frac{b_2}{2^2} + \dots, \quad b_k \in \{0, 1\},$$

alors la fonction « réciproque » s'exprime par

$$C^*(y) = \frac{2b_1}{3} + \frac{2b_2}{3^2} + \dots.$$

Le graphe de C^* est tracé en figure 1 à droite. Montrez que la suite définie par la récurrence diviser pour régner

$$u_n = 3u_{\lfloor \frac{n}{2} \rfloor} + n, \quad u_0 = 0, \quad u_1 = 1$$

s'exprime à l'aide de C^* . De là tirez l'asymptotique de cette suite. [Cet exercice est dû au Dr Salvy [59].]

EXERCICE 14 — Nous voulons trouver un développement asymptotique pour la somme

$$s_N = \sum_{0 \leq n < N} 2^{s_2(n)},$$

dont nous savons (exemple 14, page 20) qu'elle représente le nombre de coefficients binomiaux impairs dans les N premières lignes du triangle de Pascal. Pour cela nous considérons la suite (u_n) de ses différences arrière, qui s'exprime par

$$u_n = 2^{s_2(n-1)} \quad \text{pour } n > 0, \quad u_0 = 0.$$

Montrez que cette suite (u_n) est rationnelle en base 2 et par là même trouvez-en une représentation linéaire L, A, C . Quelle est le rayon spectral de la famille A ? Quelles sont les valeurs propres de la matrice Q et comment se décompose le vecteur colonne C sur les vecteurs propres de Q ? Explicitiez l'équation de dilatation relative à la valeur propre dominante. Quelle est la première composante de la solution? Pour ce qui est de la deuxième composante, retournez voir l'exemple 31, page 51. Nommons f cette deuxième composante. Fournissez un développement asymptotique pour la suite (s_N) en utilisant cette fonction f .

Réponses

RÉPONSE 1 — Pour la fraction considérée, le maximum des degrés du numérateur et du dénominateur est $d = 2$. Nous présumons qu'il en est de même pour les sections. Pour reconstruire par l'approximation de Padé, une fraction rationnelle dont le degré maximum du numérateur et du dénominateur est d , il faut disposer des $2d + 1$ premiers coefficients du développement. Cependant nous utilisons les sections et pour avoir $2d + 1$ coefficients de la section $T_{b,r}f(x)$, il faut aller jusqu'au coefficient d'indice $b(2d + 1) - 1$ dans le cas pire ($r = b - 1$). Nous développons donc $f(x)$ avec un terme d'erreur $O(x^{b(2d+1)})$, soit $O(x^{15})$ pour l'exemple. Nous développons donc $f(x)$ avec un terme d'erreur en $O(x^{15})$,

$$f(x) = 1 + 2x + 3x^2 + 5x^3 + 8x^4 + 13x^5 + 21x^6 + 34x^7 + 55x^8 + 89x^9 + 144x^{10} \\ + 233x^{11} + 377x^{12} + 610x^{13} + 987x^{14} + O(x^{15})$$

Nous extrayons les développements des sections avec un terme d'erreur en $O(x^5)$,

$$T_{3,0}f(x) = 1 + 5x + 21x^2 + 89x^3 + 377x^4 + O(x^5), \\ T_{3,1}f(x) = 2 + 8x + 34x^2 + 144x^3 + 610x^4 + O(x^5), \\ T_{3,2}f(x) = 3 + 13x + 55x^2 + 233x^3 + 987x^4 + O(x^5).$$

À ce point, nous calculons les approximants de Padé qui nous fournissent les sections, concrètement en utilisant notre système de calcul formel préféré,

$$T_{3,0}f(x) = \frac{1+x}{1-4x-x^2}, \\ T_{3,1}f(x) = \frac{2}{1-4x-x^2}, \\ T_{3,2}f(x) = \frac{3+x}{1-4x-x^2}.$$

Nous vérifions que les sections permettent bien de retrouver la fraction rationnelle.

$$\frac{x^3+1}{1-4x^3-x^6} + 2\frac{x}{1-4x^3-x^6} + \frac{x^2(3+x^3)}{1-4x^3-x^6} = \frac{1+x}{1-x-x^2}.$$

RÉPONSE 2 — La relation de récurrence se traduit, à l'aide de la formule (30), page 11, pour ce qui concerne la fonction plafond, en

$$u(x) = \sum_{n \geq 2} u_{\lfloor \frac{n}{2} \rfloor} x^n + \sum_{n \geq 2} u_{\lfloor \frac{n+1}{2} \rfloor} x^n + \frac{x^2}{1-x}.$$

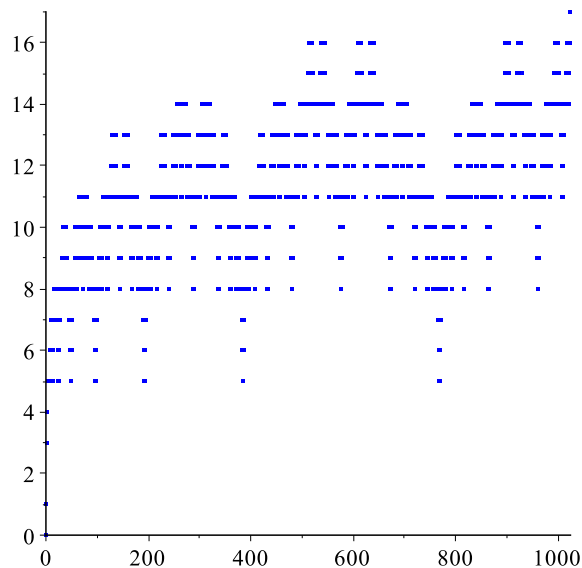


FIGURE 1. Le graphe d'une suite rationnelle en base 2 (exercice 3).

Ensuite la formule (31) fournit, en tenant compte de $u_0 = u_1 = 0$,

$$u(x) = (1+x)u(x^2) + x^{-1}(1+x)u(x^2) + \frac{x^2}{1-x},$$

soit

$$xu(x) = (1+x)^2u(x^2) + \frac{x^3}{1-x}.$$

RÉPONSE 3 — 1. La suite est rationnelle en base 2. En effet sa série génératrice vérifie l'équation de Mahler de base 2

$$(1+x^3)u(x) = (1+x)u(x^2) + x(1+x)$$

soit

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

Le coefficient $1-x+x^2$ a pour racine les racines primitives sixièmes de l'unité et 6 est pair, donc la série est 2-rationnelle. Même si les conditions initiales n'avaient pas permis la simplification par $1+x$, le résultat aurait perduré car -1 est la racine primitive d'ordre 2.

2. Il en est donc de même de sa suite sommatoire (s_n) , puisque la série génératrice de celle-ci s'obtient comme le produit

$$s(x) = \frac{1}{1-x}u(x)$$

de deux séries rationnelles en base 2. La figure 1 montre le graphe de la suite (s_n) .

RÉPONSE 4 — La suite $(\delta_n)_{n \geq 0}$ commence par les termes 0, 1, 2, 2, 4, 3... Nous préférons travailler avec les séries et nous considérons

$$\delta(x) = \sum_{n \geq 0} \delta_n x^n, \quad \lambda(x) = \sum_{n \geq 1} \lfloor \log_2 n \rfloor x^n.$$

Les relations fournies se traduisent en

$$\begin{aligned} T_{2,0}\delta(x) &= \delta(x) + \lambda(x) + \frac{x}{1-x}, & T_{2,1}\delta(x) &= \delta(x) + \frac{1}{1-x}, \\ T_{2,0}\lambda(x) &= \lambda(x) + \frac{x}{1-x}, & T_{2,1}\lambda(x) &= \lambda(x) + \frac{x}{1-x}, \\ T_{2,0}\frac{1}{1-x} &= \frac{1}{1-x}, & T_{2,1}\frac{1}{1-x} &= \frac{1}{1-x}, \\ T_{2,0}\frac{x}{1-x} &= \frac{x}{1-x}, & T_{2,1}\frac{x}{1-x} &= \frac{1}{1-x}. \end{aligned}$$

Elles montrent que la série $\delta(x)$ est 2-rationnelle et vit dans l'espace engendré par les séries $\delta(x)$, $\lambda(x)$, $1/(1-x)$, $x/(1-x)$. En prenant dans chaque suite, les coefficients d'indices 0, 1, 3, 4 nous montrons que la famille est libre. Nous arrivons à la représentation linéaire

$$L = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}, \quad A_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

La série $\delta(x)$ est 2-rationnelle. Il en est donc de même de $u(x)$ qui est le produit de la précédente par la fraction rationnelle $1/(1-x)$, qui est 2-rationnelle d'après la proposition 6, page 24.

RÉPONSE 5 — Nous reprenons le raisonnement de l'exemple 21 avec des notations similaires. La matrice $A(x)$ est

$$A(x) = \begin{bmatrix} 1 & 1-x \\ x & 1+2x \end{bmatrix}.$$

Les familles de vecteurs colonnes $(A(x)C)$, puis $(A(x^2)C, A(x^2)A(x)C)$, etc, donne les matrices

$$\begin{aligned} \Gamma_0(x) &= \begin{bmatrix} 1 \\ x \end{bmatrix}, & \Gamma_1(x) &= \begin{bmatrix} 1 & -x^3 + x + 1 \\ x^2 & 2x^3 + x^2 + x \end{bmatrix}, \\ \Gamma_2(x) &= \begin{bmatrix} 1 & -x^6 + x^2 + 1 & -2x^7 - x^6 - x^5 + x^3 + x^2 + 2x + 1 \\ x^4 & 2x^6 + x^4 + x^2 & 3x^7 + 2x^6 + 3x^5 + x^4 + 2x^3 + x^2 + x \end{bmatrix}. \end{aligned}$$

Cette dernière ne peut pas être de rang supérieur à 2. Nous trouvons une relation de liaison entre les colonnes exprimée par le vecteur

$$K(x) = \begin{bmatrix} 1 + x^2 + x^4 \\ -(1 + x + 2x^2) \\ x \end{bmatrix}$$

et cela nous donne l'équation de Mahler

$$xu(x) - (1 + x + 2x^2)u(x^2) + (1 + x^2 + x^4)u(x^4) = 0.$$

Celle-ci n'est pas l'équation minimale de la série génératrice (comme on le voit à l'exercice suivant). En effet l'opérateur se factorise en

$$x - (1 + x + 2x^2)M + (1 + x^2 + x^4)M^2 = (1 - M)(x - (1 + x + x^2)M).$$

Autrement dit, même si la représentation linéaire est réduite, ce qui est le cas ici, le procédé de calcul ne garantit pas que l'équation de Mahler obtenue soit minimale.

RÉPONSE 6 — La forme de la série génératrice donne tout de suite l'équation de Mahler $xu(x) = (1 + x + x^2)u(x^2)$. Nous la récrivons

$$xu(x) = \frac{1 + x + x^2}{1 + x} ((1 + x)u(x^2)),$$

soit

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

et nous appliquons la formule (31), page 11. Ici le paramètre s est négatif pour chaque emploi de la formule et il n'y a pas de terme correctif. Nous obtenons

$$(x + x^2)u(x) = \sum_{n \geq 0} (u_{\lfloor \frac{n}{2} \rfloor} + u_{\lfloor \frac{n-1}{2} \rfloor} + u_{\lfloor \frac{n-2}{2} \rfloor}) x^n$$

et la récurrence (nous prenons le coefficient de x^m avec $m = n + 1$)

$$u_n = -u_{n-1} + (u_{\lfloor \frac{n+1}{2} \rfloor} + u_{\lfloor \frac{n}{2} \rfloor} + u_{\lfloor \frac{n-1}{2} \rfloor}).$$

Nous pourrions la récrire

$$u_n = -u_{n-1} + (u_{\lceil \frac{n}{2} \rceil} + u_{\lceil \frac{n-1}{2} \rceil} + u_{\lfloor \frac{n-1}{2} \rfloor}).$$

Avec les conditions initiales $u_0 = 0$, $u_1 = 1$, ces récurrences définissent la suite.

RÉPONSE 7 — Nous regardons les développements binaires des entiers

$$n_r = \frac{4 \cdot 2^r - (-1)^r}{3}.$$

En appliquant la formule

$$2^k - (-1)^k = (2 - (-1))(2^{k-1} - 2^{k-2} + 2^{k-3} - \dots + (-1)^{k-1}) = 3(2^{k-2} + 2^{k-4} + \dots)$$

avec $k = r + 2$, nous voyons que cette écriture binaire dépend de la parité de r , plus précisément nous trouvons

$$n_{2s} = ((10)^s 1)_2, \quad n_{2s+1} = ((10)^s 11)_2.$$

La représentation linéaire donne donc

$$m_{2s} = L(A_1 A_0)^s A_1 C, \quad m_{2s+1} = L(A_1 A_0)^s A_1^2 C.$$

Nous avons affaire à deux suites rationnelles entrelacées, c'est-à-dire à une suite rationnelle. La matrice

$$A_1 A_0 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

a pour polynôme caractéristique $\chi(x) = x^2 - 3x + 1$. Nous en tirons

$$m_{2s} = \lambda_0 \left(\frac{3 + \sqrt{5}}{2} \right)^s + \bar{\lambda}_0 \left(\frac{3 - \sqrt{5}}{2} \right)^s, \quad m_{2s+1} = \lambda_1 \left(\frac{3 + \sqrt{5}}{2} \right)^s + \bar{\lambda}_1 \left(\frac{3 - \sqrt{5}}{2} \right)^s.$$

Pour trouver les coefficients λ , nous avons besoin des premières valeurs que nous calculons

$$m_0 = 1, \quad m_2 = 2, \quad m_3 = 3, \quad m_4 = 5,$$

ce qui n'est pas sans nous mettre la puce à l'oreille (de lapin, bien sûr). Nous arrivons à

$$m_{2s} = \frac{1}{\sqrt{5}} \left(\frac{3 + \sqrt{5}}{2} \right)^{s+1} - \frac{1}{\sqrt{5}} \left(\frac{3 - \sqrt{5}}{2} \right)^{s+1},$$

$$m_{2s+1} = \frac{2 + \sqrt{5}}{\sqrt{5}} \left(\frac{3 + \sqrt{5}}{2} \right)^s + \frac{-2 + \sqrt{5}}{\sqrt{5}} \left(\frac{3 - \sqrt{5}}{2} \right)^s.$$

La dernière expression n'est pas bien plaisante. Alerté par notre vaste culture nous jetons un œil sur les puissances du nombre d'ordre d'or $\phi = (1 + \sqrt{5})/2$,

$$\phi^2 = \frac{3 + \sqrt{5}}{2}, \quad \phi^3 = 2 + \sqrt{5}$$

et nous sortons du terrier. Bien sûr les formules s'écrivent

$$m_{2s} = \frac{\phi^{2s+2} - \bar{\phi}^{2s+2}}{\sqrt{5}}, \quad m_{2s+1} = \frac{\phi^{2s+3} - \bar{\phi}^{2s+3}}{\sqrt{5}}$$

et m_r n'est rien d'autre que le nombre de Fibonacci F_{r+2} . De manière équivalente nous aurions pu remarquer l'égalité matricielle

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Une fois de plus nous sommes passés d'une suite rationnelle dans une base de numération à une suite rationnelle au sens classique en la testant sur des entiers qui forment eux-mêmes une suite rationnelle parce que leur écriture dans la base est essentiellement la puissance d'un motif. La puissance des mots!

RÉPONSE 8 — Nous voyons tout de suite la récurrence

$$\chi_{3n} = \chi_n, \quad \chi_{3n+1} = 0, \quad \chi_{3n+2} = \chi_n,$$

d'où pour la série génératrice $\chi(x)$ l'équation de Mahler $\chi(x) = 1 \times c(x^3) + x \times 0 + x^2 \times c(x^3)$. Si nous regardons cette série formelle $\chi(x)$ comme un élément de $\mathbb{F}_3[x]$, l'équation de Mahler $\chi(x) = (1 + x^2)\chi(x^3)$ se récrit

$$\chi(x) = (1 + x^2)\chi(x)^3.$$

Comme $\chi(x)$ n'est pas la série nulle, elle vérifie $1 = (1 + x^2)\chi(x)^2$. Ceci fournit l'expression

$$\chi(x) = \frac{1}{\sqrt{1+x^2}} = 1 + x^2 + x^6 + x^8 + x^{18} + x^{20} + x^{24} + x^{26} + \dots \pmod{3}.$$

Mais nous connaissons le développement

$$\frac{1}{1-t} = \sum_{n=0}^{+\infty} \frac{1}{2^{2n}} \binom{2n}{n} t^n.$$

Il nous donne

$$\frac{1}{\sqrt{1+x^2}} = \sum_{n=0}^{+\infty} \frac{(-1)^n}{2^{2n}} \binom{2n}{n} x^{2n}.$$

Modulo 3, l'entier 2 vaut -1 et il vient

$$\frac{1}{\sqrt{1+x^2}} = \sum_{n=0}^{+\infty} (-1)^n \binom{2n}{n} x^{2n}.$$

Nous concluons

$$\chi_{2n} \equiv (-1)^n \binom{2n}{n} \pmod{3}, \quad \chi_{2n+1} \equiv 0 \pmod{3}.$$

RÉPONSE 9 — Pour k entier naturel non nul, il y a entre les entiers 3^k et $3^{k+1} - 1$ un nombre d'éléments de cette suite (c_n) égal à 2^k , car le premier chiffre (de poids fort) est nécessairement 2 et les k autres chiffres sont 0 ou 2. La formule est encore valable pour le cas particulier $k = 0$. Supposons que nous ayons fabriqué la suite finie $(c_n)_{0 \leq n < 2^k - 1}$, c'est-à-dire la suite des c_n qui sont entre 0 et 3^k (ce dernier exclus). Nous faisons précéder chacun des développements triadiques de ces 2^k entiers d'un chiffre 2 et nous obtenons les c_n entre 3^k et 3^{k+1} (ce dernier exclus). Nous voyons ainsi la formule

$$c_{2^k+s} = 2 \cdot 3^k + c_s, \quad 0 \leq s < 2^k.$$

Elle donne pour un entier n qui s'écrit

$$n = 2^{k_1} + 2^{k_2} + \dots + 2^{k_\ell}, \quad \text{avec } k_1 > k_2 > \dots > k_\ell \geq 0$$

la valeur

$$c_n = 2 \cdot (3^{k_1} + 3^{k_2} + \dots + 3^{k_\ell}).$$

Comme nous voulons montrer que la suite (c_n) est 2-rationnelle, nous regardons les expressions c_{2n} et c_{2n+1} . À l'aide du résultat précédent, nous trouvons facilement

$$c_{2n} = 3c_n, \quad c_{2n+1} = 3c_n + 2.$$

De cette formule nous tirons, en passant aux séries génératrices,

$$c(x) = 3c(x^2) + x \left(3c(x^2) + \frac{2}{1-x^2} \right).$$

Cette équation de Mahler s'écrit $Lu = v$, avec

$$L = 1 - 3(1+x)M, \quad v(x) = \frac{2x}{1-x^2}.$$

La fraction rationnelle v est annulée par l'opérateur

$$L' = x - (1+x^2)M.$$

Par multiplication à gauche de L par L' , nous obtenons le nouvel opérateur

$$L'L = x - (1 + 3x + 4x^2)M + (3 + 6x^2 + 3x^4)M^2$$

et la nouvelle équation, homogène cette fois,

$$xc(x) - (1 + 3x + 4x^2)c(x^2) + 3(1 + x^2)^2c(x^4) = 0.$$

RÉPONSE 10 — Le rayon spectral vaut 1. En effet les quatre matrices ont une norme égale à 1 pour la norme subordonnée $\|\cdot\|_1$, qui est le maximum des sommes par colonnes des valeurs absolues des coefficients. Il en résulte que tous les produits de longueur un entier ℓ ont une norme inférieure ou égale à 1, d'où l'inégalité $\hat{\rho}(A) \leq 1$. Cependant les quatre matrices admettent la valeur propre 1. Prenons par exemple A_0 et son vecteur propre E_1 associé à la valeur propre 1. De $1 = \|E_1\|_1 = \|A_0^\ell E_1\|_1 \leq \|A_0^\ell\|_1 \|E_1\|_1 \leq \hat{\rho}_\ell(A)^\ell$, valable pour tout entier ℓ , nous tirons $\hat{\rho}(A) \geq 1$ et finalement l'égalité $\hat{\rho}(A) = 1$.

RÉPONSE 11 — Nous cherchons une équation de dilatation dans une version scalaire avec conditions aux limites (page 49), naturellement $C(x) = 0$ pour $x \leq 0$, $C(x) = 1$ pour $x \geq 1$. La base 3 s'impose. Supposons d'abord $0 \leq x \leq 1/3$. Nous voyons bien que la portion de graphe entre les abscisses 0 et $1/3$ est similaire au graphe entre 0 et 1, mais avec une variation verticale de $1/2$ et non de 1. Ceci nous fait introduire un terme $C(3x)/2$. La partie entre les abscisses $2/3$ et 1 ayant la même structure, nous introduisons aussi un terme $C(3x - 2)/2$. Nous arrivons ainsi à

$$C(x) = \frac{1}{2}C(3x) + \frac{1}{2}C(3x - 2).$$

Vérifions brièvement que nous sommes dans le vrai. Pour $0 \leq x \leq 1/3$, le terme en $C(3x - 2)$ est nul à cause de l'inégalité $3x - 2 \leq -1 < 0$. Pour $2/3 \leq x \leq 1$, le terme $C(3x)/2$ vaut $1/2$, à cause de l'inégalité $3x \geq 2$, et ceci fournit la valeur $1/2$ qui décale adéquatement le graphe vers le haut. Enfin pour $1/3 \leq x \leq 2/3$, le premier terme vaut ici encore $1/2$ et le second vaut 0, ce qui donne bien la valeur $1/2$ de C sur l'intervalle. D'après le lemme 6, avec $a_0 = a_2 = 1/2$, $a_1 = 0$ et $\hat{\rho}(a) = 1/2$, $\rho = 1$, la fonction de Cantor est höldérienne d'exposant $\log_3 2 - \varepsilon$ avec $\varepsilon > 0$. Il est connu que cette fonction est dérivable hors de l'ensemble de Cantor (avec une dérivée nulle), ce qui fait qu'en les points du complémentaire de l'ensemble de Cantor elle admet 1 comme exposant de Hölder local.

RÉPONSE 12 — Les mêmes arguments qu'à l'exercice 10 montrent que le rayon spectral vaut $\hat{\rho}(A) = 1$. La matrice

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

a comme polynôme caractéristique $\chi = z^2 - 2$ et comme valeurs propres $\pm\sqrt{2}$. Nous attendons donc un développement asymptotique pour la suite sommatoire de la forme

$$\sum_{0 \leq n \leq N} =_{N \rightarrow \infty} N^{1/2} (\varphi_1(\log_2 N) + e^{i\pi \log_2 N} \varphi_2(\log_2 N)) + O(N^\varepsilon),$$

avec $\varepsilon > 0$ et des fonctions φ_1, φ_2 qui sont 1-périodiques et höldériennes. Pour éviter la présence du terme en $\exp(i\pi \log_2 N)$, cet exemple est généralement traité

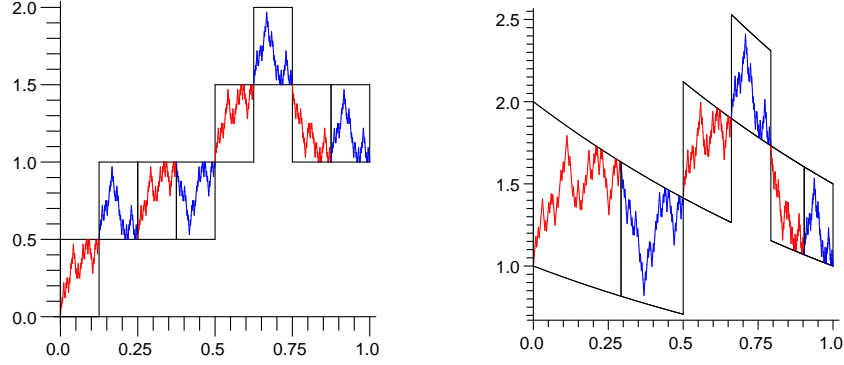


FIGURE 2. La solution de l'équation de dilatation en base 4 et la fonction périodique pour la suite de Rudin-Shapiro.

en base 4. Cela revient à utiliser une représentation linéaire de matrices A_0^2 , A_0A_1 , A_1A_0 , A_1^2 et donc la matrice Q^2 . Cette approche conduit à un développement équivalent au précédent

$$\sum_{n \leq N} u_n \underset{N \rightarrow +\infty}{=} \sqrt{N} \varphi(\log_4 N) + O(1),$$

réécrit ici avec une amélioration sur le terme d'erreur que nous n'avons pas évoquée dans ce cours [37, Lemme 4]. Le graphe de la fonction f solution d'une équation de dilatation en base 4 et le graphe de la fonction φ , définie par $\varphi(t) = 2^{1-\{t\}} f(4^{\{t\}-1})$, sont représentés en figure 2, toutes les deux dessinées par l'algorithme en cascade. La première (à gauche) montre une autosimilarité et des symétries qui sont parfaitement masquées dans la seconde (à droite).

RÉPONSE 13 — Supposons que l'entier n soit dans l'intervalle $[2^k, 2^{k+1}[$, ce qui fait que la longueur de son écriture binaire est $k + 1$. La récurrence donne

$$u_n = n + 3u_{\lfloor \frac{n}{2} \rfloor} = n + 3 \left\lfloor \frac{n}{2} \right\rfloor + 9 \left\lfloor \frac{n}{4} \right\rfloor + \cdots + 3^k \left\lfloor \frac{n}{2^k} \right\rfloor + u_0.$$

En tenant compte de l'écriture binaire de n

$$n = (n_k n_{k-1} \dots n_1 n_0)_2 = 2^k n_k + 2^{k-1} n_{k-1} + \cdots + 2n_1 + n_0,$$

cette expression de u_n donne

$$\begin{aligned} u_n &= 2^k \left(1 + \frac{3}{2} + \frac{9}{4} + \cdots + \frac{3^k}{2^k} \right) n_k \\ &\quad + 2^{k-1} \left(1 + \frac{3}{2} + \frac{9}{4} + \cdots + \frac{3^{k-1}}{2^{k-1}} \right) n_{k-1} \\ &\quad + \cdots + 2 \left(1 + \frac{3}{2} \right) n_1 + n_0, \end{aligned}$$

soit

$$\begin{aligned} u_n &= 2^k \frac{(3/2)^{k+1} - 1}{3/2 - 1} n_k + 2^{k-1} \frac{(3/2)^k - 1}{3/2 - 1} n_{k-1} + \cdots + 2 \frac{9/4 - 1}{3/2 - 1} n_1 + \frac{3/2 - 1}{3/2 - 1} n_0 \\ &= (3^{k+1} n_k + 3^k n_{k-1} + \cdots + 3^2 n_1 + 3 n_0) - (2^{k+1} n_k + 2^k n_k + \cdots + 4 n_1 + 2 n_0) \\ &= 3 (3^k n_k + 3^{k-1} n_{k-1} + \cdots + 3 n_1 + n_0) - 2n. \end{aligned}$$

Nous constatons que les chiffres binaires de n sont utilisés comme chiffres triadiques. Nous arrivons à

$$u_n = 3^{k+1} \left(\frac{n_k}{3} + \frac{n_{k-1}}{9} + \cdots + \frac{n_0}{3^{k+1}} \right) - 2n,$$

ou encore en utilisant $k = \lfloor \log_2 n \rfloor$

$$u_n = \frac{3^{k+2}}{2} C^* \left(\frac{n}{2^{k+1}} \right) - 2n = \frac{9}{2} 3^{\lfloor \log_2 n \rfloor} C^*(2^{\{\log_2 n\}-1}),$$

soit

$$u_n = n^{\log_2 3} \varphi(\log_2 n), \quad \varphi(t) = \frac{9}{2} 3^{\{t\}} C^*(2^{\{t\}-1}).$$

L'écriture avec les accolades $\{ \}$ désigne la partie fractionnaire, $\{t\} = t - \lfloor t \rfloor$. Il y a aux puissances de 2 un effet de compensation entre le saut de la partie fractionnaire du logarithme et le saut de la fonction C^* . Si nous avons une écriture sous la forme d'une fonction puissance par une fonction périodique, la fonction φ n'est cependant pas continue, ce qui signifie que le lemme 6 ne s'applique pas. D'ailleurs, nous avons une représentation linéaire utilisant les deux suites $(u_n - u_{n-1})$ et 1 qui s'écrit

$$A_0 = \begin{pmatrix} 3 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

Son rayon spectral est $\hat{\rho}(A) = 3$ et la valeur propre dominante est $\rho = 3$.

EXERCICE 15 — Nous voyons rapidement

$$u_{2n} = 2^{s_2(2n-1)} = 2^{s_2(2(n-1)+1)} = 2^{s_2(n-1)+1} = 2u_n$$

et la formule $u_{2n} = 2u_n$ est valable même si n est nul. Pour les entiers impairs, nous ne voyons pas de dépendance entre u_{2n+1} et u_n . Nous introduisons donc

$$v_n = u_{2n+1} = 2^{s_2(2n)} = 2^{s_2(n)}.$$

Du coup, nous regardons les parties paire et impaire de (v_n) , ce qui donne

$$v_{2n} = v_n, \quad v_{2n+1} = 2v_n.$$

Les sections de (u_n) et (v_n) vivent dans l'espace engendré par (u_n) et (v_n) . Ceci prouve la 2-rationalité de la suite (u_n) . De plus le calcul nous fournit une représentation linéaire

$$L = \begin{bmatrix} 0 & 1 \end{bmatrix}, \quad A_0 = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Avec la proposition 13, page 43, nous trouvons tout de suite que le rayon spectral est $\hat{\rho}(A) = 2$. Quant à la matrice

$$Q = \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}$$

elle se diagonalise en la matrice Λ par la matrice de passage P avec

$$\Lambda = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}, \quad P = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}.$$

Si nous appelons V_3 et V_2 les deux vecteurs propres qui forment les colonnes de P , nous avons $C = V_3 + V_2$ et seule la composante V_3 nous est utile. L'équation de dilatation relative à la valeur propre 3 et au vecteur propre V_3 s'écrit

$$F(x) = \frac{1}{3}A_0F(2x) + \frac{1}{3}A_1F(2x-1)$$

avec les conditions aux limites

$$F(x) = 0 \quad \text{pour } x \leq 0, \quad F(x) = V_3 \quad \text{pour } x \geq 1.$$

Plus explicitement si les composantes de F sont z et f , le système s'écrit

$$\begin{aligned} z(x) &= \frac{2}{3}z(2x), \\ f(x) &= \frac{1}{3}f(2x) + \frac{1}{3}z(2x-1) + \frac{2}{3}f(2x-1) \end{aligned}$$

avec

$$z(x) = f(x) = 0 \quad \text{pour } x \leq 0, \quad z(x) = 0, \quad f(x) = 1 \quad \text{pour } x \geq 1.$$

Nous savons que ce système possède exactement une solution et nous voyons bien que $z = 0$ convient, donc z est la fonction nulle. Il nous reste donc l'équation scalaire

$$f(x) = \frac{1}{3}f(2x) + \frac{2}{3}f(2x-1)$$

avec les conditions aux limites $f(x) = 0$ pour $x \leq 0$, $f(x) = 1$ pour $x \geq 1$, qui définit parfaitement la fonction f . Nous appliquons les formules (60) et (61), page 50, et nous obtenons

$$s_N \underset{N \rightarrow \infty}{=} N^{\log_2 3} 3^{1-\{t\}} f(2^{\{t\}-1}) + O(N^{1+\varepsilon})$$

avec $\varepsilon > 0$. Il est possible de montrer que le terme d'erreur est nul.

Bibliographie

- [1] Jounaïdi Abdeljaoued et Henri Lombardi. *Méthodes matricielles : Introduction à la Complexité Algébrique*. Mathématiques & applications. Springer, Paris, Berlin, Heidelberg, 2004.
- [2] Boris Adamczewski et Tanguy Rivoal. Irrationality measures for some automatic real numbers. *Math. Proc. Cambridge Philos. Soc.*, 147(3) :659–678, 2009.
- [3] Alfred V. Aho, John E. Hopcroft et Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, première édition, 1974.
- [4] Jean-Paul Allouche et Jeffrey Shallit. The ring of k -regular sequences. *Theoret. Comput. Sci.*, 98(2) :163–197, 1992.
- [5] Jean-Paul Allouche et Jeffrey Shallit. The ubiquitous Prouhet-Thue-Morse sequence. Dans *Sequences and their applications (Singapore, 1998)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pages 1–16. Springer, London, 1999.
- [6] Jean-Paul Allouche et Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.
- [7] Guy Barat, Valérie Berthé, Pierre Liardet et Jörg Thuswaldner. Dynamical directions in numeration. *Annales de l'institut Fourier*, 56(7) :1987–2092, 2006.
- [8] Jason P. Bell et Michael Coons. Transcendence tests for Mahler functions. Récupéré le 6 mars 2016 de <http://arxiv.org/abs/1511.07530>, 2015.
- [9] Jon Louis Bentley, Dorothea Haken et James B. Saxe. A general method for solving divide-and-conquer recurrences. *SIGACT News*, 12(3) :36–44, September 1980.
- [10] Jean Berstel et Christophe Reutenauer. *Noncommutative Rational Series with Applications*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2011.
- [11] Jean Berstel et Christophe Reutenauer. *Les séries rationnelles et leurs langages*. Masson, 1984.
- [12] Jean Berstel et Christophe Reutenauer. *Rational series and their languages*, volume 12 de *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin, 1988.
- [13] Patrick Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics : Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, troisième édition, 1995.
- [14] Vincent D. Blondel, Julien Cassaigne et Raphaël M. Jungers. On the number of α -power-free binary words for $2 < \alpha \leq 7/3$. *Theoret. Comput. Sci.*, 410(30-32) :2823–2833, 2009.
- [15] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy et Éric Schost. Algorithmes Efficaces en Calcul Formel. Récupéré le 6 mars 2016 de <http://specfun.inria.fr/chyzak/mpri/poly.pdf>, 2016.
- [16] John Brillhart and Leonard Carlitz. Note on the Shapiro polynomials. *Proc. Amer. Math. Soc.*, 25 :114–118, 1970.
- [17] John Brillhart, Paul Erdős et Patrick Morton. On sums of Rudin-Shapiro coefficients. II. *Pacific J. Math.*, 107(1) :39–69, 1983.
- [18] John Brillhart et Patrick Morton. Über Summen von Rudin-Shapiroschen Koeffizienten. *Illinois J. Math.*, 22(1) :126–148, 1978.
- [19] John Brillhart et Patrick Morton. A case study in mathematical research : The Golay-Rudin-Shapiro sequence. *American Mathematical Monthly*, 103(10) :854–869, 1996.

- [20] Julien Cassaigne. Counting overlap-free binary words. In *STACS 93 (Würzburg, 1993)*, volume 665 de *Lecture Notes in Comput. Sci.*, pages 216–225. Springer, Berlin, 1993.
- [21] Louis H.Y. Chen, Hsien-Kuei Hwang et Vytas Zacharovas. Distribution of the sum-of-digits function of random integers : a survey. *Probabilty Surveys*, 11 :177–236, 2014.
- [22] Gilles Christol. Ensembles presque périodiques k -reconnaissables. *Theoret. Comput. Sci.*, 9(1) :141–145, 1979.
- [23] Gilles Christol, Teturo Kamae, Michel Mendès France et Gérard Rauzy. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France*, 108(4) :401–419, 1980.
- [24] Frédéric Chyzak, Thomas Dreyfus, Philippe Dumas et Marc Mezzaroba. Computing solutions of linear Mahler equations. En préparation.
- [25] Jean Coquet. A summation formula related to the binary digits. *Invent. Math.*, 73(1) :107–115, 1983.
- [26] Thomas H. Cormen, Charles E. Leiserson et Ronald L. Rivest. *Introduction to algorithms*. The MIT Electrical Engineering and Computer Science Series. MIT Press, Cambridge, MA, 1990.
- [27] Ingrid Daubechies et Jeffrey C. Lagarias. Two-scale difference equations. I. Existence and global regularity of solutions. *SIAM J. Math. Anal.*, 22(5) :1388–1410, 1991.
- [28] Ingrid Daubechies et Jeffrey C. Lagarias. Two-scale difference equations. II. Local regularity, infinite products of matrices and fractals. *SIAM J. Math. Anal.*, 23(4) :1031–1079, 1992.
- [29] N. G. De Bruijn. On Mahler’s partition problem. *Indagationes Mathematicae*, 10 :210–220, 1948. Réimpression de Koninklijke Nederlandsche Akademie van Wetenschappen, Ser. A.
- [30] James W. Demmel. *Applied Numerical Linear Algebra*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1997.
- [31] David L. Donoho et Thomas P.-Y. Yu. Deslariers-Dubuc : Ten years after. Dans S. Dubuc et G. Deslauriers (dir.), *Spline Functions and the Theory of Wavelets*, pages 355–369, 1999. CRM (Centre de Recherches Mathématiques, Université de Montréal) Proceedings & Lectures Notes, Volume 18.
- [32] Thomas Dreyfus, Charlotte Hardouin et Julien Roques. Hypertranscendance of solutions of Mahler equations. *J. Eur. Math. Soc.*, 2015. À paraître.
- [33] Michael Drmota et Peter J. Grabner. Analysis of digital functions and applications. Dans *Combinatorics, automata and number theory*, volume 135 de *Encyclopedia Math. Appl.*, pages 452–504. Cambridge Univ. Press, Cambridge, 2010.
- [34] Michael Drmota, Gerhard Larcher et Friedrich Pillichshammer. Precise distribution properties of the van der Corput sequence and related sequences. *Manuscripta Math.*, 118(1) :11–41, 2005.
- [35] Serge Dubuc. Interpolation through an iterative scheme. *Journal of Mathematical Analysis and Applications*, 114 :185–204, 1986.
- [36] Philippe Dumas. *Réurrences mahlériennes, suites automatiques, études asymptotiques*. Thèse de doctorat, Université de Bordeaux I, Talence, 1993, Rocquencourt, 1993. Récupéré le 6 mars 2016 de <http://tel.archives-ouvertes.fr/docs/00/61/46/60/PDF/these.pdf>.
- [37] Philippe Dumas. Joint spectral radius, dilation equations et asymptotic behavior of radix-rational sequences. *Linear Algebra and its Applications*, 438(5) :2107 – 2126, 2013.
- [38] N. J. Fine. Binomial coefficients modulo a prime. *Amer. Math. Monthly*, 54 :589–592, 1947.
- [39] N. Pytheas Fogg. *Substitutions in dynamics, arithmetics and combinatorics*, volume 1794 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002. Edited by V. Berthé, S. Ferenczi, C. Mauduit et A. Siegel.
- [40] Marcel J. E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *Journal of the Optical Society of America*, 41(7) :468–472, Juillet 1951.
- [41] R.L. Graham, D.E. Knuth et O. Patashnik. *Concrete Mathematics*. Addison Wesley, 1989.
- [42] Peter Henrici. *Applied and computational complex analysis. Volume 2. , Special functions - Integral transforms - Asymptotics - Continued fractions*. Pure and applied mathematics. John Wiley and Sons, New-York, London, Sydney, 1977.

- [43] The OEIS Foundation Inc. Stern's diatomic series. Récupéré le 6 mars 2016 de <https://oeis.org/A002487>.
- [44] Raphaël Jungers. *The joint spectral radius*, volume 385 of *Lecture Notes in Control and Information Sciences*. Springer-Verlag, Berlin, 2009. Theory and applications.
- [45] Tomasz Kisiekewski. Criteria for regularity of Mahler power series and Becker's conjecture, 2015. Récupéré le 6 mars 2016 de <http://arxiv.org/abs/1512.04326>.
- [46] Donald E. Knuth. *The art of computer programming. Volume 3*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1973. Sorting and searching, Addison-Wesley Series in Computer Science and Information Processing.
- [47] Benoit B. Mandelbrot and Rudolf H. Riedi. Inverse measures, the inversion formula, and discontinuous multifractals. *Adv. in Appl. Math.*, 18(1) :50–58, 1997.
- [48] Charles A. Micchelli et Hartmut Prautzsch. Uniform refinement of curves. *Linear Algebra and its Applications*, 114/115 :841–870, 1989.
- [49] Donald J. Newman. On the number of binary digits in a multiple of three. *Proc. Amer. Math. Soc.*, 21 :719–721, 1969.
- [50] Sam Northshield. Stern's diatomic sequence 0, 1, 1, 2, 1, 3, 2, 3, 1, 4, ... *The American Mathematical Monthly*, 117(7) :581–598, 2010.
- [51] Oystein Ore. Theory of Non-Commutative Polynomials. *Annals of Mathematics*, 34 :480–508, 1933.
- [52] Johan Oudinet. *Approches combinatoires pour le test statistique à grande échelle*. Thèse de doctorat, Université Paris-Sud XI, 2010.
- [53] Johan Oudinet, Alain Denise et Marie-Claude Gaudel. A new dichotomic algorithm for the uniform random generation of words in regular languages. Dans *Conference on random and exhaustive generation of combinatorial objects (GASCom)*, Montreal, Canada, September 2010. 10 pages.
- [54] Franco P. Preparata et Michael Ian Shamos. *Computational geometry An introduction*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1985.
- [55] William H. Press, Saul A. Teukolsky, William T. Vetterling et Brian P. Flannery. *Numerical Recipes 3rd Edition : The Art of Scientific Computing*. Cambridge University Press, New York, NY, USA, troisième édition, 2007.
- [56] Michel Rigo. Numeration systems : a link between number theory and formal language theory. Dans Yuan Gao, Hanlin Lu, Shinnosuke Seki et Sheng Yu (dir.) *Developments in Language Theory*, volume 6224 de *Lecture Notes in Computer Science*, pages 33–53. Springer, 2012. 14th International Conference, DLT 2010, London, ON, Canada, August 17-20, 2010. Actes de colloque.
- [57] Gian-Carlo Rota et Gilbert Strang. A note on the joint spectral radius. *Nederl. Akad. Wetensch. Proc. Ser. A 63 = Indag. Math.*, 22 :379–381, 1960.
- [58] Walter Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10 :855–859, 1959.
- [59] Bruno Salvy. Conversation privée, 2013.
- [60] Harold S. Shapiro. Extremal problems for polynomials and power series. Thèse de maîtrise, Massachusetts Institute of Technology, 1951.
- [61] Gilbert Strang. Wavelets and dilation equations : A brief introduction. *SIAM Review*, 31(4) :614–627, 1989.
- [62] Jacques Theys. *Joint Spectral Radius : theory and applications*. Thèse de doctorat, Université catholique de Louvain, 2005.
- [63] Chee Yap. A Real Elementary Approach to the Master Recurrence and Generalizations. Dans *Theory and Applications of Models of Computation - 8th Annual Conference, TAMC 2011, Tokyo, Japan, May 23-25, 2011*. Actes du colloque, pages 14–26, 2011.

Index

- algorithme
 - en cascade, 51
 - dichopile, 21, 22
 - de Karatsuba, 18
 - de recherche du maximum et du minimum, 57
 - de Batcher, 57
 - du tri fusion, 24
- arithmétique euclidienne, 6
- Batcher, Kenneth
 - algorithme de tri de, 57
- Billingsley, Patrick, 51
- Brillhart, John, ii
- Brocot, Achille
 - suite de, 36
- Cantor, Georg
 - ensemble de, 58
 - fonction de, 59, 60, 68
 - suite de, 58
- cascade, algorithme en, 51
- comportement asymptotique d'une suite
 - b -rationnelle, 50
- conditions aux limites, 49, 50, 67
- Coquet, Jean
 - suite de, 59, 67
- décalage, opérateur de, 4
- dilatation, équation de, 48, 67
- écriture binaire
 - nombre de 1, 19
- équation
 - de dilatation, 48, 67
 - de Mahler, 7, 8
- Erdős, Paul, ii
- Fekete, Michael
 - lemme de, 43
- fonction hölderienne, 49
- Golay, Marcel
 - suite de, ii, 59, 67
- Gray, Frank
 - code de, 3, 13, 27, 28
- Hölder, Otto
 - exposant de, 49, 51
- Karatsuba, Anatoly
 - algorithme de, 3, 12, 18, 23, 26, 40, 43–45, 52, 60
- Lucas, Édouard
 - théorème de, 20
- Mahler, Kurt
 - équation de, 7, 8
 - résolution d'une, 15
 - et série rationnelle, 22, 23, 57
 - équation minimale de, 6, 64
 - opérateur de, 4
- Morton, Patrick, ii
- Newman, Donald
 - suite de, 59, 67
- nombre b -adique $(0.w)_b$, 46
- norme subordonnée, 42
- notation fractionnaire, 7, 58
- numération
 - en base -2 , 32
 - en base b , 36
- opérateur
 - de décalage, 4
 - de Mahler, 4
 - de section, 4, 8
- Padé, Henri
 - approximant de, 57
- Pascal, Blaise
 - triangle de, 20, 60, 69
- polynôme tordu, 6
- produit matriciel A_w , 46
- rayon spectral, 43
- récurrence diviser pour régner, 7, 12
 - bien fondée, 14, 29
 - fractionnaire, 7, 58
 - par cas, 3

- plancher plafond, 3, 11
 - vraie, 24, 30
- représentation linéaire, 25, 57
 - insensible aux zéros à gauche, 37
 - réduite, 37, 64
- Rudin, Walter
 - suite de, ii, 59, 67
- Salvy, Bruno, 60
- section
 - d'une fraction rationnelle, 5, 57
- section, opérateur de, 4, 8
 - et arbre, 30
 - et système linéaire, 30, 35
- série
 - génératrice, 3
 - rationnelle
 - dans une base de numération, 21, 36
 - classique, 38, 41, 58, 65
 - de la théorie des langages formels, 37
 - représentation linéaire d'une, 25
- Shapiro, Harold
 - suite de, ii, 59, 67
- Stern, Moritz
 - suite de, 36
- suite
 - b -rationnelle, 21
 - comportement asymptotique d'une, 50
 - de Fibonacci, 64
 - de Golay-Shapiro-Rudin, ii, 59, 67
 - de Gray, 3
 - de Newman-Coquet, 59, 67
 - rationnelle dans une base de numération, 21
 - de Stern-Brocot, 36, 41, 58, 63, 64
- systeme
 - bien posé, 30, 35
 - quasi bien posé, 33, 35
- théorème lyonnais, 35